RIPRENDIAMOCI LA RETE!

Piccolo manuale di autodifesa digitale per giovani generazioni

Arturo Di Corinto

NUOVI CONTENUTI oltre il Covid-19

RELOADED!

Da video chat a smart working

Quando trovi il simbolo play  cliccaci sopra!
Potrai vedere un video di approfondimento.

Si ringrazia Kaspersky Lab per la concessione
all'utilizzo gratuito delle illustrazioni presenti nel testo.

Progetto grafico e impaginazione di Simona Pontremolesi

LINK University CAMPUS

RIPRENDIAMOCI LA RETE!

Piccolo manuale di autodifesa digitale per giovani generazioni

Arturo Di Corinto

SCOPRI
LINK CAMPUS UNIVERSITY

#CYBERSECURITY

#Blockchain

#Economics

#GenerazioneProteo

#Criminologia

#Psicologia

#LINKTHEATRE

#SPORT

#DIGITALCOMMUNICATION

#StudiInternazionali

CORSI DI LAUREA

DAMS (Discipline delle Arti figurative, della Musica, dello Spettacolo e della Moda)

FilmMaking Theatre making

TECNOLOGIE INNOVATIVE PER LA COMUNICAZIONE DIGITALE

Innovation and digital Video games

TECNOLOGIE E LINGUAGGI DELLA COMUNICAZIONE

Game development, marketing and communication Interaction design

INTERNATIONAL BUSINESS ADMINISTRATION

Impresa e innovazione Financial management Marketing & brand management
Economia e politiche dello sport Fashion & luxury

BUSINESS MANAGEMENT

Impresa e innovazione Financial management Marketing & brand management
Sport business management

SCIENZE DELLA POLITICA E DEI RAPPORTI INTERNAZIONALI

Politica e istituzioni Governo e amministrazione International relations

STUDI STRATEGICI E SCIENZE DIPLOMATICHE

Leadership e decisione politica International relations and cyber diplomacy
Intelligence e sicurezza

GIURISPRUDENZA

Tecnologia, intelligenza artificiale e nuove frontiere del diritto Giurisprudenza dello sport
Scienze penali, criminologiche e investigative Internazionalistico e comparatistico

CONSULENZA DEL LAVORO E SISTEMI DI WORKFARE

SCIENZE DELLA DIFESA E DELLA SICUREZZA

Sicurezza interna ed esterna Sicurezza economico finanziaria

CONTATTI

UFFICIO ORIENTAMENTO

email: orientamento@unilink.it

tel.: + 39 06 94802282

UNILINK.IT

Arturo Di Corinto

Professore docente del Corso di Laurea in Tecnologie e Linguaggi della Comunicazione presso l'Università degli Studi Link Campus University.

Ricercatore e docente alla Stanford University, alla Sapienza di Roma e all'Accademia di Belle Arti di Carrara, ha lavorato a lungo come esperto di comunicazione pubblica presso la Presidenza del Consiglio dei Ministri.

Giornalista esperto di innovazione, privacy e cybersecurity, ha collaborato con numerose testate come Il Sole24Ore, Wired e L'Espresso. Attualmente scrive per AGI, Il Manifesto e La Repubblica.

Autore Treccani, wikipediano d'adozione, è un'attivista per i diritti digitali, fan del software libero e difensore della privacy, critico verso il copyright di "Tutti i diritti riservati".

Ha pubblicato diversi libri sul mondo digitale, tra cui Revolution Open Source (Feltrinelli/Apogeo, 2005), I nemici della Rete (Rizzoli, 2011), Un dizionario hacker (Manni, 2014).

Inviato per il programma di RaiUno “Codice. Tutta la vita è digitale", il suo ultimo libro - con Laura Abba - è “Trent'anni di futuro. Quando Internet è arrivata in Italia" (Manni Editori, 2017).

@arturodicorinto


123456

Indice

Introduzione alla versione 2.0 di Riprendiamoci la Rete

LA SOLIDARIETÀ DELL'UNIVERSITÀ AL TEMPO DEL CORONAVIRUS

Maggio 2020. Continua la lotta dell'umanità contro il Coronavirus. Dall'inizio della pandemia abbiamo visto il meglio e il peggio dell'umanità che combatte contro il nemico invisibile, abbiamo visto la dedizione dei medici e degli infermieri e la colpevole sottovalutazione della minaccia sanitaria dei capi di Stato.

Adesso che anche in Italia non si canta più l'inno nazionale dal balcone e si torna a dividersi sui social network sugli effetti del lockdown, la regolarizzazione dei migranti o le riaperture diversificate, la speranza di un mondo più unito e consapevole sembra svanire. Ma ad un'analisi più attenta le energie messe in moto dalle difficoltà non sono scemate, anzi. La solidarietà, fatta di pacchi di pasta e giacigli per i meno fortunati, non si è fermata ed ha assunto le forme del digitale.

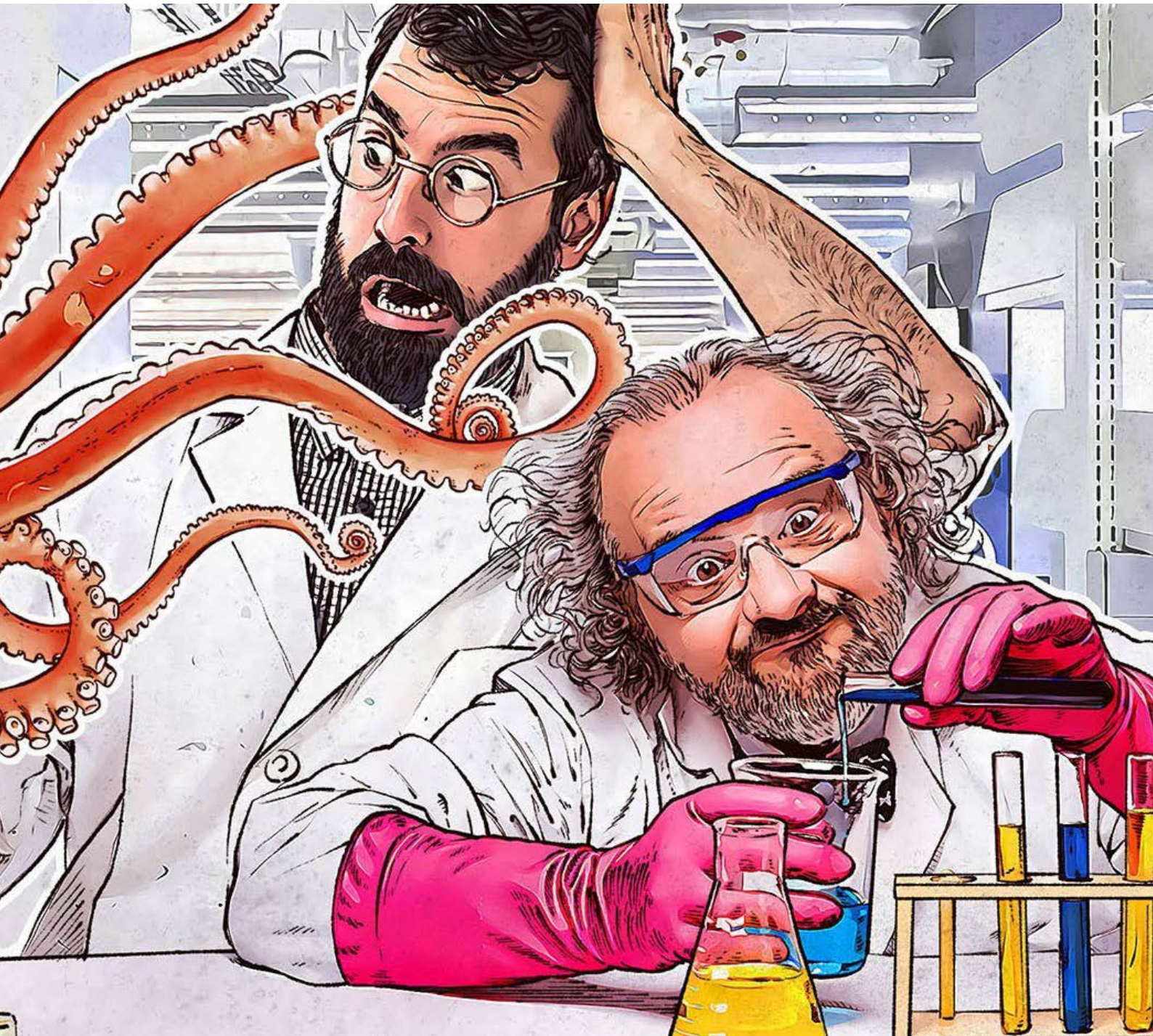
Fin da subito il Governo italiano aveva attivato una rete di donatori che, attraverso il portale Solidarietà digitale dell'Agenzia per l'Italia Digitale - Agid, hanno messo a disposizione servizi di telefonia e di posta elettronica gratuiti per i cittadini confinati nelle zone rosse, e poi servizi per lo Smart Working e la teledidattica, da Amazon a Microsoft passando per Google. Da quel momento in poi però, i cittadini si sono organizzati e hanno cominciato a fare da soli, promuovendo una serie di attività per l'uso gratuito, critico e consapevole del digitale e delle sue risorse.

Una delle più belle è stata senz'altro l'iniziativa di un gruppo di giovani di Fabriano che hanno creato una piattaforma, **iorestoacasa.work**, per consentire a tutti di collegarsi a servizi di videoconferenza in maniera facile e veloce, usando software libero e creando un circuito di server di streaming che nelle scuole ha gareggiato con le applicazioni commerciali come Zoom e Google Meet, anche grazie all'intervento del Consiglio Nazionale delle ricerche e del Garr, Gruppo Armonizzazione Reti della ricerca, che gestisce appunto le infrastrutture dell'Internet italiana per docenti e ricercatori.

Altrettanto importanti le iniziative solidali nel campo della cybersecurity. Cyberoo, Cybertech, Kaspersky e gli altri, sono entrati in pista per offrire protezione informatica gratuita durante la pandemia regalando software anti hacker. Occasione per le aziende di mantenere un buon rapporto coi clienti, rafforzare il branding e farsi benvolere dall'opinione pubblica.

Si chiama Cyberoo Defence for Italy l'iniziativa di Cyberoo, da poco sbarcata in borsa, grazie alla quale vengono messi a disposizione delle aziende italiane che ne faranno

richiesta, gratuitamente e per tre mesi, alcuni servizi di cyber security per lo smart working. Un'altra azienda italiana, Cybertech, ha messo a disposizione delle realtà ospedaliere servizi gratuiti in grado di misurare l'estensione della superficie esposta agli attacchi, pronta a fornire supporto in caso di compromissioni. L'idea, nata da un giovane tecnico del pronto intervento informatico di Cybertech è stata sviluppata con l'Ospedale Lazzaro Spallanzani centro di riferimento per la capitale italiana nella lotta al Coronavirus attaccato dagli hacker. Lo stesso ha fatto Kaspersky, azienda russa di cybersecurity con 400 milioni di clienti che ha deciso di offrire in prova gratuita per sei mesi i gioielli di famiglia. Tra questi anche la protezione per Microsoft Office 365. E altre iniziative sono in campo per contrastare l'impennata di attacchi al settore sanitario e della ricerca, bancario e assicurativo bersagliati con phishing, ransomware e trojan.



LA CULTURA, NUTRIMENTO DELLO SPIRITO

Consapevoli che il pane dello spirito è importante per affrontare l'isolamento e la paura, molte organizzazioni continuano a costruire ponti di collegamento fra le persone, con la tecnologia, per lanciare un'ancora di salvataggio a chi è in difficoltà.

Una di queste iniziative si chiama **Riconnessi**. Organizzata dalla onlus Cittadinanza Attiva, punta a raccogliere donazioni in denaro per acquistare computer e abbonamenti Internet a favore delle aree svantaggiate del paese. Un'altra si chiama **SOS digitale**, una serie di webcast (trasmissioni web) destinati ai dirigenti e al personale scolastico, ma aperti a chiunque, con lo scopo di dare un aiuto concreto a genitori, insegnanti e studenti, per consentire di aggiornare le proprie competenze, confrontarsi con esperienze esemplari e stimolare i partecipanti a condividere il meglio della nostra Scuola.

Un'altra ancora si chiama **TuttiConnessi**. Sostenuta da Ansa, La Stampa e Il Sole24Ore, anche questa punta a fornire tablet e computer a chi non ce l'ha. L'iniziativa è pensata perché "tutti possano partecipare donando il proprio computer portatile, tablet, smartphone, router 4G, di qualsiasi marca e modello, purché funzionante e recente." Invito rivolto a tutti e soprattutto alle aziende che invece di mandare in discarica attrezzature funzionanti possono contribuire a regalare un sorriso e nuove opportunità.

Per i contenuti invece si sono aperte le porte digitali delle biblioteche, locali e nazionali. L'idea di Data Management e di ICCU è stata quella di mettere a disposizione in maniera gratuita 2 milioni di libri digitali centralizzando la loro ricerca attraverso il portale **ioleggodigitale.it**. Sul sito un motore di ricerca permette di accedere a tutte le risorse digitali gratuite catalogate negli anni e di scaricarsi, senza pagare, libri di geografia, sonetti, romanzi, giochi e manuali.

Anche il libro che vi apprestate a leggere è un'iniziativa di solidarietà voluta dalla **Link Campus University**. L'Università romana, tra le prime in Italia a convertire le lezioni tradizionali in lezioni interattive, in presenza, faccia a faccia, con l'ausilio di uno schermo, e da non confondere con le molte università telematiche, ha dalla sua nascita nel 1999 la missione di formare i cittadini, i professionisti, i leader di domani, insegnando l'importanza della condivisione dei saperi e della collaborazione tra pari, consapevoli che l'etica della solidarietà precede ogni forma di profitto.

Prefazione

Quando, qualche settimana orsono, Arturo Di Corinto mi ha detto che stava lavorando all'aggiornamento del suo *Manuale di autodifesa digitale per giovani generazioni*, ammetto che la mia prima reazione è stata di parziale stupore: avendo infatti letto la prima edizione, mi sfuggiva la necessità di arricchire ulteriormente un testo che già si caratterizzava per una inconsueta completezza di contenuti e spunti di riflessione. Ma non avevo fatto i conti con l'occhio attento del giornalista che, da perfetto "storico del presente" come avrebbe detto Umberto Eco, aveva saputo cogliere l'unicità del momento che stavamo vivendo.

L'emergenza Covid-19 ha infatti messo a nudo alcuni aspetti della nostra relazione con le tecnologie di cui eravamo solo in parte consapevoli fino ad appena pochi mesi orsono: per la prima volta da quando il digitale è diventato parte integrante del nostro vivere quotidiano, abbiamo infatti toccato con mano la sua imprescindibilità, ne abbiamo percepito appieno pregi e difetti, abbiamo compreso che, sempre citando Umberto Eco, tra un approccio apocalittico e uno integrato, ciò che realmente "paga" è la capacità di saper mantenere la "giusta distanza".

Le tecnologie ci hanno infatti consentito di supplire a tutto quel patrimonio di relazioni, rapporti, conoscenze di cui il lockdown forzato ci stava inesorabilmente privando. Sono state il nostro "salvagente sociale", che ci ha permesso di tenerci a galla e di proseguire il nostro viaggio in mare aperto, creando imprevedibili connessioni con altri naviganti.

Ma il lockdown ci ha anche mostrato che, se non adeguatamente padroneggiate, le tecnologie non sono immuni da "rischi", che vanno dalla giocosa sagoma della nonna o di un parente in *déshabillé* che compare sullo sfondo di un webinar alla ben più grave intrusione di un hacker sulle piattaforme formative, con tutto ciò che questo comporta, indirettamente, anche in termini di responsabilità giuridica ed etica per i docenti impegnati nella DAD.

Il richiamo alla didattica a distanza mi porta a una ulteriore considerazione, che nasce dalla mia ormai quasi decennale esperienza di direttore di "Generazione Proteo", l'Osservatorio permanente sui giovani della Link Campus University. L'emergenza Covid-19 ha infatti rafforzato in tutti noi la convinzione di quanto le tecnologie siano oggi fondamentali e irrinunciabili, così come della padronanza tecnica e pratica che ne hanno i giovani. Ma ha anche rafforzato il nostro impegno affinché questa padronanza tecnico-pratica non sia mai svincolata da una consapevolezza culturale rispetto sia ai benefici che ai rischi che derivano dal loro uso.

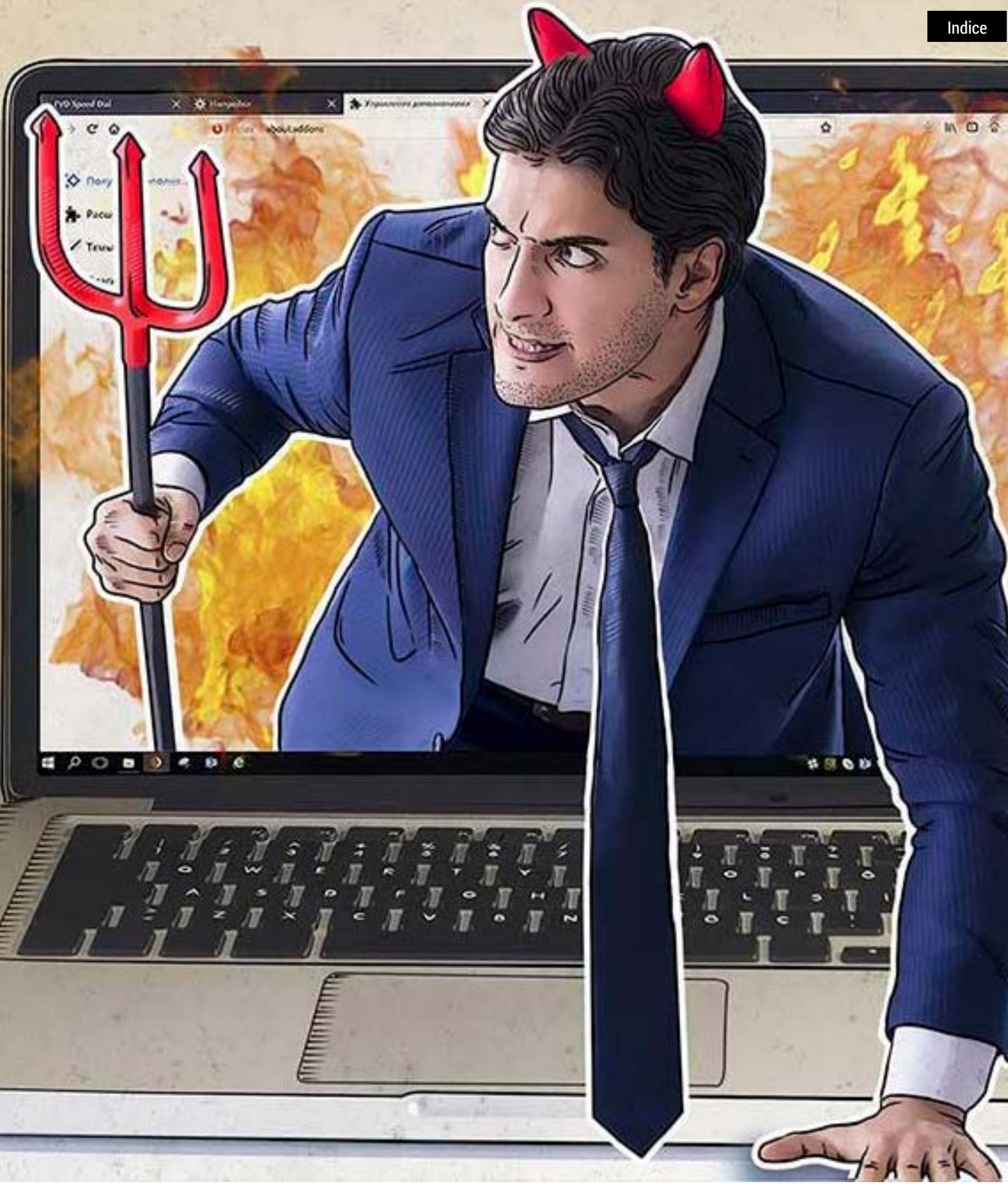
Riflessioni, queste, che trovano conferma empirica anche nel recente 8° Rapporto di ricerca del nostro Osservatorio, la somministrazione dei cui questionari si è svolta in pieno lockdown: i giovani vivono infatti una condizione di alfabetizzazione digitale

sconosciuta alla nostra generazione, vivono un rapporto con le tecnologie quasi *innato* laddove invece il nostro è *acquisito*. In una parola, le tecnologie, il digitale sono parti integranti del loro DNA. Eppure, tutto questo non li esonera dalla necessità di una "formazione permanente" circa le conseguenze che possono derivare da un uso improprio di strumenti così tanto potenti.

Oggi più che mai, dunque, il mio auspicio in quanto direttore di un Osservatorio permanente sui giovani, è che strumenti come questo *Manuale di autodifesa digitale* – che realmente contribuiscono a creare una cultura della sicurezza in Rete – siano abbinati all'acquisto di qualsiasi smartphone, tablet o pc, e sempre disponibili alla consultazione nella schermata iniziale dei nostri *device*. Conoscere a fondo ciò che scandisce la nostra vita quotidiana in maniera così *intensiva* e *invasiva*, infatti, non solo ci rende, come giustamente dice Arturo, "più liberi e indipendenti", ma ci consente anche di tutelare il bene più prezioso che possediamo, ossia la nostra *reputazione*. Perchè quello che condividiamo oggi ingenuamente o con leggerezza, potrebbe un domani danneggiare le nostre aspirazioni lavorative, la nostra vita relazionale, i nostri affetti o i nostri ricordi più intimi e profondi. In una parola, *ciò che noi siamo*.

Nicola Ferrigni

Direttore dell'Osservatorio
"Generazione Proteo"



Premessa

Questo libro vuole contribuire a rendere i più giovani maggiormente consapevoli dei rischi che comporta l'utilizzo di Internet. La "Rete" ha portato enormi vantaggi nel mondo degli affari, della comunicazione, del lavoro e dell'associazionismo, viene usata per rappresentare istanze sociali e difendere i diritti umani e accedere a ogni tipo di conoscenza, ma il suo utilizzo si sta rivelando una fonte giornaliera di problemi per chi la utilizza con leggerezza. Per questo, prendendo a pretesto alcuni fatti di cronaca, chi scrive ha provato a raccontare i rischi e le insidie di una "presenza" superficiale in rete e a precisare concetti e nozioni che si stanno perdendo a causa del fatto che usiamo "la Rete" come un elettrodomestico: senza capire veramente come funziona.

E quando usi una cosa che non capisci, sei tu a essere usato. Perciò credo che sia utile prendersi un po' di tempo per riappropriarsi della conoscenza di questo mezzo straordinario per conseguire i nostri scopi invece di favorire quelli altrui. Diciamo subito che il linguaggio del libro è un linguaggio semplificato, giornalistico, e non a caso alcuni dei temi sono stati già affrontati da chi scrive sulle pagine di testate come La Repubblica, Il Fatto Quotidiano, Il Manifesto, StartupItalia. Linguaggio semplificato di tipo giornalistico, ancoraggio a episodi di cronaca, suggerimenti e forma manualistica sono la formula usata per avvicinare soprattutto i più giovani alle tematiche della privacy e della sicurezza in rete. Non si tratta certo di un testo esaustivo delle problematiche che lo sviluppo della rete ci ha portato in dono, e infatti il titolo scelto dovrebbe già renderlo chiaro: è un "piccolo manuale", ma speriamo si riveli utile per chi lo legge.

Arturo Di Corinto

Professore docente del Corso di Laurea in Tecnologie e Linguaggi della Comunicazione presso l'Università degli Studi Link Campus University

Post Scriptum

Approfitto di questa pagina per ringraziare **Pasquale Russo**, *Direttore Generale della Link Campus University* per avermi sollecitato a scrivere il libro; **Vanna Fadini**, *Presidente Global Education Management* per le idee, il supporto e l'incoraggiamento; Simona Pontremolesi per il bellissimo progetto grafico e Chiara Calderoni per le riprese che corredano il libro. Un ultimo ringraziamento va fatto al professore **Carlo Maria Medaglia** per il sostegno a questo progetto. Il merito è tutto loro, io gli ho solo prestato la "penna".

Un grazie affettuoso va infine al professore **Paolo Prinetto**, *Direttore del Laboratorio Nazionale di Cybersecurity* del CINI per aver corretto le bozze del libro fin dalla prima stesura, e a **Kaspersky Lab** per le immagini che corredano il libro.

Quelle cose da non fare mai in rete se non si vuole essere denunciati

Partiamo da una banalità: quello che diciamo e pubblichiamo su Internet e nei social media è destinato a rimanere. La regola generale vorrebbe che quando scriviamo qualcosa in un blog o su Facebook non dovremmo mai dire cose che non diremmo al bar perché possono farci vergognare, e possono essere fraintese e farci litigare. **Ciò che "mettiamo in rete" un giorno potrebbe essere usato contro di noi**. Come afferma il fondatore di Facebook, Mark Zuckerberg, "Quello che scriviamo in rete è scritto con la penna, non con la matita." Ed è difficile da cancellare. Nonostante le leggi sulla privacy e la possibilità di invocare il "Diritto all'oblio", e quindi chiederne la cancellazione da siti e piattaforme, le cose sconvenienti che abbiamo pubblicato in rete possono rimanerci a lungo e diventare virali attraverso la condivisione nei social e nei gruppi di instant messagging, rimbalzare da un sito all'altro ed essere linkate da motori di ricerca che neanche conosciamo. In aggiunta, certi comportamenti che adottiamo con leggerezza quando siamo online configurano dei veri e propri reati come la diffamazione, lo stalking, il cyberbullismo, l'hate speech e le molestie sessuali online.

Insomma, anche in rete valgono la buona educazione e il rispetto delle leggi, ma è bene rammentare che sono diversi i comportamenti che vanno evitati se non si vuole finire in tribunale.

1. **Far finta di essere qualcun altro ad esempio può configurare la sostituzione di persona o il furto d'identità, comportamenti gravi perseguibili per legge, anche se lo si fa per gioco**. Per capirci: creare un account fasullo su Facebook è illegale. Per prima cosa si violano le condizioni di Facebook, che per questo può sbatterci fuori, ma usare la foto di un'altra persona, magari presa da Google o dal profilo di una star dello spettacolo, può essere considerato come una falsificazione della propria identità, furto di proprietà intellettuale e furto d'identità.

2. **Cyberbullismo e trolling. Infastidire una persona attraverso email ripetute è stalking, parlare male di qualcuno su Twitter è diffamazione, commentare in maniera offensiva un post su Facebook, intimidire un compagno di classe nel gruppo WhatsApp della scuola, viene considerato cyberbullismo**. Le parole sono pietre. Sono diversi i casi di ragazzi e ragazze indotti al suicidio da atti di stalking e bullismo online. In Italia il cyberbullismo è un fenomeno vasto. Secondo una ricerca raccontata dall'AGI (Agenzia Giornalistica Italia), nel nostro paese si verifica almeno un caso di bullismo al giorno in base alle segnalazioni ricevute dal Telefono Azzurro nell'anno 2017.

Sono infatti il 10% le richieste di aiuto rivolte all'associazione che riguardano episodi di bullismo e cyberbullismo. Di queste, il 46% proviene dal Nord Italia, seguono il Sud e le Isole con il 31% e il Centro con il 23%". Nel 2017 i casi conclamati sono stati 354. Le più colpite sono le ragazze. Le piattaforme social da qualche tempo hanno attivato modalità di segnalazione di comportamenti inappropriati proprio per cercare di arginare le conseguenze, spesso tragiche, di questo fenomeno. Anche le istituzioni stanno agendo. Nel 2017 è stata approvata dal Parlamento una legge per perseguire i reati di cyberbullismo e la Polizia di Stato ha creato un'app, **You Pol**, che ha lo scopo di permettere a tutti, giovani e adulti, di comunicare con la Polizia di Stato, consentendo l'invio di segnalazioni di episodi di bullismo.

3. **Revenge porn. Quando si condividono o si postano online le foto di nudo dei propri ex per ridicolizzarli e vendicarsi di un rapporto finito male, il fenomeno prende il nome di "Revenge porn", il "porno vendicativo"**. Immagini o video diffusi senza consenso, anche in gruppi chiusi, generano ansia e vergogna in chi ne è vittima, perciò porta a molte accuse, anche di carattere penale: dallo stalking alle molestie sessuali. È stato il caso di Tiziana Cantone, la trentunenne suicidatasi a causa della gogna mediatica a cui è stata sottoposta dopo la diffusione dei materiali erotici che la riguardavano.

4. **Hate speech**. Incitare alla violenza, fomentare l'odio verso "i diversi", minoranze sessuali, religiose o etniche, si configura come hate speech, il linguaggio dell'odio e può sfociare in quelli che sono definiti **hate crimes**, che possono comportare vendette materiali. Fomentatori d'odio online sono stati ad esempio quelli che chiedevano la morte di Italo D'Elisa, il vastese colpevole di aver travolto una giovane sposa in un incidente stradale, morte sopraggiunta per la vendetta del marito.

L'hate speech, insieme al **trolling**, il disturbo costante con post, commenti, informazioni non richieste che arrivano sul proprio profilo social sono tra i comportamenti più frequenti in rete e possono essere sanzionati duramente dai giudici come la diffamazione, cioè quando attribuiamo alle persone caratteristiche che ne ledono l'onorabilità. Un altro modo di intimidire e infastidire e procurare un danno agli altri è sostituirsi a loro, adottandone il nome, usandone la foto nel profilo, fino a rubarne la password per cambiare i contenuti pubblicati online, dentro e fuori i social. Si tratta di comportamenti perseguibili per legge, che configurano la violazione dell'identità e dell'immagine, fino al reato di sostituzione di persona.

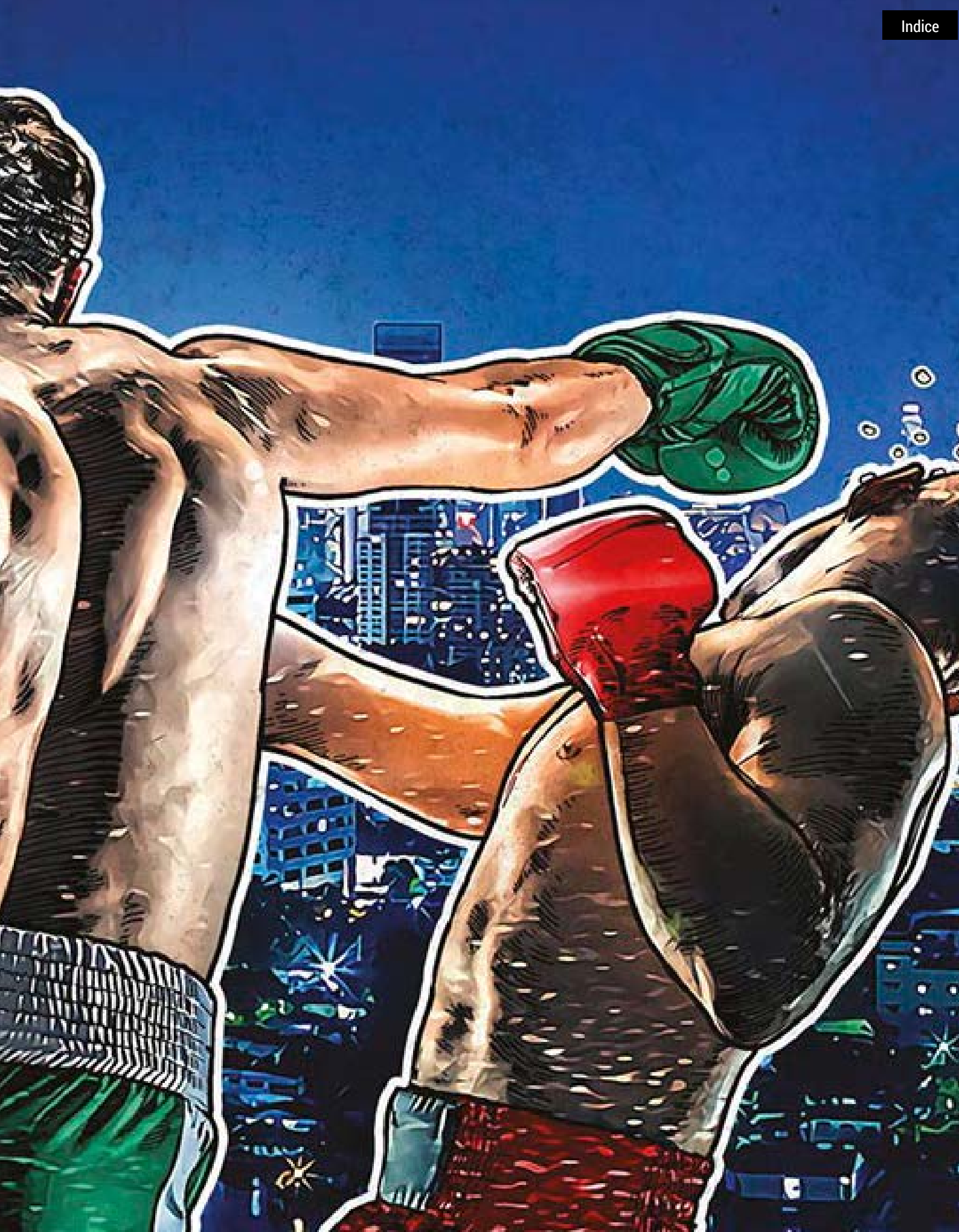
Violazione della privacy. Cyberbullismo, hate speech, revenge porn, stalking, sono tutti comportamenti associati alla violazione della privacy altrui e comportano molte conseguenze, anche penalmente rilevanti. Tuttavia, mentre è importante rispettare la privacy degli altri è altrettanto importante proteggere la propria per non cadere vittima dei comportamenti menzionati. **Privacy**, termine inglese usato da due avvocati nel 1890 per indicare il diritto di ognuno a essere lasciato in pace, "schermato all'occhio inquisitore degli estranei", ha oggi un significato molto più ampio che nel passato e coincide con il concetto di "autodeterminazione informativa".

Significa che poiché viviamo in simbiosi con le tecnologie che tracciano ogni nostro comportamento la privacy non tutela soltanto il diritto a essere lasciati in pace e proteggere la propria sfera privata, ma anche il diritto di controllare l'uso e la circolazione dei propri dati personali che costituiscono il bene primario dell'attuale società dell'informazione.

Dati personali come l'email, il numero di telefono o l'indirizzo di casa, dati sensibili come l'appartenenza politica, religiosa e sindacale, informazioni sull'orientamento sessuale, i dati sanitari, tutti sono protetti dalle leggi sulla privacy.

Nonostante alcune limitazioni legali però gli **Internet Service Provider, le piattaforme social e i sistemi di storage e condivisione o quelli di posta elettronica** sono autorizzati a utilizzare e in molti casi a rivendere a terzi quel tesoretto di informazioni che identificano i nostri comportamenti quotidiani: dai dati di navigazione al luogo dove ci siamo connessi, per quanto tempo, con quali strumenti. Per questo diventa fondamentale fare attenzione al tipo di informazioni che si caricano o condividono in rete: potremmo perderne il controllo.

Con un'aggiunta. La violazione della privacy non riguarda solo la diffusione pubblica di comportamenti privati, ma riguarda la manipolazione dei comportamenti. Se ti conosco, posso colpirti dove ti fa più male, ma posso anche offrirti quello che già desideri. E farlo nel momento in cui lo vuoi. Questa in estrema sintesi è la logica del direct marketing online, il marketing diretto su Internet. Offrire al **cliente** quello che è più propenso a desiderare: oggi è molto più facile di prima grazie alla scienza dei big data e ai sistemi di profilazione online che ricostruiscono personalità e desideri degli individui a partire dai dati personali che abbiamo lasciato in rete o condiviso con le piattaforme.



L'autodifesa digitale

STRUMENTI DI SOPRAVVIVENZA DIGITALE NELL'ERA DELLA SORVEGLIANZA GLOBALE

Non è possibile tenere sotto controllo e proteggere la grande mole di dati digitali che ci riguardano. Per questo è importante ricordare che nell'era dell'informazione gli stessi dispositivi possono essere usati sia per la protezione della privacy e della propria identità digitale sia per rubare informazioni sensibili e riservate. Computer, tablet, smartphone, sono strumenti di comunicazione, elaborazione e archiviazione dei dati, ma anche porte d'accesso attraverso cui soggetti diversi sono in grado di arrivare a conoscere ogni più piccolo dettaglio delle nostre vite e a esercitare differenti forme di controllo sui comportamenti dei singoli per condizionarli. Per chi nell'infosfera vive e lavora, è inevitabile la collisione con un mondo che rappresenta simultaneamente il veicolo per il supremo esercizio della libertà espressiva e la creatività umana, come pure un incredibile sistema di profilazione, sorveglianza e condizionamento. La necessità di proteggere qualunque aspetto delle nostre «attività» digitali, online e offline, è fattore critico in uno scenario dove la comunicazione digitale è pervasiva e occupa uno spazio rilevante del nostro quotidiano.

Gli scandali che hanno segnato la stagione delle rivelazioni sui sistemi di sorveglianza globale adottati dalle agenzie governative e dai grandi player commerciali come Facebook - evidenziati nello scandalo di Cambridge Analytica - colpevole di aver utilizzato i dati degli utenti di Facebook a fini di manipolazione politico-elettorale - hanno reso tangibile un luogo comune spesso abusato quando si parla di «sicurezza informatica» e cioè che **nessuno è mai al sicuro**, ma, fatto ancora più grave, quelle rivelazioni hanno compromesso il patto di fiducia che lega i cittadini ai fornitori di servizi digitali.

In un contesto sociale dove la raccolta e lo scambio di informazioni, il reperimento, la verifica e la protezione di dati e informazioni, o il loro utilizzo a fini scientifici è cruciale, significa dover mettere in discussione molte delle azioni e delle pratiche quotidiane che ci mettono a rischio: telefonate, chat, SMS, scambio di email, archiviazione in sistemi cloud, trasmissione di documenti, uso di strumenti collaborativi.

Senza aprire in questa sede una riflessione sulle grandi sfide aperte nel panorama dei diritti umani digitali, o lasciarsi travolgere dall'idea di un confronto impari con forze non sempre identificabili, è possibile invece cominciare a cambiare le proprie abitudini, conoscere - e imparare a usare - strumenti in grado di accrescere il nostro personale livello di sicurezza e privacy.

Vediamo perché.

Che cos'è la privacy

La privacy è un limite al potere di governi e aziende. Chi conosce gusti e inclinazioni e modelli di comportamento degli altri è potenzialmente in grado di manipolarne le decisioni.

La privacy serve a mantenere il controllo sulla nostra vita. La gestione di terzi dei nostri dati personali decide se meritiamo un mutuo, se possiamo avere l'assicurazione o se possiamo svolgere un certo lavoro. I dati personali sono usati per decidere indagini di polizia o la possibilità di viaggiare all'estero. I dati personali riguardano spesso quello che facciamo su Internet. Se non sappiamo come vengono usati i nostri dati non siamo neppure capaci di correggerli e modificarli. Se non siamo autonomi non possiamo fare scelte libere.

La privacy ci consente di gestire la nostra **reputazione**. Quello che gli altri sanno di noi influenza opportunità, amicizie e benessere. Conoscere i dettagli della vita di una persona non significa tuttavia averne un'idea più accurata e la privacy ci aiuta a evitare giudizi inaccurati che possono diventare fonte di problemi.

La privacy ci aiuta a erigere un confine tra noi e gli altri. Ognuno di noi stabilisce i confini fisici e informazionali della sua vita. A volte abbiamo bisogno di ritirarci e stare in solitudine, lontano dall'occhio indagatore degli altri. Spesso regoliamo anche i confini delle informazioni che ci riguardano in base al tipo di relazione che abbiamo con le persone. La privacy ci aiuta a definire questi confini.

Molte delle nostre relazioni sono basate sulla fiducia. Se qualcuno viola la nostra privacy anche le relazioni personali più delicate possono essere compromesse. Pensateci quando andate dallo psicoanalista o parlate col consulente della banca. In aggiunta, se qualcuno ha un motivo per mantenere qualcosa privato va rispettato in questa sua intenzione, è un suo diritto che va contemperato con altri diritti. È il caso del diritto di cronaca che spesso si presenta come l'altro polo del diritto alla privacy.

La privacy ci consente di esprimere opinioni socialmente discriminate ma anche di conoscere e sperimentare fatti e situazioni non conformi alle regole sociali dominanti. Pensateci quando volete raccontare la storia di un abuso, dare libera espressione alle vostre passioni o chiedere consiglio su qualcosa.

Elemento centrale dell'attività politica e sindacale è la riservatezza che gode il perseguimento di queste scelte. È il motivo per cui il voto è segreto, serve a evitare condizionamenti e rappresaglie.

La privacy ci permette di ricominciare, cambiare vita, fallire per imparare. Per questo è importante esercitare il **diritto all'oblio**, il diritto a essere dimenticati e a dimenticare fatti, situazioni, eventi distanti nel tempo che non sono più rilevanti per definire il nostro essere sociali. È il caso di chi ha subito una condanna e l'abbia scontata, di chi è salito alla ribalta delle cronache suo malgrado, di chi è stato ingiustamente accusato di qualcosa.

Un ultimo motivo nella difesa della privacy è che grazie a essa non dobbiamo sempre spiegare le nostre scelte, soprattutto quelle che ci fanno vergognare perché non sono condivise da quelli che conosciamo. Questo può valere sia per il lavoro che facciamo sia per una situazione familiare. Pensate a quanti giovani oggi sentono la necessità di nascondere la propria omosessualità a genitori, insegnanti e perfino amici.

Privacy, Cybersecurity, Cyber-Hygiene

Cybersecurity è il termine generico che usiamo per riferirci alla sicurezza informatica, sicurezza dei dati, delle reti, dei dispositivi digitali. Non è una definizione precisa, ma ci aiuta a capire. La sicurezza informatica è l'altra faccia della privacy. Poiché la privacy, attiva e passiva, riguarda i dati digitali e i comportamenti online che ci identificano come persone, figli e genitori, studenti e insegnanti, lavoratori e imprenditori, elettori ed eletti, ammalati e medici, attivisti, consumatori e vicini di casa, la loro protezione ha a che fare con la sicurezza informatica.

In questo contesto potremmo dividere il tema in due dimensioni che però sono intrecciate: quello delle misure di protezione di dati e dispositivi digitali e quella della **Cyber-hygiene**, l'igiene informatica, cioè l'insieme di procedure che riducono i rischi di prendersi una "malattia informatica". Per capirci: se prima di mangiare ci laviamo le mani per non prenderci una malattia, prima di mettere mano su un computer o un telefonino dovremmo fare lo stesso: mantenerlo pulito da virus e ospiti indesiderati.

Ed è proprio di questo che parleremo nel corso di questo libro.

Perché la tua sicurezza online non è un optional

Il profilo di Mark Zuckerberg, fondatore di Facebook, è stato violato. Usava la stessa password, '**dadada**', per Twitter, Instagram, LinkedIn, Pinterest. Ma gli era stata sottratta nel 2012 durante un'incursione su LinkedIn. Su Pinterest gli autori del furto hanno modificato il nome del suo profilo in 'Hacked By Our Mine Team'. Era già accaduto a Katy Perry, la popstar con più follower del Papa.

Era il 6 giugno 2016.

Da allora quasi ogni giorno si è verificato nel mondo un fenomeno simile frutto dell'appropriazione indebita di account, email e password. I casi sono moltissimi e alcuni hanno colpito pesantemente anche l'Italia. Tra questi il furto di 400 mila profili digitali di risparmiatori in seguito all'attacco di un'azienda di prestiti al consumo che lavorava per Unicredit, il caso Cambridge Analytica relativo alla manipolazione di oltre 50 milioni di profili Facebook attraverso un'app di terze parti fino a una lunga serie di attacchi di portata avanti dagli hacktivisti di Anonymous contro sindacati, polizia, università, regioni e industriali.

Ma che succede?

Succede che aumentando il numero di utenti online, aumenta il numero di persone che lo fanno senza una preparazione specifica e che usano gli strumenti digitali come una moderna lavatrice: cioè senza sapere come funziona. Ma, a differenza della lavatrice, i danni potenziali per chi non protegge le proprie informazioni online sono notevoli, basti pensare a quanti di noi oggi si collegano ai siti della pubblica amministrazione per pagare multe e tasse, ai siti delle banche per compiere transazioni, e quanti di noi usano gli stessi account e gli stessi pc sia per svago sia per lavoro e che perciò contengono anche dati sanitari, foto di familiari, fatture e pagamenti.

IL NOSTRO SÉ DIGITALE CI PRECEDE SEMPRE

Aumentando le attività e il numero di persone online, aumenta anche la platea di vittime potenziali di criminali che a partire da un semplice nome, un indirizzo di lavoro, possono ricavare un'email personale a cui mandare virus sotto forma di documenti allegati che una volta aperti si installano nel computer e "lo prendono in ostaggio" fino al pagamento del riscatto (si chiamano Ransomware). Oppure lo trasformano in un computer zombie da risvegliare per operare attacchi su larga scala (DDoS) a siti governativi e commerciali a nostra insaputa.

Lo stesso avviene con i profili sui social network. A partire dal nome della vittima

prescelta o dalla sua email, con software appositi si può provare a generare la password giusta per impossessarsene e usare l'account per compiere varie operazioni che possono metterci nei guai.

Social Engineering. Ad esempio, se si conosce il nome di una persona è relativamente facile risalire a una serie di dati che la riguardano (codice fiscale, residenza, eccetera), e diventa facile individuare o ricostruirne l'indirizzo di posta elettronica. La conoscenza di dettagli della vita privata facilmente accessibili attraverso una ricerca su Google o i social più frequentati può permettere di ricostruire la password della casella di posta elettronica che spesso colpevolmente è costruita usando il nome dei figli, del coniuge, le date importanti della vita.

Se la password generata funziona è possibile usare l'indirizzo di posta elettronica del legittimo proprietario per resettare l'account di servizi web e, usando altri dettagli privati, si può perfino spacciarsi per il titolare di un conto corrente, una cartella clinica, una polizza assicurativa. A loro volta quei documenti saranno usati per ricostruire il profilo dei soggetti coinvolti e farli bersaglio di minacce o ricatti.

Insomma, usando le logiche del **social engineering** è possibile sostituirsi alle identità dei proprietari degli account che si vogliono attaccare e poi svolgere operazioni di natura bancaria o commerciale al posto del legittimo correntista o cliente.

Per questo il nostro sé digitale va protetto e non è un caso che la stessa email vada considerata come un dato personale che gode di particolare protezione nella disciplina della privacy ormai di tutti i paesi.

Tenere al sicuro i propri dati non serve soltanto ai giornalisti minacciati dalle mafie (circa 3 al giorno nella sola Italia) e neppure a blogger e attivisti, ma alle persone comuni che possono cedere al ricatto dei criminali per non vedere la propria reputazione rovinata dalla diffusione di informazioni compromettenti. Ma è proprio quello che può accadere e quando si accetta di chattare con nuove "amicizie" in rete, quando si forniscono i propri dati personali a estranei o peggio ancora quando si accetta di comunicare in chat e video con uomini e donne sconosciuti che ci chiedono di fare sesso virtuale. Bastano lo screenshot di una posa equivoca e ci ritroviamo su siti e canali YouTube, "photoshoppati" e montati in video in atteggiamenti che non ci sogneremmo mai di avere.

Si tratta spesso di attacchi finalizzati ai ricatti e alle truffe monetarie e, seppure non abbiano sempre conseguenze drammatiche o durature, di sicuro ci mettono di cattivo umore e ci fanno perdere tempo e soldi per riparare ai problemi che creano.

Non esiste una strada diversa dall'apprendimento e dalla conoscenza di questi meccanismi per evitare di diventare delle vittime, ma non c'è neanche bisogno di diventare hacker esperti per proteggersi, perciò ecco le misure di precauzione minime per stare un po' più tranquilli.

10 COSE DA FARE PER PROTEGGERE IL SÉ DIGITALE

1. **Proteggere i propri account con password lunghe e complesse**: mai e poi mai usare i nomi di senso compiuto, nomi di parenti, figli, animali domestici, personaggi famosi e città.
2. **Cambiare costantemente le proprie password di accesso a pc, telefoni, social network, posta elettronica**; usare un **password manager** e implementare l'**autenticazione a due fattori**.
3. **Non usare mailbox gratuite**, ma servizi di email a pagamento.
4. **Non usare mai l'email privata nel lavoro e viceversa**. Con pochi euro all'anno è possibile avere un indirizzo di posta elettronico sicuro che non sia associato al vostro nome o al vostro lavoro.
5. **Mantenere il proprio sistema operativo sempre aggiornato**: gli aggiornamenti colmano falle di sicurezza e ripuliscono i dispositivi da file potenzialmente dannosi.
6. **Installare un antivirus**, meglio se a pagamento.

7. **Fare continui backup dei propri dati** e conservarli su memorie non connesse in rete e in luoghi sicuri.
8. **Duplicare i file importanti** su cui state lavorando e se sono "molto" importanti **crittografarli**.
9. **Non aprire le email di sconosciuti** e soprattutto non aprire i file a essi allegati prima di fare una verifica sul mittente.
10. **Non accettare file inviati in chat o via Sms** e in ogni caso prima di aprirli scansionarli con un antivirus.

La prima linea di difesa rimane la vostra password. Alcuni hacker, che sono bravi programmatori e non sinonimo di criminali, consigliano di mettere quattro numeri casuali davanti alle password e gli stessi numeri alla fine della password, oppure di usare come password frasi intere provenienti dalle vostre letture preferite oppure formule chimiche e lingue antiche, che però non dovrete mai trascrivere sugli stessi post-it che appiccicate allo schermo del computer per ricordarvi gli appuntamenti. La cosa migliore da fare è usare sistemi che generano password casuali in cui si alternano caratteri alfanumerici: numeri, simboli e lettere maiuscole e minuscole.

Autenticazione a due fattori. E tuttavia se vogliamo mettere al sicuro la nostra vita digitale potrebbe non bastare una sola password. Per questo da tempo i fornitori di servizi consigliano di usare la verifica in due passaggi che consiste nell'usare un codice di sicurezza aggiuntivo, una specie di seconda password (detta anche OTP, One Time Password), che può esserci recapitata sul nostro telefono tramite Sms, con una telefonata o con un'app per tablet e smartphone, o perfino un "token di sicurezza", cioè un dispositivo fisico, una chiavetta USB da inserire nel computer. Troppo complicato? No. Se si usa sempre lo stesso dispositivo dopo la prima volta la verifica in due passaggi non sarà più necessaria, mentre rimane per dispositivi diversi, quando usiamo il computer dell'ufficio, dentro un Internet cafè o a casa di un amico.

ANONYMOUS

ANONYMOUS BUCA SITI E DATABASE DEL MINISTERO DELLA PUBBLICA ISTRUZIONE: 26MILA EMAIL E PASSWORD ADESSO VANNO A SPASSO NEL CYBERSPACE

A come Anonymous. Anonymous è il nome che si danno gruppi di attivisti che dal 2004 contestano in rete istituzioni, governi e poteri commerciali attraverso azioni di comunicazione e di sabotaggio. Quando si parla di Anonymous si parla di un collettivo/non collettivo di persone che si ritrovano a svolgere azioni di provocazione e di critica politica verso i protagonisti di casi di corruzione e abuso di potere, almeno dal punto di vista di chi si riconosce nelle modalità di azione di Anonymous.

Ecco il collettivo di hacker attivisti, o meglio, una loro costola italiana, nel corso del 2018 si è scagliato contro il Ministero dell'Istruzione italiano e più esattamente contro il progetto di Alternanza scuola lavoro prevista dalla Riforma dell'Istruzione. Per protestare contro il progetto che considerano occasione di sfruttamento degli studenti hanno deciso di rendere pubblici nomi, email, password di un pezzo consistente della Scuola Italiana: circa 26mila indirizzi di posta elettronica e gli accessi di amministrazione a siti e database scolastici. L'azione dimostrativa serviva anche a lamentare il cattivo funzionamento della scuola italiana "per le infrastrutture inadeguate o fatiscenti, gli insegnanti ignoranti e negligenti e per tutta la farsa di studiare materie improntate non alla logica ma al puro nozionismo". E l'hanno fatto anche per rimarcare la cattiva gestione della sicurezza informatica da parte degli organismi preposti a questo.

Il risultato dell'operazione del marzo 2018 è stato quello di 52 database hackerati, 1048 email ministeriali divulgate, circa 7000 indirizzi privati di insegnanti, finanche quelli degli amministratori dei siti wordpress dove erano contenuti. Per finire con 12.819 email dai Licei Morandi di Finale Emilia, del Fermi di Bologna, del San Vitale di Parma, l'Istituto Comprensivo di San Giovanni in Persiceto, fino all'alberghiero di Riccione.

Si trattava di email di professori e dirigenti scolastici di scuole di diverso grado, sia pubbliche che private, cattoliche, soprattutto dell'area dell'Emilia Romagna. Nelle informazioni sottratte compaiono anche i 190 nomi e le password di accesso dei referenti universitari del Miur di tutto il territorio nazionale.

Perché è grave? Se si è in possesso delle credenziali di un professore, ottenuto il pin di accesso ci si può facilmente spacciare per lui e modificare in maniera illegittima i Registri On Line dove i professori comunicano direttamente con le famiglie degli studenti. Lo scenario più semplice da ipotizzare è che uno studente, grazie a tali credenziali, possa andare sul registro digitale e cancellare le note ricevute oppure fare un dispetto ai suoi compagni di scuola. Pensate ancora che la sicurezza informatica non vi riguardi?

ASTROTURFING

I PROFILI FASULLI INFESTANO I SOCIAL. DA LINKEDIN A INSTAGRAM E TWITTER I SOCKPUPPET INQUINANO IL DIBATTITO PUBBLICO MA POSSONO ESSERE SCOPERTI ANCHE SENZA PARTICOLARI DOTI INFORMATICHE, FORSE

L'«astroturfing» è un termine coniato nell'ambito del marketing per definire la creazione a tavolino del consenso dal basso per un'idea, un prodotto o un candidato alle elezioni.

Wikipedia, l'enciclopedia online libera e gratuita riporta che l'origine del termine viene da *AstroTurf*, il marchio registrato di un'erba artificiale prodotta dall'azienda Monsanto a partire dal 1966, anno in cui fu utilizzata per la copertura del terreno di gioco dell'Astrodome di Houston, in Texas.

La tecnica dell'«astroturfing», che usa soggetti pagati apposta, può anche servire ad alterare la percezione del pubblico su un certo argomento nell'ambito della comunicazione politica, dove però si preferisce parlare di fake news e disinformazione online.

A differenza che nel passato, per inquinare il dibattito pubblico nei social network oggi si usano profili fasulli generati via software da aziende specializzate – sono chiamati volgarmente bot –, e automatizzare compiti come la ripetizione ossessiva di certi messaggi per dare l'impressione che esista ampio consenso attorno a sindaci, partiti e uomini politici.

Nel 2019 ha destato curiosità un hashtag a favore della sindaca di Roma Virginia Raggi. Data la viralità, #SiamoTuttiVirginiaRaggi ha fatto pensare all'azione di bot dedicati. Forse si è trattato di un «tweet-storm», una tempesta di tweet, ben coordinata, e che ha comunque prodotto in mezza giornata 19.300 tweet sul «Malaffare che rivuole Roma» a partire da 350 account che ripetevano lo stesso messaggio.

Raggi a parte, i profili fasulli ormai infestano i social e al netto dei «follower» acquistati in rete per pochi spiccioli – o generati da macchinette simili a quelle che stampano i bigliettini da visita, documentate nella metropolitana di Mosca -, li troviamo in grande presenza su Instagram, Facebook, Twitter e LinkedIn e dovunque si possano creare profili con un nome, una foto, una biografia, e qualche collegamento ad aziende e persone reali.

Su LinkedIn, sito dedicato al mondo del lavoro, è possibile creare un profilo fake con un ruolo inesistente presso un'azienda reale, impossibilitata a moderare i propri profili aziendali. Il social permette di moltiplicare le connessioni ad altre persone che in una grande azienda difficilmente si

conosceranno tutte, rispondendo con un «Sì» alla domanda se si conoscano davvero. Oltre alle connessioni con i top manager, anche per LinkedIn, come per TripAdvisor, è possibile acquistare pacchetti di raccomandazioni fasulle.

Su Facebook e Twitter molti profili fasulli sono governati da «bot» in grado di intavolare una banale discussione in chat e che producono una discreta mole di messaggi.

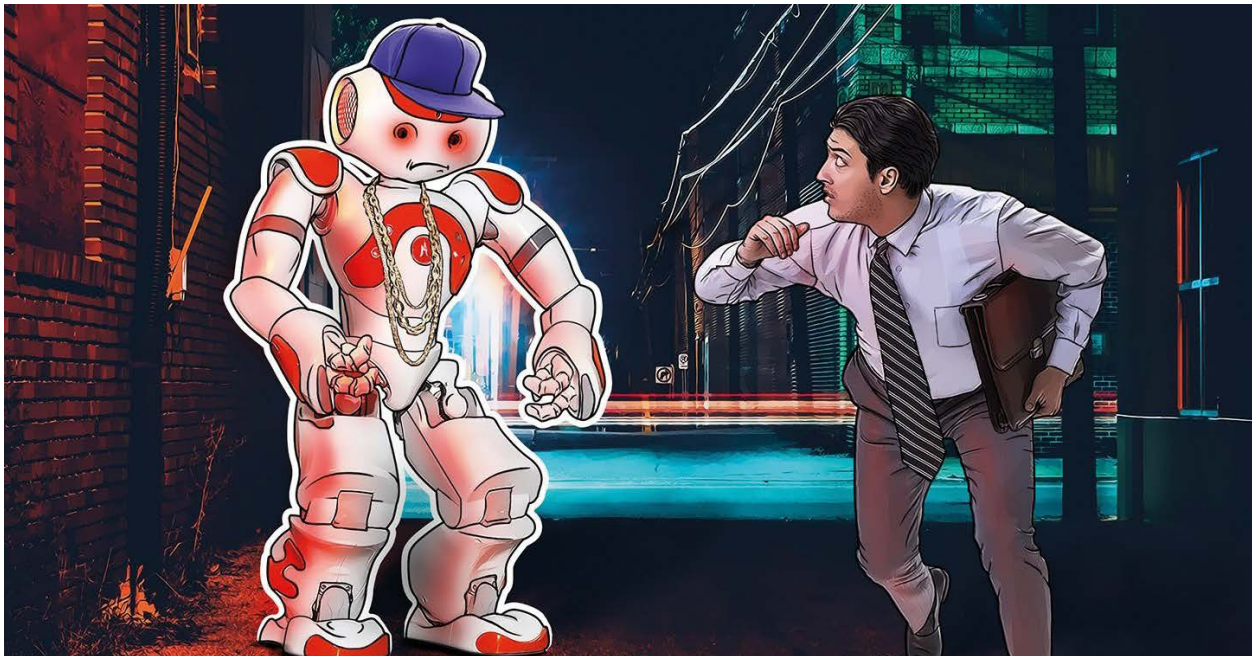
Spesso si tratta di esche sessuali o di truffatori che offrono soldi in prestito o altri servizi a pagamento.

Nel caso di Twitter scovarli è abbastanza semplice: i profili fasulli tipo «GiUsY12345», hanno pochi follower, producono sempre gli stessi messaggi, lo fanno di notte, e replicano raramente a quelli degli altri.

Anche evitare di cascarci tuttavia è abbastanza semplice: si scrive il nome del profilo su un motore di ricerca e se la persona compare su siti di notizie e altri social potrebbe essere una persona vera; incollando nella sezione immagini di Google il suo volto, si potrà poi facilmente scoprire con un confronto incrociato se quella persona esiste realmente oppure è solo il parto di un software.

Adesso però le cose si sono fatte complicate a causa degli «Attacchi Sybil». Questo tipo di attacchi coinvolgono singole organizzazioni che creano e controllano più account fasulli, i **sockpuppet**, utilizzando come avatar immagini provenienti da social legittimi o da foto di archivio.

Così mentre prima i «fantocci» li scoprivamo col «reverse engineering» delle immagini di profilo, ora è più difficile perché con tecniche di intelligenza artificiale è possibile generare immagini uniche di persone inesistenti come dimostra il sito thispersondoesnotexist.com («This Person Does Not Exist»).



B

BITCOIN

CRIMINALI E ONG: ECCO CHI USA BITCOIN

Alla fine di agosto 2013 il Dipartimento della sicurezza nazionale degli Usa ha sequestrato l'equivalente di 5 milioni di dollari in bitcoin a **Mt.Gox** – uno dei servizi più noti di compravendita di bitcoin -, con l'accusa di non avere la licenza necessaria per il trasferimento di denaro.

Ma la moneta virtuale ha avuto forse il suo maggiore momento di notorietà il 1 ottobre 2013 quando l'FBI ha sequestrato circa 26 mila bitcoin a Ross Ulbricht in seguito al suo arresto e alla chiusura del sito di e-commerce da lui creato, **Silk Road**.

È chiaro che la criptovaluta è uno strumento utilizzabile per fini illegali o criminali, ma può essere un buon metodo per convogliare risorse ad attività perfettamente legali ma scomode, come Ong, organizzazioni per i diritti umani o associazioni di cittadini messe fuorilegge da stati autoritari e dittatoriali.

Può essere anche un ottimo metodo di pagamento per sfuggire al blocco effettuato dalle aziende di carte di credito o da Paypal, come è avvenuto nel caso di **Wikileaks** dopo lo scandalo del **Cablegate**.

Negli ultimi mesi del 2015 notizie mai veramente verificate hanno attribuito l'uso di bitcoin alla rete terroristica che fiancheggia l'**ISIS,** il sedicente **Stato Islamico**, per finanziarne le attività.

Nell'aprile del 2016 Craig Steven Wright, un imprenditore australiano, ha ripetuto in diverse occasioni di poter dimostrare di essere lui il creatore di Bitcoin, ma non è riuscito a dimostrarlo, decidendo successivamente di scusarsi con coloro i quali lavorano allo sviluppo della rete su cui la cryptomoneta si basa.

Oggi con il bitcoin ci si paga anche il caffè in molti paesi scandinavi e perfino in Italia, dove sono sorte rivendite di bitcoin sotto forma di bancomat: si inseriscono gli euro nella macchinetta e si aumenta il proprio conto in bitcoin, controllandolo con una app per telefonino.

La frenesia che circonda questa moneta virtuale ha fatto sì che molte truffe siano perpetrate per ottenere dei bitcoin attraverso dei **cryptominer**, dei software malevoli che generano bitcoin e altre criptovalute usando la potenza computazione di computer personali e telefonini.

MA FACCIAMO UN PO' DI STORIA E SPIEGHIAMO ESATTAMENTE COS'È IL BITCOIN

Bitcoin è una moneta matematica. Risultato di un progetto di **cryptocurrency**

concluso da **Satoshi Nakamoto** nel **2009** indica un tipo di valuta che viene scambiata elettronicamente su reti digitali. Non è l'unica né la prima. Oggi nel mondo se ne contano circa 2000, "coniate" da aziende, attività commerciali, università e associazioni. Bitcoin continua ad essere la più famosa e nessuno sa chi si nasconda dietro lo pseudonimo di Satoshi Nakamoto.

Da quando se ne cominciò a parlare nelle mailing list **cypherpunk**, molti progetti di moneta virtuale sono nati. Uno era quello del cinese **Wei Dai**, che nel 1998 aveva proposto la **b-money** per favorire il commercio elettronico. Avversato da banche e governi, ogni successivo tentativo di "coniare" e usare moneta elettronica era fallito fino alla comparsa di **bitcoin**.

Il progetto del bitcoin venne "caricato" su Source Forge **nel novembre del 2008 e con i bitcoin oggi è possibile acquistare beni e servizi di qualsiasi natura in maniera anonima attraverso Internet**.

Il nome **Bitcoin** si riferisce sia alla moneta (ma con la b minuscola) sia al software open source progettato per implementare il protocollo di comunicazione e la rete peer-to-peer che ne consente lo scambio (con la B maiuscola) e rende concreta la possibilità di evitare il ricorso a un ente centrale grazie a un database distribuito tra i nodi della rete che tengono traccia di tutte le transazioni.

COME FUNZIONA

Ogni importo bitcoin è legato a una coppia di codici, le chiavi crittografiche, una privata nota solo al proprietario, che gli permette di spenderlo, una pubblica, e cioè l'indirizzo bitcoin, che permette di riceverlo. Bitcoin quindi non viene "coniata" da banche o enti centrali, ma grazie a un algoritmo residente su computer attraverso il **mining**. Tanto più ampia è la rete dei **miners**, tanta più moneta verrà controllata e generata attraverso l'algoritmo del software bitcoin.

La rete bitcoin crea un blocco casuale di monete che deve essere verificato dai miners per poterle utilizzare. Oggi esistono numerosi servizi su Internet che vendono bitcoin accettando come controvalore anche le monete nazionali.

La rete bitcoin che memorizza la produzione di tale moneta virtuale ha un limite dato dall'algoritmo di produzione del bitcoin, **21 milioni di bitcoin**, un asintoto che si prevede raggiunto dopo l'anno **2100** se si mantiene l'attuale produzione di bitcoin.

L'intero sistema monetario bitcoin risiede in un database replicato in tutti i nodi della rete bitcoin e questo semplice fatto rende superfluo l'intervento di un'autorità centrale. Per creare il proprio portafoglio virtuale è sufficiente scaricare il client bitcoin su **qualsiasi piattaforma software**, divenendo subito parte della rete che ne garantisce stabilità e affidabilità, anche contro il double spending.

Bitcoin infatti usa la crittografia per proteggersi da furti e manipolazioni, consentendo al titolare di spenderla una sola volta e solo a lui.

Le transazioni in bitcoin sono pseudoanonime tra chi possiede un indirizzo bitcoin (se ne può creare uno per ciascuna transazione); ogni possessore può tenerle in un portafoglio virtuale sul proprio computer o presso terze parti. Il numero di bitcoin circolanti stabilito a priori algoritmicamente in 21 milioni di unità rende particolarmente oneroso in termini computazionali manipolare il numero dei bitcoin. Il controvalore del bitcoin è variabile in relazione al numero di bitcoin circolanti, alle transazioni e quindi agli acquisti effettuati. Segue le leggi della domanda e dell'offerta.

LA LOGICA DEL BARATTO

Il framework concettuale del suo successo è abbastanza semplice. Poiché da molto tempo la produzione di moneta usata come controvalore per l'acquisto di beni e servizi **non è più vincolata alle riserve auree** ma segue criteri flessibili, è sufficiente che un adeguato numero di soggetti decidano di usarla stabilendone il valore. È inoltre da considerare che ogni oggetto, ogni dato, ogni informazione può essere scambiato con qualcos'altro come pagamento. È la logica del baratto.

Tuttavia affinché funzioni è necessario creare un sistema fiduciario che assicuri di poter continuare a spendere il controvalore del bene venduto. Nel sistema bitcoin ciò si ottiene diventando la propria banca e uno dei nodi della rete in grado di replicare tutte le informazioni necessarie a mantenere il sistema sicuro ed efficiente in una logica di **peering**.

KERCHOFF E IL SOFTWARE LIBERO: ECCO PERCHÉ FUNZIONA

In realtà, secondo **hacker e programmatori** l'elevata fiducia attribuibile al sistema dipende dal software usato. Bitcoin è basato su software libero, quindi oggetto di una verifica costante e indipendente da parte di tutti gli interessati. La sua sicurezza dipende dal principio di Kerchoff: "In un sistema crittografico è importante tener segreta la chiave, non l'algoritmo di crittazione."

Uno dei motivi del successo di questa moneta parallela è considerata l'eliminazione degli intermediari e dei costi di transazione nell'acquisto delle merci. Ma il suo motore è la Blockchain, ecco perchè non si fermerà mai.

LE "MONEY FARM"

Considerato il suo successo, aziende e startup che si dedicano al "mining" di criptovalute – Bitcoin, Monero, e-Toro, eccetera – costruiscono le "miniere" per produrle nei paesi dove c'è grande quantità di energia a poco prezzo. Fra questi paesi ci sono quelli caucasici del vecchio impero sovietico, ma anche dell'Europa dell'Est e l'Islanda.

In Islanda le computer-farm di bitcoin e similari stanno diventando così popolari che il paese probabilmente utilizzerà più elettricità per estrarre le monete elettroniche che per le case dei suoi abitanti. Un fatto che ha indotto Johann Snorri Sigurbergsson, portavoce dell'impresa energetica islandese HS Orka, a dire che è tempo di valutare se sarà possibile sviluppare tutti i progetti industriali che vogliono impiantare nel paese fabbriche di cryptomonete. Infatti gli strumenti per il mining di cryptovaluta, che consistono principalmente di computer e dispositivi di raffreddamento di grandi dimensioni, utilizzeranno più elettricità di quella necessaria nel 2018 a servire una popolazione numerosa all'incirca come quella della città di Firenze.

Il costo dell'energia in Islanda è relativamente contenuto perché nella "terra del fuoco e del ghiaccio" quasi tutta l'energia del paese proviene da fonti rinnovabili, geotermia e cascate, e questo favorisce l'insediamento di aziende che producono moneta elettronica, a fronte però di scarsi investimenti infrastrutturali e dello scarso impiego di manodopera specializzata da reperire sul posto. Morale: perfino i membri del Partito Pirata Islandese - che nel 2017 hanno mancato di poco il risultato del governo – cominciano a dubitare che si tratti di un buon investimento. Le tasse pagate dai miners sono molto basse e, come ci ha confermato Smari McCarthy del partito Pirata islandese, "non è detto che le cose debbano restare così".

Attualmente sono circa 17 milioni i bitcoin emessi in rete e, nonostante bolle e oscillazioni, nel marzo 2019 avevano ciascuno un controvalore di circa cinque mila dollari americani.

BOTNET

HACKER IN ERBA AFFITTANO BOTNET SU INSTAGRAM

Instagram, il social network dei gattini e degli influencer da palcoscenico, è diventato la bacheca degli annunci di chi affitta botnet a poco prezzo per attaccare servizi online. "Sei stato licenziato? Buttagli giù il sito". "Vuoi guadagnare tanti soldi in poco tempo? Minacciali di infettargli i computer". Ma come si fa? Affittando una rete di computer zombie per "sdraiare" il loro sito di e-commerce o per bucare la sicurezza aziendale e prendere il controllo di computer, stampanti, telecamere e impianto elettrico. I computer zombie sono quelli infettati e comandati a distanza a insaputa dei proprietari.

I giovanissimi che pubblicano gli annunci sono facile preda di criminali veri che guadagnano grazie alla loro incoscienza. È questa la nuova formula del "crime as a service", i servizi criminali su richiesta, usati per attaccare il mondo digitale cui Instagram si fa veicolo pubblicitario. Sono giovani, e in molti dei loro post c'è tutta la retorica anti-sistema che attinge a piene mani da *Mr. Robot* e da *Black Mirror*, le serie distopiche su hacker, informatica e dark web rese celebri da Netflix.

COME FUNZIONANO LE BOTNET SU INSTAGRAM

Prima era facile, ma non troppo, affittare una botnet da hacker russi o arabi. Bisognava immergersi nel dark web e pagare in bitcoin, adesso questi adolescenti fanno tutto alla luce del sole. Sono gli *script kiddies*, ragazzini che copiano codici fatti da altri, – anche italiani – che registrano brevi video dove dimostrano il loro potere di "*boaters*", come vengono definiti coloro che affittano le botnet e li postano su Instagram liberamente, confondendosi con gli appassionati di barche (in inglese, "boats").

La semplice ricerca per parole chiave sul social network quando digitiamo #botnet, solo per dare un'idea del fenomeno, ci restituisce migliaia di post. Alcuni sono innocui, altri no, e le didascalie sotto le foto spiegano come funzionano le reti infettate e pronte all'uso, altri invece sono annunci di vendita del servizio che mostrano la potenza della botnet: 30 dollari il costo base per poterli utilizzare, naturalmente a tempo.

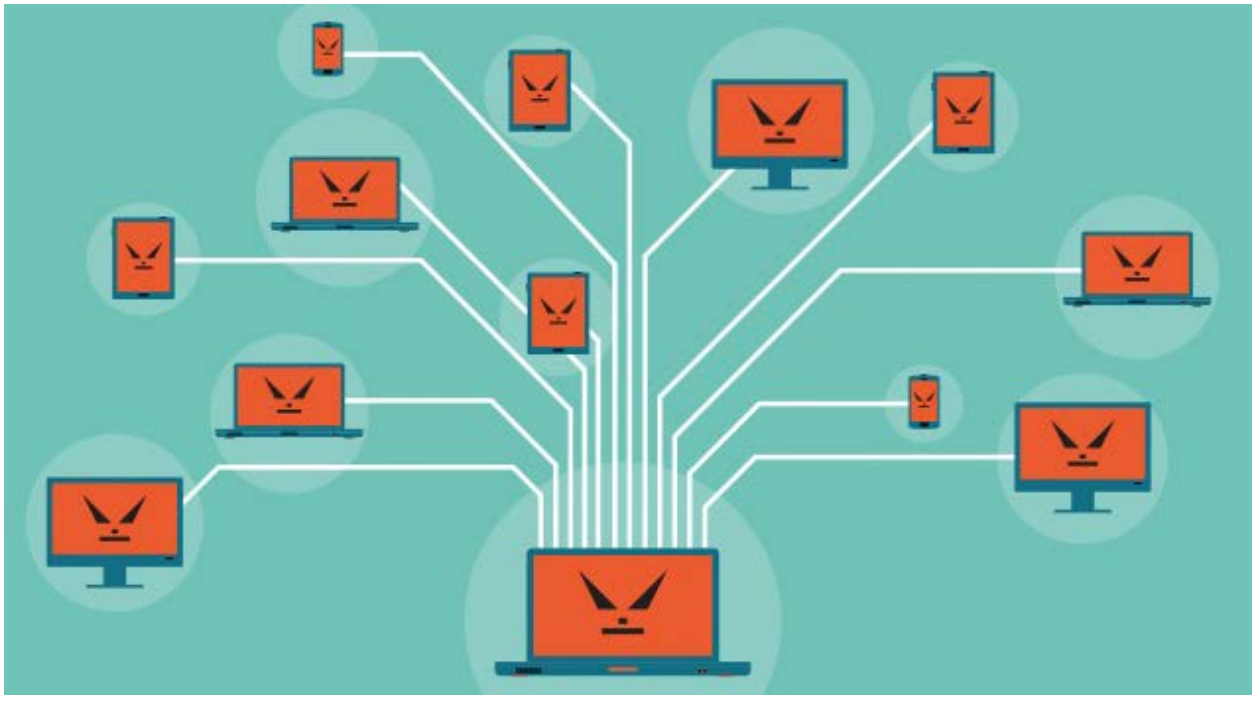
LE BOTNET, UN PROBLEMA SERIO

Le botnet, reti di computer dormienti "riportati in vita" dal loro *botmaster* quando servono, sono diventate uno dei problemi più seri per la sicurezza di banche, assicurazioni e compagnie elettriche, ma sono usate soprattutto

per reclutare e talvolta mettere fuori uso l'Internet delle cose (IoT) di interi palazzi commerciali. Così facendo – al grido di "Ehi, se lo sono meritato!" – spesso l'attività di questi *script kiddies* consiste nell'inoculare malware in reti e computer poco protetti. Il software malevolo prende possesso delle macchine altrui e le trasforma in obbedienti soldatini digitali, in questo modo provocando disservizi e allarmi, ma anche concorrenza sleale.

Per Odisseus, nickname di un ricercatore informatico esperto di cybersecurity che agisce sotto anonimato: "spesso si tratta di Executable and Linkable Format. Elf è un codice eseguibile binario: i malware scritti per piattaforme Linux o Unix like (per Windows si chiamerebbe .exe) lo scaricano nei dispositivi presi di mira e siccome la maggioranza sono piattaforme IoT, notoriamente deboli dal punto della sicurezza, assistiamo a una infezione generalizzata di dispositivi che fino a ieri non credevamo potessero essere preda".

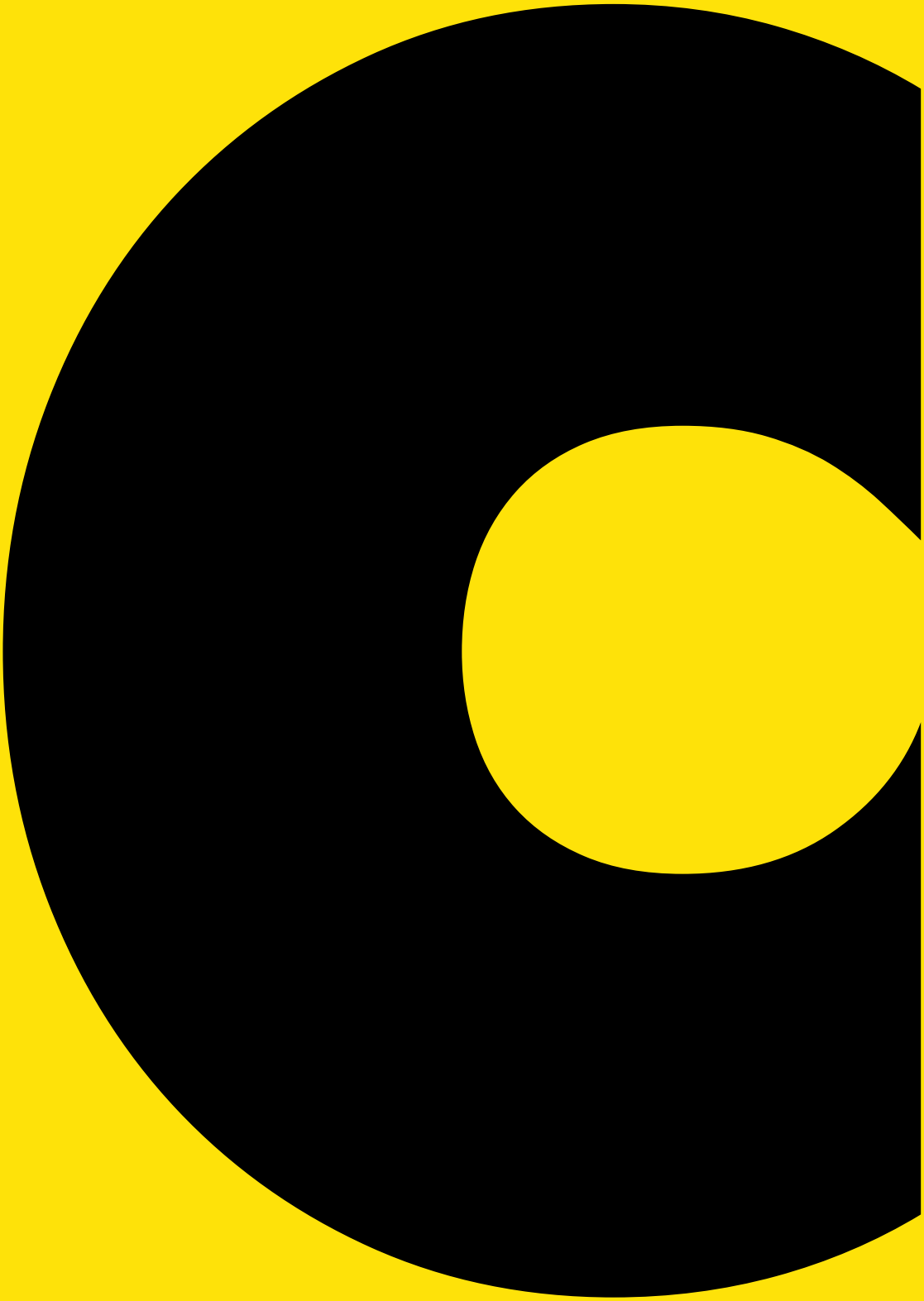
Script kiddies, crackers e black hat (hacker malvagi o criminali) cercano le macchine con gli scanner, le 'bucano' con i codici che ne sfruttano le vulnerabilità e se ne impossessano. A quel punto i dispositivi infettati, spesso installati con le password di default del venditore, senza antivirus e non presidiate, diventano cyberarmi con cui attaccare i siti bersaglio tramire DDoS, un attacco distribuito da negazione di servizio, che fa collassare i sistemi per le troppo richieste contemporanee. Era accaduto con Mirai, la botnet che nel 2016 aveva causato il blocco dei server da cui dipendevano Amazon, Twitter e il *New York Times*. Un emulo del suo autore, **Anna Senpaii**, è proprio su Instagram. In una analisi di Kaspersky l'Italia sta diventando la patria di questi attacchi che secondo altri studi complessivamente sono aumentati del mille per cento durante il 2018.



ARRIVANO I CACCIATORI DI VIRUS

Come dicevamo, i ragazzini fanno soldi pubblicizzando le botnet ma sono spesso solo le avanguardie di adulti che invece istruiscono le reti malevole e vendono il codice sorgente nell'ecosistema del malware per puro malaffare. Dietro agli adolescenti che ci cascano su Instagram si nascondono i delinquenti veri, quelli che affittano gli *hitman* (i sicari) nel dark web per colpire fisicamente chi li combatte. **Malware Must Die** è uno dei team internazionali di esperti che danno loro la caccia. Di poche parole, si esprimono in gergo tecnico e collaborano con le polizie nazionali ed è anche questo il motivo per cui questi 'cacciatori di virus' si nascondono dietro nomi fantasiosi. Il leader del gruppo, tra i più famosi analisti di malware a livello mondiale, si chiama **unixfreaxjp**, e come gli altri ha ricevuto minacce di morte dai criminali di cui hanno debellato le infrastrutture. Eppure insistono nel cercarli per combatterli perché "questi imperversano, entrano su qualsiasi device, lo infettano e poi 'dossano' (da DDoS) tutto il mondo", dice Odisseus.

B



CLICKTIVISM

COM'È BANALE L'ATTIVISMO DEL CLICK

C'è un aspetto legato alla sicurezza che riguarda da vicino il comportamento di chi usa con leggerezza strumenti di comunicazione come i social network ed è il **clicktivism**.

Il *clicktivism* è la versione social dell'attivismo da tastiera, quell'attitudine che ci fa sentire partecipi e sostenitori di una qualche causa sociale, politica o ambientale e che ci aiuta a metterci in pace con le ingiustizie del mondo. "Il Polo Nord è inquinato?" Clicca qui. "Sei indignato?" Clicca qua.

Clicktivism è però un termine dispregiativo perché indica un tipo di attivismo facile, poco impegnativo che spesso si risolve nella sua forma peggiore, lo *slacktivism*, l'attivismo inconcludente e fannullone. E tuttavia dice molto di quali sono le nostre preferenze culturali e politiche, proprio quelle che sono collezionate nei giganteschi database che i padroni dei dati come Google, Amazon e Facebook usano per definire i nostri profili sociali, economici, ed elettorali.

Il *clicktivism* è basato sulla persuasione. Alla base di ogni forma di comunicazione, quella politica e quella pubblicitaria, la persuasione cerca di farci fare quello che non faremmo di nostra spontanea iniziativa, scatenando risposte pre-programmate dalla cultura e dall'educazione.

Se uno ti saluta, tu rispondi, anche se non lo conosci. In Rete rispondiamo ai segnali digitali di persone che fanno parte delle nostre cerchie sociali: se un mio amico condivide una notizia io ci piazzo un like o la rimbalzo su Twitter. Magari neanche la leggo ma intanto non è faticoso e faccio contento il mio amico dichiarando la mia adesione alla sua visione del mondo.

Dopo lo scandalo di Cambridge Analytica siamo tutti concentrati su Facebook, ma tutte le piattaforme digitali basano il loro modello di business sull'estrema personalizzazione delle informazioni che ci propongono. Ad esempio, basta cliccare su un certo video e Youtube ci proporrà argomenti simili e sempre più coerenti. Hai guardato il video di un concerto di Kate Perry? Appena ti connetti a Youtube ti vengono suggeriti i video degli altri suoi concerti. Viceversa, se guardi un paio di concerti di Lady Gaga, la piattaforma ti proporrà i video di Lady Gaga.

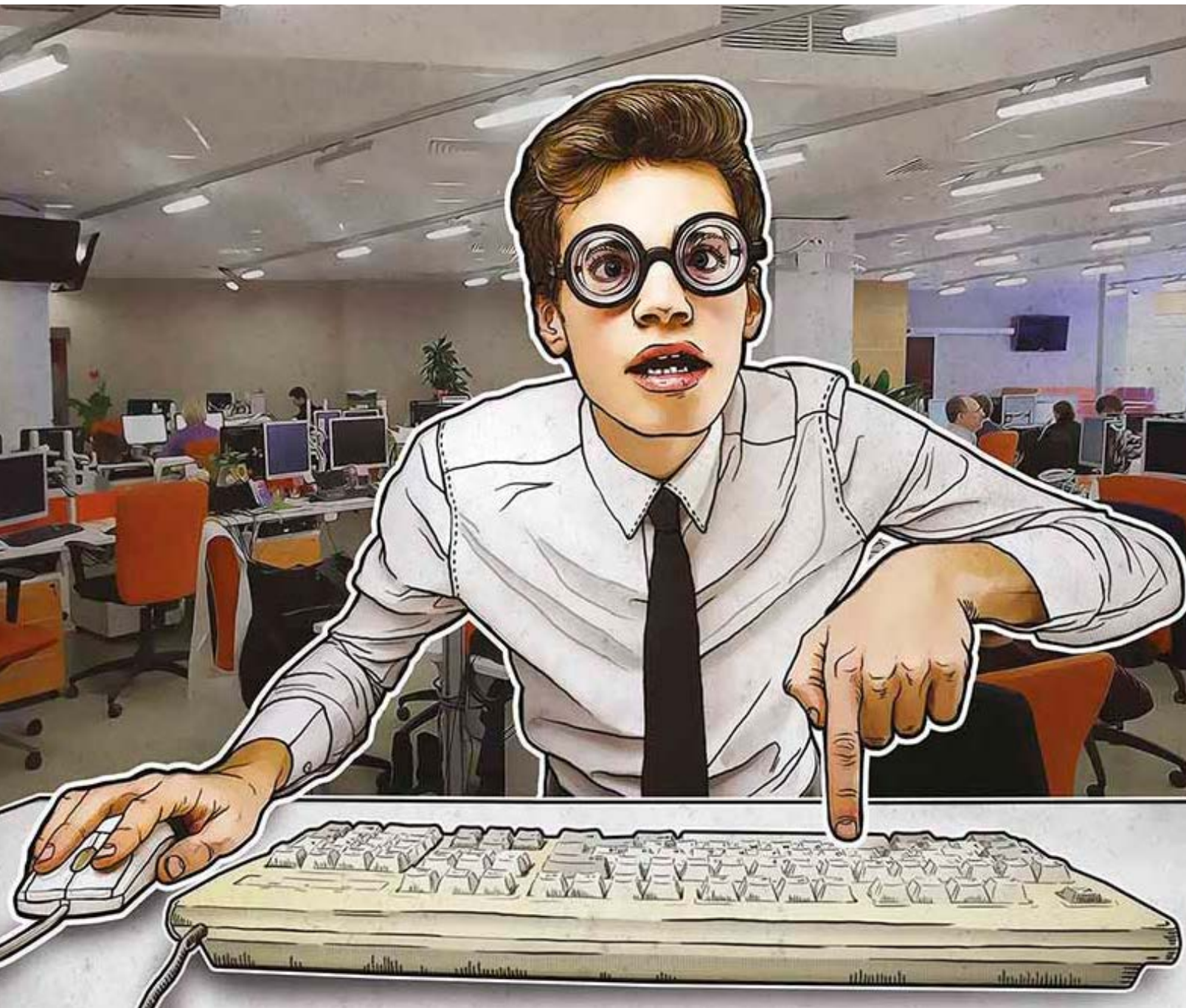
Le piattaforme sono interessate ad ampliare i volumi del traffico e per farlo devono offrirci esperienze sempre meglio ritagliate sui nostri gusti e le nostre abitudini.

Potremmo perfino dire che le piattaforme digitali sono neutrali e che lavorano per noi, in fondo cercano di proporci quello che ci piace e quello che ci piace viene dedotto dai click fatti nel passato.

Ogni ricerca online ne tiene memoria, come su Google. Ma queste informazioni possono essere usate per comunicazioni mirate e geolocalizzate di tipo sia commerciale sia elettorale.

È così che funzionano i "*dark ads*" durante le elezioni: messaggi promozionali a pagamento diretti solo a specifici indirizzi o territori precedentemente selezionati e profilati. Qui la manovra però diventa a tenaglia: prima l'esposizione alle *fake news* per polarizzare l'elettorato, poi il messaggio politico ritagliato *ad hoc* sotto forma di una comunicazione nominativa, ma diretta a una moltitudine di singoli elettori, ai quali viene recapitata in maniera ossessiva un'informazione specifica e coerente con il proprio profilo psicologico ed elettorale.

Insomma, poiché ogni click viene usato per costruire un profilo dei comportamenti degli utenti in rete, evitare il clicktivism è più importante di quello che pensiamo.



COPYRIGHT

NON RUBARE IL LAVORO ALTRUI, CHIEDI UN COPYRIGHT 2.0

Un comportamento spesso messo in atto in rete è l'utilizzo di opere creative senza averne il permesso. L'uso abusivo di opere creative è però sanzionato dalla legge in base alla sua gravità. La cosa da ricordare sempre è che per usare una foto, un testo musicale, un video o un pezzo di codice software bisogna chiederne il permesso, perché lo prevede la legge.

Il copyright è una formula giuridica che protegge le idee espresse in una forma narrata e riconoscibile – un libro, un film, un software, una canzone – e rappresenta il riconoscimento del valore del lavoro intellettuale di chi le realizza. Il diritto d'autore moderno ha sempre avuto come obbiettivo quello di garantire la remunerazione dell'autore e

lo sfruttamento economico dell'opera per stampatori, editori, distributori, con il fine di consentirne la più ampia circolazione possibile per l'avanzamento della società. Dal tempo dei dogi veneziani ad oggi, le autorità hanno concesso agli autori e agli editori questo monopolio temporaneo basato sullo sfruttamento esclusivo delle opere, ma facendosi garanti dei diritti di tutti.

Per questo il diritto d'autore in Italia è automaticamente imposto e senza spese. Purtroppo negli anni il diritto d'autore è diventato un diritto degli editori e degli intermediari, lasciando agli autori solo le briciole, ponendo un freno alla diffusione delle opere, gestendone male i proventi e creando scarsità artificiale per aumentarne il prezzo.

Il 26 Marzo 2019 il Parlamento Europeo ha approvato la riforma europea del copyright.

Una riforma frutto di tatticismi e mediazioni al ribasso per proteggere un patrimonio comune, la conoscenza nell'era digitale. Due dei suoi articoli più controversi, il numero 11 e il 13 - divenuti 15 e 17 -, introducono il primo una sorta di tassa per chiunque riproponga online contenuti creativi anche parziali, come un link e la sua descrizione, senza pagare il giusto compenso ai titolari dei diritti, mentre il secondo mira ad applicare un controllo preventivo ai materiali digitali caricati su piattaforme come Youtube, social network o siti collaborativi affinché non violino il copyright.

Per questi motivi le versioni italiana, spagnola, lettone, di Wikipedia, l'enciclopedia libera collaborativa più grande al mondo, sia nel 2018 che nel 2019 hanno deciso una serrata di protesta. Secondo Wikipedia, infatti, la direttiva in votazione minerebbe i diritti fondamentali dei cittadini europei, come quello di decidere liberamente cosa produrre e pubblicare in rete, consegnando ai privati la decisione finale di cosa sia lecito diffondere online.

Le associazioni di categoria di autori, editori e giornalisti, le società per l'intermediazione dei diritti, Anica, Siae, Confindustria, ritengono invece che la direttiva serva a educare i più giovani al rispetto del lavoro altrui, a porre un argine alla pirateria digitale e impedire agli aggregatori come Google di fare profitti senza remunerare gli autori dei contenuti.

Hanno ragione entrambi. La legge di riforma è scritta male e probabilmente non è adatta alla società della condivisione a cui, volenti o nolenti, apparteniamo.

Tuttavia nonostante la riforma, Internet continuerà a esistere e Wikipedia pure, mentre l'industria editoriale non risolleverebbe le sue sorti compromesse dalla cultura della gratuità.

Lo Stato, l'Europa, possono tornare a farsi garanti di questo rapporto tripartito tra autori, editori e pubblico dei fruitori ormai divenuti prosumer, rigettando la riforma del copyright e facendone una migliore. Come? Con un copyright 2.0, mettendo tutte le opere nel pubblico dominio, liberamente utilizzabili per produrne di nuove, tranne che gli autori, i titolari dei diritti, vogliano altrimenti, ma esplicitandolo, e pagandone la protezione con un piccolo contributo se la ritengono remunerativa. La società tutta ne trarrebbe beneficio, che è da sempre l'obiettivo primario del diritto d'autore.

CREATIVE COMMONS

Il copyright tradizionale non è l'unico strumento per proteggere un'opera creativa. Le licenze Creative Commons possono utilmente servire allo scopo con una serie di vantaggi. Ma cosa sono le Creative Commons?

Creative Commons identifica un set di licenze che specifica i diritti legali attinenti a un'opera creativa precedentemente definiti dal suo autore. Tale specificazione si fonda su una peculiare combinazione di simboli e descrizioni per indicare ex ante il tipo di utilizzo dell'opera concesso in regime di diritto d'autore.

Creative commons è anche il nome dell'organizzazione non-profit fondata nel 2001 da Lawrence Lessig per promuovere le licenze creative commons con l'obiettivo di facilitare la più ampia condivisione delle opere creative in contrasto alle rigidità del copyright tradizionale.

L'idea alla base delle licenze Creative commons è quella di favorire il controllo dell'autore sulla propria opera definendone di volta in volta gli usi possibili attraverso una combinazione di scelte. La combinazione di tali scelte porta a sei differenti articolazioni del diritto d'autore specificate dall'uso di simboli grafici e descrittivi. Creative commons offre anche dei metadati RFD/XML con cui definire in maniera automatizzata il tipo di licenza prescelto attraverso il sito creativecommons.org e quelli dei chapter nazionali.

L'innovazione introdotta da creative commons tramite le licenze e gli strumenti informatici per definire le condizioni d'uso dell'opera ribaltano la logica del diritto d'autore tradizionale basata sull'imperativo di "all rights reserved" ("tutti i diritti riservati"), mediante la formula "some rights reserved" ("alcuni diritti riservati"). Tale formula indica che con l'opera si può fare tutto tranne ciò che è specificamente proibito, consentendo di mantenere il copyright sulla propria opera e di lasciare i fruitori liberi di farne l'uso concesso dal titolare dei diritti.

Le Creative Commons offrono quindi strumenti e licenze basate sul copyright per creare un nuovo equilibrio all'interno della formula "tutti i diritti riservati" stabilita dalle leggi sul copyright.

I simboli e i permessi o clausole sono quattro (BY-SA-NC-ND) e danno origine e sei combinazioni che vanno dalla più liberale a quella più restrittiva tipica del copyright tradizionale.

LE QUATTRO CLAUSOLE

BY=Attribuzione
Implica che bisogna sempre indicare l'autore dell'opera.

Non-commerciale
Implica che non è possibile farne usi commerciali.

No-Derivati
Implica che non è possibile modificare e rielaborare l'opera.

Condividi allo stesso modo
Implica che l'opera può essere modificata ma deve essere rilasciata sotto le stesse condizioni decise dall'autore originale.

LE SEI COMBINAZIONI

La licenza **Attribution (CC-BY)**, ad esempio richiede solo che venga specificato l'autore dell'opera che è resa disponibile per ogni tipo di utilizzo.

La licenza **Attribution-Share Alike (CC-BY-SA)**, invece consente ogni tipo di utilizzo dell'opera fintanto che l'autore viene citato e implica che ogni uso successivo dell'opera è consentito secondo gli stessi termini della licenza.

Le opere **Attribution-Non commercial (CC-BY-NC)** invece non implicano lo stesso regime di redistribuzione, sia nella forma originale che modificata, ma non sono disponibili per un uso commerciale.

La licenza **Attribution-No-Derivatives (CC-BY-ND)** consente ogni uso possibile dell'opera tranne la modifica.

La licenza **Attribution- Non Commercial-Share Alike (CC-BY-NC-SA)** implica che l'autore deve essere sempre citato, che l'opera non può essere commercializzata senza permesso e che ogni uso successivo deve rispettare la licenza originaria (condividi allo stesso modo).

La licenza **Attribution-Non-Commercial-No-Derivatives (CC-BY-NC-ND)** implica la semplice condivisione dell'opera che non può essere né modificata né usata a fini commerciali ed è la più restrittiva.

Esiste anche una licenza detta **"Creative Commons 0" (CC0)** che equivale al pubblico dominio e in base alla quale l'autore rinuncia a ogni pretesa sull'opera tranne quelle che secondo le legislazioni nazionali sono irrinunciabili come nel caso del diritto morale in Italia.

DRM-CC

Spesso si parla di creative commons come di Drm descrittivi (in quanto descrivono gli usi possibili dell'opera) in opposizione ai Drm prescrittivi che implicano l'utilizzo delle TPM, le Technical Protection Measures, misure tecniche di protezione, che sono implementate a livello informatico tramite codici crittografici.

Da precisare che nonostante il copyright e il diritto d'autore siano spesso considerati equivalenti, portano delle differenze. Il copyright indica il regime giuridico della tutela delle opere d'ingegno nella giurisprudenza di derivazione anglosassone, il diritto d'autore ha le sue fondamenta nel diritto romano. Tali differenze tendono ad annullarsi in sede internazionale presso gli istituti che ne risolvono le controversie o decidono standard comuni come la Wipo (World Intellectual Property Organization).

Questa differenza è importante però nel caso delle Creative commons. L'intuizione del suo "inventore" Lawrence Lessig rimanda infatti alla causa (Eldred vs. Ashcroft) da lui stesso intentata agli Stati Uniti, paese in cui una sentenza in tribunale crea giurisprudenza generando un precedente all'interno della cornice del Common Law.

Nel mondo molti progetti di informazione hanno scelto la tutela delle Creative Commons, è il caso del repertorio creative commons di Al Jazeera e della BBC o del giornale La Stampa di Torino.

Creative commons è oggi un'organizzazione con numerosi chapter nazionali impegnati a tradurre, localizzare e adattare il set di licenze offerte alle specifiche legislazioni nazionali.

CRITTOGRAFIA

La crittografia è la branca della crittologia che si occupa di come rendere illeggibile un messaggio a un ricevente indesiderato con un'operazione nota come cifratura. Un testo realizzato secondo i principi della crittografia si chiama testo cifrato e perché sia riportato nella sua forma in chiaro il destinatario deve compiere un'operazione che si chiama decifrazione.

La stessa operazione (la decifrazione) attuata da chi non è autorizzato a leggere il messaggio si chiama decrittazione, mentre la crittanalisi è l'insieme delle teorie e delle tecniche che se ne occupano.

Chiaro? Ok, andiamo avanti

Poiché la crittografia è la scrittura segreta basata su di un codice condiviso fra gli interlocutori, il livello di segretezza di un testo cifrato dipende da due fattori: il cifrario utilizzato, ovvero il codice, e la complessità della chiave di cifratura che determina il modo in cui un messaggio viene cifrato.

La chiave di cifratura nella crittologia moderna è creata attraverso algoritmi matematici.

Tanto più è robusto l'algoritmo e complessa la chiave di cifratura che esso genera, più sicuro sarà il messaggio, anche di fronte a un attacco di forza bruta, cioè l'esplorazione di tutte le combinazioni matematiche che permettono di risalire alla chiave.

Nel corso della storia sono state sviluppate numerose tecniche crittografiche per garantire la segretezza delle comunicazioni scritte.

La crittografia è salita alla ribalta delle cronache nel 2010 con il Cablegate, lo scandalo legato alla diffusione dei cablogrammi riservati della diplomazia americana da parte del sito anticorruzione Wikileaks, che raccoglie, attraverso una piattaforma di whistleblowing, informazioni privilegiate e top secret garantendo la sicurezza e la segretezza delle fonti grazie all'uso della crittografia. Prima di scoprire che era stato il soldato Bradley "Chelsea" Manning a fornire le informazioni alla base dello scandalo – e per questo condannato a 35 anni di prigione - si era temuto che fosse stata l'incursione di crittoanalisti avversari a determinare la falla di sicurezza che aveva causato il leaking dei documenti. Non era così, però la vicenda ha avuto il merito di ravvivare il dibattito pubblico sulla sicurezza informatica e gli standard crittografici.

LA STORIA DELLA CRITTOGRAFIA

In realtà da tempo immemorabile la gente protegge i propri segreti con corrieri, bisbigli, porte e buste chiuse. Ma anche attraverso codici cifrati, tanto che nel corso della storia sono state sviluppate speciali tecniche crittografiche per garantire la segretezza delle comunicazioni scritte.

Giulio Cesare fu tra i primi uomini di stato a elaborare un proprio cifrario per comunicare coi suoi generali e l'Italia vanta una eccellente tradizione di quest'arte di cui scrissero Leon Battista Alberti (il De Cifris), Girolamo Cardano, Pierluigi Sacco ed altri. Una tradizione la cui importanza è, secondo gli esperti, all'origine della riscossa degli alleati contro i nazisti quando riuscirono a decifrare lo storico codice Enigma, il risultato di uno sforzo considerato alla base dello sviluppo dei primi computer.

L'esigenza di segretezza in ambito militare ha fatto sì che la crittografia fosse per lungo tempo considerata appannaggio di generali, diplomatici e spie. Le cose cambiano radicalmente con l'introduzione delle macchine elettroniche e oggi, in un mondo interconnesso dagli apparati di comunicazione digitale, la crittografia è una componente fondamentale della vita quotidiana anche se non ce ne rendiamo conto.

Quando usiamo un bancomat o guardiamo la pay-tv, quando ci colleghiamo a un sito web sicuro per le operazioni bancarie o compriamo qualcosa su Internet, quando parliamo al telefono cellulare o accediamo a una rete wireless, usiamo la crittografia.

Pochi sanno però che la crittografia odierna è il risultato della testardaggine di un pugno di libertari pacifisti, accademici non ortodossi e imprenditori d'assalto che sono riusciti, attraverso uno sforzo disorganizzato ma convergente negli obiettivi, a rompere il monopolio di militari e servizi segreti nell'uso delle tecniche crittografiche e quindi nella capacità

di rendere sicuro ciò che porte e buste chiuse non bastano più a proteggere: le comunicazioni digitali. (Crypto. I ribelli del codice in difesa della privacy, Shake, 2003)

Una vicenda che è testimonianza esemplare di come lo spirito della frontiera americana – l'ansia di libertà, la ricerca, talvolta ossessiva, della privacy e la diffidenza verso l'autorità – sia stato messo a dura prova dai poteri costituiti attraverso il ricorso sistematico alla censura e all'uso della forza che non disdegna trucchi e colpi bassi. Un conflitto paradigmatico, tipicamente americano, fra la strenua difesa della privacy e delle libertà individuali e il totem della sicurezza nazionale, spauracchio usa e getta quando «la patria chiama» alla guerra (fredda, d'aggressione, al terrorismo, preventiva o comunque si chiami).

Dietro le quinte la NSA, la potentissima National Security Agency, al centro dello scandalo del Datagate, l'organismo deputato alle intercettazioni telefoniche e digitali voluto nel 1952 dal presidente Truman con quartiere generale a Fort Meade nel Maryland. Un'agenzia che, grazie al quasi assoluto monopolio delle tecniche crittografiche e crittoanalitiche, ha sempre vegliato sul buon andamento dell'american way of life, spiando qua e là come se la guerra fredda non fosse mai finita.

[UN SURPLUS DI STORIA]

La storia della rivoluzione crypto con i cryptoribelli che sfidano la NSA comincia con Whitfield Diffie, che insieme a Marty Hellman nel 1976 dà alle stampe "New Directions in Cryptography" per illustrare il concetto di cifrario a doppia chiave pubblica basato sulle «funzioni asimmetriche», un tipo di funzione matematica equivalente al famoso caso del piatto che una volta rotto in mille pezzi non torna mai uguale a prima. Un salto concettuale enorme che mise in crisi tutta la crittografia precedente basata sul concetto di chiave simmetrica: una unica chiave usata sia per cifrare sia per decifrare i messaggi. L'intuizione di Diffie risolveva il problema della sicurezza dello scambio della chiave fra gli interlocutori dovuto alla presenza di un intercettatore potenziale, il *man in the middle*, perché nel sistema a chiave asimmetrica, dalla prima chiave usata per cifrare il messaggio non si può risalire all'altra necessaria a decifrarlo, né viceversa, e solo usandole insieme permettono di leggere il testo in chiaro. Una trovata geniale, a cui anche James Ellis del General Communication Headquarters – l'equivalente britannico della NSA – stava lavorando in assoluto segreto per l'ossessione propria dei governi di garantire l'affidabilità dei propri sistemi tramite «comunità chiuse» di crittografi per «minimizzare l'informazione disponibile ai nemici».

Una rivoluzione che però molti ignorarono o cercarono di nascondere, perché faceva dubitare della sicurezza di un intero settore industriale, quello cresciuto intorno alle prime transazioni elettroniche bancarie.

Alcuni anni prima, infatti, il governo americano aveva cominciato a paventare i pericoli di sistemi di crittografia commerciale incompatibili fra di loro, serio ostacolo alla comunicazione e alla collaborazione tra imprese, tra organismi governativi e tra imprese e istituzioni governative. Perciò in maniera

occulta, la NSA lavorò a facilitare il lavoro di corporations vicine al governo, in particolare l'IBM, per realizzare uno standard crittografico potente ed efficace di cui si incaricò il National Bureau of Standards. L'algoritmo scelto per garantire la sicurezza matematica dello standard fu il DES (Data Encryption Standard). Nel 1977 il DES divenne lo standard federale, ma alla sua comparsa fu subito aspramente criticato. Si sospettava infatti l'intervento del governo nella sua realizzazione e si temeva che al suo interno contenesse una funzione di key recovery.

CHE COS'È LA KEY RECOVERY

La key recovery ricorda concettualmente il passaggio segreto voluto da un castellano nel suo maniero: è sicuro fintanto che solo e soltanto il proprietario del castello lo conosce. Per quanto riguardava la key recovery, il timore era che lo conoscesse anche il governo. L'altra critica al DES era che non dava sufficienti garanzie di robustezza. La sua chiave di cifratura era stata infatti volutamente accorciata per indebolire il sistema e renderlo vulnerabile a un attacco di forza bruta, che all'epoca pochi programmatori o esperti di computer avrebbero potuto operare. Tra questi c'erano, ovviamente, gli stessi militari. A testimonianza della vulnerabilità del sistema di crittografia, va ricordato che nel ventennale della sua comparsa, con l'"operazione Deschall" il DES fu «rotto» da un attacco di «forza bruta» e i cypherpunks scrissero un software apposta per farlo, il DES Cracker.

RSA IL NUOVO ALGORITMO E IL PGP

E tuttavia, mentre infuriava la polemica, alcuni programmatori e ricercatori critici del sistema trovarono la soluzione alla presunta debolezza del DES in un altro algoritmo, l'RSA, sviluppato in maniera indipendente da Rivest, Shamir e Adleman e successivamente usato dall'altro grande protagonista di tutta la vicenda crypto: Philip Zimmermann, autore del più noto software di crittografia pubblica oggi ancora in uso, il PGP (Pretty Good Privacy for the masses).

Il PGP è un software che genera una chiave pubblica, consultabile da chiunque, e una segreta, nota solo all'interessato. Il crittosistema di Zimmermann concretizzava l'intuizione di Diffie, perché il messaggio codificato con la chiave pubblica, la sola scambiata fra gli interlocutori, risulta incomprensibile a chi non possiede entrambe le chiavi (a questo proposito si può consultare il sito internet https://www.openpgp.org/). Inoltre, proprio perché il software di Zimmermann si basava sul concetto di protezione forte (una lunga chiave di cifratura di tipo asimmetrico), fu considerato un'arma da guerra e per questo ne fu proibita l'esportazione.

Ma Zimmermann, attivista politico e militante pacifista, era affascinato dall'idea di dare a chiunque un sistema crittografico a prova di spione, convinto come Diffie che il processo democratico si origina solo attraverso la libera discussione e che impedirla attraverso la sorveglianza elettronica equivalga a costruire uno stato di polizia. Perciò, nonostante i divieti governativi e i problemi di utilizzo del brevetto della chiave RSA, il PGP venne distribuito velocemente in tutto il globo da migliaia di «ribelli del codice» per garantire la privacy delle comunicazioni telematiche. Negli USA, questo avvenne grazie a un gruppetto di persone che se ne andava in giro con computer e accoppiatori acustici per riversarlo da anonime cabine telefoniche nei BBS (Bulletin Board System) della federazione, mentre in Europa fu diffuso, dopo aver passato la dogana, stampato su carta. Da lì nacque una lunga causa legale che vide l'assoluzione del «traditore» Zimmermann.

Nel frattempo il governo statunitense continuava a lavorare su nuovi sistemi di cifratura scoraggiando liberi ricercatori dal proseguire nei loro studi e manovrando le leve della politica per mantenere il monopolio delle conoscenze crittografiche dell'epoca. Il Clipper chip prometteva di essere la soluzione d'equilibrio cui la NSA lavorava da sempre: un sistema crittografico basato su un meccanismo di cifratura abbastanza potente da scoraggiare tagliaborse elettronici, ma non abbastanza forte da essere invulnerabile per i militari stessi e che prevedeva l'obbligo di legge di depositare la chiave di cifratura presso un ente governativo che avrebbe potuto utilizzarla alla bisogna (la key escrow, più o meno la chiave di cifratura data in deposito).

Il progetto fallì grazie alla comunità cripto anarchica e all'opposizione di molti imprenditori. L'argomentazione del loro rifiuto era semplice: quanti di voi accetterebbero di depositare una copia delle chiavi di casa alla

stazione di polizia? Ma il progetto fallì anche per l'intervento di un deputato del congresso considerato vicino alla lobby hi-tech, da sempre perplessa dalla scelta del governo di consentire la crittografia forte per gli Usa e un sistema di crittografia debole per l'estero, un fattore che ne avrebbe scoraggiato la commercializzazione, danneggiando profitti, ricerca e sicurezza.

Il progetto del Clipper Chip fu abbandonato, il PGP si impose come standard nelle comunicazioni private. Da allora, sono stati sviluppati sistemi proprietari per le transazioni elettroniche sicure e oggi anche i normali browser per il web e diversi client email usano sistemi che garantiscono l'anonimato nelle comunicazioni via computer e la «cifratura» dei dati basati sulle intuizioni della comunità cryptoanarchica che, adeguatamente usati, garantiscono abbastanza bene la riservatezza delle nostre comunicazioni via Internet.

Questa storia dimostra che nell'era di Internet una comunità adeguatamente motivata può ottenere risultati che solo entità ben organizzate e opportunamente finanziate sono in grado di raggiungere. Come, ad esempio, fare di un software freeware (gratuito e liberamente distribuibile con tanto di codice sorgente) lo standard mondiale della crittografia a uso privato. Il secondo è che creatività e conoscenza non possono essere monopolio di agenzie governative e che l'innovazione non può essere ingessata da brevetti o copyright, sia perché il modo in cui opera la scienza è tale che le scoperte parallele e le riscoperte sono la norma, sia perché la conoscenza per definizione è un'impresa collettiva, basata sul libero scambio di informazioni. Il terzo motivo è che in un campo tanto delicato come quello della privacy e della sicurezza dei dati il principio della security through obscurity caro alle agenzie di governo è totalmente inadeguato. Sia perché, e molto più banalmente, quattro occhi sono meglio di due, che' la fiducia è un bene scarso e va centellinato e non si chiede mai all'oste se il suo vino è buono. La logica conclusione, applicata alla crittografia, è che, in omaggio al principio di Kerchoffs, l'unica garanzia di affidabilità dell'algoritmo usato per la cifratura è la sua natura pubblica, affinché chiunque possa verificarne la robustezza o individuarne falle ed errori.

Anche se PGP è diventato uno standard mondiale e la comunità del software libero ha sviluppato anche l'equivalente GNU Privacy Guard, nessuna chiave crittografica può proteggere dagli errori di chi la usa e colpevolmente dimentica la propria chiave o la fornisce ad altri per eccesso di fiducia e sicurezza o sotto ricatto. Il phishing e l'ingegneria sociale fanno il resto. Questo è uno dei motivi per cui la comunità cypherpunk usa ancora autenticare e scambiarsi le chiavi pubbliche durante dei PGP party.

La paranoia è la prima arma di difesa.

CYBERCRIME

IL CRIMINE INFORMATICO È LA TERZA POTENZA ECONOMICA MONDIALE

Secondo l'ultimo rapporto del World Economic Forum sui rischi globali le attività degli hacker si stanno industrializzando, e per il 2021 i danni causati dai cybercriminali potrebbero arrivare a 6 trilioni di dollari, l'equivalente del prodotto interno lordo della terza economia mondiale. Per capirci Tesla, Walmart, Facebook, Microsoft, Apple, Amazon messi insieme non arrivano a un trilione e mezzo di ricavi.

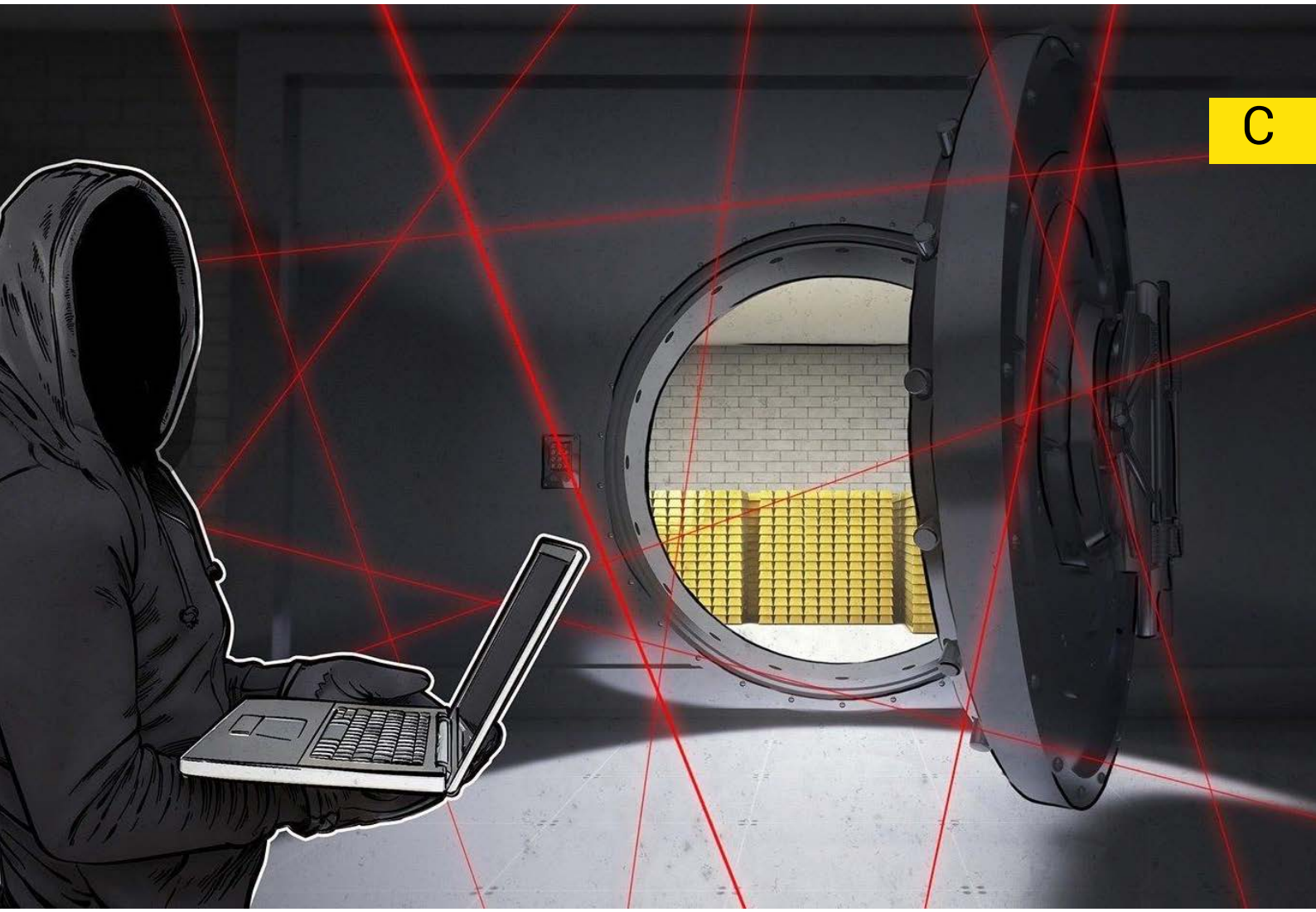
I malvagi di cui parla il rapporto però non vestono più il cappuccio, ma si organizzano in team ben strutturati, non si nascondono nel Dark Web ma fanno pubblicità e proseliti nei social media, e sono anche capaci di offrire un «customer care» alle loro vittime, una sorta di ufficio di relazioni con i clienti attaccati via ransomware o DDoS.

Con la remotizzazione delle attività di studio, lavorative e terapeutiche causate dalla pandemia di Coronavirus, lo scenario, secondo gli analisti, potrebbe complicarsi. Gli attacchi alle strutture sanitarie, ai sistemi di videoconferenza e di teledidattica, le intrusioni aziendali favorite dal remote working insicuro avvenuti in questi giorni si aggiungerebbero così agli attacchi a energia, trasporti, Internet delle Cose.

Nel rapporto il Wef afferma che il crimine informatico sarà il secondo rischio più grave per il commercio globale nel prossimo decennio fino al 2030. Stilato prima della dichiarazione della pandemia da parte dell'Oms, già considerava la relazione tra tecnologia ed eventi disastrosi su scala globale.

Nel 2019 i target principali sono stati banche e servizi finanziari. Ma di fronte all'obbiettivo della ripartenza dell'economia in recessione a causa del Coronavirus ci si aspetta che saranno moltiplicati gli attacchi alla filiera industriale e commerciale: dai mobili all'agroalimentare passando per i negozi online.

Il crime as a service, l'industria del crimine su richiesta, offre di tutto, dagli attacchi distribuiti (DDoS) per bloccare siti e servizi, ai malware e alle campagne di phishing, Trojan e sequestro di database, tutte opzioni nel portafoglio di organizzazioni criminali che agiscono come il board di imprese legittime: tengono riunioni, fanno scouting di talenti, li impiegano per i loro scopi. Quando un «kit di attacco» funziona bene si occupano di sviluppo del prodotto, supporto tecnico, distribuzione, e ne certificano la qualità. Raramente competono fra concorrenti, piuttosto si scambiamo metodi e tecniche di cui rivendicano l'ideazione nel codice, con commenti in lingua e con riferimenti criptici agli informatici che li hanno messi a punto.



C

Alcuni gruppi hanno persino personaggi pubblici che ne curano la reputazione nel Dark Web. I loro «team leader» guidano i «minatori di dati», i coder che scrivono codice dannoso, e gli «specialisti delle intrusioni», che si infiltrano nelle aziende target.

Le loro incursioni possono durare giorni e costare da $10 per un piccolo attacco a migliaia di dollari per quelli più complessi. Possono essere parte di un piano di riscatto – l'Italia è tra i paesi europei più colpiti dai ransomware –, atti di vandalismo e sabotaggio, o semplicemente un modo per mascherare un altro attacco.

L'Università di Cambridge ha scoperto che tali assalti sono diventati così comuni che i loro acquirenti includono persino adolescenti che attaccano i registri scolastici online.

Secondo il Wef però la spesa per la sicurezza informatica è sottodimensionata vista l'entità della minaccia, e considerato che negli Usa la probabilità di portare in tribunale i cybercriminali è stimata intorno allo 0,05% dei casi.

CYBERSECURITY

PERCHÉ LA SICUREZZA INFORMATICA CI RIGUARDA TUTTI

La sveglia non è suonata e la lampada accanto al comodino non si accende. Andate in bagno e l'acqua calda non arriva. Provate a farvi un caffè con la macchinetta che sembra morta e poi vi rendete conto che la casa è fredda e che il televisore rimane muto. Cosa è successo? **Non c'è la corrente elettrica**. Quello che scoprirete qualche ora dopo è che la rete elettrica nazionale è stata colpita da un attacco cibernetico che ha letteralmente spento il paese. Il telefono intanto si è scaricato e nelle ore successive scoprirete il caos nelle strade, peggio che durante un temporale.

CYBER ATTACCHI ALLE RETI ELETTRICHE

Non è uno scenario improbabile. Negli ultimi mesi le aziende di cyber security **hanno rilevato pattern di attacco alle reti elettriche nazionali di diversi paesi europei**. Alcuni sono andati a vuoto, e non ne abbiamo saputo niente, ma di quest'ultimo ce ne siamo accorti eccome.

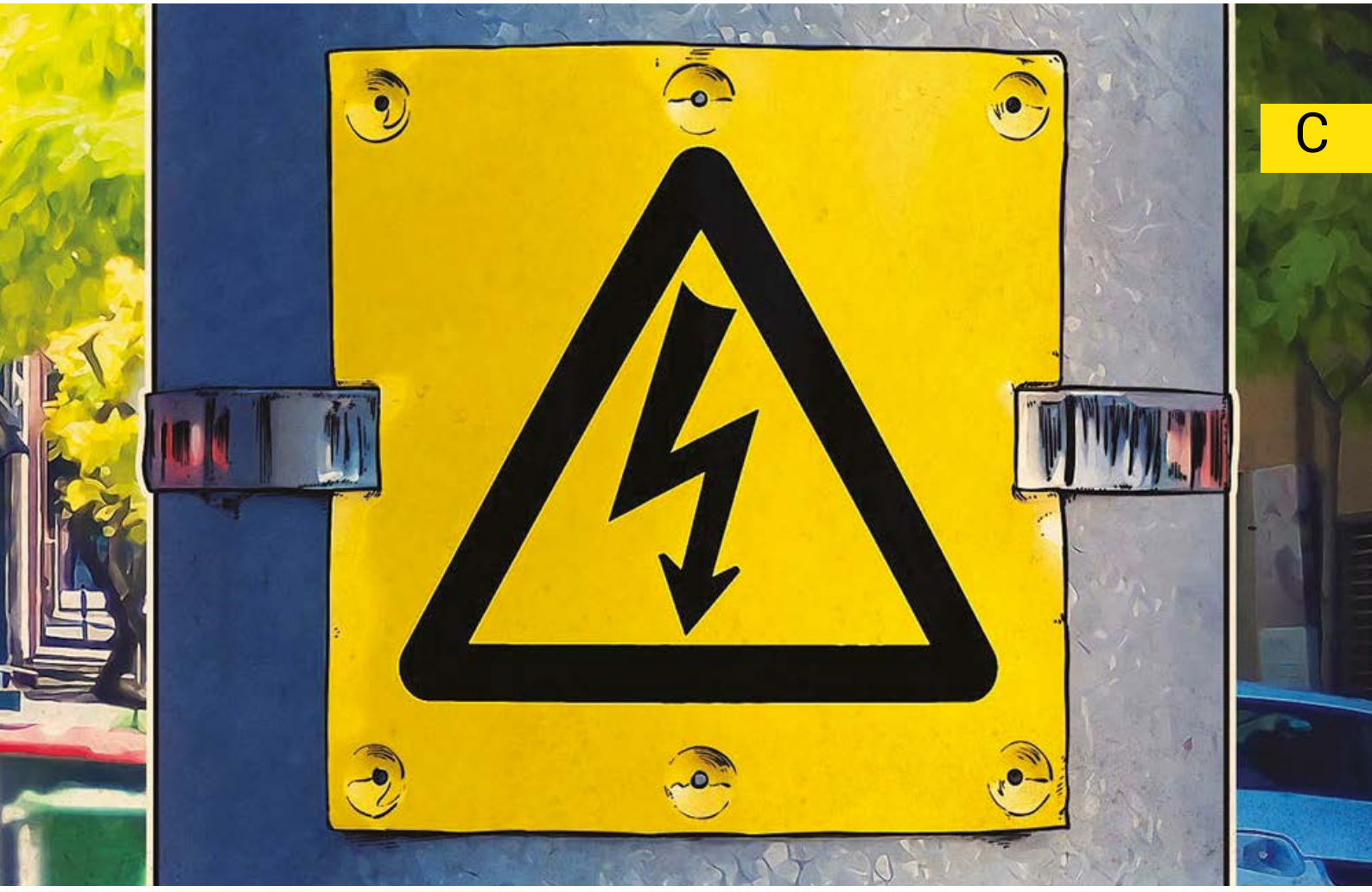
È successo veramente in Canada, Usa, Ucraina ed Estonia. Negli ultimi due casi, a portare questo tipo di attacchi sono stati attori organizzati noti come APT, Advanced Persistent Threat, "minacce informatiche persistenti", che mutuano il loro nome dalla tecnica che utilizzano: si intrufolano nei sistemi informatici del bersaglio, anche per anni, e solo dopo avere acquisito i dati e le informazioni che gli servono sferrano il loro devastante attacco.

Poiché sono gruppi ben organizzati e finanziati, si parla spesso di questi autori come ***Nation state actors***, attori sponsorizzati da stati canaglia, e le loro azioni sembrano avere più a che fare con la cyber-guerra, quella combattuta dagli Stati nel cyberspace, piuttosto che con la quotidianità della nostra vita connessa.

Eppure metodi e strumenti sono gli stessi di gruppi di cybercriminali interessati più al profitto che alla politica. Anzi, spesso gli stessi gruppi si dedicano al cybercrime solo per finanziare lo sviluppo di nuove cyber-armi.

PERCHÉ LA CYBERSECURITY RIGUARDA TUTTI

Ad ogni modo un normale cittadino non dovrebbe preoccuparsene visto che si tratta di cose più grandi lui, e poi, in fondo ci sono gli specialisti che se ne occupano. O no? Il punto è che è spesso il semplice cittadino ad aprire la



porta principale a questi attaccanti, nel suo ruolo di lavoratore, consumatore, volontario o attivista. Forse ha solo fatto l'errore di aprire una email infetta; magari avrà lasciato usare ai bambini il telefono con cui accede alla rete aziendale; dal computer ha cliccato uno strano pop-up; oppure ha usato una password banale per proteggere l'account social che usa per lavorare e chattare. I criminali spesso pescano a casaccio, ma a volte anche questa è una tecnica per colpire proprio te, che fai il giornalista, sei consulente del governo, presiedi una commissione parlamentare o vai a trattare fusioni e acquisizioni per un cliente di alto livello. Potresti anche esserne figlio o figlia. O più semplicemente sei uno che lavora per una grande azienda ma non ti hanno insegnato niente sulla sicurezza informatica.

Ma a un attaccante cyber basta violare l'accesso personale alla rete aziendale per mettere in crisi un'intera organizzazione: **il fattore umano è sempre l'anello debole della cybersecurity**.

Eppure di cybersecurity si parla solo quando succede qualcosa. Sapete del caso **Meltdown** e **Spectre**? L'anno 2018 si è aperto con l'allarme del baco nei processori hardware di Intel e AMD,

vicenda conclusa coi sospetti di insider trading del CEO di Intel che sapendo anzitempo della falla sarebbe riuscito a liberarsi delle azioni aziendali prima che la falla venisse divulgata.

Poi è venuto il caso di Cambridge Analytica che ci ha fatto scoprire che qualcuno era in grado di utilizzare la profilazione di gusti e tendenze personali non per venderci libri, shampoo e viaggi, ma perfino i candidati alle elezioni.

L'anno prima, nel 2017, il ransomware Wannacry, aveva bloccato 300 mila computer in 150 paesi e messo in ginocchio per qualche giorno aziende di logistica come Maersk e l'intera Sanità del Regno Unito. Quello precedente, il 2016, aveva portato alla ribalta delle cronache un **attacco ai server Dyn** che aveva messo in ginocchio Internet nell'intera costa orientale americana rendendo impossibile accedere a Twitter, Amazon, Netflix e il New York Times. Era stato realizzato sfruttando un esercito di 100 mila smart object connessi in rete dalla **botnet Mirai**. Una sua variante era stata poi usata per attaccare la rete Deutsche Telekom impedendo a diversi milioni di tedeschi di usare telefoni e computer.

Potremmo continuare con gli esempi: questi attacchi sono all'ordine del giorno, ma sono solo le cose grosse che vengono raccontate dai telegiornali.

IL PREZZO DELL'INSICUREZZA

Secondo gli ultimi rapporti le aziende e le istituzioni non sono preparate ad affrontare le minacce cibernetiche sotto forma di attacchi DDoS, malware, phishing, zero-day, backdoor e altri "exploit".

L'azienda di antivirus McAfee sostiene che i danni all'economia portati dal cybercrime sono pari a 600 miliardi di dollari annui, lo 0,8% del PIL globale. Altri rapporti parlano di cifre diverse, ma è solo perché hanno un modo diverso di valutare i danni. Oggi, all'inizio dell'anno 2019 si parla addirittura di 6 trilioni di dollari entro il 2021.

Secondo il rapporto dell'associazione italiana dei professionisti informatici del Clusit il crimine informatico in Italia vale almeno 10 miliardi e secondo Fastweb un cittadino italiano è colpito da un attacco informatico ogni cinque minuti. La Confcommercio ha stimato che nel 2017 gli esercizi commerciali italiani abbiano subito danni per 2 miliardi di euro a causa degli attacchi cibernetici.

Quello che va capito è che ogni settore industriale è a rischio e che per questo vanno adottate le necessarie misure di sicurezza. A partire da una consapevolezza: **la sicurezza è un investimento e non è un costo**.

Eppure, secondo un report della Banca d'Italia, nel 2016 per prevenire gli attacchi informatici l'impresa italiana mediana ha speso una somma modesta, pari a 4.530 euro: il 15% della retribuzione annuale lorda di un lavoratore rappresentativo. I valori medi però variano dai 3.120 euro delle piccole imprese ai 19.080 euro di quelle del settore ICT e ai 44.590 euro delle grandi imprese.

Piuttosto poco, non credete?

PREPARARSI A DIFENDERE IL PERIMETRO

Un attacco informatico di successo potrebbe rappresentare il punto di non ritorno per la credibilità di un'azienda o fare così tanti danni da metterla prima in ginocchio e poi fuori dal mercato. La strada non è quella di negare l'attacco avvenuto con successo, ma essere preparati ad affrontarlo, minimizzando i danni. **La questione non è infatti se verremo attaccati**, **ma quando**, e la migliore strategia di difesa è rendere costoso e complesso l'attacco, perché impedirlo non sarà sempre possibile.

Alcune aziende hanno incominciato a capirlo e sanno che la prima linea di difesa rispetto agli attacchi cyber è costituita da personale preparato e da una buona organizzazione in grado di valutare e mettere al sicuro gli asset informatici aziendali, predisporre gli strumenti per una corretta gestione del rischio, e avere un piano di disaster recovery.

Per valutare la **sicurezza informatica è necessario individuare le minacce**, **le vulnerabilità e i rischi associati agli asset** informatici, per proteggerli da possibili perdite o attacchi. La cosiddetta analisi del rischio parte dall'identificazione dei beni da proteggere, per poi valutare le possibili minacce in termini di probabilità, occorrenza, e gravità del danno. In base alla stima del rischio si decide se, come, e quali contromisure di sicurezza adottare (Risk management).

Questi processi sono importanti perché l'obiettivo dell'attaccante non è rappresentato dai sistemi informatici in sé, ma dai dati in essi contenuti. La sicurezza informatica deve quindi preoccuparsi di impedire l'accesso sia agli utenti non autorizzati sia ai soggetti con privilegi limitati, per evitare che i dati appartenenti al sistema informatico vengano copiati, modificati, cancellati o "esfiltrati".

Le violazioni possono essere molteplici: vi possono essere tentativi non autorizzati di accesso a zone riservate, furto di identità digitale o di file riservati, utilizzo di risorse che l'utente non dovrebbe potere utilizzare. La sicurezza informatica si occupa anche di prevenire eventuali situazioni di Denial of Service (DoS) con l'obiettivo di rendere inutilizzabili alcune risorse in modo da danneggiare gli utenti del sistema: clienti, fornitori, utenti.

I danni sono spesso causati accidentalmente dall'utente stesso a causa di una cattiva configurazione dell'hardware e del software, oppure da interruzioni di servizio o guasti imprevisti.

Per evitare gli eventi accidentali non esistono soluzioni uniche: un primo rimedio è il backup del sistema, dei dati e delle applicazioni, procedura cruciale per il cosiddetto "**disaster recovery**".

Gli attacchi intenzionali invece appartengono alla categoria dei furti, dei danneggiamenti, dei sabotaggi, e includono l'accesso non autorizzato a dati, sistemi, informazioni. Sono i più pericolosi. Per questo è importante essere preparati, scambiarsi costantemente informazioni e condividere conoscenze e competenze ai più alti livelli, facendo parlare gli esperti di sicurezza col management aziendale e collaborare con gli enti e le istituzioni preposte alla difesa e alla gestione delle infrastrutture critiche e dei servizi digitali dal cui funzionamento dipende la vita quotidiana.

Nella sicurezza informatica è bene ricordare che sono sempre coinvolti elementi tecnici, organizzativi, giuridici e umani. La direttiva europea sul trattamento dei dati GDPR e quella per la sicurezza delle reti e delle informazioni NIS costituiscono un passo avanti nello sviluppo di questa consapevolezza, nonostante qualche ritardo da parte di aziende e pubbliche amministrazioni.

È ora di occuparsene. Prima che sia troppo tardi.

La sicurezza informatica è come l'acqua, non possiamo farne a meno

C

"La cybersecurity è come l'acqua: non possiamo farne a meno. Mettere il cyberspace in sicurezza dovrebbe essere l'obbiettivo di ogni governo." Per questo motivo, intervenendo al Security analyst summit 2017, Bouki Carmeli, il direttore dell'Agenzia nazionale israeliana di cybersecurity dice che "la condivisione di informazioni è la chiave per approntare le difese più vantaggiose per le nostre democrazie". Difficile dargli torto. Quando parliamo di cyberspace parliamo infatti di tutti i processi e di tutti i dati digitali prodotti nella vita quotidiana, dall'uso delle mappe di Google per trovare il ristorante all'invio delle email con la dichiarazione dei redditi fino al controllo a distanza di dighe, droni, e televisori intelligenti.

RISCHIO APT
(Advanced Persistent Threat)

Tutti d'accordo che oggi ci confrontiamo con uno scenario diverso dal passato. Nel 1996 il 99% degli attacchi era portato da hacktivisti e l'1% era opera di "attori statali". Adesso le percentuali si sono invertite. Gli hacktivisti, cioè hacker con finalità ideali ed etiche, contano quasi niente nello scenario della guerra informatica in corso nel cyberspace, mentre i nation state hackers sono responsabili del 99% degli attacchi più dannosi.

Questi attori, detti anche APT Advanced Persistent Threat, gruppi di hacker esperti e ben finanziati, che provengono dal mondo dell'intelligence, sono usati dagli stati per spiarsi a vicenda, influenzare dinamiche politiche e destabilizzare interi settori produttivi. Pensiamo agli effetti generati dal furto dei dati del comitato elettorale democratico americano noto come **DNCLeaks**, e ai suoi strascichi attuali: i responsabili appartengono proprio a questi gruppi, in particolare all'APT di nome Sofacy.

QUATTRO TIPI DI MINACCE AVANZATE

Secondo Dmitry Bestuzhev, capo del team di ricerca di Kaspersky in America Latina, questi gruppi hanno già adesso la capacità tecnica di attaccare interenazioni con arsenali di sofisticate cyberarmi, "Bisogna perciò anticipare il momento in cui decideranno di operare l'attacco in relazione alla situazione internazionale." "C'è da ricordare - continua Bestuzhev - che esistono quattro grandi famiglie di questi attaccanti: quelli di lingua

russa, sono i meglio finanziati, i cinesi, che hanno la maggiore "forza lavoro", i terzi che parlano inglese e infine quelli di lingua spagnola che provengono con molta probabilità dall'Ecuador."

Per Vitaly Kamluk, senior researcher a Kaspersky, lo scenario peggiore di fronte al quale potremmo trovarci è quello di un attacco massiccio alle borse mondiali, ad esempio con un software capace di bloccare tutti gli scambi in corso per determinare incertezza geopolitica.

Potrebbe essere sotto forma di un **ransomware**, i software che bloccano i computer finché non si paga un riscatto, oppure un codice malevolo, un malware, capace di modificare per pochi minuti la proprietà delle azioni delle maggiori aziende o attaccare e distruggere i computer di 35 mila pc delle stazioni petrolifere della Saudi Aramco, come accaduto col virus Shamoon per tre volte di seguito.

I RISCHI PER LE INFRASTRUTTURE CRITICHE

"Per ora i gruppi con la capacità di fare questo stanno agendo in maniera chirurgica, ma nel futuro potrebbe accadere di tutto", aggiunge Kamluk che lavora a stretto contatto con l'Interpol. Kim Baumgartner, esperto di malware, pure la pensa così: "Questi gruppi stanno testando la loro capacità di interferire col normale funzionamento di Internet su una scala sempre più vasta. Il tracollo dei **Dyn server** a ottobre 2016 attraverso la botnet Mirai è stata una sorta di prova generale."

Proviamo a immaginare cosa succederebbe se qualcuno attaccasse una diga e poi il sistema elettrico di una capitale europea e poi bloccasse i computer delle banche più note. Uno scenario che indurrebbe panico, risposte isteriche delle popolazioni, caduta dei titoli e tutti poi a incolpare il governo che non fa abbastanza per proteggere i propri cittadini e i servizi che usiamo ogni giorno: acqua, elettricità, trasporti.

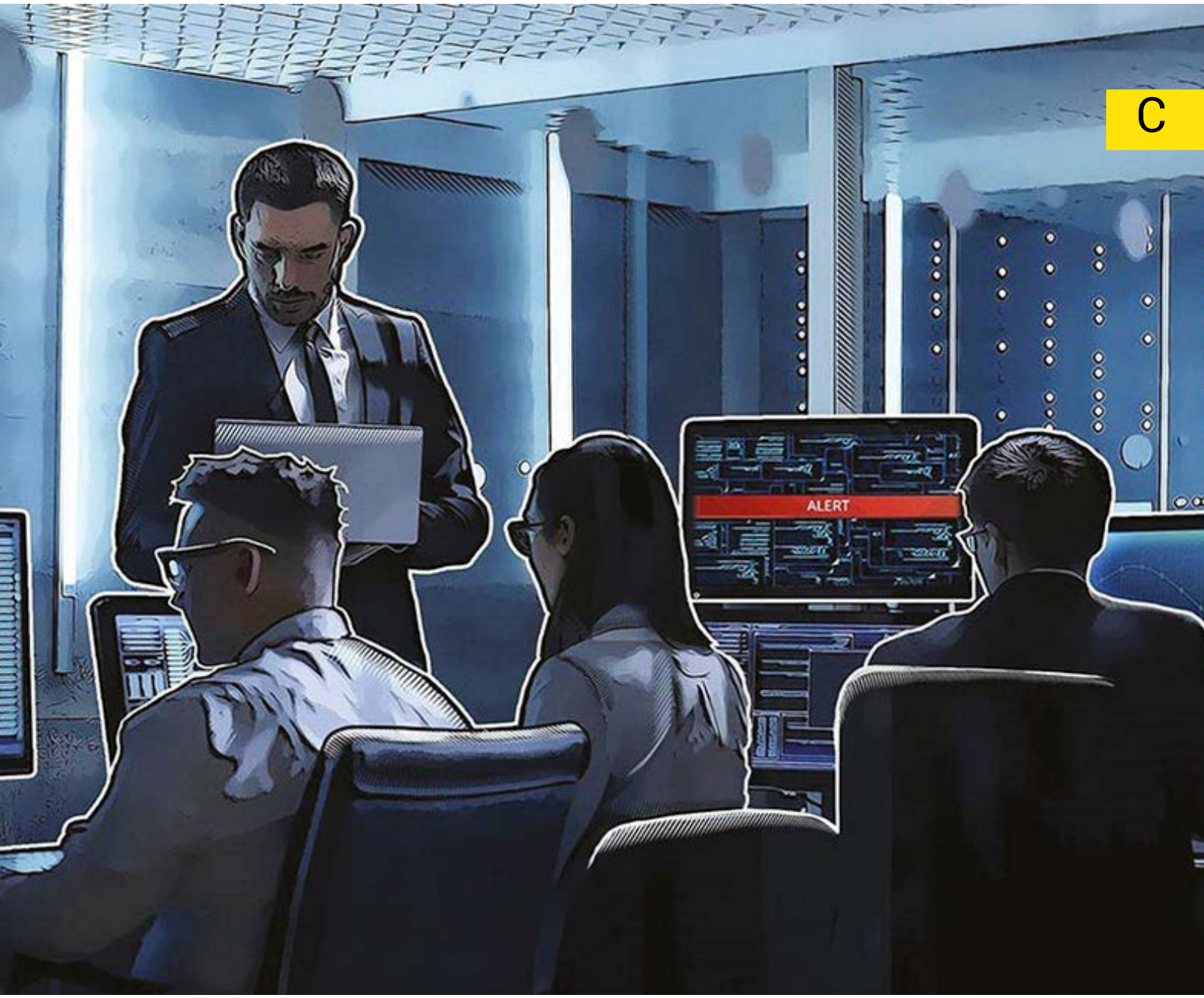
"È già successo nel passato, con la rete elettrica, nel dicembre del 2015 in Estonia e nel dicembre 2016 in Ucraina" ha detto Peter Zinn, consulente della Cybercrime Unit olandese.

I sistemi di controllo industriale sono un altro punto di attacco. Pensate cosa succede se viene bloccata una centrale di trattamento delle acque, per lo smaltimento rifiuti o una diga. Anche questo è già successo negli Usa nel 2013 quando fu attaccato il sistema di controllo della diga di New York.

RISCHIO IOT
(Internet of Things)

Lo scenario è ancora più pericoloso se pensiamo che sono gli oggetti d'uso quotidiano collegati a Internet che ci si potrebbero rivoltare contro: tra poco si stima che saranno 50 miliardi, forse di più. Ognuno di noi entro il 2020 potrebbe averne anche parecchi addosso: smartwatch, telefonini, computer, abiti intelligenti, pacemaker, eccetera.

Se qualcuno è in grado di prendere il controllo di questi dispositivi può farci passare dei guai seri.



Dice Kamluk: “Io temo che le flotte di droni per la consegna delle merci saranno tra i primi bersagli”.

Per questi motivi i ricercatori riuniti consigliano alcuni comportamenti di sicurezza basilari che includono, tra l'altro, l'aggiornamento costante di software e hardware in tutti i settori produttivi, l'uso della crittografia per ogni tipo di transazione e la corretta gestione dei dispositivi mobili e dei dispositivi IoT che dovrebbero essere costruiti in base a specifiche norme di sicurezza. Proprio quello che finora non abbiamo fatto.

CYBERSPIONAGGIO

SPIONI, ATTIVISTI E CRIMINALI INFORMATICI. I RISCHI DEL CYBERSPACE ITALIANO SECONDO I SERVIZI SEGRETI

C come cyber-espionage. Lo spionaggio cibernetico verso cittadini, imprese e istituzioni è, secondo i servizi segreti italiani, la minaccia più pericolosa che oggi corre il nostro "spazio cibernetico". E non è un problema di poco conto. **Il cyberspace, parola coniata dallo scrittore William Gibson, è la somma delle interazioni reali e virtuali che costruiamo ogni giorno coi nostri computer e si configura sempre di più come ambiente di sviluppo, cooperazione e conflitto delle società odierne**.

Secondo la relazione presentata il 20 febbraio 2018 dall'intelligence al premier **Paolo Gentiloni** lo spionaggio digitale, appannaggio di attori strutturati, ha colpito target critici "per sottrarre loro know-how pregiato e informazioni sensibili da impiegare in sede di negoziazione di accordi di natura politico-strategica". Un'attività anche più pericolosa di altre, come le campagne di influenza che, usando tattiche di disinformazione e fake news, "mirano a condizionare l'orientamento e il sentiment delle opinioni pubbliche, specie quando quest'ultime sono chiamate alle urne".

Campagne che "hanno dimostrato di saper sfruttare, con l'impiego di tecniche sofisticate e di ingenti risorse finanziarie, sia gli attributi fondanti delle democrazie liberali, sia le divisioni politiche, economiche e sociali dei contesti d'interesse, con l'obiettivo di introdurre, all'interno degli stessi, elementi di destabilizzazione e di minarne la coesione".

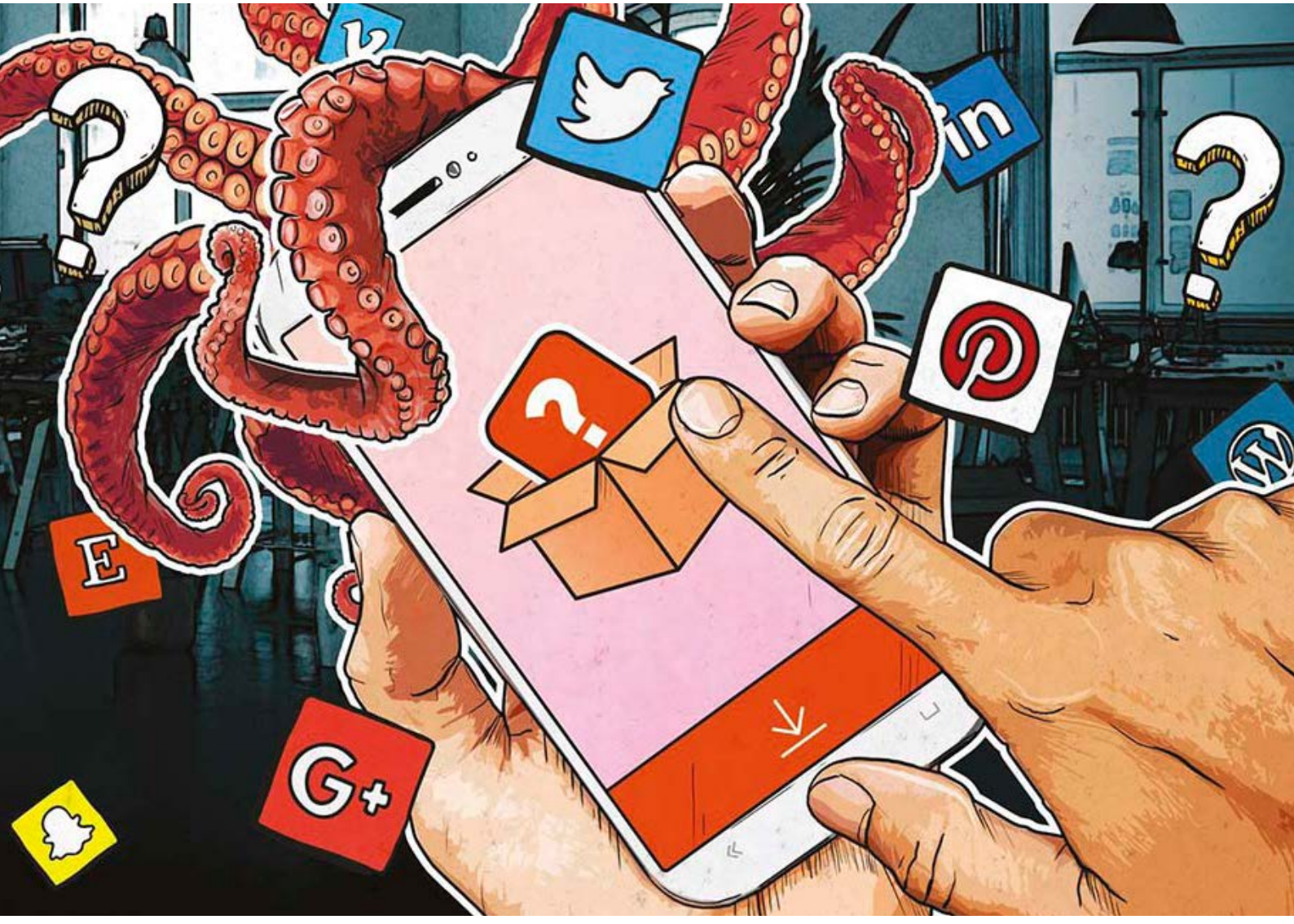
Le campagne di spionaggio digitale sono in gran parte condotte da attori statuali e contano per il 14% degli attacchi cibernetici complessivi. Nel rapporto non viene specificato, ma è facile si tratti di milizie digitali collegate ai servizi segreti e agli eserciti di nazioni "ostili" come la Russia, la Cina e la Corea del Nord. Altri "attori non meglio identificati", sono responsabili del 36% delle incursioni cyber. Si tratta insomma di un miscuglio di cybercriminali e paramilitari informatici difficili da distinguere. I nomi fantasiosi che li identificano, **Fancy Bear**, Cozy Bear, **Lazarous**, Reaper, **APT10**, sono gli stessi degli attacchi ai nostri ministeri, alle ambasciate americane e alle istituzioni europee, ma anche alle banche, alle cryptovalute e ai cittadini occidentali che affollano i social network.

Ma esiste un'altra tipologia di attori ostili secondo gli 007 e cioè, i gruppi di **hacktivisti**, gli hacker-attivisti che usano i computer come strumenti di conflitto nello spazio telematico, e che sarebbero responsabili del 50% di tutti gli attacchi.

Tra questi ci sono anche gruppi di propaganda jihadista.

La riprova della loro esistenza l'abbiamo avuta nei giorni segnati dalle incursioni ai siti della galassia leghista e dall'esposizione di migliaia di indirizzi del Partito Democratico. Nel primo caso il gruppo **LulzSec** ha rivendicato le azioni e sparpagliato sul web 70 mila email di elettori, simpatizzanti e sponsor leghisti, comprese quelle del candidato della destra come governatore della regione Lombardia. Nel secondo caso si è trattato di email, indirizzi e telefoni di sostenitori di Renzi, compreso un suo numero di telefono.

Le tecniche più utilizzate dagli attaccanti secondo l'intelligence italiana spaziano dalle email di phishing, maggiore vettore d'attacco per inoculare malware ed esfiltrare informazioni, alla *impersonation*, ovvero al furto di identità che permette all'attaccante di spacciarsi per qualcun altro e operare al posto suo tramite conti bancari, account aziendali e profili sociali.



CYBERWAR

LA CYBERSPIA CHE SORVEGLIA I PARLAMENTI

C come Cyberwar. La guerra cibernetica usa strumenti capaci di violare e mettere fuori uso sistemi computerizzati per sabotare le comunicazioni degli avversari e danneggiare la loro capacità di attacco e di difesa.

L'evoluzione delle armi cibernetiche però consente anche di fare delle vittime e produrre il caos in territorio nemico quando esse sono usate per interrompere servizi essenziali come il sistema elettrico nazionale di un paese, i suoi trasporti o il funzionamento delle strutture sanitarie.

La cyberwar utilizza un armamentario che consente forme di spionaggio digitale e online basate su software malevoli come i malware che, usati per operazioni mirate di *phishing* (pesca dei dati) possono essere usati con lo scopo di esfiltrare informazioni utili per gli attaccanti. Ed è il motivo per cui gli Stati, per non sporcarsi direttamente le mani, finanziano i cosiddetti APT, gli *Advanced Persistent Threats*, gruppi di mercenari digitali spesso provenienti dai ranghi dell'esercito o dell'intelligence. Hanno nomi fantasiosi come Bluronoff, Gaza Cyber Gang, Desert Falcon, Fancy Bear, eccetera, e spesso una lingua in comune: coreano, arabo, russo, cinese, inglese.

La "cyberguerra fredda" oggi sta diventando calda, proprio come i rapporti diplomatici fra i nuovi blocchi contrapposti in Siria: gli Usa e l'Europa da una parte e la Russia, la Turchia e l'Iran dall'altra.

C'è però una buona notizia. Mentre i governi stentano a collaborare per fronteggiare una cyberguerra mondiale a pezzi, alla RSA Conference 2018 di San Francisco Microsoft, Cisco, Avast, Facebook e altre trenta aziende hanno firmato il **Cybersecurity Tech Accord**, che ha lo scopo di migliorare la sicurezza online e la resilienza delle reti in tutto il mondo. In base all'accordo i membri si impegnano a proteggere tutti gli utenti e i clienti ovunque si trovino, siano essi individui, organizzazioni o stati, mentre si impegnano a non supportare i governi nel lancio di cyber attacchi contro gli innocenti.

C

D

DARK WEB

CHE COS'È IL DARK WEB E PERCHÉ NON CI FA PAURA

Il web non è solo quello che conosciamo. Quando parliamo di "web" parliamo di "siti web" e quindi del sito web del nostro giornale preferito, di quello dell'università, del motore di ricerca preimpostato dal nostro browser, del blog di un attore o di un social network. Ma questo è soltanto il **surface web**, il web di superficie. È la punta dell'iceberg di tutti questi servizi che emergendo da Internet, chiamiamo WEB.

D

Perciò qui va fatta una precisione: **il web non è Internet**. Il web è la rappresentazione grafica, multimediale, interattiva e ipertestuale dei dati raggiungibili attraverso Internet. Internet è invece un insieme di protocolli di comunicazione che regolano lo scambio di dati tra computer diversi con caratteristiche diverse attraverso mezzi di comunicazione differenti: le onde radio, la linea telefonica, i cavi ottici.

Il web o World Wide Web o WWW, è stato implementato da sir Tim Berners Lee e Robert Cailleau tra il 1990 e il 1991 e i primi due siti web sono stati creati al Cern di Ginevra, dove Lee lavorava, e a Stanford per lo Slac, il Linear Accellerator Center. La sua caratteristica principale è che consente il collegamento tra risorse diverse – contenuti, siti e servizi – attraverso gli **hyperlink**, i collegamenti ipertestuali, e si basa su di un'architettura client-server dove il client, ad esempio il nostro browser, richiede a un server di trasferirgli le informazioni cercate che vengono visualizzate in un certo modo grazie a uno specifico linguaggio di marcatura, l'HTML, l'HyperText Markup Language.

Internet invece è una piattaforma di comunicazione basata sui protocolli TCP/IP sviluppati tra il 1972 e il 1973 da Vinton Cerf e Robert "Bob" Kahn, inizialmente usati da alcune istituzioni accademiche collegate da reti dedicate per scambiarsi informazioni scientifiche. Su Internet viaggiano molti altri servizi, ma nel tempo il web, per la sua facilità d'uso, si è imposto come il servizio più diffuso.

Bene. Se immaginiamo il web come la punta di un iceberg che emerge dall'oceano di Internet, sotto il pelo dell'acqua potremo trovarne una parte più grande: il Deep Web o "web profondo". Per convenzione si definisce **Deep Web** la parte del web non indicizzata dai motori di ricerca. I motori di ricerca infatti funzionano raccogliendo i link relativi alle risorse accessibili in rete, ma è possibile che non siano in grado di ispezionarli tutti per limiti propri dei software che li raccolgono o perché l'owner della "risorsa web" non vuole che accada, usando il comando robots.txt. Questo vale per molti siti o per singole porzioni di essi contraddistinte da una URI (Uniform Resource Identifier), che può rimandare al singolo articolo di un quotidiano oppure a un intero sito web. Quindi chi la cerca dovrà conoscere in anticipo il suo "indirizzo", la URL, perché il motore di ricerca non può indicizzarlo e farcelo trovare. Questo è il caso di molti servizi web a pagamento nel Deep Web: biblioteche online, database, e siti che aprono e chiudono nel volgere di una notte.

All'interno del Deep Web possiamo individuarne una parte ancora più complessa da esplorare che è chiamata **Dark Web**, il "web oscuro". Il nome viene dalle **darknet**, le reti all'epoca separate da Darpanet, antesignana di Internet. Il Dark web è quella parte di Internet che non viene indicizzata dai motori di ricerca e in aggiunta necessita di software speciali per accedervi. TOR (https://www.torproject.org/) è uno di questi.

TOR, The Onion Router, è un software sviluppato negli anni '90 da Paul Syverson e Micheal Reed per proteggere le comunicazioni dei servizi segreti americani. Rilasciato in codice libero nel 2004 costituì nel 2006 la base di avvio per The Tor project, un progetto per lo sviluppo della comunicazione anonima su Internet a disposizione di tutti. Tor

oggi indica una rete di server, detti anche nodi Tor o Tor relay, gestiti in parte dalla fondazione omonima, in parte da volontari e fanno una cosa molto semplice: cifrano la comunicazione tra il client e il server sovrapponendo successivi strati di crittografia ai dati di trasmissione che vengono fatti transitare attraverso questi computer intermedi, gli Onion router per l'appunto. Il nome 'onion', cipolla, è stato usato per indicare proprio questa caratteristica stratificazione che ha lo scopo di anonimizzare le comunicazioni. E infatti è molto usato da giornalisti, **whistleblower** e dissidenti che non possono esprimersi liberamente e sono a rischio di rappresaglia da parte di criminali e stati autoritari.

Grazie agli strumenti che TOR offre si possono ricercare siti del web di superficie oppure i siti del network TOR, quelli descritti dall'estensione .onion, e si possono spedire email, chattare e creare i cosiddetti “hidden service” cioè server per il web publishing o l'instant messagging.

La rete costituita dai siti che finiscono con l'estensione .onion è essa stessa una porzione del Dark Web: anonima, cifrata e non cercabile con i tradizionali motori di ricerca.

Chiaro fin qui? Bene.

E adesso liberiamoci di false convinzioni: nel Surface Web, nel Deep Web e nel Dark Web possiamo trovare contenuti di ogni tipo: legali e illegali, moralmente accettabili o immorali, utili e inutili, pericolosi o sicuri.

La differenza vera quindi fra i tre livelli dell'iceberg quindi non riguarda tanto i contenuti, ma il modo in cui vi si accede. Essendo il dark web più difficile da accedere per gli utenti meno esperti ed essendo protetto da login e password e crittografia è più facile che dei malintenzionati possano costruire lì trappole per allocchi, mettere in vetrina merci illegali, scambiarsi documenti e informazioni segrete o riservate. Ma allo stesso tempo i siti del Dark Web sono quelli usati dagli attivisti di regimi autoritari per passarsi informazioni, organizzare riunioni di sette religiose pacifiche ma fuorilegge nel loro paese, vendere e comprare bitcoin.

No, il dark web non è oscuro perché è cattivo, è solo più difficile da trovare, esattamente quello che accade quando si cerca qualcosa nel fondo dell'oceano.

DATA BREACH

IL TUO DNA IN VENDITA AL MERCATO NERO

Oggi con soli 69 euro si può risalire alla propria origine etnica e trovare dei parenti che non sappiamo di avere grazie al test del DNA.

Almeno questo è quello che dice di poter fare il sito MyHeritage, in grado perfino di darci informazioni sui nostri antenati cercandone il nome in un gigantesco database di documenti storici e giornali d'epoca. Il nostro albero genealogico invece può essere ricostruito gratis online avvisandoci via email delle corrispondenze trovate di volta in volta.

Il sito MyHeritage è stato hackerato. Nel giugno 2018 gli indirizzi email e le password del suo database clienti, circa 92 milioni di account, registrati fino al 26 ottobre 2017, sono stati trovati su un server privato.

In gergo tecnico si chiama *databreach*. Un *databreach* è la violazione di una base di dati che contiene informazioni di ogni tipo.

Le cronache giornalistiche riportano che la maggior parte dei database dei servizi gratuiti che usiamo sono stati violati. Famoso è stato il caso del sito di *Ashley Madison* per gli incontri tra chi vuole concedersi una scappatella amorosa, quello di *Snapchat* dove un finto capo d'azienda ha chiesto e ottenuto dai suoi dipendenti tutti i dati anagrafici e di sapere perfino quanto prendevano di stipendio. Poi ci sono i noti *databreach* di *Yahoo!*, *Hotmail*, *Adobe*, *Dropbox*, *Twitter*, eccetera.

In Italia a fare rumore sono state le violazioni di database bancari come quelli di Intesa e Unipol e quella relativa a 400 mila profili di risparmiatori Unicredit che avevano chiesto un piccolo prestito.

Il *databreach* dipende da una cattiva configurazione di hardware e software, dalla mancata manutenzione, da un errore umano. Ogni *databreach* ha sempre una cosa in comune: chi lo subisce, lo nega.

Ma questa strategia dello struzzo non è l'unica possibile. Infatti l'amministratore delegato di MyHeritage, saputo della violazione, ha subito spiegato agli utenti quello che avevano scoperto, quali misure stavano adottando per affrontare il problema e come proteggevano i dati dei clienti suggerendo un immediato cambiamento delle password per evitare che qualche malintenzionato potesse sfruttare l'accaduto. Dall'analisi del DNA si può infatti risalire a "difetti genetici" e alla predisposizione verso specifiche malattie e farti rifiutare l'assicurazione o peggio.

In genere accade il contrario, chi è colpito da un *databreach* fa tre cose: nega che ciò comporti una crisi reputazionale dell'azienda, la rappresenta minimizzandola, la esorcizza.

Questo viene fatto utilizzando diverse retoriche comunicative e alla fine si traduce in un arroccamento sulle proprie posizioni.

E tuttavia questo accade perché non si è mai preparati alla crisi che viene da un danno di reputazione, soprattutto quando il comportamento dei responsabili è considerato doloso oppure omissivo.

Ma il danno raddoppia se non si comunica con onestà e sincerità l'accaduto.

Con l'entrata in vigore dal 25 maggio 2018 del Regolamento europeo sulla protezione dei dati, il GDPR, le aziende sono obbligate a notificare il *databreach* entro 72 ore, e a tutti gli interessati se la violazione mette a rischio dei diritti fondamentali.

Ma l'unico vero antidoto è essere preparati a gestire la crisi, perché la domanda non è se accadrà, ma quando.

DATA BREACH COMPILATION

1 MILIARDO E 400 MILIONI DI EMAIL E PASSWORD DIFFUSE IN RETE: IL COLLEZIONISTA CHIEDE UNA DONAZIONE IN BITCOIN

L'hanno chiamata Breach Compilation: raccoglie 252 leak precedenti ed è aggiornata alla fine di novembre 2017. La password usata per posta e social da 9 milioni di account è sempre la stessa: "password".

Un miliardo e 400 milioni di nomi, email e password in chiaro. Tutto in un unico database messo a disposizione in un forum del deep web. È il più grande leak di dati personali della storia di Internet.

A "scoprirlo" per primi gli spagnoli di **4iq**, una società di analisi del rischio cibernetico operante anche in California.

Il leak era menzionato su Reddit da un utente col nome di 'tomasvanagas' che ne forniva il link (torrent) per recuperarlo, indicando poi la possibilità di fare una donazione in bitcoin a chiunque lo trovasse utile.

Il database, ancora in circolazione, sarebbe la somma di altri leak come Antipublic ed Exploit.in ma è aggiornato a fine novembre 2017 con milioni di nuovi indirizzi e password in chiaro. Il database contiene moltissimi indirizzi della Rai, la televisione pubblica, dell'Università Sapienza di Roma, del Ministero della Difesa, del quotidiano La Repubblica, di banche, ministeri e pubbliche amministrazioni con le password, sempre le stesse, per accedere a social e posta elettronica. Molti di questi indirizzi sono vecchi e le organizzazioni colpite come la Rai hanno da tempo avvertito i propri dipendenti di resettare email e password.

Ma a rendere prezioso questo leak cumulativo non è tanto la mole dei dati, quanto la loro organizzazione in 1900 diversi file e la presenza nel pacchetto di uno script di ricerca in grado di restituire in pochi secondi i dati associati ad una email o username.

LA PASSWORD PIÙ USATA È SEMPRE LA STESSA: 123456

Dall'analisi sul dump compiuta dalla Cyber Division di Var Group, Yarix, nota società di sicurezza italiana, emerge, grazie anche alla collaborazione di alcuni utenti coinvolti, la presenza nel leak di password vecchie o mai impiegate dagli utenti, utili però a creare uno storico delle password impiegate da cui trarre indicazioni preziose per la realizzazione di attacchi di tipo password, basati cioè sugli schemi di generazione della password che gli utenti usano ripetere.

Essendo i dati associati alla stessa username provenienti da vecchi

D

databreach, di Yahoo, Linkedin, Twitter, YouPorn, Myspace, eccetera, è chiaro che il fenomeno del riuso della stessa password per servizi web diversi è assai frequente.

E in effetti a leggere il database si nota che 9 **milioni di account usano la stessa password "123456"**, oltre un milione "password" e trecentomila le parole "monkey e "dragon".

Inoltre il 14% di queste accoppiate username/password non erano mai state decifrate nei precedenti leak e questo potrebbe significare che "il collezionista" che le ha raccolte ha trovato il modo per portarle in chiaro.

DAL CRIME-AS-A-SERVICE AL CRIME-FOR-SHARING

A questo punto la domanda è: chi ha interesse a diffondere tutti questi dati? Si potrebbe pensare a una questione economica: è la prima volta che chi mette in giro un leak di questo tipo chiede una "donazione" da destinare al suo portafoglio bitcoin. Ma secondo gli esperti il motivo potrebbe essere un altro. Secondo Pierluigi Paganini, Chief Technology Officer di CSE Cybsec: "La quasi totalità dei dati è già reperibile online e quindi il loro valore è pressoché nullo per la vendita nell'ecosistema criminale. Il "collezionista" di tali dati potrebbe essere interessato a interferire con la vendita di concorrenti o rovinare la reputazione a servizi che offrono l'accesso a pagamento dei dati." Una sorta di concorrenza sleale, insomma. Ma c'è un'ipotesi peggiore. Nell'underground ci sono gruppi di esperti e criminali informatici uniti da una fede o una ideologia comune che collaborano e condividono quello che apprendono gli uni dagli altri. Secondo l'esperto "In alcuni ecosistemi specifici non è raro trovare attori che condividono informazioni e strumenti a titolo gratuito. Questo accade in collettività in cui altre motivazioni fanno da collante, ad esempio nell'ecosistema criminale Medio Orientale-Africano la componente religiosa agevola questi fenomeni di condivisione." E continua: "In altri casi ciò accade quando uno specifico attore cerca rapidamente di acquisire notorietà ed aumentare la propria reputazione in specifiche comunità."

Ma l'ipotesi del depistaggio vale sempre: continuando ad arricchire il database diventa sempre più difficile seguire le tracce di chi ha realizzato le violazioni, i databreach, aiutandolo a mimetizzarsi nel web profondo.

D

DATA MINING

QUANDO NON PAGHI QUALCOSA IL PRODOTTO SEI TU. COME FUNZIONA IL DATA-MINING POLITICO-ELETTORALE

D come data mining. Per Wikipedia il data mining "è l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un'informazione o di una conoscenza a partire da grandi quantità di dati". Il processo avviene attraverso metodi automatici o semi-automatici. E aggiunge che con data mining "si intende anche l'utilizzo scientifico, industriale o operativo di questa informazione."

Nell'epoca di Facebook e dei Big Data, il data mining è cruciale per individuare la propensione all'acquisto dei consumatori, ma anche per definirne il profilo politico, sessuale, religioso. Perfino il rischio sanitario o creditizio. I dati, provenienti dalle fonti più disparate, come l'uso di app, computer e smartphone, carta degli sconti, tessere elettroniche e per la pay-tv, vengono raccolti in grandi database e,

incrociati fra di loro, possono essere usati per costruire profili singoli e aggregati, individuali e collettivi di consumatori, lavoratori o elettori. Questi dati, shackerati con i metodi della statistica e delle scienze sociali grazie a sistemi automatizzati, definiscono la nostra data-immagine. Che è il profilo digitale della nostra persona, quello che ci precede quando andiamo a chiedere un mutuo in banca o cerchiamo di contrattare con l'assicurazione. Però, mentre prima questi dati andavano raccolti e con fatica da fonti diverse, oggi basta usare quelli accumulati da social network come Facebook, Instagram, Twitter e altri per fare una profilazione completa degli individui ed essere in grado di offrire al consumatore quello che è più propenso a desiderare.

Per capire come questo accade, la società Data X, di base a New York, ha creato un add-on, un'estensione per Mozilla Firefox o Chrome, che si chiama Data Selfie (www.dataselfie.it). Scaricata e installata sul nostro computer, fino al primo luglio 2018 permetteva di vedere quanto tempo passiamo a leggere i post dei nostri amici, quanti like produciamo, quanti link clicchiamo e che cosa digitiamo o cancelliamo dai post di Facebook. Dopo avere interagito un poco sulla piattaforma avremmo avuto un quadro preciso e dettagliato del tipo di dati che sono in possesso di Facebook e capire perché sia al centro dello scandalo di Cambridge Analytica accusata di aver contribuito a manipolare il voto della Brexit e quello per Trump, proprio grazie a un uso spregiudicato dei dati degli utenti di Zuckerberg.

Ma Data Selfie faceva di più: usando degli algoritmi matematici impilati in un software dall'Università di Cambridge era in grado **di generare un profilo psicologico dettagliato** dell'utente legato a età, genere, preferenze sessuali, intelligenza, ma anche soddisfazione per la vita, orientamento politico e religioso. Per farlo usava anche alcuni strumenti di IBM Watson, l'intelligenza artificiale di IBM, che è in grado di identificare emozioni, propensioni sociali e stili di vita dei soggetti di cui elabora i dati.

È proprio quello che faceva Cambridge Analytica a giudicare dal rapporto creato da Michael Phillips, suo impiegato esperto di Big Data: con poche righe di codice reso pubblico sul sito GitHub, Phillips era in grado di geolocalizzare gli elettori e poi attraverso gli hashtag usati, i link cliccati e le conversazioni intrattenute, ricavarne il "sentiment", cioè l'inclinazione emotiva e cognitiva verso temi elettorali per poi cucirgli addosso un messaggio politico che non erano in grado di rifiutare.

DELETE FACEBOOK

A Marzo 2019 l'ennesima notizia di una falla di sicurezza su Facebook ha messo in allarme i suoi utilizzatori: il social network ha comunicato che le password di centinaia di milioni di utenti, archiviate per anni in semplici file di testo, quindi senza alcun adeguato sistema di sicurezza, erano visibili agli impiegati di Mark Zuckerberg.

Nonostante le rassicurazioni provenienti dal quartiere generale di Facebook è possibile che non sarà l'ultima volta che dovremo affrontare una tale minaccia per la nostra privacy. Cosa possiamo fare?

Paul Ducklin, senior technologist di Sophos, azienda di sicurezza informatica, ha provato allora a rispondere alle domande che tutti noi ci facciamo di fronte a questi avvenimenti.

Devo cambiare la mia password di Facebook?

Perché no? È importante sottolineare la possibilità che nessuna delle password sia caduta nelle mani di hacker (*quelli malevoli, ndr.*). Tuttavia, se questi dati sensibili sono finiti nelle mani sbagliate allora è scontato che diversi account verranno sfruttati per scopi malvagi. Cambiare una password richiede poco tempo e può evitare guai peggiori quindi noi di Sophos consigliamo di modificare immediatamente le proprie credenziali di accesso.

Devo abilitare l'autentificazione a due fattori?

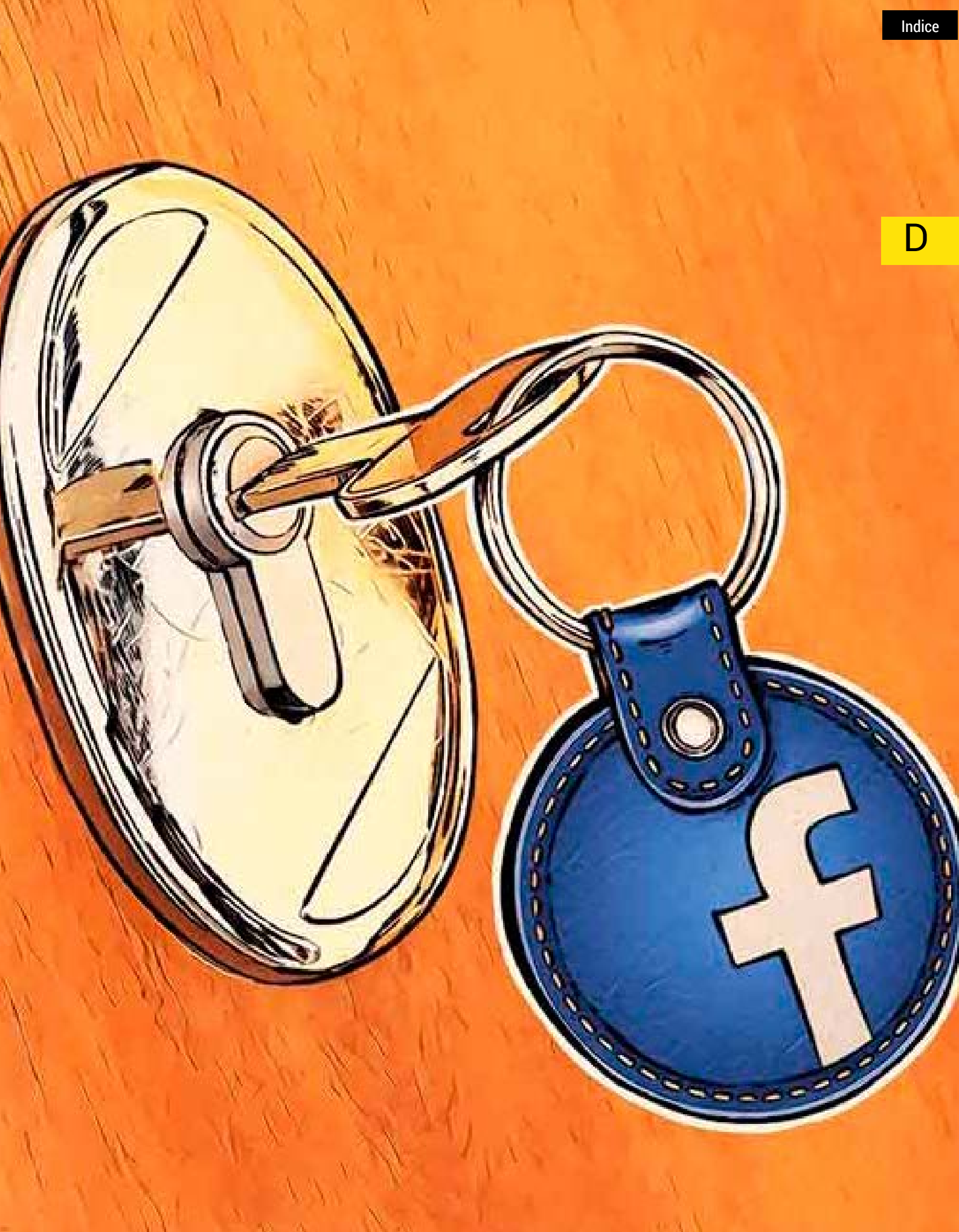
È assolutamente consigliato attivare l'autentificazione a due fattori (2FA) su qualsiasi account, non solo quello di Facebook. La password non è sufficiente a proteggersi dagli hacker! Qualora l'utente non voglia condividere il proprio numero di cellulare con Facebook, è possibile attivare l'autenticazione a due fattori tramite l'app, lo smartphone genererà in automatico un codice ogni volta che si effettuerà l'accesso al social network.

Devo chiudere il mio account Facebook?

Considerato che le password memorizzate erroneamente non erano facilmente accessibili in un database, o deliberatamente memorizzate per un uso quotidiano da parte dei dipendenti di Facebook, non pensiamo che questa violazione da sola sia un motivo sufficiente per chiudere l'account.

D'altra parte, potrebbe essere l'ennesima conferma dei dubbi sulla corretta gestione della privacy da parte di Facebook. La scelta se cancellare o meno il proprio account è quindi una decisione assolutamente personale, qualora l'utente sia in dubbio segnaliamo che gli esperti di Sophos hanno deciso di non chiudere i propri account.

D



DATING ONLINE

MARITI GELOSI, UTENTI FASULLI E CYBERTRUFFATORI: LE FAKE NEWS INVADONO IL MONDO DEL DATING ONLINE

La rete, si sa, è piena di imbroglioni. E di ladri, come nelle piazze delle città turistiche, nei paesini e nei ministeri. Ma ci sono degli imbroglioni che fanno più male degli altri perché sono quelli che riescono a truffarti manipolando i tuoi sentimenti. E dove si nascondono? Ovunque, anche nei siti di dating online, proprio quelli dove si cerca un po' di compagnia e magari l'anima gemella.

Una ricerca di Kaspersky Lab Italia ha evidenziato che la metà degli utenti italiani (il 44%) di questi servizi imbroglia su nome, sesso, età, e altro ancora, e che spesso si iscrive a questi servizi per

truffare gli altri o per controllare mariti e mogli in cerca d'evasione. Il risultato è che un utente italiano su dieci (10%) è stato ingannato da foto fasulle, uno su sette (15%) da false aspettative dichiarate nel profilo e il 7% da bugie sulla situazione sentimentale del partner desiderato.

L'indagine, che è stata condotta da B2B International e Kaspersky Lab ad agosto 2017 su un campione di 21.081 utenti dai **16 anni in su** in ben 32 Paesi, Italia compresa, ha però evidenziato che **un gran numero di questi profili, molti dei quali rivelatasi fasulli, hanno cercato di iniettare malware, ransomware e software spia nei dispositivi degli utenti con cui venivano in contatto**.

Insomma, non bastavano le richieste d'amicizia fasulle di ragazze procaci su Facebook, la maggior parte delle quali ignare che la loro foto reale sia usata da software automatici e chatbot per irretire persone in cerca di nuove conoscenze, adesso anche i siti come Tinder, Badoo e Ok Cupid sono diventati un'enorme rete da pesca per truffatori e malintenzionati.

Insomma, dopo la notizia che milioni di utenti di Pornhub, il più grande sito per adulti al mondo, sono stati bersagliati da un attacco di malvertising, pubblicità "pirata" che installava codice malevolo sui loro computer, veniamo a scoprire che anche i siti e le app di dating online sono pieni di cybertruffatori.

Secondo la ricerca di Kaspersky i finti utenti sono specializzati nella raccolta e profilazione dei dati personali degli utenti reali e ci sono perfino dei cybertruffatori che cercando di estorcere dati finanziari dalle potenziali vittime.

Prima forse potevamo passare sopra al comportamento dei quegli utenti che barano su età e aspetto per apparire migliori di quello che sono, ma oggi non ci si può più permettere di dare confidenza agli sconosciuti che fanno domande troppo personali.

In realtà in tutti i siti di dating online c'è un vademecum di buon comportamento e spesso anche un assistente virtuale che dispensa **consigli su come comportarsi dal primo contatto al primo appuntamento**: mai dare il proprio indirizzo di casa, mai farsi accompagnare in automobile al primo appuntamento, avvertire almeno una persona amica che si va a incontrare una sconosciuta o uno sconosciuto, e così via. E soprattutto, **mai e poi mai inviare foto e video erotici a persone da poco conosciute**: possono essere usati per il revenge porn, l'odiosa pratica di rendere pubblici chat e foto intime per vendicarsi di un rifiuto, fare un dispetto, ricattarne la vittima.

Ricordiamoci inoltre che grazie al social engineering è possibile costruire un profilo di qualsiasi utente del web a partire da singoli dati anche non correlati fra di loro e acquisiti da fonti diverse: il tipo di lavoro, la località di residenza, i bar frequentati, il cognome, l'indirizzo email, per risalire ai servizi web che usa, attaccarne le password e rubargli l'identità.

Inoltre la ricerca deve farci pensare che i dati della nostra vita online vanno protetti meglio di quanto facciamo visto che quando la profilazione per i siti e delle app di dating online viene certificata da piattaforme come Facebook dobbiamo stare attenti due volte.

Nei social infatti siamo inclini a condividere molte cose della nostra vita privata: sogni, desideri e debolezze, e colpevolmente lasciamo in bella vista email di lavoro, telefono e foto di famiglia diventando l'esca perfetta per i malintenzionati.

DIGITAL LIBRARY

"IO LEGGO DIGITALE", L'INIZIATIVA ITALIANA PER LEGGERE DA CASA GRATIS

I libri sono un tappeto volante per l'immaginazione. E al tempo della quarantena che obbliga metà della popolazione mondiale a ridurre le occasioni di incontro, i libri rappresentano un'ancora di salvataggio dalla solitudine e dall'ansia della pandemia. Per questo, in attesa che librerie, biblioteche e caffè letterari tornino ad essere luoghi di ritrovo, si moltiplicano le iniziative per leggere online gratis.

L'Internet Archive ha annunciato l'avvio della National Emergency Library, iniziativa per il prestito gratuito di 1 milione e mezzo di libri senza liste d'attesa affinché tutti gli studenti possano accedere immediatamente ai materiali di cui hanno bisogno. L'Internet Archive, una sorta di magazzino della cultura digitale che conserva senza fini di lucro siti Internet e altri manufatti digitali, lo ha deciso in seguito alla decisione del governo americano di chiudere le biblioteche fino alla fine dell'emergenza Coronavirus. Ma lo stesso cominciano a fare altri produttori di contenuti, da Apple ad Amazon. E lo stesso hanno fatto l'Unesco ed altre istituzioni internazionali.

Ma anche l'Italia si muove. Grazie a un accordo tra l'**Istituto centrale per il catalogo unico delle biblioteche italiane e per le informazioni bibliografiche** e DM Cultura, oltre 2 milioni di risorse digitali sono oggi accessibili a tutto il pubblico, non solo italiano, che può scaricarle gratuitamente e senza obbligo di iscrizione attraverso il portale ioleggodigitale.it, realizzato con la collaborazione di Amazon Web Services. Con quasi 2.200.000 di titoli a scelta tra ebook, audiolibri, musica, film, corsi di lingua, lezioni, e perfino videogiochi, la piattaforma di "digital lending" mette a disposizione di scuole, biblioteche e privati quello che serve per stare a casa e continuare a leggere, insegnare ed imparare.

L'iniziativa si chiama "Uniti per ripartire", e grazie a Rete Indaco consente a chiunque di scaricare testi di ogni tipo, dalla Divina Commedia di Dante alle poesie di Ugo Foscolo passando per i sonetti di William Shakespeare in inglese e poi Dickens, Hemingway, Bronte, e altri mostri sacri della letteratura. Il sito è semplice e pulito e funziona come Google: si inserisce il nome del testo che si cerca e l'algoritmo lo trova per noi. I generi vanno dalla letteratura alla cucina passando per la musica e la poesia. Un mare di letture.

Così, se ad esempio si cerca "Divina Commedia" si possono consultare pagine e pagine di risorse correlate all'opera principale: commentari, grafiche, testi esplicativi e biografie dell'autore collezionate e rilanciate da

D


PDF
RAR
JPG
DOC
AVI

tutti i portali che le offrono in lettura. Un unico punto di approdo per i testi messi a disposizione in maniera gratuita, dai musei alle associazioni culturali per colmare una piccola parte del digital divide nazionale. I libri arrivano da varie fonti, ad esempio da editori come Rizzoli, dalla Biblioteca centrale di Firenze o da LiberLiber ma ci sono anche i contenuti di Cinecittà, la città del cinema di Roma.

Anche l'**Unesco** permette di **accedere liberamente** alla sua biblioteca digitale mondiale. Si tratta della **World Digital Library** che riunisce **migliaia di documenti storici**, come libri, manoscritti, mappe, riviste, giornali, fotografie, audio e filmati. Una biblioteca che comprende **193 paesi** e ha l'obbiettivo di promuovere la comprensione internazionale e interculturale, nonché di ridurre il divario digitale. L'annuncio è stato da su Twitter con gli hashtag #QuarantineLife #StaySafe #Covid19.

Con **oltre 20mila documenti**, anche rari, si può curiosare tra le pagine del diario di Napoleone durante la campagna in Egitto, o approfondire un tema di interesse culturale. Dai testi antichi fino a quelli moderni, dai documenti storici del Novecento fino ad una quantità sterminata di libri disponibili "Con la World Digital Library è possibile svolgere un autentico viaggio nel tempo" immergendosi nelle ere storiche che hanno segnato l'evoluzione culturale dell'umanità. Il materiale disponibile è **in versione originale e sette lingue di ricerca** - inglese, arabo, cinese, spagnolo, francese, portoghese e russo-, che raccontano i gioielli culturali di tutte le biblioteche del pianeta.

Ma questa dei libri gratis in digitale è una storia che viene da lontano. All'inizio c'era il Progetto Gutenberg, dal nome dell'inventore della stampa a caratteri mobili, per l'accesso gratuito a 60 mila libri di pubblico dominio o di cui è scaduto il diritto d'autore, poi è arrivato il Progetto Manuzio dell'associazione no profit italiana Liber Liber. L'iniziativa di Marco Calvo, Gino Roncaglia e altri, dal 1993 ha accumulato nel suo sito 4000 libri, 8000 brani musicali e centinaia di audiolibri, un'autentica Biblioteca virtuale, che mette gratuitamente a disposizione dei lettori il *download* dei testi in tutti i formati che possiamo immaginare: Pdf, Doc, Audiolibri, e-Pub o pagine web. Per ciascun autore, ***liberliber*** offre anche un profilo biografico e l'elenco delle opere disponibili per il download grazie a un data-base interrogabile con brevi informazioni e l'incipit dell'opera. Ma se oggi abbiamo dei libri da leggere gratis online o dopo averli scaricati, è solo perché hanno cominciato tanti anni fa e forse lo Stato dovrebbe finanziare iniziative come questa.

Anche dal sito delle Biblioteche di Roma e di altre città è possibile accedere a un vasto numero di opere e in questi giorni vanno forte le iniziative di lettura collettiva in videoconferenza.

Tra le iniziative commerciali invece, Mondadori Store offre una vasta raccolta di libri e la sua iniziativa di testi gratuiti per l'insegnamento si trova su Mondadori education. Fra tante offerte la parte del leone continua però a farla Google che ha digitalizzato una cospicua parte del patrimonio librario digitale mondiale facendo arrabbiare e non poco gli editori per le perdite economiche che avrebbe prodotto. Per accederlo comunque basta andare alla sezione Libri dell'omonimo motore di ricerca e digitare quello che si cerca e, come per magia, probabilmente comparirà.

DOXXING

L'INSOSTENIBILE LEGGEREZZA DELLE UNIVERSITÀ

In meno di due ore un gruppo di hacker etici ha dimostrato di poter superare le difese di 50 università inglesi senza troppa fatica.

Il «penetration test», voluto nel 2019 dall'agenzia britannica che si occupa di fornire servizi Internet a università e centri di ricerca nel Regno unito, ha evidenziato in questo modo l'estrema facilità di accedere a dati personali, sistemi finanziari e reti di ricerca. In molti casi i white hat hacker sono stati capaci di ottenere le informazioni su studenti e impiegati con un successo del 100% usando tecniche di «spear phishing», la pesca mirata di dati personali che usa email personalizzate e siti clone che chiedono di reimpostare login e password per appropriarsi delle credenziali utente.

Ma perché l'hanno fatto? Università e centri di ricerca britannici hanno subito solo l'anno scorso più di mille tentativi di attacco orientato al furto di dati o all'interruzione dei servizi.

Il motivo è facile da capire: le università hanno molte informazioni sensibili sugli studenti ma spesso non hanno definito misure minime di sicurezza informatica, inoltre detengono grandi quantità di dati provenienti dalla ricerca in settori avanzati, sfornano brevetti, sviluppano prodotti commerciali ad alta tecnologia, partecipano a progetti internazionali come partner di industrie ed istituzioni.

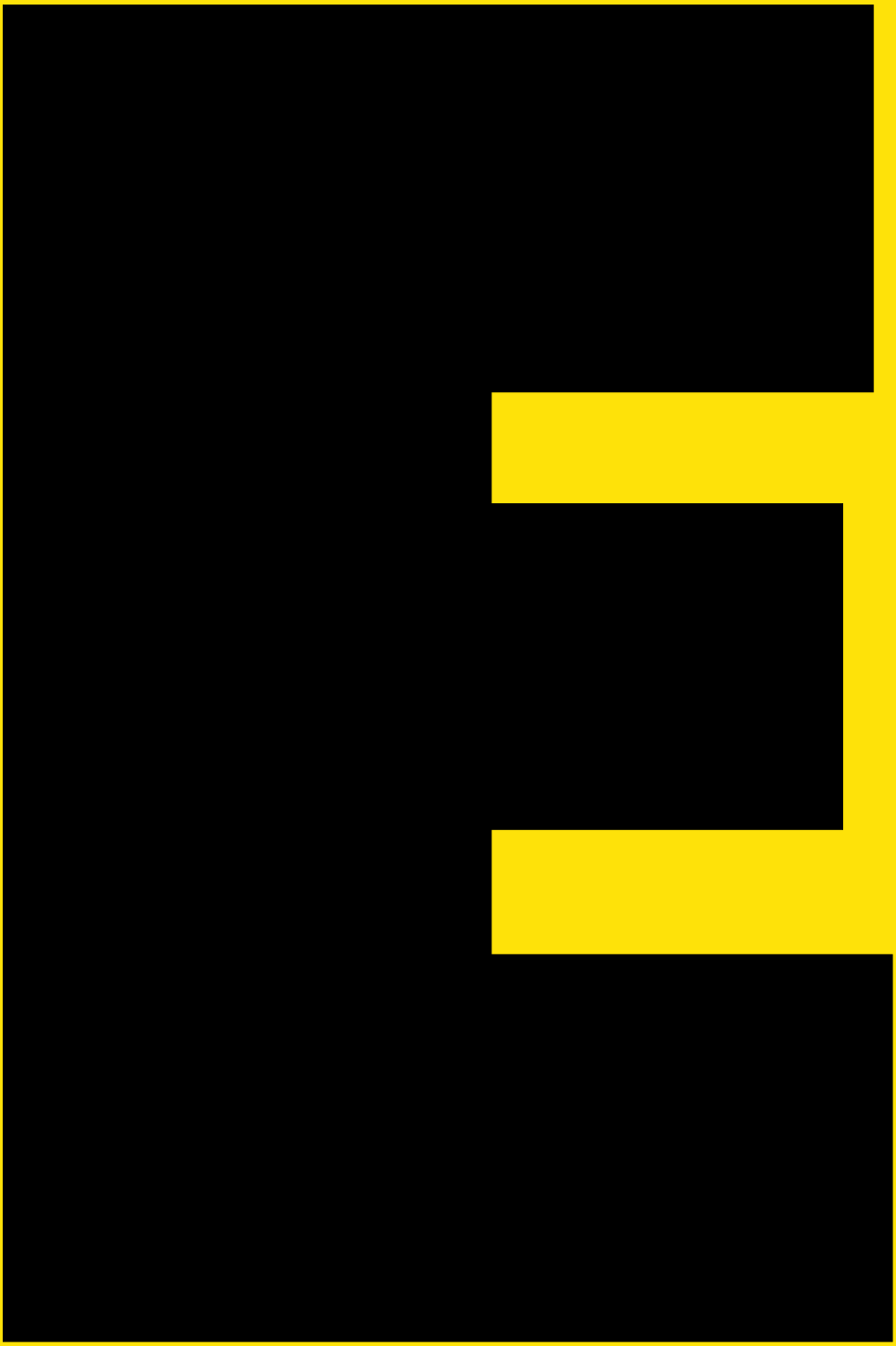
L'ultimo test è avvenuto lo stesso giorno in cui il Georgia Institute of Technology, di Atlanta, negli Usa, nota come Georgia Tech – una delle università più prestigiose al mondo –, ha confermato l'esposizione delle informazioni personali di oltre un milione di studenti e professori causata dalla violazione di una semplice web app universitaria.

L'accesso non autorizzato è avvenuto per la prima volta il 14 dicembre 2018, ma non si sa per quanto tempo l'intrusore abbia avuto accesso a nomi, indirizzi, numeri della previdenza sociale, data di nascita degli studenti, attuali, precedenti e futuri, che hanno chiesto di iscriversi presso l'università.

Tutto questo è accaduto ripetutamente su una scala ridotta anche in Italia per opera degli Anonymous che – a loro dire – volevano sensibilizzare i giovani sul tema della sicurezza informatica, sia per opera di soggetti ancora sconosciuti.

Questi ultimi sono entrati in possesso dei dati del personale universitario e degli iscritti di varie università italiane attraverso il databreach di 763 milioni di account di verifications.io, un servizio di validazione delle email da usare a fini di marketing commerciale e politico. Il team di cybersecurity dell'Università Sapienza di Roma, tra i meglio preparati contro queste evenienze, ne ha dato notizia a febbraio 2019. Ad essere coinvolti sono stati 1675 indirizzi della Sapienza che hanno usato i servizi MyHeritage, MyFitnessPal e ShareThis.

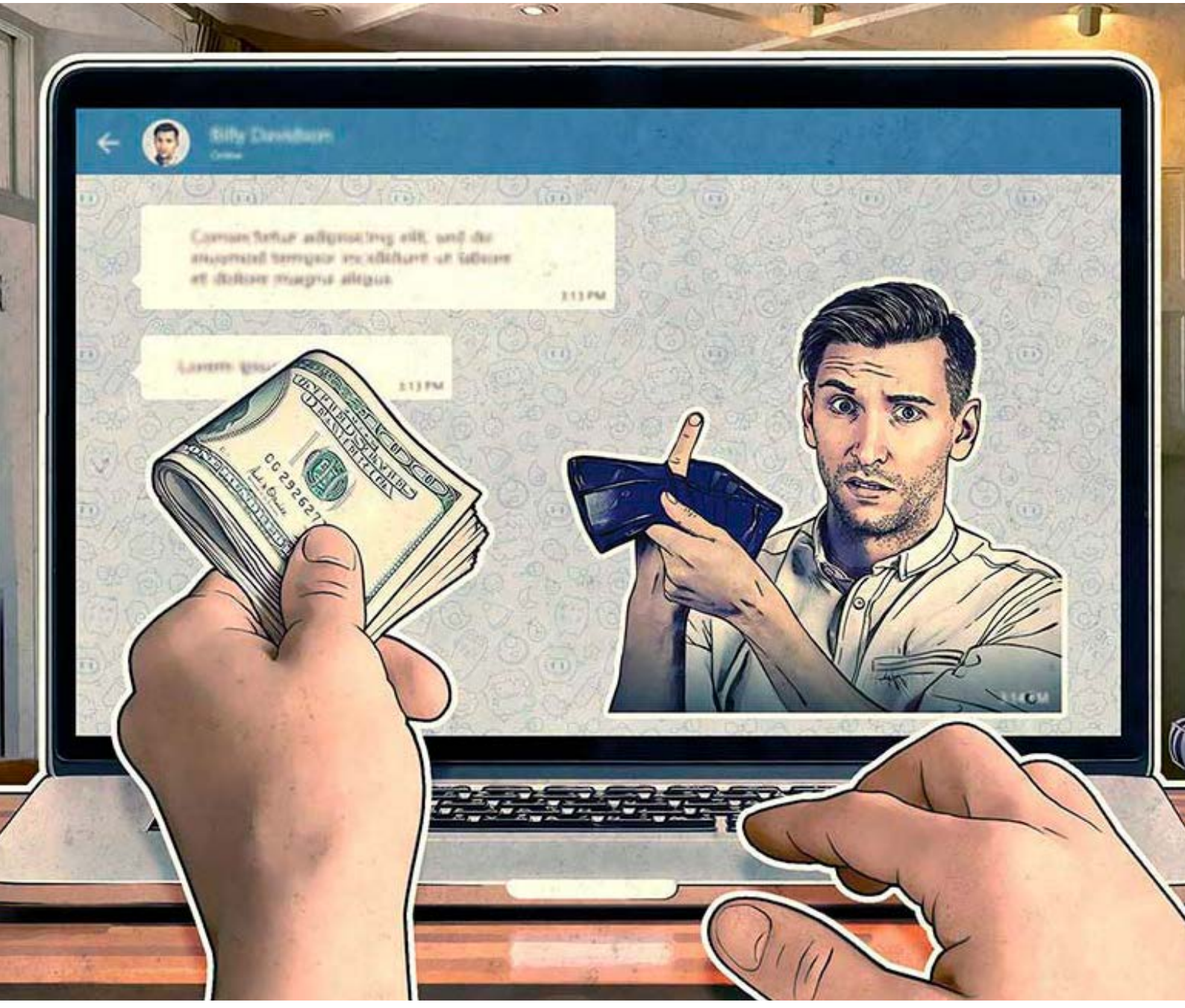
Bucare un account universitario è insomma più facile che attaccare le infrastrutture di aziende come Eni o Leonardo, ma in genere l'attività degli hacker non si ferma qui. L'esfiltrazione di dati sensibili di studenti e ric ercatori universitari viene spesso integrata con un'attività di **doxxing**, la pratica cioè di costruire dei «dossier» relativamente ai soggetti di interesse. Il doxxing, come spiegato in un bell'articolo di Fastweb digital magazine – uno dei migliori in Italia – non è solo il risultato di un'attività di stalking online che punta a rovinare la reputazione delle vittime, ma è uno strumento di spionaggio che usa tecniche avanzate che vanno dallo sniffing delle connessioni alla geolocalizzazione. È così che la mancata protezione del nostro account si trasforma per l'attaccante nel trampolino di lancio dentro la vita di qualcun altro.



106 EXPLOIT

EXPLOIT

LA GUERRA FREDDA DI INTERNET E LE NUOVE CYBER-ARMI



L'Exploit è un'azione che mira a prendere il controllo di una risorsa informatica o a danneggiarla. Il termine indica anche un pezzo di software, una stringa di comandi, un pezzo di codice che, sfruttando una vulnerabilità o un bug presente nel sistema attaccato, punta ad acquisirne il controllo.

Gli Exploit sono le armi della guerra cibernetica che si combatte tra le grandi potenze nel cyberspazio. Un terreno nel quale il conflitto diplomatico e militare diventa conflitto digitale e la cyberwar globale uno scenario plausibile. Con effetti potenzialmente devastanti sulla vita quotidiana: dalla sicurezza degli hub aeroportuali alle vie di trasporto, fino agli elettrodotti. Con un attacco diffuso alla rete elettrica non funzionerebbero illuminazione, ospedali e fabbriche, con effetti di panico e di blocco delle attività produttive capaci anche di influenzare la risposta a un attacco militare tradizionale.

È già successo il 23 dicembre 2015 in Ucraina ad opera del gruppo **Sandworm**. Per questo l'escalation della tensione tra le potenze mondiali si sta configurando come una situazione da guerra fredda. La cyberwar è insomma diventata un'opzione. Ma non da ieri.

Consapevoli della rilevanza del dominio del cyberspace, gli stati nazionali hanno creato strutture e dipartimenti ad hoc, dal Cybercommand negli Usa all'Enisa europea, mentre Russia, Regno Unito e Cina hanno inglobato la guerra cibernetica nella loro intelligence militare. Le aziende nazionali dal canto loro hanno intensificato la produzione di pallottole digitali, cyberkatiuscia e cannoni informatici.

La stessa Nato a Varsavia ha dichiarato il cyberspazio come il quinto dominio sottoposto alla sua protezione militare, dopo la terra, il mare, l'aria e le stelle. Era il 7 luglio 2016.

LA GUERRA IBRIDA

Distinta dalla guerra di propaganda o dell'informazione, la guerra cibernetica usa strumenti capaci di violare e mettere fuori uso sistemi computerizzati ma si aggiunge alle tradizionali forme di spionaggio digitale e online. Le armi della cyberwar servono a conquistare un vantaggio tattico e strategico nei confronti degli avversari, sottraendo, manipolando e inquinando le loro informazioni, oppure possono essere finalizzate al sabotaggio delle infrastrutture critiche. In quest'ultimo caso sono strumenti che servono a distruggere economie ed eserciti, ma anche a demoralizzare e creare paura nelle popolazioni.

Usati sia per lo spionaggio che per il sabotaggio e gli attacchi veri e propri, si tratta per lo più di **software exploits**, cioè strumenti software progettati per sfruttare falle di funzionamento di strumenti e sistemi digitali. Come gli **zero-days**, codici software in grado di sfruttare vulnerabilità del software non ancora scoperte dagli stessi produttori del software, oppure come i **virus trojan**, capaci di sottrarre dati e manipolare o distruggere le informazioni contenute in server, database, e computer online. E poi ci sono gli strumenti in grado di prendere il controllo di pc e smartphone o di bloccarne il funzionamento, come i **RAT** (Remote Access Tools) e i **REC** (Remote

Execution Code). Una tecnica d'attacco molto diffusa è anche la **SQL injection** che colpisce le applicazioni di gestione dei dati per diventare amministratori di server altrui. Insomma, si tratta di software che modificano il comportamento di hardware e software.

Armi usate in aggiunta agli attacchi "brute force" per violare le password, codici crittografici e Vpn a protezione dei sistemi informatici e usarli a proprio vantaggio. Esiste un'intera industria che produce questo cyber-armamentario. Insieme a tecnologie di sorveglianza come gli **spyware**, per intercettare le conversazioni di capi di Stato e presidenti di banche, oppure quelle per il **riconoscimento facciale** di agenti nemici, fino ai software che traducono conversazioni di oppositori scesi in piazza in testi scritti. Sono le famose **tecnologie dual-use**, che possono essere usate per fini legittimi di polizia, o per reprimere pacifiche manifestazioni di protesta e perseguire i dissidenti in Paesi autoritari.

LE ARMI

Una volta iniettate nei computer avversari, queste cyber-armi possono essere rivolte contro gli stessi utilizzatori o target sensibili, ad esempio per attacchi **DDoS** (Distributed Denial of Service attacks) che rendono inservibili server e siti web occupandone le risorse e rendendoli irraggiungibili via internet. Questi attacchi possono essere operati attraverso le botnet, reti di computer zombie controllabili a distanza da utenti illegittimi a dispetto degli ignari proprietari infettati dai virus oppure reti di computer create appositamente per questo scopo e che richiedendo massicce risorse computazionali e pertanto finanziate a livello statale.

La **sottrazione di dati** invece utilizza più facilmente le tecniche di **phishing** e **spear-phishing** oppure i **watering holes** (gli abbeveratoi avvelenati): si riceve un'email da conoscenti ignari (spear phishing) che invita a cliccare sopra un link o un pdf che installa il virus che prende il controllo del proprio computer o del proprio telefonino: da lì tutte le opzioni sono possibili, spionaggio o sabotaggio. Sono **tecniche di ingegneria sociale** (social engineering), un metodo che permette di risalire all'identità, alle risorse e ai conti online della vittima, per sostituirsi ad essa aggiungendo di volta in volta un pezzo di informazione al profilo che l'attaccante vuole utilizzare per poter operare al posto suo. Pensiamo a cosa succederebbe se un malvivente prendesse il controllo della nostra casella di posta: nelle email troverà comunicazioni relative alla carta di credito o alla compilazione online delle tasse e potrà riconfigurare l'accesso ai servizi online semplicemente resettando la password di software ed app che usiamo per fare di tutto: dalla prenotazione dei viaggi fino ai pagamenti digitali. E se accadesse a un individuo che prende decisioni importanti, ad esempio un alto funzionario, un parlamentare o un generale?

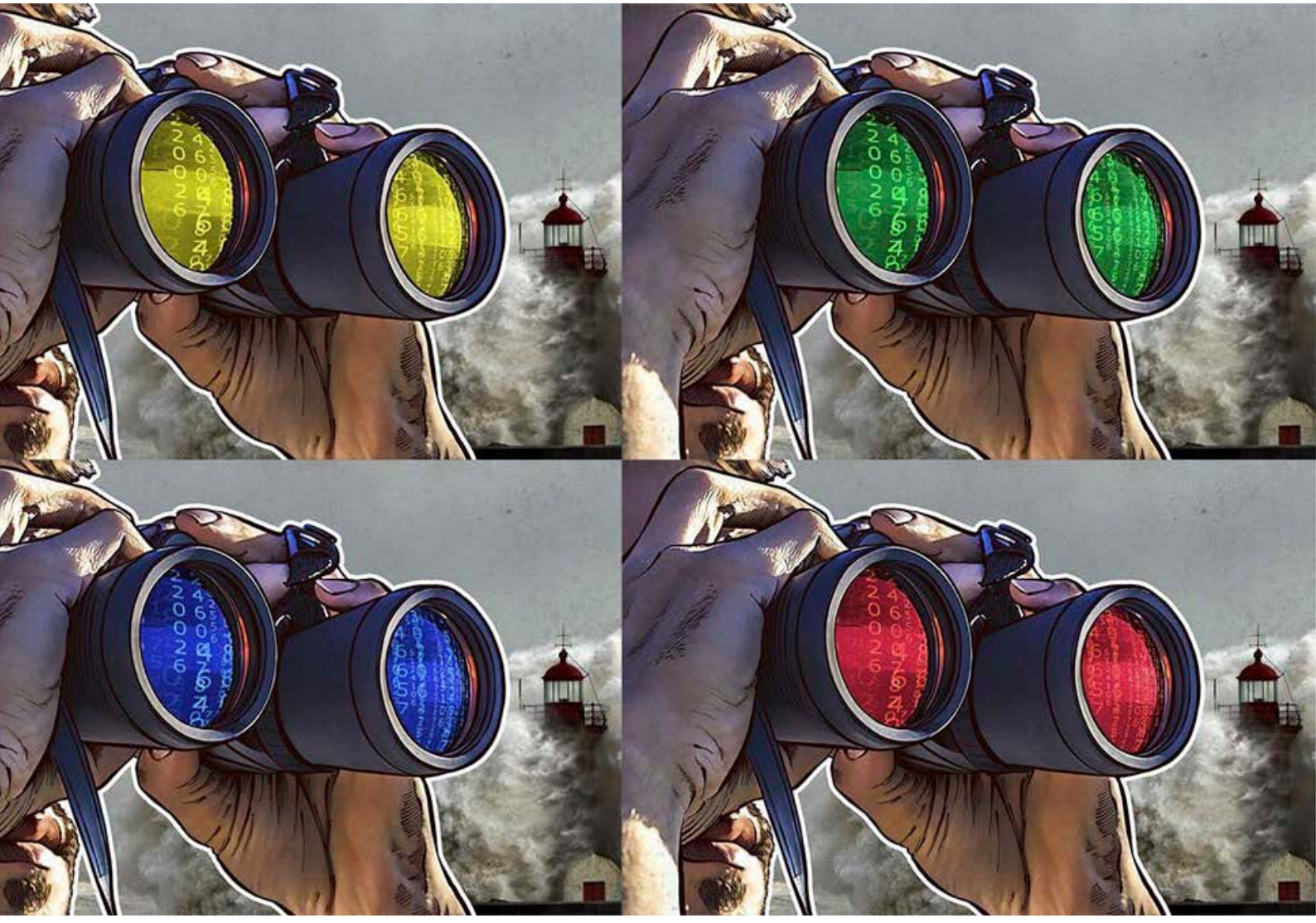
LO SCENARIO

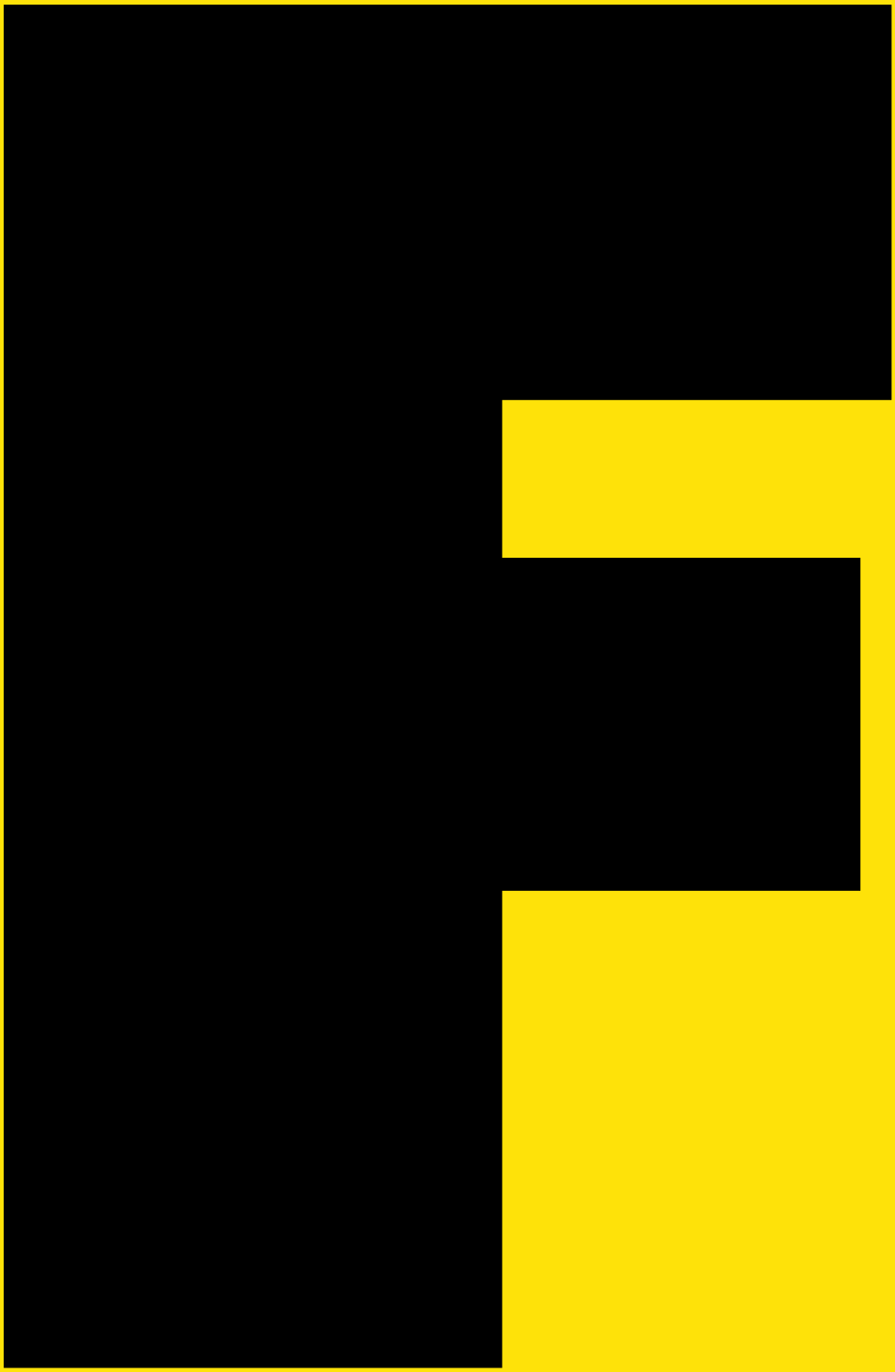
Insomma, siamo di fronte a una **cyberwarfare** di tipo ibrido che usa sia

la propaganda mediatica di tv e social network che squadre di mercenari informatici e paramilitari cibernetici. E tutto questo in un contesto dove le azioni sono coperte ed è sempre difficile stabilire chi è stato.

Per questo nell'escalation cibernetica tra Usa e Russia si è tanto parlato del coinvolgimento del governo russo negli attacchi al Comitato elettorale democratico e al sistema di voto elettronico di 25 stati americani e perfino nel "Rapporto Mueller" sulle collusioni fra il presidente Donald Trump e il presidente Vladimir Putin.

E





FAKE NEWS
COME RICONOSCERLE

"Gli hacker russi attaccano la rete elettrica americana", ma è una **fake news**, **una "notizia falsa"**. A poche ore dall'articolo del **Washington Post** che parla dell'attacco – citando fonti interne di una compagnia elettrica locale situata a Burlington, nel Vermont -, la rete si popola di articoli che raccontano dettagliatamente che "Hacker russi sono penetrati in una rete elettrica del Vermont.", e che "La scoperta è stata possibile grazie alla condivisione, da parte delle autorità federali con le utility nazionali, dei codici associati alle operazioni degli hacker russi, in questo caso 'Grizzly Steppe'."

Ma la notizia è falsa. **Gli hacker non hanno penetrato la rete**, invece si è scoperto che un singolo computer laptop, disconnesso dalla rete, era stato infettato da un malware simile a quello usato in altri attacchi informatici attribuiti ad hacker russi. Così succede che a qualche ora di distanza dalla pubblicazione dell'articolo il Washington Post corregge il tiro e in testa all'articolo dice di aver dato una notizia sbagliata.

Tim Berners Lee è intervenuto tra i primi contro le fake-news. Nell'appello ripreso dalla BBC, rivolto ai ricercatori e alle aziende sul web, lo scienziato che ha inventato gli ipertesti elettronici su cui si basa il web ha un obiettivo dichiarato: **frenare l'abuso della diffusione di dati personali in nome di una male interpretata "libertà di parola"; denunciare l'uso di algoritmi che promuovono la diffusione di informazioni inattendibili e svelare forme occulte di pubblicità politica**.

Allo stesso tempo Berners Lee si oppone a ogni tentativo di lasciare a governi, authority e piattaforme aziendali il potere di "stabilire quali notizie siano vere e quali no".

Berners Lee non è l'unico a scagliarsi contro le fake news. Facebook qualche mese or sono aveva deciso di segnalare con la dicitura "disputed", "contestato", le notizie false che circolano in rete marcandole con una sorta di "bollino rosso", che avrebbero dovuto accompagnare le notizie che team di giornalisti professionisti definiscono false dopo adeguata indagine.

La prima fake news contestata da Snopes.com e PolitiFact, che collaborano con Facebook per il fact checking delle news online sulla piattaforma di Zuckerberg aveva riguardato Donald Trump il cui telefono avrebbe favorito fughe di notizie dalla Casa Bianca a causa della scarsa sicurezza del suo sistema operativo Android.

Che il sistema operativo Android montato su alcune famiglie di cellulari non sia a prova di delinquente è stato dimostrato diverse volte, ma non è questa la fake news, quanto piuttosto la "notizia" che è dal telefono di The Donald che sarebbero

trapelate informazioni imbarazzanti per il vulcanico inquilino della Casa Bianca. Il contenuto "contestato" era comparso sul Seattle Tribune, sito che secondo i segugi delle due testate non è neanche un quotidiano online ma una vera e propria "fabbrica" di notizie false che si autodefinisce blog di satira online.

CONTRO BUFALE E NEWS ACCHIAPPACLICK

È proprio a questo genere di iniziative che si è rivolto Tim Berners Lee, cioè alle news acchiappa-click, ma anche alla pretesa dei giganti del web di indicare come bufale quelle che altro non sono che parodie, interventi satirici, goliardate, scritte con un obiettivo e un linguaggio che hanno un senso all'interno di certi contesti e certe culture.

Le fake news hanno successo a causa di una serie di fattori che incidono direttamente sui destinatari della comunicazione: overload informativo, bias cognitivi, guerra dell'attenzione, personalizzazione estrema dell'informazione, omofilia, filter-bubble, confirmation bias, eccetera. Ne parliamo successivamente in questo libro.

Ma allora come si fa a capire se una notizia è una bufala? In genere le fake news sono notizie verosimili, talvolta romanzate e condite da particolari curiosi o singolari. Qui è la nostra dotazione culturale e la conoscenza dei fatti che devono venirci in aiuto. Ma ci sono anche altri modi per stabilire quando ci troviamo di fronte a una fake news. E fanno tutti perno sulla media literacy di chi le news le legge o le ascolta.

TITOLI SENSAZIONALISTICI. Ad esempio, nelle fake news sul web il titolo è sempre di carattere sensazionalistico per indurre una reazione emotiva, suscitare curiosità e farsi cliccare: è la tecnica dell'acchiappa-click (o click-baiting) e serve ad aumentare le visite sul proprio sito le cui finalità economiche sono evidenti nell'uso smodato di banner commerciali. Da un punto di vista formale i titoli sono "**sparati**", cioè ricchi di aggettivi che suscitano o dovrebbero suscitare immediato interesse, del tipo: "Incredibile, ecco tutta la verità sul fatto più…".

ITALIANO SGANGHERATO. Queste "news" sono assai brevi e scritte in un italiano spesso sgangherato, con una punteggiatura incerta e termini vernacolari (dialettali), segni grafici che precedono il titolo come "+++ Attenzione! +++" che mimano i lanci d'agenzia, e un invito all'azione del tipo "+++ DIFFONDETE! È IMPORTANTE +++", ma altrettanto spesso sono notizie "strane", mai sentite o inverosimili.

INDIRIZZI WEB FASULLI. Da un punto di vista tecnico, un modo per capire che si tratta di una fake news è l'indirizzo web che ospita la notizia: il suo dominio è spesso la parodia di una testata giornalistica riconosciuta come affidabile oppure ne contiene una parte: "Ilfattoquotidaino", "il menzognero", eccetera. Ma si tratta spesso di siti di **phishing**. Quindi la prima regola per scremare le news vere da quelle fasulle è fare una ricerca online per vedere se già ne parlano siti affidabili, registrati al tribunale della stampa, se gli articoli sono firmati e da chi.

FACT CHECKING. In genere una ricerca sull'autore ci fa capire se vale la pena darsi tanto cruccio. Inoltre è sempre utile

fare una verifica sui siti anti-bufale che hanno già fatto per noi questo lavoro di debunking o fact checking.

CANCELLARE LE FAKE NEWS DAL NEWSFEED. Se si sente puzza di bruciato a questo punto, su social come Facebook è possibile dis-iscriversi dai gruppi che propagano fake news e nascondere i post delle persone che diffondono le notizie false, premere sull'icona a forma di apice presente in alto a destra sul post e scegliere l'opzione "Non seguire più" seguito dal nome della persona o della pagina.

Intanto possiamo seguire il suggerimento del quotidiano americano Washington Post che propone di accantonare il termine fake news e di tornare tutti a parlare di bugie.


F

Bufale online: censura e stuoli di poliziotti non bastano a sconfiggere la tendenza delle persone a credere ai propri pregiudizi

F come fake news. Purtroppo è vero che attraverso le notizie false è possibile manipolare l'opinione pubblica e orientare le decisioni di governi, delegittimare personalità e Istituzioni e sovvertire il dibattito scientifico. Le notizie false sono sempre esistite, ma oggi hanno un alleato potente: la viralità del web che ne facilita la propagazione a colpi di click.

E non possono essere contrastate a partire da chi sul modello di business della selezione e personalizzazione delle notizie online ha costruito vere e proprie community di consumatori, come Facebook, ad esempio. Il funzionamento dei suoi algoritmi predittivi è tale che se hai cliccato una certa notizia sarai pronto a cliccarne una simile, anche fasulla, e per questo ce la presenteranno prima di altre.

I giornali e i media in generale non sono immuni dalle fake news. I giornali accusati dal presidente americano Donald Trump di diffondere notizie false su di lui hanno potuto esibire gli anticorpi alla loro diffusione riconoscendo da una parte la pubblicazione di notizie imprecise o non adeguatamente verificate, dall'altra hanno potuto certificare la bulimica produzione trumpiana di notizie fasulle, centinaia nel primo anno di presidenza.

Questo vuol dire che è possibile contrastare le fake news e che giornali e giornalisti hanno un ruolo importante da giocare in quest'arena. Si chiama fact checking.

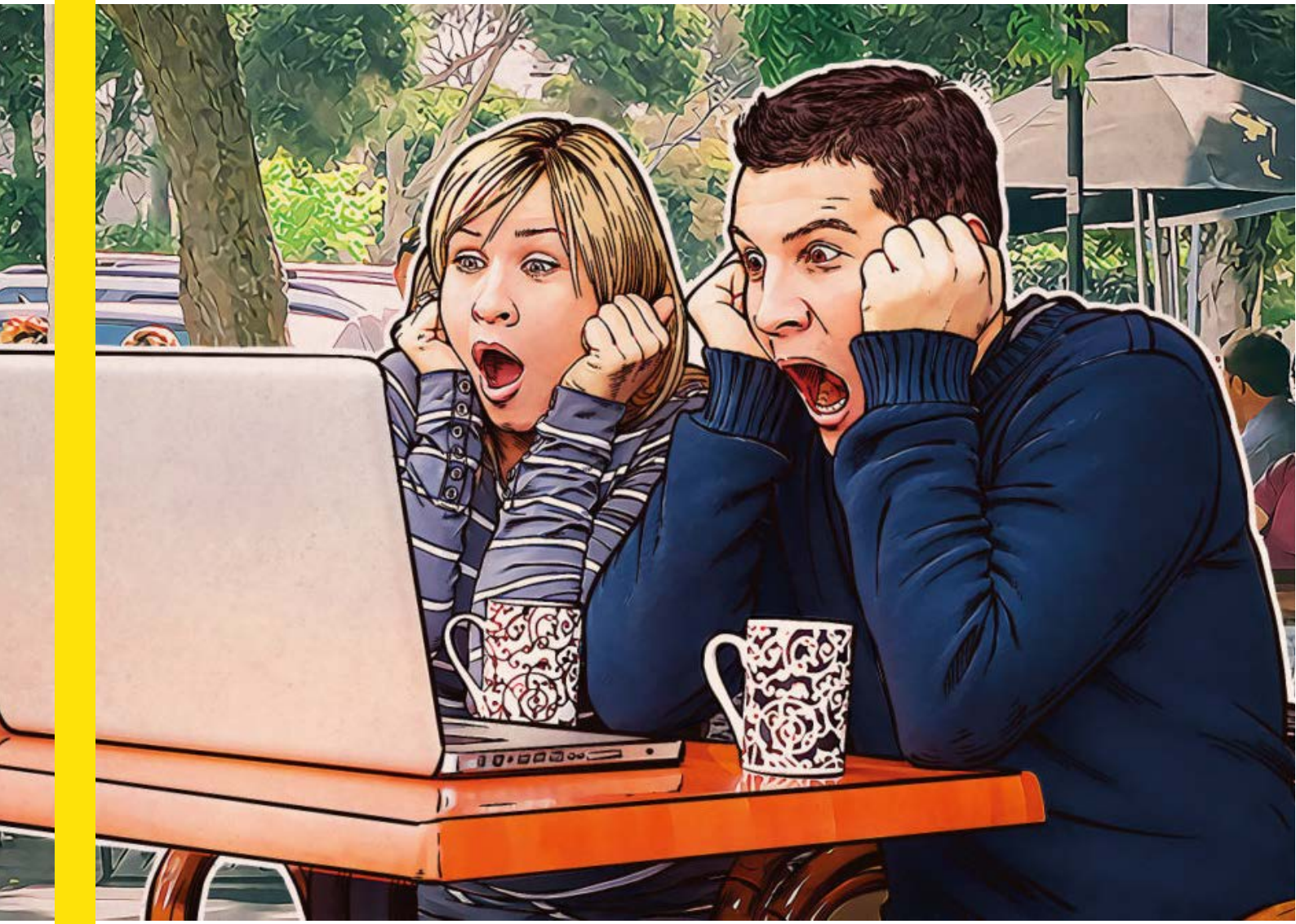
Il punto però è che anche se sveliamo quali sono le fake news, gli individui non vogliono riconoscerle come tali. Le persone, come hanno dimostrato diversi studi, non sono capaci di riconoscere le notizie vere da quelle false perché sono notizie verosimili, e quindi capaci di ingannare, ma è pur vero che **le persone alle notizie false ci vogliono credere**.

Questo accade quando tali notizie confermano i propri pregiudizi, consentono di spiegare fatti complessi senza sforzo, legittimano orientamenti politici e culturali preesistenti, producono un vantaggio nel gruppo di appartenenza. Sono tutti effetti noti in letteratura come "**confirmation bias**", il pregiudizio di conferma, "**effetto bandwagon**", l'adeguamento alla maggioranza; quando favoriscono le "**echo chambers**" (le casse di risonanza) prodotte dalla

"**filter bubble**", la tendenza a interagire solo con chi la pensa come noi. Tutte reazioni a un overload (sovraccarico) informativo che ci porta a semplificare e banalizzare il mondo circostante. È un principio basilare di economica cognitiva, ma anche frutto della tendenza tutta umana ad avere sempre ragione che nutre i "backfire effects", cioè la reazione aggressiva a tesi che non condividiamo.

Se a questi "bias cognitivi" aggiungiamo la **guerra dell'attenzione** che i media combattono a colpi di sensazionalismo e titoli strillati, e che il modello di business del capitalismo delle piattaforme si basa sulla **personalizzazione estrema dell'informazione** generata da siti, app e social, capiamo dove sta la gran parte del problema.

Qualità e pluralismo di giornali, **radio e tv**, **fact checking**, **media literacy**, **rispetto e dialogo** sono le principali risorse a cui appellarsi per combattere la disinformazione che fa perno sulle fake news.



FAKE SEX

LA TRUFFA DELLE RAGAZZE BELLISSIME CHE TI CHIEDONO L'AMICIZIA SU FACEBOOK (E 3 CONSIGLI PER NON CASCARCI)

Capita continuamente di ricevere richieste di contatto su Facebook (e altrove) da donne in bikini o uomini belli e impossibili. Ecco, prima di iniziare a chattare con loro è bene stare molto attenti, perché si tratta (quasi sempre) di truffe che sfociano in ricatti sessuali.

Se non ti chiami **Ben Affleck**, **Richard Gere** o **Justin Bieber**, chiediti perché una giovane e prosperosa Estefani Zamora, single texana e senza contenuti da mostrare ti abbia chiesto l'amicizia. Rifatti la domanda con Ester Atanga, Natalie Cassell o Alice Ciambelle. Fai lo stesso se non hai già sviluppato la carica sessuale di **Lady Gaga** o di **Madonna**, e se non puoi vantare i caratteri sessuali secondari di **Kim Kardashian**. In questo caso probabilmente l'affascinante giovanotto arabo o il procace attore di Bollywood che ti chiede l'amicizia non sta cercando proprio te: in entrambe i casi **sono banali esche sessuali**.

IDENTIKIT DELL'ADESCATRICE SESSUALE

È infatti molto facile che giovani e avvenenti individui ti abbiamo chiesto l'amicizia per popolare di "amici" il proprio profilo e **arrivare piano piano a delle "vittime" a te collegate**. Oppure cercano proprio te, ma per intavolare una chat notturna nella quale prima o poi **ti chiederanno di spogliarti per rubarti le foto e chiederti del denaro** per non divulgarle alla tua lista di amici, professori, compagni di classe e colleghi dell'ufficio.

Tranquilli, non si tratta di persone vere. Nella stragrande maggioranza dei casi si tratta di **profili fake**, costruiti a partire da foto-book di utenti veri, dal portfolio di attrici in erba, dalle foto di una sfilata o da una festa di compleanno. Se si controllano questi profili in genere non riportano molte informazioni personali e quelli meglio costruiti hanno qualche post di tema amoroso, oppure fiori, poesie e l'**immancabile dicitura "single"**.

Sono "esche sessuali", costruite ad arte da **organizzazioni criminali**, spesso basate in paesi africani o nei Balcani, che lucrano sull'ingenuità di chi vuole fare nuove amicizie, trovare l'anima gemella o fare (video)sesso virtuale con gli sconosciuti, al riparto da occhi indiscreti, magari dopo aver messo i figli a dormire.

SONO QUASI SEMPRE DEI BOT

Questi **profili fasulli sono spesso governati da "bot"** (chatbot) in grado di intavolare una banale discussione in chat, ma che falliscono nel rispondere a domande complesse e in genere si esprimono per mononsillabi e frasi fatte: "ok", "mi chiamo Patrizia", "vivo a Nantes", "faccio l'infermiera", "ho voglia di sesso", eccetera. Che poi già il fatto che nel profilo sia indicata una laurea conseguita in Italia per andare a fare la fiorista a Marsiglia dovrebbe insospettire, ma quando addirittura dopo poche battute in chat ti chiedono di fare sesso virtuale, lo scopo diventa evidente.

C'è chi ci casca, **molti ci cascano**, e diventa anche una questione di responsabilità verso il proprio network di amici evitare questi profili fake non confermando la richiesta di amicizia. È infatti molto probabile che se i tuoi amici ti vedono nel network dell'esca sessuale, siano più propensi a concedergli l'amicizia.

DALLA CHAT AL RICATTO IL PASSO È BREVE

Queste esche, anche quando non riescono a farti spogliare nella chat per usare le tue foto nude come ricatto, possono sempre operare dei fotomontaggi con te vestito, o vestita, e minacciare la loro divulgazione. Fotomontaggi di bassa qualità ma che possono raggiungere lo scopo se riescono a impaurire il malcapitato.

E se non paghi il riscatto richiesto, via money transfer o talvolta in Bitcoin, il passo successivo dei malviventi è quello di pubblicare il tuo fotomontaggio nudo, magari intento in un atto sessuale, sotto i post dei tuoi amici. Se anche lì fai resistenza, creano un videomontaggio e lo pubblicano al volo su Youtube e arrivano finanche a pubblicare la chat e le foto su un sito col tuo nome acquistato prima del tentativo di truffa.

I casi sono purtroppo molti e documentati, grazie alle denunce delle persone che hanno preferito dare spiegazioni a fidanzati e famiglie pur di non farsi ricattare, denunciando il fatto alla Polizia Postale. Altri però hanno ceduto e pagato, altri ancora ci si sono ammalati.

Trovare i responsabili di tanta angoscia non è facile neanche per le Autorità.

3 CONSIGLI PER NON FARSI FREGARE

Ma niente paura, si possono fare tre cose semplici semplici per trovare nuove amicizie riducendo il rischio di incappare in questi truffatori, a partire dalle domande che possiamo fare a noi stessi:

1. **Mi piace aggiungere nuove amicizie** e sono disposto a correre il rischio di incontrare un profilo fasullo: come posso fare per non farmi fregare da un robot? La risposta è semplice: scrivi il nome del nuovo contatto e incollalo su un motore di ricerca: se la persona compare su siti di notizie, album collettivi e social diversi da Facebook, potrebbe essere una persona vera, con tanto di lavoro e indirizzo. Informati, leggi quali informazioni ti offre il motore di ricerca e poi decidi.

2. **Sono ancora indeciso**, questa persona ha anche altri profili e pubblica su canali diversi foto di gatti e di fiori, ci ho parlato, è una persona sensibile! Come posso esserne sicuro? Anche qui si può fare una cosa semplice: fai uno screenshot del profilo del nuovo contatto, ritaglia il volto, salvalo come immagine e incollalo su Google, nella sezione immagini: Google ti proporrà una serie di volti e di link associati alla sua foto. Avrai un altro elemento di valutazione per decidere come comportarti.

3. **Mi sembrava una persona carina**, era veramente interessata a me, ma dopo aver fatto una videochiamata via Skype ha cominciato a ricattarmi minacciando di pubblicare le sequenze del nostro sesso virtuale. **L'ho denunciato alla polizia, ma continua a importunarmi**, mi subissa di telefonate e mi manda immagini disgustose!

La prima regola è non dare mai il proprio numero di telefono o l'indirizzo reale, ma se l'hai fatto, cambia i setting della privacy di Facebook e del telefonino (puoi anche bloccare chiamate e messaggi), vedrai che smetterà. Ma soprattutto non uscire mai dalla chat dove si è stati contattati.

Le chat di FB rimangono in memoria e costituiscono una prova dell'accaduto. Ma se hai fatto sesso virtuale a quel punto c'è poco da fare: pagare mai, denunciare sempre, cercare aiuto e consiglio dagli amici veri. Fino all'ultima opzione: l'outing protetto per evitare che altri cadono vittima dello stesso tranello.

F

124 GAMING

GAMING

Ma come fa un ragazzo di venti anni a guadagnare 200mila euro al mese giocando ai videogame? Grazie a milioni di persone che guardano i suoi tutorial su Youtube. E ai proventi della pubblicità e del marketing associato al suo nome e alle sue imprese. Gli youtuber più importanti in Italia, Favij, St3pNy e i Mates, sono gli idoli delle nuove generazioni che si riversano in massa ad ascoltarli, vederli, toccarli, in occasione delle loro comparsate pubbliche.

E tuttavia il loro successo dipende dal fatto che i videogame di cui realizzano i tutorial mostrando trucchi e strategie di gioco – *Fortnite*, *Brawl Stars*, *Apex Legends* – sono giocati da centinaia di milioni di giocatori in tutto il mondo. Insomma, dietro i videogame c'è un'intera industria di designer e sviluppatori, dove l'Italia è leader di mercato e anche nelle università si insegna come realizzarli e comunicarli.

Un successo che ha però delle ricadute negative: i videogame creano dipendenza al pari dei social network, e lo fanno attraverso quel complesso sistema di ricompense che aumenta la voglia di giocare tanto da rendere i giocatori indifferenti a tutto il resto. Con conseguenze negative sul piano personale, familiare, sociale e lavorativo. L'Organizzazione mondiale della Sanità ha riconosciuto nel maggio 2019 la dipendenza da videogame come una malattia: chi gioca troppo smette di mangiare, dorme poco, diventa irritabile, esce poco di casa. Ma secondo alcuni medici videogiocare favorisce la memoria e l'apprendimento in giovanissimi e anziani.

VIDEOGAME E CRIMINALI INFORMATICI

Proprio per la loro enorme diffusione, i videogame sono diventati un bersaglio preferito dai criminali informatici.

I motivi sono principalmente tre: la facilità con cui i criminali riescono a scambiarsi elementi di valore interni al gioco, la giovane età delle vittime, la loro disponibilità economica.

Secondo il rapporto sullo Stato della sicurezza di Internet 2019 pubblicato da Akamai, tra novembre 2017 e marzo 2019 ci sono stati 12 miliardi di attacchi di *credential stuffing* contro i siti web di *gaming*.

Il credential stuffing (abuso di credenziali) è un tipo di attacco che è basato sull'utilizzo di credenziali compromesse – nome, cognome, email e password – per accedere al profilo delle vittime a causa del fatto che gli utenti impiegano spesso la stessa email e la stessa password per servizi diversi. Così se la violazione del database delle credenziali di un social network va a buon fine, l'attaccante userà le stesse su altri servizi, come le piattaforme per il *gaming* online dove è probabile che i giocatori abbiano utilizzato la stessa email e la stessa password usata altrove.

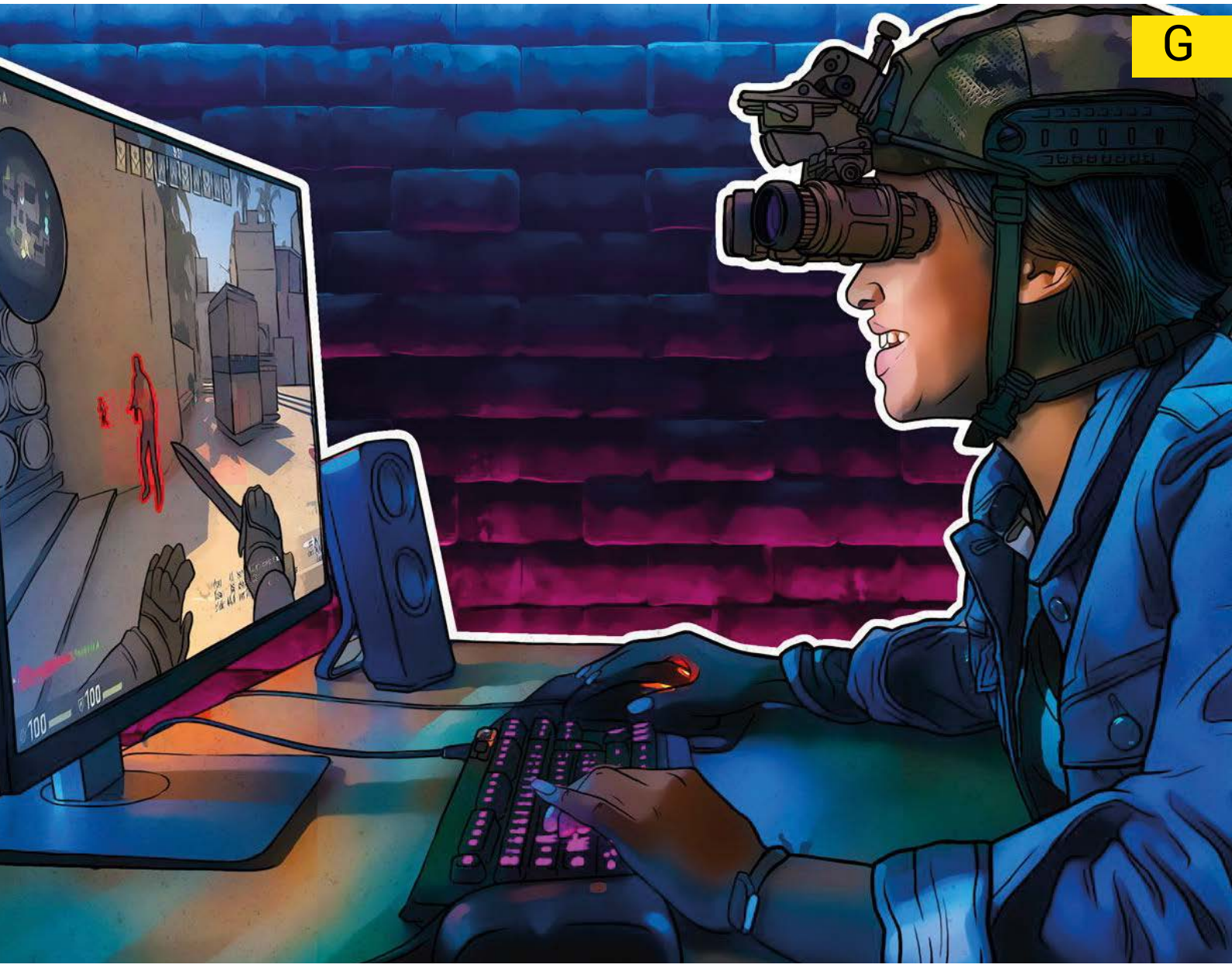
I criminali prendono di mira giochi molto conosciuti e, dopo essere stato

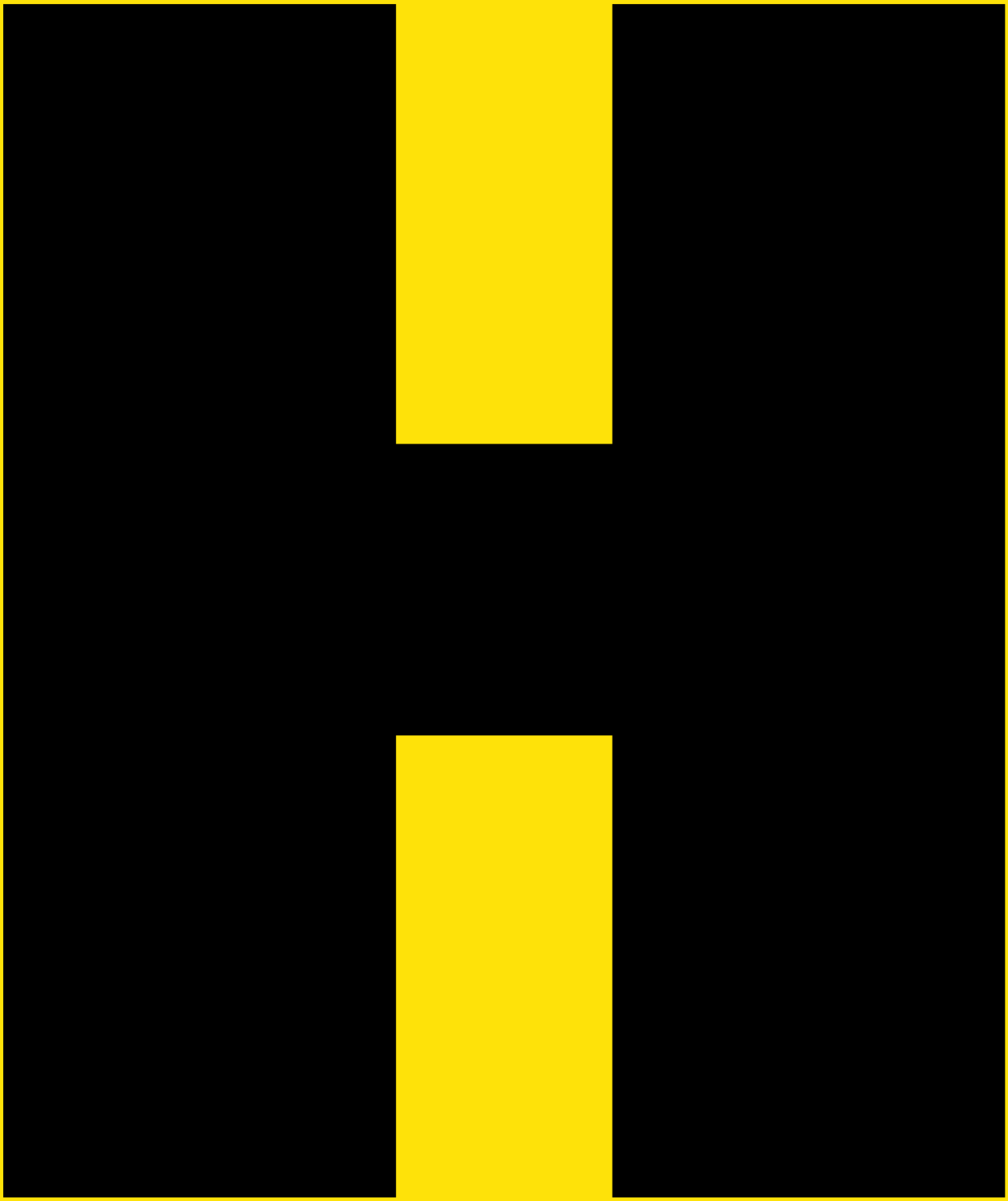
compromesso, l'account di un giocatore può essere scambiato o venduto. E la moneta usata nel gioco da virtuale può diventare reale.

«I *gamer* sono una nicchia nota per spendere cifre notevoli, e di conseguenza anche la loro disponibilità economica è un obiettivo allettante», ha detto Martin McKeay, Security Researcher di Akamai che ha curato il rapporto 2019.

La gaming community si è così trasformata in uno dei target degli attacchi di credential stuffing in più rapida crescita, nonché uno dei target più redditizi per i criminali alla ricerca di profitti rapidi.

Nello stesso periodo citato, sono stati 55 miliardi gli attacchi di *credential stuffing* registrati da Akamai in tutti i settori e non solo in quello del *gaming*.





HACKER

L'HACKING COME NUOVA FORMA DI CIVISMO

"Hacker, in informatica, in particolare con riferimento alla rete Internet, esperto di programmazione e di reti telematiche che, perseguendo l'obiettivo di democratizzare l'accesso all'informazione e animato da princìpi etici, opera per aumentare i gradi di libertà di un sistema chiuso e insegnare ad altri come mantenerlo libero ed efficiente. Il termine, originatosi a cavallo degli anni 1960 al MIT di Boston, è passato nei decenni successivi a designare una vera e propria cultura, il cui percorso fu coevo a quello di internet che gli hacker stessi contribuirono a sviluppare, e tra i cui esponenti di spicco vanno citati i padri fondatori del movimento del software libero e dell'*open source* R. Stallman e B. Perens. Sebbene generalmente si tenda a confondere gli hacker con i pirati informatici, o *crackers*, il cui scopo è danneggiare un sistema informatico, quest'ultimo termine, dal valore fortemente spregiativo, è stato invece coniato dagli hacker stessi per definire chi non abbia rispetto delle proprie abilità informatiche. In relazione agli scopi perseguiti, si distinguono tre differenti categorie di hacker: *white hat hacker*, il cui operato corrisponde a un rigoroso rispetto dell'etica hacker; *black hat hacker*, chi violi illegalmente sistemi informatici con o senza vantaggi personali; *gray hat hacker*, l'hacker cui non siano applicabili queste distinzioni o che passi facilmente dall'una all'altra categoria."

Questa è la definizione di hacker scritta per la Treccani dallo stesso autore di questo libro.

Vale la pena ricordarla oggi che il dibattito su hacker buoni e cattivi ha assunto nuovo vigore.

L'occasione è stata fornita dalle polemiche seguenti l'individuazione dell'hacker che nel 2017 aveva scoperto e subito comunicato le vulnerabilità della piattaforma Rousseau attraverso cui i Cinquestelle scelgono i loro rappresentanti, presentano e discutono le leggi fra gli iscritti e con i propri eletti.

Ma se l'hacker ha denunciato le falle senza sfruttarle per un vantaggio personale, perché tanto accanimento dai vertici del Movimento Cinquestelle che lo ha accusato di operare per conto terzi e con fini politici? La risposta è ovvia: il giovane studente colpevole dell'accaduto è finito nel bel mezzo di una polemica elettorale senza esclusione di colpi. Ma c'è un altro motivo, lo ha fatto senza chiedere permesso a nessuno. Che è quello che in genere gli hacker etici fanno: scoprono un problema, lo segnalano e si ritirano in buon ordine. Li chiamano per questo cavalieri bianchi o white hat, diversi dai **blue hat hacker** che lo fanno pagati dalle aziende.

La polemica è però stata rinfocolata da un articolo di Michele Serra su La Repubblica che ha enfatizzato

il carattere politico dell'azione dell'hacker connotandola come un'azione machista e spavalda. Perciò studenti di ingegneria e ricercatori in cybersecurity hanno deciso di sfidare quella errata interpretazione dell'hacker e hanno scritto a Michele Serra: "Meno male che esistono queste segnalazioni disinteressate, perché non vengono certo da malintenzionati interessati a sfruttare più a lungo possibile la falla. Vengono da persone come noi, come Evariste Gal0is, lo pseudonimo usato dal ragazzo indagato. Infatti il suo nome è elencato tra i ringraziamenti ufficiali del "Computer Emergency Response Team" europeo. Il motivo? Una segnalazione che ha reso i sistemi informatici dell'UE più sicuri. Un comportamento non dissimile da quello tenuto nel caso di Rousseau, ma con esito drasticamente diverso." L'hacking come nuova forma di civismo.

HACKER E CYBERDIFENDER

Essere un hacker significa smontare e rimontare le cose. Metterci le mani dentro. Trasformarle secondo i propri desideri. Questo è l'hacking. Un modo irriverente e giocoso di misurarsi con la complessità delle macchine informatiche. E oggi, finalmente, maneggiare hardware e algoritmi, scoprire difetti nel codice e risolvere problemi matematici per proteggere le reti, bloccare un attacco informatico, ottimizzare un software con un hack, si può fare alla luce del sole.

Dopo molti anni in cui pessime narrazioni e troppi pregiudizi hanno portato tanti giovani hacker a coltivare il proprio talento da soli, incompresi, di nascosto, CyberchallengeIT, consente ai più giovani di uscire dal bozzolo e trasformarsi in hacker impegnati a proteggere quello che conta veramente: la pace, la democrazia, il benessere di tutti. Possibile? Forse sì, se scegliamo la strada giusta.

CyberchallengeIT, ha questo obbiettivo. L'iniziativa che si prefigge il Laboratorio Nazionale di Cybersecurity del CINI che la organizza la è quella di addestrare gratuitamente i giovani talenti informatici italiani fra i 16 e i 23 anni. Anche quest'anno la partecipazione alla CyberchallengeIT servirà a selezionare i più meritevoli in un percorso che culminerà nella gara finale e nelle premiazioni del prossimo giugno 2019. Il progetto punta a sviluppare nei partecipanti le competenze necessarie ad affrontare le sfide che un cyberspace sempre più affollato impone per garantire la sicurezza di tutti.

La sicurezza di tutti? Sì, proprio quella, la sicurezza quotidiana in gioco ogni volta che usiamo una carta magnetica, un computer, un dispositivo digitale. La sicurezza di non essere spiati, derubati o bullizzati. La sicurezza di arrivare a destinazione, di avere le cure necessarie, di poter richiedere un diploma o accedere al mondo del lavoro.

Non ci pensiamo mai, però in un mondo senza confini come il cyberspace dove il reale e il virtuale si confondono, il normale funzionamento di quello che di buono la società ci offre, scuole, ospedali, trasporti, è costantemente minacciato da cybercriminali, stati canaglia e software scritti male. Una minaccia che prende la forma di furti di identità, virus e attacchi alle infrastrutture di base, dal trattamento dell'acqua che beviamo alla fornitura di energia elettrica.

È proprio per impedire che le attività basate sulle infrastrutture digitali vengano compromesse il Laboratorio Nazionale di Cybersecurity per il terzo anno consecutivo ha chiamato a raccolta (diciotto) università e scuole per contribuire allo sforzo di modernizzare il paese favorendo la cultura informatica dei giovani e la selezione di quei talenti che, se vorranno, potranno diventare i cyberdefender che l'Industria e la Pubblica Amministrazione spesso cercano invano.

LA NAZIONALE HACKER

Nella pratica dell'hacking l'Italia vanta una bella "scuola". Parafrasando un vecchio adagio, quello italiano è un popolo di santi, poeti, navigatori e hacker. E, come per il calcio, l'atletica leggera e la pallavolo, l'Italia vanta anche una nazionale di hacker. Non lo sapevate? Il

nostro paese compete a livello mondiale in cucina con la nazionale dei cuochi, perché non dovrebbe avere una nazionale hacker per rappresentare l'eccellenza raggiunta in questo campo? Parliamo ovviamente di "hacker buoni", i cosiddetti hacker etici o «white hat hacker». L'hacker, come abbiamo detto, non è l'uomo nero che i media accusano quando non sanno che nome dare ai criminali informatici, alla stupidità umana e all'avidità delle imprese che ci hanno venduto per anni microprocessori e software bacati. L'hacker è un virtuoso della programmazione informatica. E quando parliamo della Nazionale hacker, parliamo dei «cyberdefender», di quei ragazzi cioè che sono impegnati a mettere l'italico cyberspazio al sicuro da cybercriminali ed eserciti cibernetici.

La nazionale hacker italiana è stata chiamata *TeamItaly*, partecipa alle competizioni europee come la European Cyber Security Challenge (ECSC) e tiene alta la nostra bandiera nelle competizioni chiamate CTF, Capture The Flag. In queste competizioni, una sorta di rubabandiera digitale a squadre, ognuno deve difendere il suo fortino e penetrare in quello avversario. Il TeamItaly lo ha fatto anche a Londra nell'Ottobre e 2018 insieme alle nazionali di altri 17 paesi che si sono sfidate in una serie di prove di bravura informatica sotto gli auspici della Commissione Europea e dell'Enisa, l'Agenzia Europea per la sicurezza informatica. Andrea, Marco Christian, Jacopo, Quian e gli altri, dodici in tutto, più tre allenatori, sono stati selezionati durante la Cyberchallenge.IT, il programma italiano di addestramento gratuito alla sicurezza informatica. Organizzato dal Cini, il Consorzio Interuniversitario per l'Informatica, insieme alle università, Cyberchallenge. IT ha visto aumentare progressivamente il numero degli studenti partecipanti: nel 2017 erano meno di mille, nel 2018 erano 1800 e nel 2019 sono diventati 3200.

La nazionale che ha partecipato all'ultima ECSC di Londra era composta da cinque giovani di categoria junior (14-20 anni) e cinque giovani di categoria senior (21-25 anni) e, oltre ai partecipanti della CyberchallengeIT, includeva membri del team italiano «mHACKeroni» che ha anche partecipato alle finali del Defcon a Las Vegas, la più importante gara di sicurezza informatica al mondo, ottenendo la settima posizione.

«I nostri ragazzi», esperti di web security, crittografia, serrature elettroniche e lettori di smart card nell'edizione del 2017 a Malaga sono arrivati terzi dopo Spagna e Romania, alla Cyberchallenge di Londra si sono piazzati al sesto posto in una competizione dove, oltre ad eccellere in ambito tecnico, hanno dovuto collaborare con le squadre degli altri paesi per fronteggiare i problemi complessi creati per la competizione usando particolari "soft skills": attitudine alla cooperazione, alla condivisione e alla diplomazia.

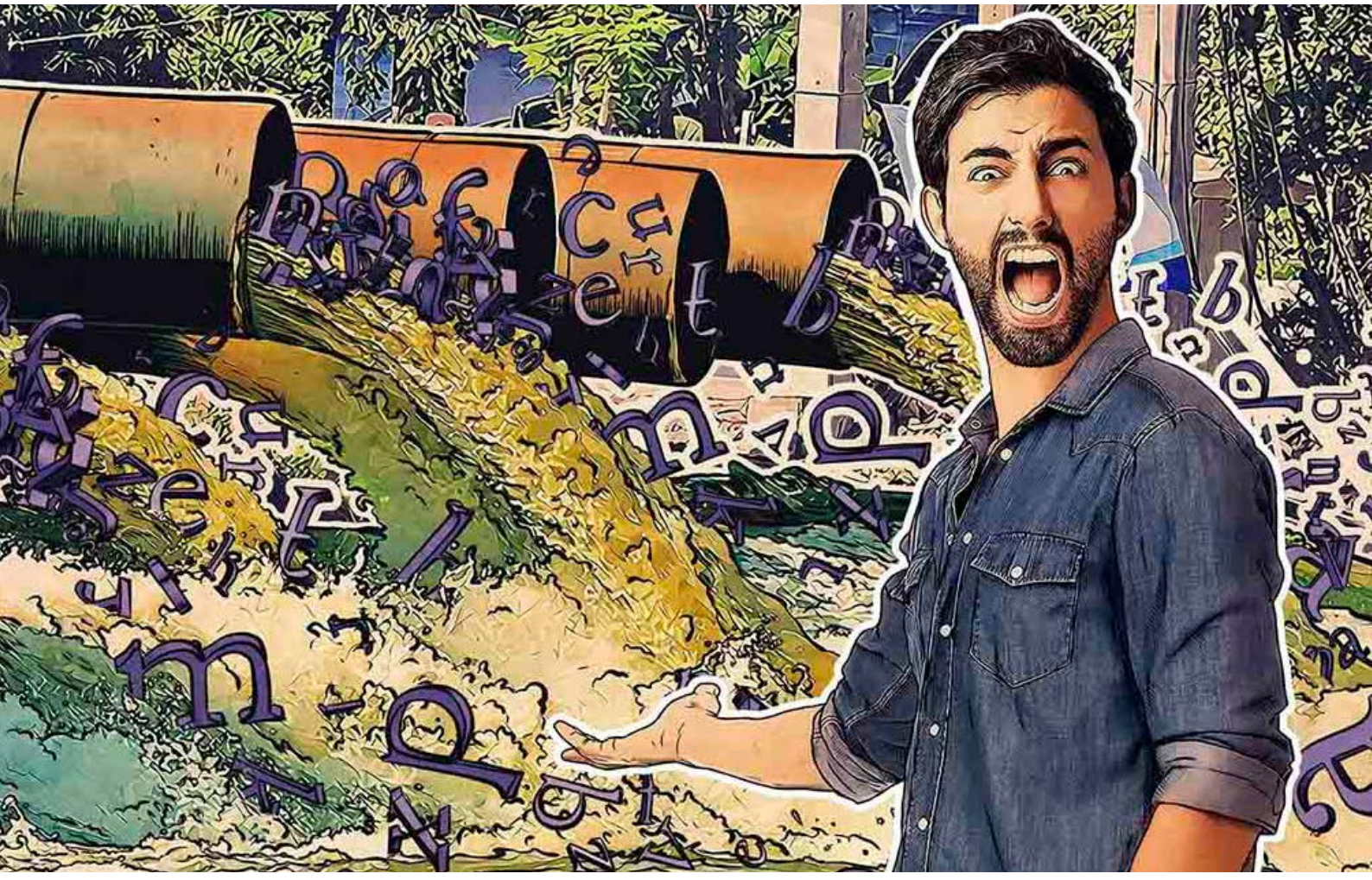
Gli organizzatori della CSCS hanno insistito molto su questo aspetto: stimolare la collaborazione tra i giocatori dei paesi partecipanti mentre ribadivano l'importanza della trasparenza e del rispetto per le regole durante tutte le fasi della competizione. Tra gli obiettivi dell'ECSC vi è quello di porre la cybersecurity a servizio dell'umanità, per promuovere la pace, preservare la democrazia, la dignità e la libertà di pensiero, principi basilari dell'etica hacker.

HASHTAG

LA GUERRA DEGLI HASHTAG E IL MOSTRO MITE DEL WEB

Gli hashtag ormai vengono usati per creare fazioni politiche sul web. Ad esempio nella guerra di hashtag sulla formazione del governo Lega-Cinquestelle ci ha mostrato un web istericamente diviso tra i sostenitori del Presidente Mattarella e i suoi detrattori.

Da una parte l'hashtag #IoStoConMattarella, di chi si è schierato a difesa delle Istituzioni incarnate dal professore capo dello Stato e dall'altra quello di chi ne ha chiesto finanche l'impeachment, #IlMioVotoConta.



Entrambi usati per essere visibili nel flusso della comunicazione di un evento che ha indotto molti a prendere posizione a favore o contro per far pesare la propria opinione.

La funzione dell'hashtag è infatti proprio quella di aggregare e categorizzare i contenuti presenti sulle piattaforme sociali in relazione al tema trattato e rendere quindi più facile agli utenti individuare contenuti specifici senza perdersi. Nel caso del dibattito della formazione di questo governo, l'hashtag è diventato la bandiera di opposte tifoserie per affermare posizioni che cambiano anche nel volgere di minuti in funzione degli avvenimenti e che in molti casi faranno vergognare chi le ha scritte una volta rilette.

Eppure la regola d'oro del web è infatti che non si debba mai scrivere ciò che vorremmo dimenticare.

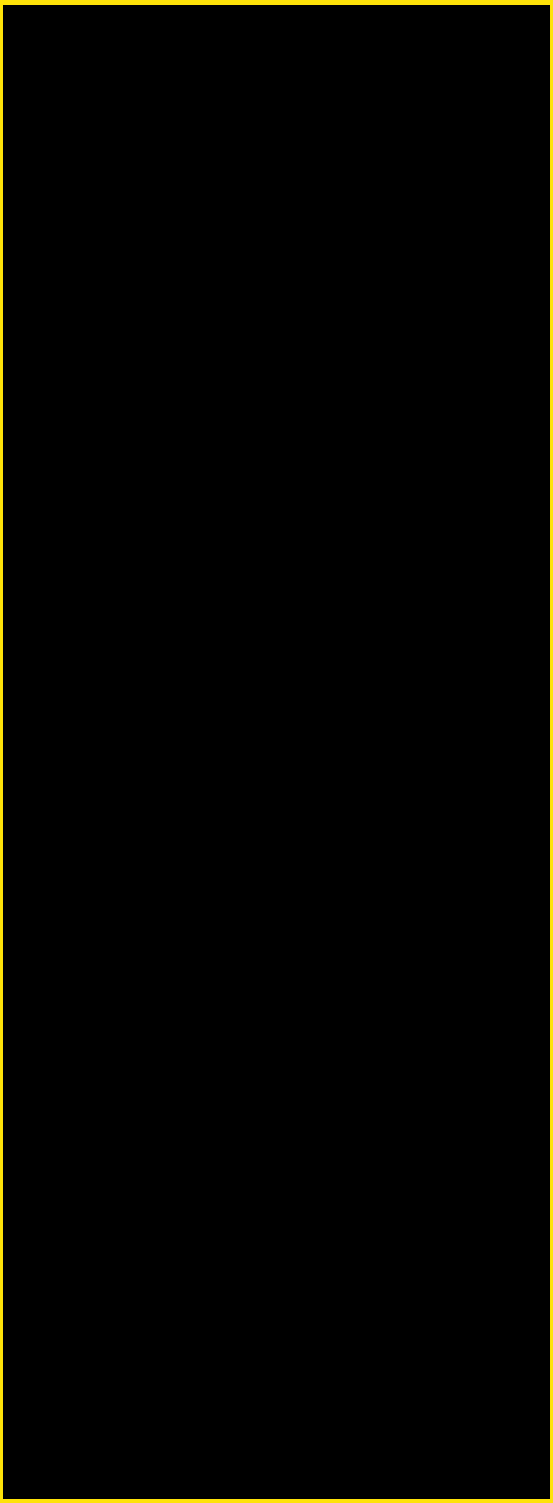
Infatti, nonostante le leggi e i regolamenti che, come il GDPR (la Direttiva europea sulla protezione dei dati personali), prevedono il diritto all'oblio, quello che è scritto sul web è destinato a rimanerci, copiato, replicato, retwittato o congelato nello screenshot dell'avversario dopo essere rimbalzato su siti, app e giornali. L'hashtag ci aiuterà a ritrovarlo, e nel nostro caso aiuterà la Polizia Postale a incriminare più facilmente gli autori delle offese al Capo dello stato.

Ma allora perché tanta foga? Secondo Raffaele Simone, psicolinguista emerito, è perché non siamo capaci di sottrarci alla dinamica del narcisismo voyeuristico che i social network stimolano in noi. Una dinamica di autorappresentazione che dietro l'urgenza di testimoniare manifesta un'ansia da prestazione sociale, come se non esistessimo fuori dello schermo, come se fossimo inutili senza un palcoscenico anche quando il pubblico in sala è poco ma la voglia di fare parte dello show è molta.

A parere suo, questa ansia di rappresentazione è un portato del «mostro mite», che dà il nome a un suo interessante saggio del 2009, e cioè un regime globale di governo che si basa su un sistema mediatico, televisivo, culturale, cognitivo, che crea un ambiente «infantilizzante» che pesa su tutta la società.

«Un regime che – come ebbe a dire in un'intervista al saggista francese Frederick Joignot – si appoggia a una destra anonima e diffusa decisa a ridurre il controllo dello Stato, ostile alla lentezza del processo decisionale democratico, sprezzante della vita intellettuale e della ricerca, impegnata a sviluppare un'ideologia del successo individuale, a imbavagliare l'opposizione, violenta nei confronti delle minoranze, populista nel senso che aggira le regole della democrazia in nome di ciò che "vuole il popolo"».

Il ritratto perfetto del populismo del web, quello che brandisce gli hashtag di fake news e post-verità, ritratto di una folla che urla senza essere ascoltata, dimentica della lezione di Shakespeare che al Macbeth fa dire: «L'uomo è solo un povero pupazzo che si agita sul palcoscenico della vita durante la sua ora e poi non è più ascoltato da nessuno». Ma quello che ha scritto non è scritto sull'acqua.



INSTAGRAM

INSTAGRAM E IL FURTO DEI PROFILI

Con oltre un miliardo di utenti, Instagram è il secondo social network più diffuso al mondo. Per questo motivo il social, specializzato nella condivisione di immagini, è anche uno dei più bersagliati dai criminali informatici. Negli ultimi tempi sono aumentati i tentativi di impossessarsi degli account presenti sulla sua piattaforma per accedere alle informazioni personali degli utenti e ai loro messaggi per ricattarli, ma anche per veicolare virus o diffondere spam. Secondo i ricercatori di **Kaspersky** dopo aver preso il controllo dell'account, i cybercriminali cambiano la foto del profilo, la descrizione, l'indirizzo email e il numero di telefono per impedire ai titolari di riappropriarsi del proprio account. Ovviamente a essere presi di mira sono gli account più attivi, quelli con molti follower e quelli delle celebrità, soprattutto se fanno girare i soldi della pubblicità legata alla loro capacità di influenzare comportamenti di consumo.

Nel passato gli agenti di **Europol** hanno identificato su Instagram anche sospetti jihadisti e account di propaganda politica con follower fasulli.

Per tutti questi motivi Instagram ha deciso di prendere di petto la questione degli account fasulli sul social e ha deciso di consentire agli utenti di accedere a informazioni sui membri più popolari della piattaforma con una sezione ad hoc.

La funzione «About this account» dovrebbe contenere una serie di informazioni sugli account che hanno molto seguito: la data di iscrizione, il paese di provenienza, i cambi di nome nell'ultimo anno e le eventuali pubblicità in corso. La novità arriva insieme ad altre due in chiave sicurezza: l'estensione dei profili verificati con la «spunta blu» – come su Twitter – e l'autenticazione a due fattori con app esterne. «La community ci ha detto che è importante comprendere gli account che raggiungono molte persone, specie se condividono informazioni su attualità, politica e società», ha detto in un post Mike Krieger, cofondatore e direttore tecnico di Instagram. Tutto bene allora? Certo, ma secondo gli esperti è proprio in questa fase che aumenteranno i tentativi di truffa per impossessarsi degli account.

È in occasione di cambiamenti di policy nei servizi online che i cybercriminali creano dei siti con le sembianze di pagine di assistenza che richiedono informazioni personali dell'account: username, password, indirizzo email, nome, cognome, data di nascita. Nel caso di Instagram per rilasciare un badge di verifica fasullo, impossessarsi dei dati dell'utente e prenderne il posto.

Quelle stesse informazioni aiuteranno i ladri a bypassare la procedura di autenticazione a due fattori. Il delinquente non deve far altro che richiedere il codice o altre informazioni di sicurezza via sms con cui contattare il vero servizio di assistenza e compromettere definitivamente l'account.

Ai siti fake ci si arriva in molti modi, ma la tecnica prevalente rimane il phishing: una finta email del team di Instagram che chiede di cliccare un link specifico per portare l'ignaro utente sul sito fasullo dove immettere i suoi dati personali «perché l'account è stato hackerato» o «per aggiornare le credenziali di accesso». Oppure, semplicemente si invita l'utente a dare un'opinione su una foto e, per fare ciò, deve collegarsi al social network.

Per questo è fondamentale non cliccare mai su link sospetti; verificare che l'URL del sito sia Instagram.com; scaricare le app di servizio solo dagli store ufficiali e utilizzare quelle e solo quelle per gestire i propri profili. E soprattutto, mai e poi mai usare le credenziali di accesso del social per collegarsi ad app e servizi che non conosciamo abbastanza.

INSTANT MESSAGING

SIGNAL, TELEGRAM E WHATSAPP. MOXIE, PAVEL E MARK: IL BUONO, IL BRUTTO E IL CATTIVO

A capodanno gli utenti di WhatsApp hanno inviato oltre 100 miliardi di messaggi in sole 24 ore. Adesso che il Coronavirus ci obbliga a mantenere le distanze la famosa app di messaggistica ha superato quel traguardo. Se la forza di WhatsApp è l'abitudine, mentre l'ideologia quella di Telegram, sempre unite alla gratuità, oggi che gli operatori regalano messaggi illimitati il caro vecchio Sms potrebbe prendersi la sua piccola rivincita: perfino Google ha annunciato gli Sms 2.0. Ma quali sono le app di messagistica più sicure?

I messaggi su WhatsApp sappiamo che possono essere spiati. La conferma viene dalla causa che Facebook, proprietaria di WhatsApp, ha intentato a NSO group, azienda israeliana di cybersecurity, per avere utilizzato la popolare app di messaggistica per sorvegliare giornalisti, attivisti e difensori della privacy. Ovviamente non si è trattato di un'operazione semplice. Non riuscendo a violare il sistema crittografico di WhatsApp la NSO ha creato un malware apposito in grado di consentire l'accesso ai contenuti dei suoi utenti con una semplice telefonata.

Una volta aggiornato WhatsApp l'exploit, il trucco, non ha più funzionato. E tuttavia la reputazione di WhatsApp ne ha risentito, favorendo due concorrenti: Telegram e Signal. E adesso che il loro uso si sta diffondendo persino la Commissione Europea ne suggerisce l'uso, o almeno pare averlo fatto per Signal.

La Commissione ha fornito le linee guida per l'uso della messaggistica istantanea via Whatsapp, Messenger, Skype, Telegram, eccetera, per ragioni di servizio, suggerendo le applicazioni open source come Signal quando non occorre un livello di sicurezza superiore. Caso in cui vanno usati altri sistemi, ma di fatto esprimendo sfiducia verso le app più popolari come Whatsapp e Messenger.

Però Signal usa lo stesso sistema di crittografia end-to-end (E2E) delle app di Facebook come Messenger e WhatsApp per proteggere le comunicazioni riservate dall'occhio indiscreto di hackers, criminali e degli stessi operatori. Quali sono le differenze?

UNO SPIRITO DIVERSO

Intanto diciamo che le app di messaggistica ormai utilizzano tutte la crittografia E2E, cioè i messaggi non possono essere letti da un eventuale spione che si intrufola nella comunicazione, proprio perché cifrati. E il sistema di cifratura è lo stesso di

Signal, realizzato da Trevor Perrin e Moxie Marlinspike nel 2013 proprio con l'obbiettivo di garantire la privacy di tutti. Dall'app Textsecure e RedPhone è nata l'app Signal. Il suo protocollo di cifratura è stato acquistato da WhatsApp nel 2016, usato da Messenger di Facebook, ed è stato pure implementato in Skype di Microsoft. Nel frattempo Moxie e i suoi compagni hanno creato la startup Open Whisper System per migliorare l'app Signal che consente messaggi, chat di gruppo e chiamate vocali a prova di spione secondo un modello collaborativo e solidale. Il protocollo di cifratura adesso si chiama **Signal protocol**.

Signal, a differenza di WhatsApp, è gestito da una fondazione, e la fondazione riceve fondi e finanziamenti da singoli individui e supporto finanziario dalla Electronic Frontier Foundation e dall'Associazione americana per le libertà civili (ACLU). Il suo modello di business è quindi basato sulle donazioni e non sulla monetizzazione dei dati degli utenti. Ed ha appena ricevuto in regalo 50 milioni di dollari da Brian Acton (il creatore di WhatsApp). Per garantire la sua indipendenza Signal ha sempre dichiarato di non conservare i metadati delle conversazioni. Il contrario di WhatsApp. Uno dei motivi per cui gli viene preferito.

UNA DIVERSA GESTIONE DEI DATI

Infatti seppure il percorso del messaggio dal mittente al destinatario è illeggibile al "man in the middle", lo spione in agguato, grazie alla crittografia E2E, questo non vale per i metadati: con chi, per quanto tempo e da dove abbiamo comunicato. WhatsApp conserva i metadati in forma non cifrata, come pure Telegram, l'altra app concorrente e creata da due russi, i fratelli Nikolaj e Pavel Durov, noti avversari del regime di Vladimir Putin. I metadati, cioè data e ora di invio, i numeri di telefono del mittente e del destinatario, la loro localizzazione possono fornire ad un soggetto terzo informazioni importanti a un malintenzionato e per questo Signal conserva solo il numero di telefono, la data di registrazione dell'account e l'ultima connessione ai server.

Inoltre con Signal i messaggi non vengono salvati nel backup di iCloud o iTunes mentre con Android la funzione di backup può essere utilizzata solo per trasferire i messaggi da uno smartphone ad un altro. Al contrario con WhatsApp il backup delle chat può essere salvato al di fuori dello smartphone (sul cloud).

Eppure Whatsapp ha circa il 70% del mercato dei software di Instant Messaging con 2 miliardi di utenti connessi ogni giorno al suo circuito. Il motivo è sicuramente il marketing. Ma anche il fatto che è nata prima in un contesto in cui scambiarsi SMS costava parecchio: era il 2009. Nel primo mese dalla nascita WhatsApp aveva già raggiunto un milione di utenti. Telegram ne ha 400 milioni e Signal non sappiamo quanti ne abbia oggi.

A FAVORE DI SIGNAL

- Realizzato con l'obbiettivo di garantire la privacy
- Basato su software free ed open source
- Consente telefonate e audio cifrati
- Consente messaggi a scomparsa
- Non conserva i messaggi
- Non conserva i metadati
- Oggetto di analisi indipendente del software

CONTRO SIGNAL

- Qualche perdita di segnale telefonico in assenza di wi-fi
- Con una piccola base di utenti non riesce ancora a sfruttare l'effetto rete

A FAVORE DI WHATSAPP

- Usa la crittografia End to End
- Leader di mercato lo usano tutti
- I messaggi sono cifrati in automatico
- Telefonate, audio e video sono cifrati

CONTRO WHATSAPP

- Timori di un utilizzo scorretto dei dati da parte di Facebook
- Non è open source
- Conserva i messaggi
- Conserva i metadati
- Non rende note le analisi indipendenti del software

A FAVORE DI TELEGRAM

- Interfaccia semplice
- Messaggi a scomparsa
- Funzione di condivisione di file pesanti
- Creazione di gruppi fino a 200 mila utenti
- Consente di editare i messaggi inviati al gruppo
- Non si deve esporre il numero di telefono per chattare

CONTRO TELEGRAM

- Le chat di default non sono cifrate End to End
- La crittografia funziona solo per le chat segrete
- Il software è in parte proprietario
- La base di utenti è più ristretta di WhatsApp

Nonostante la scelta di ciascuna app dipenda dal rischio percepito di ognuno, dalla consapevolezza dell'importanza della privacy e della libertà che consente, gli elementi di debolezza di queste app per comunicare in maniera riservata sono tuttavia sempre gli stessi: **le implementazioni errate del software non ancora scoperte; la compromissione del dispositivo; eventuali "backdoor" aziendali o governative**.

Per quanto sia potente la crittografia End-to-End se uno dei due 'end point' che comunicano è già stato violato, uno spione potrà leggere i dati prima che vengano cifrati. Il punto debole può essere insomma il dispositivo stesso, che si tratti di uno smartphone, un computer, un tablet, una consolle per videogame. Per questo strumenti come i captatori informatici governativi o i virus trojan rivestono una straordinaria importanza in questo tipo di attacchi.

Perciò gli esperti suggeriscono di **non lasciare mai il telefono incustodito**, di installare le app per la comunicazione sicura sui telefoni appena comprati, o almeno di scansionarli con un antivirus e aggiornare sempre sistema operativo e app usate. Facendo molta attenzione a usare un codice di sblocco complesso e dove possibile la doppia autenticazione.

Un elemento che può fare la differenza nella scelta delle app è se mantengono o no i dati sui loro server. Facebook, proprietaria di WhatsApp, essendo soggetta alle leggi antiterrorismo americane, ad esempio, come il famoso Patriot act, la legge antiterrorismo post 11 settembre, offre un facile accesso ai dati che sono eventualmente richiesti dal governo.

E questo potrebbe essere proprio il motivo della preferenza dei burocrati di Bruxelles che, scambiandosi quotidianamente email gestite dalle piattaforme Usa (Gmail, Hotmail, Outlook), cercano di sottrarsi almeno nella messaggistica agli oligopoli americani. Ma l'hanno fatto esprimendo una posizione tecnica e non politica che gli analisti hanno interpretato come un sostegno verso l'industria crittografica continentale. I tradizionali messaggi di testo e le telefonate infatti non possono essere crittografate per consentire alla autorità di sorvegliarli mentre i sistemi di messaggistica non sono ancora regolati. Ma almeno i tradizionali Sms rimangono nelle mani delle società telefoniche e per averli ci vuole un mandato del giudice.

M

144 MALWARE

MALWARE

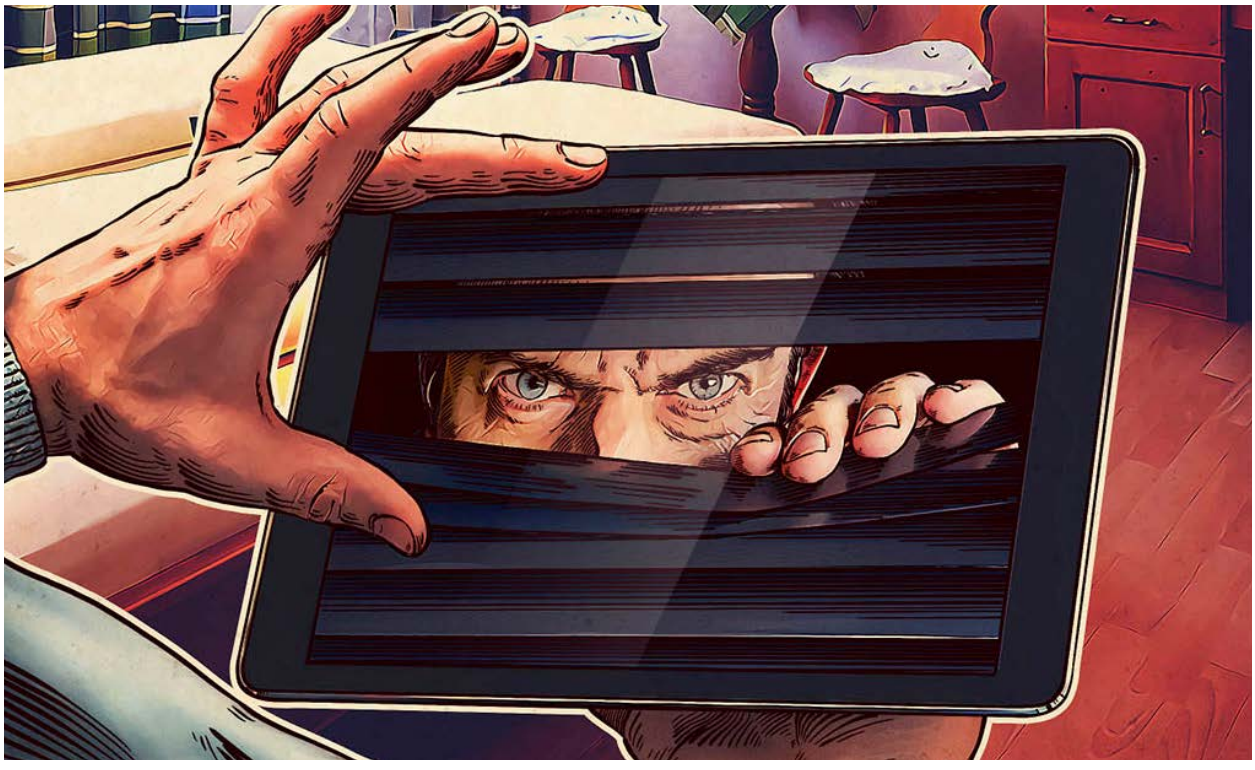
GHOSTTEAM, IL MALWARE CHE TI RUBA L'ACCESSO A FACEBOOK

Avast e Trend Micro, due aziende di sicurezza informatica, hanno scoperto un malware in grado di rubare le credenziali di accesso a Facebook. Soprannominato GhostTeam è stato a lungo presente all'interno di 56 applicazioni reperibili su Google Play Store.

Queste tipo di app nocive per dispositivi Android ha l'aspetto di programmi di utilità che promettono di potenziare il funzionamento dei telefonini ripulendoli, per scansionare codici QR, facilitare la gestione di video eccetera, ma rappresentano un pericolo per gli utilizzatori.

Una volta scaricati chiedono alla vittima l'accesso alle opzioni di amministratore del dispositivo in modo tale che "L'app raccolga informazioni sul dispositivo, come il suo identificativo, l'ID, la posizione, la lingua e i parametri di visualizzazione".

I malware, i software malevoli, sono una famiglia di virus che non contengono necessariamente codice dannoso ed è



per questo che sono riusciti a passare indenni dai controlli della piattaforma di distribuzione software di Google.

Poco male si potrebbe dire, ma non appena gli utenti aprono la loro app di Facebook sul telefonino, il malware li invita a verificare nuovamente il proprio account accedendo a Facebook. E la pagina a cui si viene ridiretti non è quella ufficiale di accesso a Facebook. Attraverso un codice particolare, (WebView), ruba il nome utente e la password di Facebook della vittima e li invia a un server controllato da malintenzionati in via remota.

I ricercatori di Trend Micro avvertono che queste credenziali rubate di Facebook possono in seguito essere riproposte per fornire "malware molto più dannosi" o "accumulare un esercito di zombie sui social media" per diffondere notizie false o generare malware di criptovaluta. Gli **zombie** sono in gergo i computer controllati da terzi all'insaputa dell'utilizzatore e possono "essere risvegliati" per effettuare attacchi su siti e servizi Internet, come i **DDoS**, i Distributed Denial of Service, che fanno collassare i servizi colpiti per le troppe richieste contemporanee di accesso.

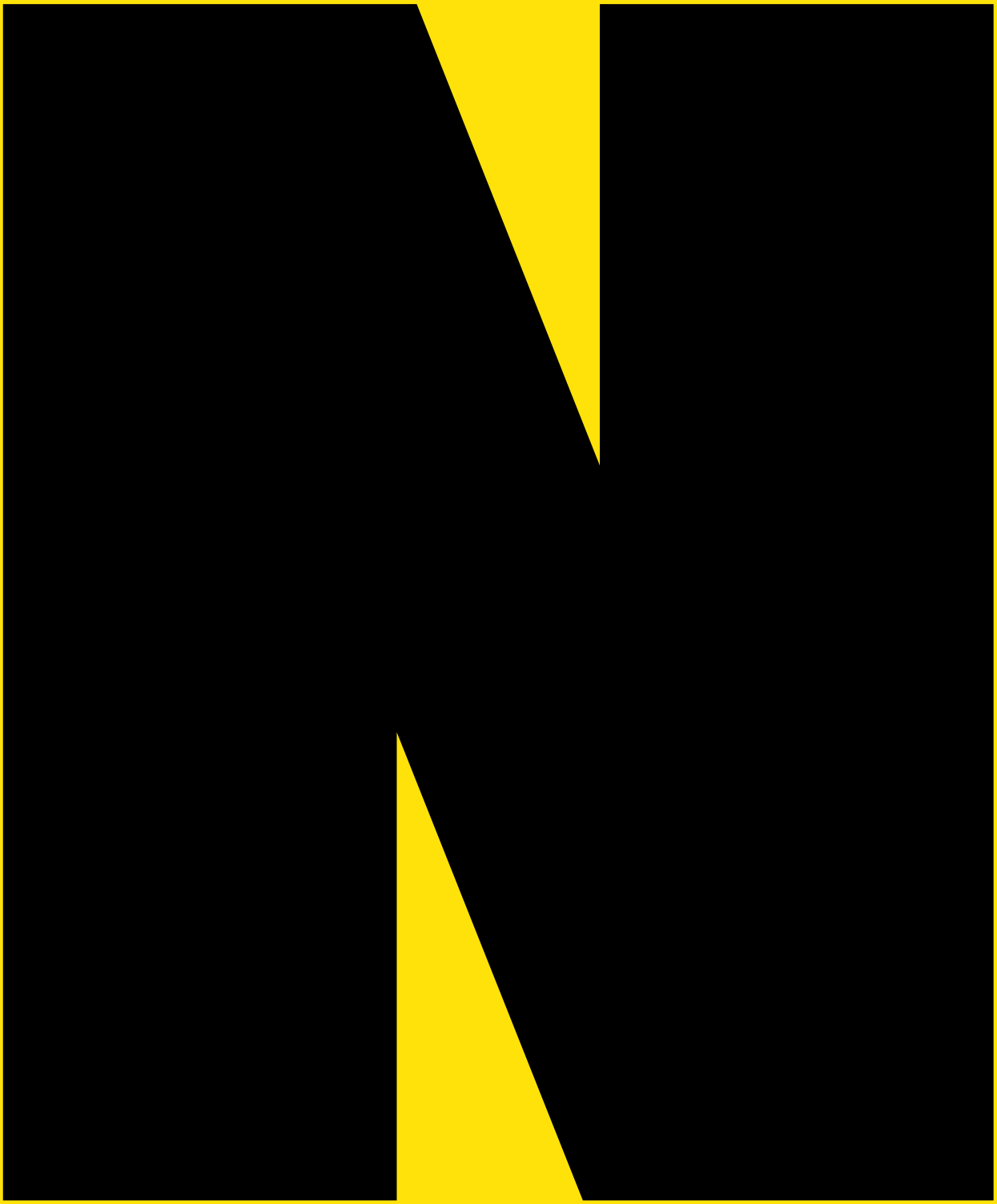
Gli account di Facebook rubati possono anche esporre "una ricchezza di altre informazioni finanziarie e di identificazione personale" che possono poi essere vendute nel Dark Web, quella porzione del web non indicizzata dai comuni motori di ricerca e composta di siti accessibili solo con software specifici e più difficili da individuare.

Le due società di sicurezza informatica ritengono che GhostTeam sia stato sviluppato e caricato sul Play Store da uno sviluppatore vietnamita a causa dell'uso considerevole della lingua vietnamita presente nel codice. Secondo i ricercatori, la maggior parte degli utenti colpiti dal malware GhostTeam risiede in India, Indonesia, Brasile, Vietnam e Filippine.

Oltre a rubare le credenziali di Facebook, il malware GhostTeam visualizza anche annunci pop-up in modo aggressivo mantenendo sempre attivo il dispositivo infetto mostrando annunci indesiderati in background.

Le app maligne sono state rimosse da Google dal Play Store ma gli utenti che hanno già installato una di tali app sui propri dispositivi devono assicurarsi di avere attivato **Google Play Protect** che utilizza l'apprendimento automatico e l'analisi dell'utilizzo delle app per disinstallare quelle dannose.

Insomma anche qui il modo migliore per proteggersi è essere attenti a scaricare app anche dai siti ufficiali e verificare le recensioni prima di farlo, sapendo che non guasta avere un buon antivirus sul proprio telefonino.



NEUTRALITÀ

LA NEUTRALITÀ DELLA RETE SPIEGATA A MIA MADRE

Trump ha voluto e ottenuto l'abolizione della neutralità della rete lasciando modificare il precedente regolamento all'uomo che ha messo a capo della Federal Communications Commission. E allora? Beh, la cosa è grossa perché va a intaccare un principio liberale secondo cui l'accesso alla rete uguale per tutti è un diritto fondamentale delle società moderne.

La neutralità della rete è infatti il termine tecnico per dire che "tutti i bit sono nati uguali" e che come tali vanno trattati. Significa cioè che non è possibile discriminare il traffico che passa nei tubi della rete e che quindi non si possono fare differenze per i contenuti che ci passano dentro. Per capirci: la neutralità della rete garantisce che quando uso Internet ho diritto di accedere in egual misura al sito di una pubblica amministrazione o di un quotidiano, di un blog antimafia oppure a Youtube. Viceversa abolire la neutralità della rete significa che potrò creare delle corsie preferenziali a pagamento, ad esempio per farti scaricare velocemente i film da Netflix, farti accedere più velocemente alle mappe di Google o a un sito di scommesse.

A patto che paghi e alla faccia della privacy. È l'abbandono dell'idea di Internet come servizio universale, principio ribadito anche dall'ex premier Paolo Gentiloni.


N

I RISCHI DELL'ABOLIZIONE DELLA NET-NEUTRALITY

Il primo rischio è quindi quello di creare una rete due velocità: l'autostrada per chi paga di più, mettiamo, come Disney e Youporn, e la mulattiera per chi non può farlo, come una startup o un negozietto online. Il secondo rischio è che i fornitori di servizi Internet si intromettano nelle tue scelte quando navighi sul web decidendo di fatto cosa puoi o non puoi fare, rallentandoti.

CONCORRENZA SLEALE

Ma questo è esattamente il principio contrario a quello che ha permesso alla rete internet di svilupparsi. L'assenza di barriere d'ingresso nel mercato della comunicazione online ha permesso la nascita di servizi web, giornali online, siti di e-commerce ugualmente legittimati a farsi raggiungere in rete e con le stesse tempistiche. Un mercato dove la velocità è fondamentale: andremmo ancora su un sito che ci mette troppo tempo a caricarsi? Probabilmente no. Andremmo più volentieri su un sito che ci permette di navigare tra i suoi servizi in un battibaleno? Probabilmente sì.

LA CARTA DEI DIRITTI DI INTERNET

Questo principio sacrosanto della rete delle origini ne ha finora garantito lo sviluppo tanto che, quando è stato proposto di abbandonarlo, il mondo libero si è espresso con una levata di scudi, e poi discussioni, negoziati, forum. Come appunto quelli sulla governance di Internet che in Italia hanno favorito la Carta dei Diritti di Internet per iniziativa della Presidente della camera Laura Boldrini che ha voluto la "Commissione Rodotà": all'articolo 4 la Carta ribadisce l'importanza della net-neutrality per la democrazia e l'economia.

CHE SUCCEDE IN ITALIA E IN EUROPA

Le nuove regole americane in teoria non dovrebbero riguardarci. In Italia, e in Europa, non è possibile discriminare il traffico Internet e creare queste corsie preferenziali. Ma è vero che gli operatori d'accesso già oggi usano sistemi di gestione del traffico, e a titolo d'esempio, quando hanno tanti abbonati collegati nello stesso momento, riducono la disponibilità di banda per ciascuno e quindi la velocità di connessione. Inoltre, come ha osservato il commissario Agcom Antonio Nicita, le regole europee dicono che “gli operatori non possono in alcun modo discriminare il traffico se non su servizi speciali, come la salute e le auto che si guidano da sole, che arriveranno in futuro e che hanno bisogno di una altissima connettività."

Insomma, la deregolamentazione della net-neutrality non ci riguarda nell'immediato. Come dice Paolo Nuti dell'Associazione degli Internet Provider “Il problema potrebbe porsi eventualmente per un fornitore di contenuti italiano o europeo che gioca sul mercato americano."

“Ma non da noi.” dice Joy Marino, pioniere di Internet in Italia. “Il problema non c'è perché in Europa il mercato della connettività è abbastanza concorrenziale, e non c'è questa integrazione verticale tra reti e contenuti, inoltre le direttive europee ci proteggono e l'Agcom misura la qualità dei servizi Internet."

Potrebbe però capitare che un fornitore di connettività diventi anche fornitore di contenuti e a quel punto potrebbe voler penalizzare un concorrente che però viaggia sulla sua rete. Quello sì, sarebbe un problema.

Più pericoloso per ora appare invece il meccanismo dello “zero rating” che ti fa continuare a navigare su certi social quanto ti finisce il credito del traffico dal telefonino, penalizzando i siti per cui non è previsto e portando i consumatori ad assuefarsi a quel tipo di utilizzo della rete. Concorrenza sleale. Sarà sanzionato in base alle regole europee.

Rimane la possibilità che se in Europa si consentisse per legge la limitazione di accesso a siti, pagine e servizi, l'operatore si troverebbe a usare strumenti raffinati che pongono evidentemente un problema di privacy, ma anche di democrazia. È questa la tesi di Stefano Quintarelli, deputato di Area Civica, che ci dice: “Potrebbe anche succedere che un operatore faccia un accordo con Netflix e farti il tappeto rosso per il suo videostreaming e fare l'opposto con la startup neonata con la quale non ha fatto alcun accordo."

Però le grandi piattaforme, gli Over The Top, stanno posizionando i loro servizi nelle regioni dove operano e non ci sarà pericolo di doversi andare a prendere il film in un server in Nevada dove il carrier costa di più.

Il timore di molti è tuttavia che l'abolizione della net-neutrality crei un precedente e rischi di giustificare uguali interventi in paesi autoritari. Lì con la scusa di gestire eventuali congestioni di traffico sarebbe più facile silenziare l'opposizione e il dissenso sul web. Nei paesi democratici invece avrebbe l'effetto di costruire una Internet su base censitaria con la scusa di garantire servizi “essenziali”. Con i fornitori di connettività già pronti a scaricare i costi maggiorati sui propri clienti.

NIS, Network and Information Security directive

Il crimine informatico oggi costa al mondo quasi 600 miliardi di dollari, ovvero lo 0,8% del Pil globale, secondo un rapporto del Centro per gli studi strategici e internazionali (Csis) e McAfee, storica azienda di antivirus.

All'origine del fenomeno ci sono la cattiva progettazione di software e hardware, l'uso di dispositivi non protetti e l'errore umano. Ma la maggior parte degli attacchi è condotta da criminali in cerca di profitto che usano tecniche sempre più sofisticate per raggirare le vittime e superarne le difese.

N

Akamai Technologies, ad esempio, ha rilevato un incremento nel numero di malware che utilizzano dispositivi infetti per produrre di nascosto cryptovalute e che gli autori di malware stanno attaccando le credenziali di accesso dei social media, oltre ai dati finanziari.

In base a una ricerca di Kaspersky Lab, nel primo trimestre del 2018 gli attacchi che bloccano siti e computer rendendoli irraggiungibili (DDoS) tramite reti di computer zombie comandate da remoto (le botnet) hanno colpito le risorse online di 79 paesi. Nella lista dei 10 paesi da cui partono ci sono tre new entry europee: Italia, Germania e Regno Unito.

Secondo il Data Breach Report di un'altra azienda, Verizon, i settori nel mondo più colpiti sono quello dell'Istruzione con attacchi di «social engineering» che mirano all'estorsione di dati personali e furti d'identità; il mondo della Finanza e delle Assicurazioni con la clonazione di carte di credito e la tecnica del «bancomat jackpotting», dove un software comanda illecitamente al bancomat di emettere denaro; la Sanità con attacchi mirati ai dati clinici da rivendere al mercato nero; Editoria e Informazione con attacchi DDoS; il Settore pubblico dove il 43 per cento delle violazioni ha come scopo il **cyberspionaggio**.

A leggere il rapporto dell'associazione Clusit, in Italia il solo cybercrime vale 10 miliardi all'anno e ogni cinque minuti, secondo Fastweb, un nostro connazionale è vittima di reato informatico.

Dopo varie vicissitudini l'Italia ha recepito la Direttiva europea sulla protezione delle reti e dei servizi informatici nota come Direttiva NIS (*Directive on Security of Network and Information systems*).

Emanata il 6 luglio del 2016, prevede una serie di obblighi per la sicurezza cibernetica di ogni paese europeo e di assicurare la continuità dei servizi essenziali quali energia, trasporti, salute, finanza, dei servizi digitali come motori di ricerca, servizi cloud, piattaforme di commercio elettronico; l'adozione di misure tecnico-organizzative per ridurre il rischio e limitare l'impatto di incidenti informatici e l'obbligo di notifica di incidenti che impattino sulla fornitura dei servizi e le relative sanzioni.

Il testo prevede anche l'istituzione presso la Presidenza del Consiglio dei Ministri di un unico centro di risposta alle emergenze informatiche, il CSIRT italiano, che andrà a sostituire gli attuali CERT Nazionale e CERT-PA.

Facciamo un passo indietro per capirci. La NIS, la Network and Information Security Directive, nelle intenzioni dei legislatori è un insieme di dispositivi normativi che dovrebbero assicurare la continuità operativa nella fornitura di servizi essenziali nel campo dell'energia, dei trasporti, in quello bancario e finanziario, ma anche nella fornitura e distribuzione di acqua potabile e delle infrastrutture digitali, dell'e-commerce, dei motori di ricerca e del cloud computing: cioè la continuità dei servizi necessari a un normale funzionamento delle società moderne. Di quei servizi si parla anche nei termini di «infrastrutture critiche», proprio perché un loro malfunzionamento potrebbe causare danni molto seri al commercio, all'industria, alla sanità, alla democrazia.

Pensate infatti cosa accadrebbe se un attacco informatico bloccasse a terra tutti gli aeroplani di Fiumicino, oppure interrompesse l'erogazione di energia

elettrica in una città come Milano o bloccasse i cellulari a Napoli.

Ecco, la direttiva identifica gli operatori di questi servizi essenziali che devono attuare misure tecnico-organizzative «adeguate» alla gestione di questo tipo di rischi e alla prevenzione degli incidenti informatici.

Che di questo ci sia un gran bisogno è sotto gli occhi di tutti visto che ogni giorno si moltiplicano gli allarmi dei danni derivanti dal cybercrime, dallo spionaggio cibernetico e dalla compromissione della supply chain di industrie grandi e piccole.

E allora torniamo a noi. L'elenco riguarda gli Operatori dei Servizi Essenziali e i Fornitori di Servizi Digitali, ma le «autorità competenti NIS» sono cinque Ministeri: Sviluppo economico, Infrastrutture e trasporti, Economia, Salute e ambiente. Il Ministero dello sviluppo economico deve occuparsi dei settori energia, infrastrutture digitali e dei fornitori di servizi digitali; quello delle Infrastrutture e trasporti, deve occuparsi appunto dei trasporti; Economia e finanze si occupa dei settori bancario e finanziario; Salute e Ambiente indovinate un po' di che si occupano? L'elenco, secretato per motivi di sicurezza, è stato fatto sulla base dell'importanza del servizio fornito alle attività socio-economiche, della dipendenza da reti e sistemi informativi e per la rilevanza sul servizio degli effetti di un eventuale incidente. In Italia sono stati identificati 465 operatori di servizi essenziali.

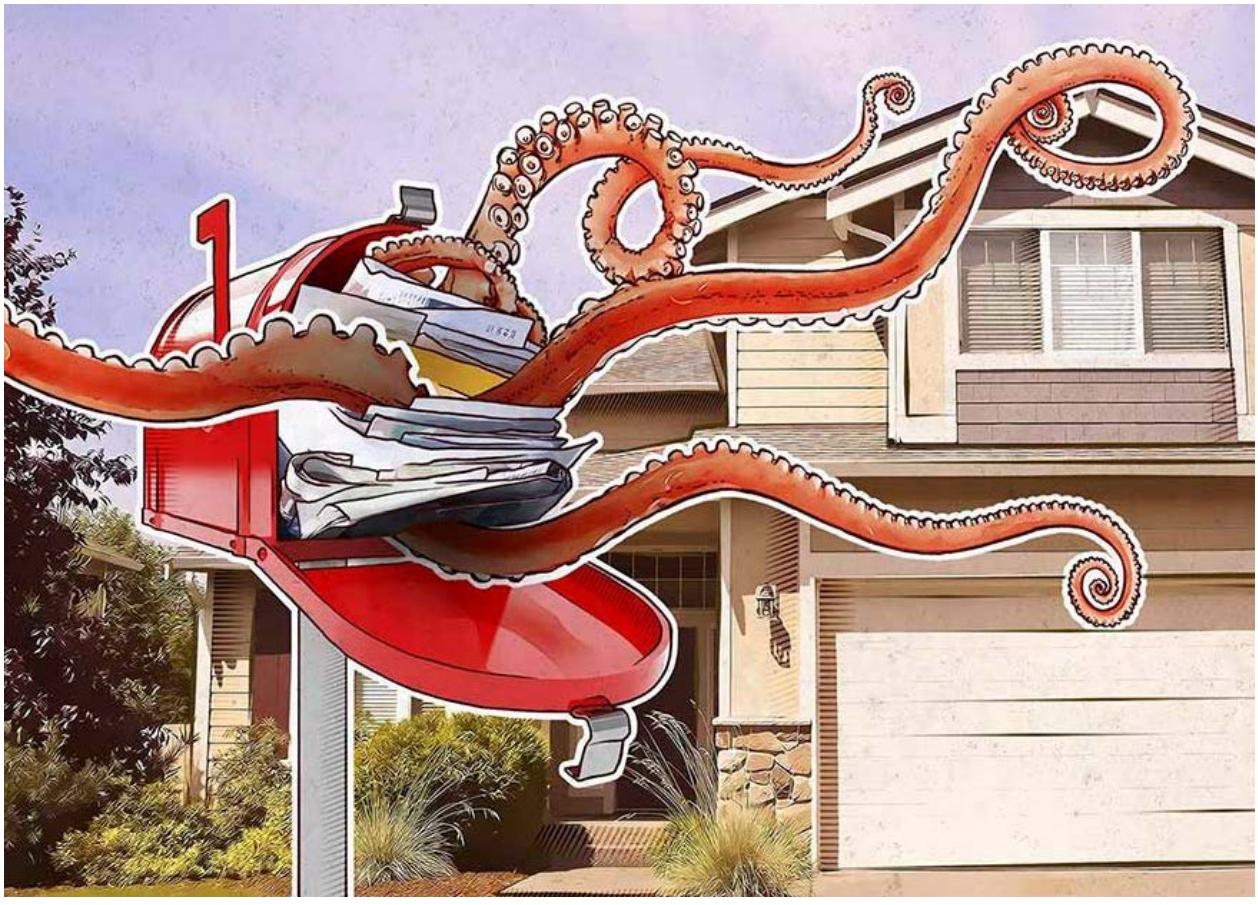
PHISHING

COME PROTEGGERSI DA CHI TI ENTRA DENTRO LA MAILBOX E TI AZZERA LA PASSWORD

Il **phishing** è una tattica fraudolenta di sottrazione delle informazioni personali online. Il suo scopo è indurre gli utenti in rete a fornire password e altri dati sensibili a siti web che sembrano legittimi ma che non lo sono. Più spesso il phishing ha la forma di una email che richiede di fornire informazioni private o di cliccare su link e allegati in grado di installare un virus all'interno di smartphone e pc.

Il phishing è in genere utilizzato dai cyber-criminali per rubare informazioni fiscali e bancarie, come è successo in Italia con finte comunicazioni dell'Agenzia delle Entrate, ma può essere usato anche a fini di spionaggio.

Il Citizen Lab di Toronto, ad esempio, ha indagato su molti casi in cui il phishing è stato utilizzato contro giornalisti, attivisti



e operatori umanitari da parte di gruppi che cercano di spiarne le attività. Il motivo è ovvio: attraverso i nostri account inviamo rapporti e resoconti, documenti legali, comunicati, liste di luoghi e di persone.

Succede in Tibet, dove gli oppositori al regime di Pechino sono bersaglio di uno spionaggio digitale decennale. La cosa funziona così. L'attivista per i diritti umani riceve un'email che sembra inviata da un membro della comunità tibetana che afferma di volere condividere le bozze di un logo da usare su un sito web d'opposizione. Ma i file allegati sono in realtà collegamenti a un sito web che somiglia a Google Drive. Una volta cliccato sui file si viene indirizzati a una finta pagina di accesso a Google dove il nome utente e la password vengono trasferiti agli spioni prima che la vittima sia reindirizzata al sito legittimo. Da quel momento in poi gli spioni possono accedere all'account della vittima e rubare informazioni preziose.

Nel corso del 2017 attivisti, avvocati e giornalisti in Egitto sono stati presi di mira da una campagna di phishing su larga scala che ha coinvolto quasi cento indirizzi implicati in una causa tra il governo egiziano e alcune organizzazioni non governative. Le email di phishing sembravano provenire da servizi come Dropbox e Google e menzionavano fatti rilevanti per convincere i destinatari a fare clic sui link proposti per ulteriori informazioni.

Questo tipo di phishing che emula un servizio legittimo si chiama “Angler Phishing” cioè “Rana pescatrice”, proprio a ricordare la funzione dell'esca davanti alle fauci del pesce predatore.

A dicembre 2016, Azza Soliman, avvocatessa egiziana che assiste molte donne in casi di **tortura, detenzione arbitraria**, **violenza domestica e stupro**, è stata arrestata a casa sua. Dopo l'arresto, mentre veniva interrogata dalla polizia, alcuni dei suoi colleghi ricevevano un'email che sembrava una notifica di Dropbox per condividere il documento del mandato di cattura di Soliman, ma non lo era. Cliccando il link si accedeva a una pagina di phishing che rubava login e password.

Sfruttando questa tecnica i malviventi possono operare su tutti i servizi per i quali abbiamo commesso l'errore di usare la stessa email e la stessa password per autenticarci: social network, servizi di prenotazione turistica, siti di gaming online. Con email e password possono resettare l'accesso a questi servizi lasciandoci fuori.

Il consiglio è pertanto di prestare grande attenzione a tutte le email che si ricevono e ai link contenenti. Passandoci sopra col mouse si vede l'indirizzo esatto, ma a volte l'indirizzo è offuscato e si viene tentati di cliccarlo lo stesso. C'è un modo per proteggersi: usare la cosiddetta autenticazione a due fattori che richiede una sorta di seconda password per accedere l'account.

Phishing e credential stuffing

Multe, conti, fatture: la maggior parte delle email di *phishing* ha come oggetto una richiesta di pagamento. In genere si presentano così: «Ti ricordi della fattura?»; «Ti abbiamo affidato una nuova attività»; «Mancato pagamento». Ma se si clicca sull'allegato o sul link per le informazioni inviate, in genere si viene infettati da software che rubano dati, trasferiscono documenti, attivano funzioni remote e la giornata diventa un incubo.

Secondo Sophos, il 41% delle aziende subisce attacchi di phishing ogni giorno e circa il 30% delle email di phishing viene aperto. Nelle aziende, il reparto contabilità è quello più attaccato dai cyber criminali, seguito dal top management.

Secondo un altro leader nel mondo della sicurezza informatica, Akamai technologies, i siti di gaming e gambling sono diventati un bersaglio privilegiato dai criminali.

I dati di alcune ricerche mostrano che ogni anno i publisher di videogiochi perdono più del 40% dei loro profitti a causa della criminalità informatica.

Alla base di questi attacchi c'è il *credential stuffing*.

Il credential stuffing presuppone il furto degli account degli utenti di un determinato sito e l'implementazione di una serie di bot per tentare l'accesso con questi dati a numerosi altri siti. Il numero di credenziali rubate (username, mail e relative password) è nell'ordine di miliardi.

Secondo la Gambling Commission inglese, ogni scommettitore online ha una media di quattro account e, dato che tre persone su quattro tendono a duplicare le password, il credential stuffing rappresenta un rischio molto serio.

Nel frattempo aumenta l'uso di fotocamere e di stampanti "intelligenti" per il lancio di attacchi da negazione di servizio, i DDoS, attacchi che interrompono normali servizi Internet e che possono essere motivati dalla protesta politica, sociale o dalla vendetta personale. Secondo Alexey Kiselev di Kaspersky Lab, «nella maggior parte dei casi questo tipo di attacco viene portato avanti per scopi economici: per questo motivo i cybercriminali, di solito, prendono di mira aziende e servizi che producono molti guadagni. Le somme di denaro guadagnate grazie a un'estorsione o a un furto possono ammontare anche a milioni». Ad esempio, in Giappone sono state utilizzate 50.000 telecamere di videosorveglianza per sferrare attacchi DDoS.

In base alle stime di Cybersecurity Ventures, **nel 2021 la lotta al cybercrime costerà alle aziende più di 6.000 miliardi di dollari all'anno e ci saranno 3,5 milioni di posti di lavoro vacanti nella sicurezza informatica**.

Questo dato è confermato da una ricerca del Ponemon Institute nella quale il 57% degli intervistati ha dichiarato di non riuscire a reperire il personale qualificato necessario per implementare

gli strumenti per l'automazione della sicurezza. «Mentre i cybercriminali continuano ad automatizzare gli attacchi, le organizzazioni devono fare i conti con team preposti alla sicurezza sottodimensionati, processi manuali, sistemi eterogenei e policy complesse che li costringono a dedicare tempo ad attività di basso livello».

L'innovazione tecnologica è quindi fondamentale ma la formazione degli operatori è insostituibile.

Scuole, università e consorzi si stanno attrezzando per colmare l'assenza di professionisti nel settore ma non basta. Bisogna considerare che anche la formazione degli utenti è fondamentale. È ora di pensare a un «maestro Manzi» della cybersecurity, uno che come lui nella Rai degli anni sessanta possa alfabetizzare gli di oggi italiani alla sicurezza informatica.

PHISHING & SMISHING

2018. Secondo una ricerca di Kaspersky Lab e Arlington Research condotta su 7.000 cittadini di sette nazioni europee tra cui l'Italia, abbiamo ormai perso il controllo dei nostri dati online: il 64% non conosce tutti i luoghi del web dove sono stati archiviati i propri dati personali e il 39% dei genitori intervistati non sa nemmeno quali dati vengono condivisi online dai propri figli. Il 57% si sente spaventato e stressato dalla possibilità che i propri dati finanziari vengano violati.

Solo il 36% crede che i dati siano effettivamente protetti sui social media e infine l'88%, si preoccupa del possibile uso illegale dei propri dati.

Hanno ragione. Secondo voi da dove vengono i numeri di telefono per le truffe via Sms e le email per il phishing?

McAfee Mobile Research ad esempio ha scoperto campagne di SmiShing, phishing via Sms, che inducono gli utenti a scaricare applicazioni fasulle di messaggistica vocale, denominate Android/TimpDoor dove la vittima riceve un Sms con un link che se cliccato la indirizza su una pagina web fasulla per scaricare l'applicazione e ascoltare messaggi vocali fasulli.

Scaricata l'applicazione, però, il malware si impossessa di informazioni come l'ID del dispositivo, la marca, il modello, la versione del sistema operativo, l'operatore mobile e l'indirizzo IP pubblico/locale, diventando una backdoor per i criminali che possono così accedere alle reti domestiche degli utenti. Solo negli Usa sono stati infettati 5000 dispositivi in sei mesi.

Dal canto loro, i ricercatori di Kaspersky Lab hanno rilevato nei 12 mesi precedenti vari cyberattacchi rivolti a 131 università in 16 paesi alla ricerca di credenziali di dipendenti e studenti, dei loro indirizzi IP e dei dati sulla loro posizione. Nella maggior parte dei casi analizzati, è stata creata una pagina web fasulla dei sistemi digitali universitari, a prima vista identica a quella legittima, per favorire l'inserimento di login e password.

È successo al dominio uniroma1.it, quello dell'Università Sapienza di Roma, il più grande ateneo d'Europa. I cyber-criminali sfruttano la somiglianza grafica tra i domini «.it» (italiani) e «.lt» (lituani) per inviare email fasulle e portare le vittime su siti clone di quelli istituzionali universitari e rubare le credenziali a chi c'è cascato.

Si tende a pensare che ai cybercriminali facciano gola le credenziali dei dipendenti delle banche o le password di manager e lavoratori, ma gli account personali degli studenti e dello staff delle università potrebbero rivelarsi ancora più preziosi: i loro database contengono molte ricerche uniche e d'impatto, dall'economia alla fisica nucleare.

Inoltre, poiché molti degli studenti collaborano con importanti aziende per i dottorati di ricerca, gli autori delle minacce potrebbero accedere a dati che contengono competenze esclusive e informazioni private potenzialmente compromettenti per le aziende sponsor.

P

POSTA ELETTRONICA

GMAIL, QUANDO LA TUA POSTA NON È LA TUA

Nell'Ottobre del 2018 Google ammette che aziende terze possono leggere i contenuti della posta elettronica dei suoi utenti. Google infatti consente a centinaia di aziende di eseguire la scansione degli account Gmail di tutti noi, leggerci la posta e persino condividerne i dati con altre aziende, «fintanto che sono trasparenti con gli utenti su come stanno utilizzando i dati». A confessarlo è stata Susan Molinari, vicepresidente per le politiche pubbliche di Google, con una lettera di risposta ai senatori americani che l'hanno interpellata in proposito.

La lettera di Molinari, repubblicana moderata e ben agganciata a Washington, risale al 20 settembre 2018 quando il Wall Street Journal ha potuto renderla nota. Mentre eravamo tutti distratti dal baco che avrebbe consentito la perdita dei dati di 500 mila utenti da Google+, il suo social network, nella lettera Molinari ammette che Google consente agli sviluppatori di app di accedere alle caselle di posta di milioni di utenti, ma che Google stessa ha smesso di farlo dal 2017 dopo una class action che l'accusava di intercettazione illegali.

Però ha ammesso che dipendenti umani hanno letto personalmente migliaia di email per aiutare ad addestrare i sistemi di intelligenza artificiale che adesso lo fanno al posto loro. Gli sviluppatori di app possono accedere ai dati di Gmail, inclusi nomi, titoli, testi, per offrire servizi come confronto dei prezzi, pianificazione di viaggi e ricerche di mercato.

La maggior parte delle operazioni di scansione viene eseguita dai computer, ma alcuni vengono eseguiti da impiegati umani che li utilizzano per verificare se l'intelligenza artificiale sta svolgendo il proprio lavoro, che è quello di raccogliere i dati per gli operatori di marketing. Eppure Molinari ha difeso questa pratica affermando che Google chiede a ogni sviluppatore di rispettare i «dati sensibili» degli utenti e di sospendere le app non trasparenti col pubblico. «In aggiunta devono dimostrare che stanno proteggendo i dati degli utenti dagli hacker (!)».

Google, che ha aperto un safety center, un centro sicurezza in sei paesi, Italia compresa, continua però a scansionare le email per consentire agli utenti di cercare quello che gli serve nelle loro caselle di posta, rilevare spam e malware e generare suggerimenti con la nuova funzione di risposta automatica. E utilizza anche dati di altre fonti per personalizzare le sue inserzioni. «Nessun essere umano su Google legge la posta Gmail degli utenti», ha detto Molinari, «tranne in casi molto specifici in cui danno il consenso o dove è necessario per motivi di sicurezza, come ad esempio l'investigazione di un bug o abuso».

Insomma, la tua posta non è tua. Interpellato a questo proposito il Garante Privacy italiano ha dichiarato che «Come lo scandalo Cambridge Analytica, anche il caso degli accessi ai contenuti degli account Gmail concessi a terze parti dimostra ancora una volta la natura di business company dei colossi della rete.

Nell'odierno neo capitalismo estrattivo i dati di milioni di utenti vengono sfruttati come una miniera da sviluppatori, società di ricerche, aziende di marketing, società di servizi di ogni genere. Ma contro questi abusi il nuovo Regolamento europeo della privacy (*GDPR, ndr*) rappresenta oggi un formidabile strumento per proteggere gli utenti».

PRIVACY

IL RE DEL MONDO CHE NON RISPETTA LA TUA PRIVACY

P come Privacy. Che non c'è. Almeno quando a gestire ogni risvolto della tua vita ci pensano Google, Amazon, Facebook e Co. Già, la privacy, un concetto di origine anglosassone accostabile a termini come "privatezza" e "riservatezza", nasce dal saggio di due avvocati, "The right to privacy" con l'idea di bilanciare i diritti della persona contro l'invadenza della tecnologia più moderna dell'epoca, la fotografia, perché uno dei due, Samuel Warren, era stufo di vedere la moglie salottiera sulle prime pagine dei giornali in situazioni decontestualizzate rispetto ai fatti di cronaca. Era il 1890. Entrata nell'ordinamento giuridico italiano sull'onda delle proteste operaie con la legge 300 del 1970, il famoso Statuto dei Lavoratori, con l'articolo 4 che vietava i controlli a distanza - di cui il Jobs Act ha fatto scempio - la Privacy è stata costituzionalizzata nella Carta di Nizza nel 2007. Divenuta diritto fondamentale dell'Unione Europea, della privacy è stata fatta strame da telefoni che fanno foto, app e social network.

Ma parliamo di Facebook. Messo con le spalle al muro per lo scandalo di Cambridge Analytica, il suo presidente e fondatore Mark Zuckerberg, davanti alle commissioni parlamentari del Congresso ha risposto da scolaretto stralunato alle domande via via meno banali dei politici che non vogliono ammazzare nella culla la creatura più importante del soft power americano, proprietaria anche di Messenger, WhatsApp e Instagram.

Domande sbagliate, che Marc Rotenberg dell'Electronic Privacy Information Center, sostiene andrebbero rifatte: non si deve chiedere a Mark se c'è stato un uso illecito dei dati, ma cosa Facebook ci fa ogni giorno e quali consegna ad altre società senza dirlo; non si chieda a Mark cosa bisognerebbe fare, ma perché non ha fatto quello che gli era già stato chiesto dal governo: garantire la privacy degli utenti. Una piattaforma come Facebook che traccia e profila gli utenti e gestisce le nostre identità lo fa sicuramente per offrirci un servizio migliore, ma questo servizio perché è gratis? Chi lo paga? Come fa Zuckerberg a guadagnarci se non dando in pasto agli inserzionisti dati dettagliati su etnia, colore, età, sesso, stili di vita e scelte commerciali dei suoi utenti?

Alla fine Zuckerberg ha dovuto ammettere che Facebook è una media company, aprendoci un mondo: dovrà soggiacere alle loro stesse regole, anche nelle competizioni politiche. Ma non ha ancora ammesso che il problema della manipolazione dei dati a fini politico-elettorali riguarda tutti gli utenti Facebook.

A proposito, i servizi segreti italiani ci avevano avvertito di potenziali furti di dati usati per influenzare il voto proprio nella relazione consegnata al Parlamento il 20 Febbraio 2018.


P

Riappropriarsi dei propri dati

Gli scandali relativi all'uso improprio dei nostri dati personali sono destinati a continuare. Non li conosceremo mai tutti quanti, non ci saranno sempre audizioni parlamentari a imbarazzare chi non ha vigilato sulla nostra privacy, e non ci sarà sempre la stessa copertura mediatica dell'affaire Cambridge Analytica, perciò è bene correre subito ai ripari.

I dati sono il petrolio della società dell'informazione e sotto forma di profili personali e big data sono le miniere da cui le aziende high tech estraggono il plusvalore che gli consente di orientare politiche e consumi. Ma, senza fare troppi discorsi, è bene ricordare che dalla cattiva gestione dei dati in possesso delle piattaforme a vedersi negata l'assunzione o bloccato un affare il passo è breve.

Dopo gli scandali Facebook ha attivato una funzione speciale per recuperare tutti i dati che ci riguardano. E gli altri? Come si sono regolati? Come facciamo a sapere che uso fanno dei dati che produciamo?

Per sapere subito cosa sanno di noi i singoli siti che usiamo, da Linkedin a Starbucks, da Instagram a TripAdvisor, da Ikea a GoogleMaps, oggi è possibile consultare una sorta di metasito dal nome evocativo: *My Data Request*. Il sito contiene un link alle app o ai siti web a cui abbiamo consegnato negli anni i nostri dati personali e cliccandoci sopra diventa facile richiedere l'archivio dei dati che ci riguardano in maniera compatibile con le leggi vigenti.

My Data Request offre anche di più. Dopo aver analizzato le pratiche di gestione della privacy e le regole legali di circa cento app e portali ha predisposto una serie di lettere standardizzate che possono essere usate per richiedere i dati in archivio senza ricorrere a un avvocato. Per gli europei le lettere sono formulate in base alla normativa europea sul trattamento dei dati, la GDPR, e contengono domande circa le finalità del trattamento; le categorie di dati personali interessati; a chi saranno comunicati; il periodo di conservazione, eccetera.

Informazioni importanti, perché se in alcuni casi si tratta di dati come l'email e altri dati identificativi quali l'età, il sesso, il paese di provenienza, in altri parliamo di foto, chat e download. In certi casi poi si tratta di metadati, cioè i dati che definiscono le relazioni tra i dati stessi: dove, come, quando, con chi, per quanto tempo abbiamo fatto questo o quest'altro. Spesso queste informazioni sono già organizzate come profili che ci identificano in base a gusti, tendenze e attitudini ed è giusto sapere se esistono e come vengono gestiti.

Il sito **My Data Request** offre insomma un modo semplice e veloce per capire quali dati vengono raccolti su di noi, dove e come è possibile scaricare tali dati per sapere in dettaglio quali e quante informazioni personali ogni determinata azienda con cui abbiamo interagito possiede su ciascuno.

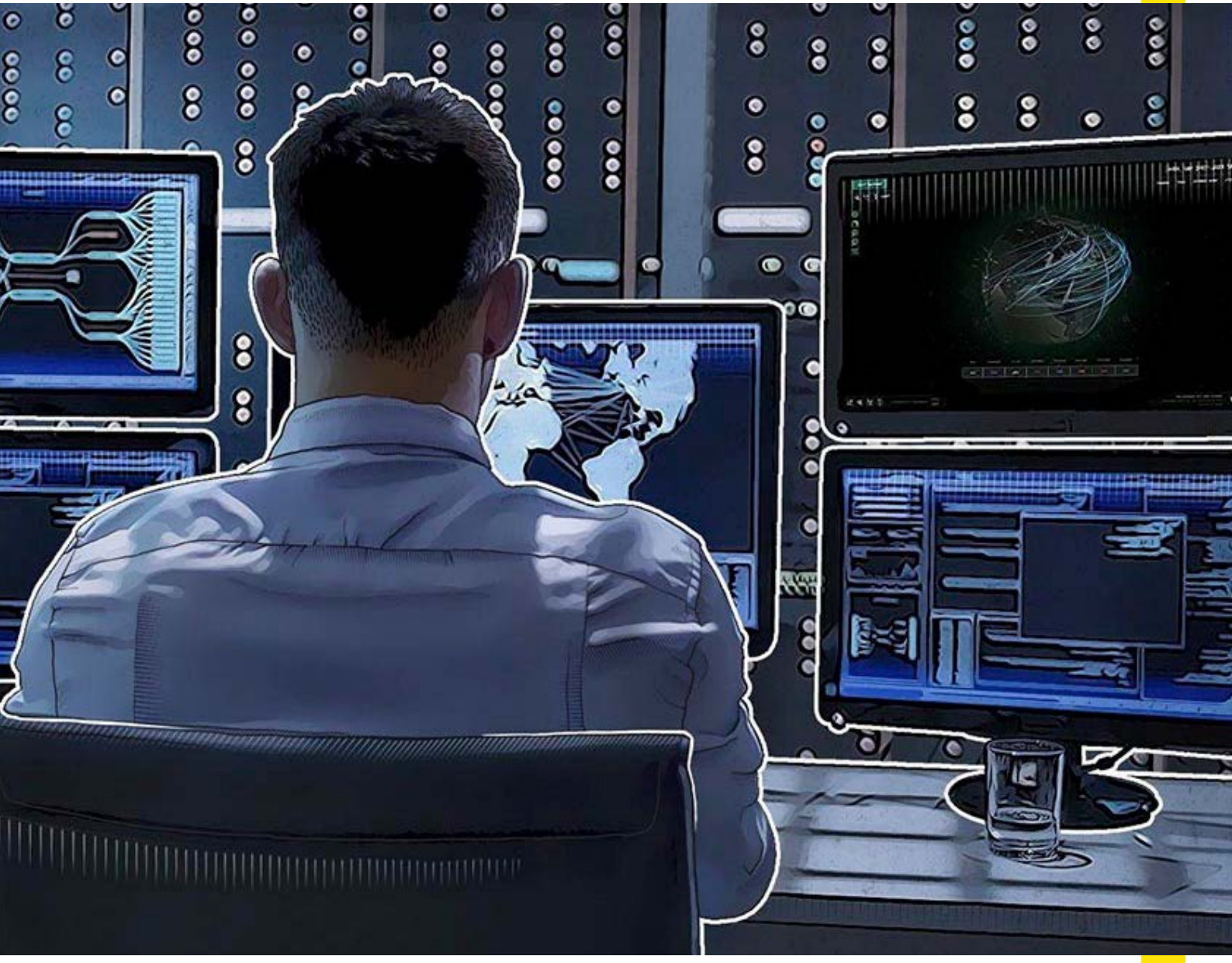
Il sito offre anche un comodo motore di ricerca interno per verificare la presenza nel loro database dell'azienda che vogliamo interpellare.

Molte di quelle censite, come Badoo, Skype e DropBox, purtroppo sono state bucate nel passato da hacker malevoli che hanno poi condiviso profili e account nel web profondo, e questo significa che quelle aziende non sono le sole ad averli. Altre hanno a che fare con giochi online per bambini e adolescenti, da Angry Birds al successo del momento, il videogame sparatutto Fortnite.

Per questo motivo il sito può essere usato anche per fare un'altra semplice verifica: che cosa queste aziende sanno dei nostri figli.

PROPAGANDA COMPUTAZIONALE

LE GUERRE DEL FUTURO SI COMBATTERANNO NEI NOSTRI CUORI



Le agenzie militari e di intelligence di tutto il mondo conducono da tempo guerre informative segrete nel cyberspazio. I meme delle loro psy-ops, le operazioni di disinformazione, influenzano profondamente le percezioni pubbliche della verità, del potere e della legittimità. La campagna del presidente Trump e il ruolo di Cambridge Analytica sono finiti sotto osservazione per il microtargeting, il dark advertising e le fake news, ma non sono state solo le elezioni presidenziali americane del 2016 a essere caratterizzate da un mix di notizie false, intromissioni straniere, attacchi informatici e propaganda social.

Uno studio dell'Università di Oxford ha rilevato campagne di manipolazione dei social network in almeno 28 paesi dal 2010. Lo studio ha anche evidenziato che "i regimi autoritari non sono gli unici né i migliori nella manipolazione organizzata dei social media". Già nel 2014 il World Economic Forum definiva la diffusione della disinformazione online una tendenza significativa da tenere sotto osservazione.

Questa minaccia si sta intensificando man mano che gli strumenti di Intelligenza Artificiale (IA) diventano più ampiamente disponibili.

I ricercatori di IA hanno dimostrato di poter creare tecnologie in grado di produrre audio e video falsi non rilevabili e secondo uno studio dell'Università di Stanford fra breve sarà estremamente facile creare inganni digitali di alta qualità la cui autenticità non potrà essere facilmente verificata. Da qui l'allarme dell'ex advisor di Bush e Obama per la cybersecurity, David Edelman, che ci ha messi in guardia dalla propaganda basata sulla manipolazione della voce e della mimica facciale di personalità influenti, compresa la posizione e la rotazione della testa in 3D.

Li chiamano Deep fake videos, e sono, come dice il nome, video profondamente falsi, cioè mai girati da nessuno. Con le tecnologie basate sull'intelligenza artificiale è infatti possibile mettere in bocca a un capo di stato, in possesso della valigetta atomica, parole che non ha mai pronunciato e innescare una crisi internazionale una volta che il messaggio sia diventato di dominio pubblico. Basta un sapiente uso di Youtube e Facebook prima e dei media locali dopo che non sono in grado di verificare autenticità di fonti e protagonisti.

Perciò, nonostante l'uso di "intelligenze artificiali difensive", capaci di individuare lo sfasamento tra le parole pronunciate e il colore del volto irrorato dal sangue in maniera non compatibile con il parlato, capaci quindi di individuare i fake, il danno potrebbe già essere stato fatto. E questo perché nella propaganda digitale la diffusione intenzionale di paura, incertezza e dubbi sarà iper-mirata a specifici utenti di Internet capaci di influenzare ampi target della popolazione. Come? Agendo attraverso la propaganda computazionale che sfrutta i social media e la credulità di chi li abita, la psicologia umana che non distingue la realtà dalla finzione, le voci e i pettegolezzi tanto cari ai cospiratori e gli algoritmi per manipolare l'opinione pubblica. Il futuro della guerra non è sul campo di battaglia, ma sui nostri schermi.

PROTONMAIL

PROTONMAIL, UNA "SICUREZZA ATOMICA"

P come password. La password del telefonino, del computer, del social network preferito, è sempre la prima linea di difesa contro chi vuole trasformare in un incubo la nostra vita digitale. E questo vale soprattutto per l'email. A patto che sia una email sicura, come ProtonMail, ad esempio. ProtonMail è un servizio di posta elettronica cifrata inventato nel 2013 al Centro di ricerche nucleari di Ginevra, il Cern, per consentire, grazie all'uso della crittografia, l'uso di un sistema di posta più affidabile di quelli gratuiti come Gmail, Hotmail e Yahoo! (gli ultimi due sono i più bucati al mondo).

A capo del progetto c'è un'intera community di scienziati e attivisti per la privacy: basato su software open source, ProtonMail è facile da usare e ha un design moderno. I suoi server di posta si trovano nella neutrale Svizzera e il modello di business è basato sulle donazioni e i micropagamenti anziché sulla pubblicità o sulla vendita dei nostri dati personali. Per il singolo utente la prima casella di posta è gratuita, le altre e i servizi aggiuntivi sono a pagamento per pochi euro.

Di certo la nostra sicurezza vale questo piccolo prezzo. Ma se volete usare ancora una di quelle email gratuite che funzionano tanto bene fate pure, però chiedetevi sempre: perché posso usare una email tale e quale al mio nome e avere a disposizione fino a 500 mega di spazio gratis? Se avevate già sentito parlare di **microtargeting** e di intelligenze artificiali che leggono il contenuto di email presunte private vi siete già risposti.

Da quando la posta elettronica è stata inventata nel 1971 da un rubicondo ingegnere newyorkese di nome Ray Tomlinson, il volume delle email prodotte non ha mai smesso di crescere, nonostante la diffusione delle chat al computer e al telefonino.

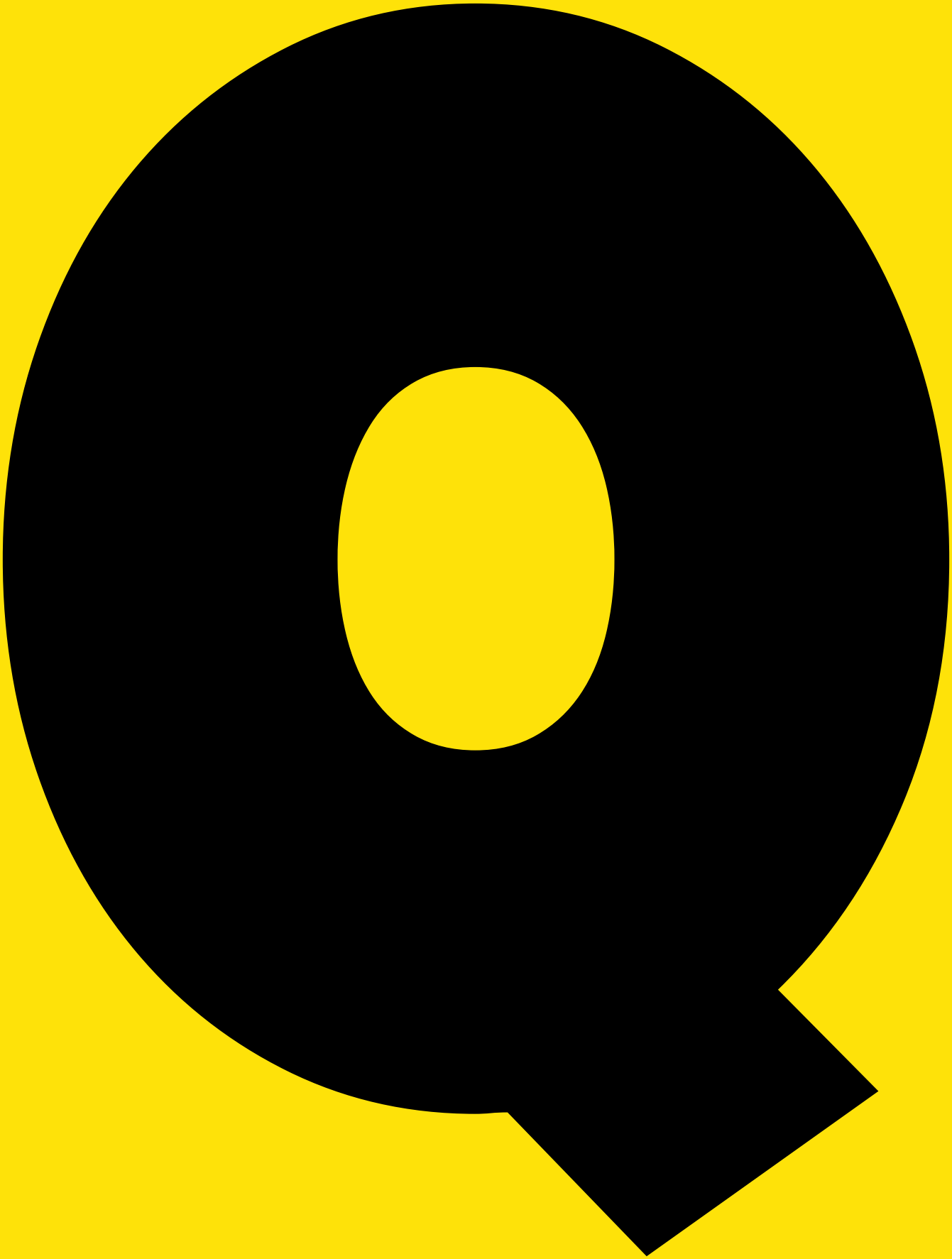
Chi si occupa di fare statistiche sostiene che nel mondo vengono inviate circa 269 miliardi di email al giorno, comprese quelle di **spamming** (la posta indesiderata che prende il nome da una carne in scatola ingiustamente accusata di essere di scarsa qualità, la carne SPAM).

Con l'indirizzo email ci si registra a un evento, si prenota l'albergo, si parla col medico, il commercialista o l'avvocato. La protezione dell'email è quindi fondamentale. Nei siti del Deep Web che non si trovano neanche con Google giace ancora un enorme database di username e password di circa un miliardo e mezzo di account che si chiama **Antipublic** ed è pieno zeppo di email e password di italiani più o meno famosi: politici (900) e giornalisti (un migliaio). Molti degli account sono ripetuti per la cattiva abitudine di usare sempre la stessa email e la stessa password per registrarsi e accedere a Facebook come a Twitter, a

Booking o TripAdvisor, a Dropbox, Adobe o Youporn. É il fenomeno noto come '**password reuse**'.

Per sapere se la vostra email è stata hackerata in qualcuno dei **databreach** più importanti degli anni scorsi come quelli di LinkedIn, DropBox, Yahoo! andate sul sito Have I Been Pwned? (Sono stato fregato?) e fate la prova. Se scoprite di essere finiti nel mucchio non prendetevela, come abbiamo detto, c'è cascato anche Mark Zuckerberg che usava le stesse credenziali per Twitter e LinkedIn.

Torniamo a ProtonMail: se usate l'app di ProtonMail dal telefonino sappiate che anche la rubrica dei contatti è crittografata: significa che è ancora più difficile per un cyber-criminale scoprire con chi vi scrivete.



176 QWANT

QWANT

COME FUNZIONA QWANT, IL MOTORE DI RICERCA CHE RISPETTA LA PRIVACY

Qwant

Qwant è il nome di una società francese che fornisce l'omonimo motore di ricerca finanziato con **25 milioni di euro dalla Banca Europea degli investimenti**. Ed è anche il motore di ricerca consigliato da Anonymous. Il motivo è presto detto: Qwant non traccia gli utenti e rispetta la loro privacy.

Fondata nel 2011 da **Jean-Manuel Rozan**, esperto di finanza, ed **Éric Leandri**, specialista di cybersecurity, la sede principale della società si trova a **Parigi**, il suo dipartimento di sicurezza a Rouen, mentre lo sviluppo del software viene fatto a Nizza.

Il motore di ricerca vero e proprio è stato lanciato agli inizi del 2013 e adesso è stato integrato in Firefox, il browser di Mozilla Foundation. È disponibile anche come semplice **add-on** per chi ha già installato Mozilla sul proprio PC.

Il nome Qwant è una crasi tra Quantity (Q), e Wanted (want). La "Q" indica la quantità di dati elaborati, mentre "Want" è la contrazione del termine "wanted".

QWANT: IL MOTORE CHE RISPETTA LA PRIVACY

Gli sviluppatori sostengono che la filosofia di Qwant si fonda su due principi basilari: **nessun tracciamento dell'utente e nessuna personalizzazione dei risultati delle ricerche in base al comportamento dell'utente**. Motivo per cui Mozilla ne supporta la diffusione. Infatti a questo proposito **Denelle Dixon-Thayer**, Chief Business e Legal Officer di Mozilla ha dichiarato: "Vogliamo costruire una Internet rispettosa degli utenti in grado di creare fiducia tra di loro salvaguardando privacy e sicurezza attraverso l'innovazione e la competizione."

COME FUNZIONA

Qwant presenta i risultati in maniera diversa dai competitor. Nella modalità "Ricerca", i risultati vengono presentati tutti insieme nella pagina web ma si può accedere alle diverse categorie singolarmente perché sono organizzate in colonna sulla sinistra dello schermo come: **Web**, **Novità e Social**, **immagini, Video**, **Acquisti**, **Musica**, **Bacheche**.

È possibile migliorare la ricerca per ogni colonna aggiungendo ulteriori parole chiave.

La modalità "Social", neanche a dirlo, serve per trovare persone o organizzazioni attraverso social network come Facebook, Twitter, Google+, Linkedin.

Gli utenti di Qwant possono creare un account gratuito che consente di lavorare su note e appunti all'interno di bacheche che funzionano come un social network e definire le preferenze dell'utente che può scegliere quali categorie mostrare e quali opzioni attivare.

Tra le funzionalità più comode "Qwick", una funzione che crea collegamenti veloci ai siti preferiti. Nella versione Qwant Junior il motore di ricerca permette anche di navigare filtrando i contenuti inadatti ai bambini. Nel mese di ottobre 2017 Qwant è stato lanciato in Italia.

R

RANSOMWARE

'VISITI SITI PORNO? ORA PAGHI'. PERCHÉ IL RICATTO SESSUALE VIA MAIL CI FA TANTO PAURA

Sextortion, revenge porn, slut shaming: sono solo alcuni dei nomi a cui **l'uso acritico di Internet** ci sta abituando. **Sextortion** è un termine che si riferisce alle estorsioni a sfondo sessuale, il **revenge porn**, la porno vendetta, alla diffusione di immagini e video a sfondo erotico per vendicarsi di un rapporto finito male; lo **slut shaming** (l'onta della sgualdrina) invece mette alla gogna i desideri e i comportamenti sessuali di giovani donne eterosessuali o di uomini gay per farli vergognare all'interno della loro cerchia sociale. Sono tutti comportamenti che possono portare a conseguenze penali, anche perché spesso assumono la forma dello **stalking online** e del **cyberbullismo**, comportamenti molesti reiterati e in violazione delle più elementari norme di rispetto della privacy altrui.

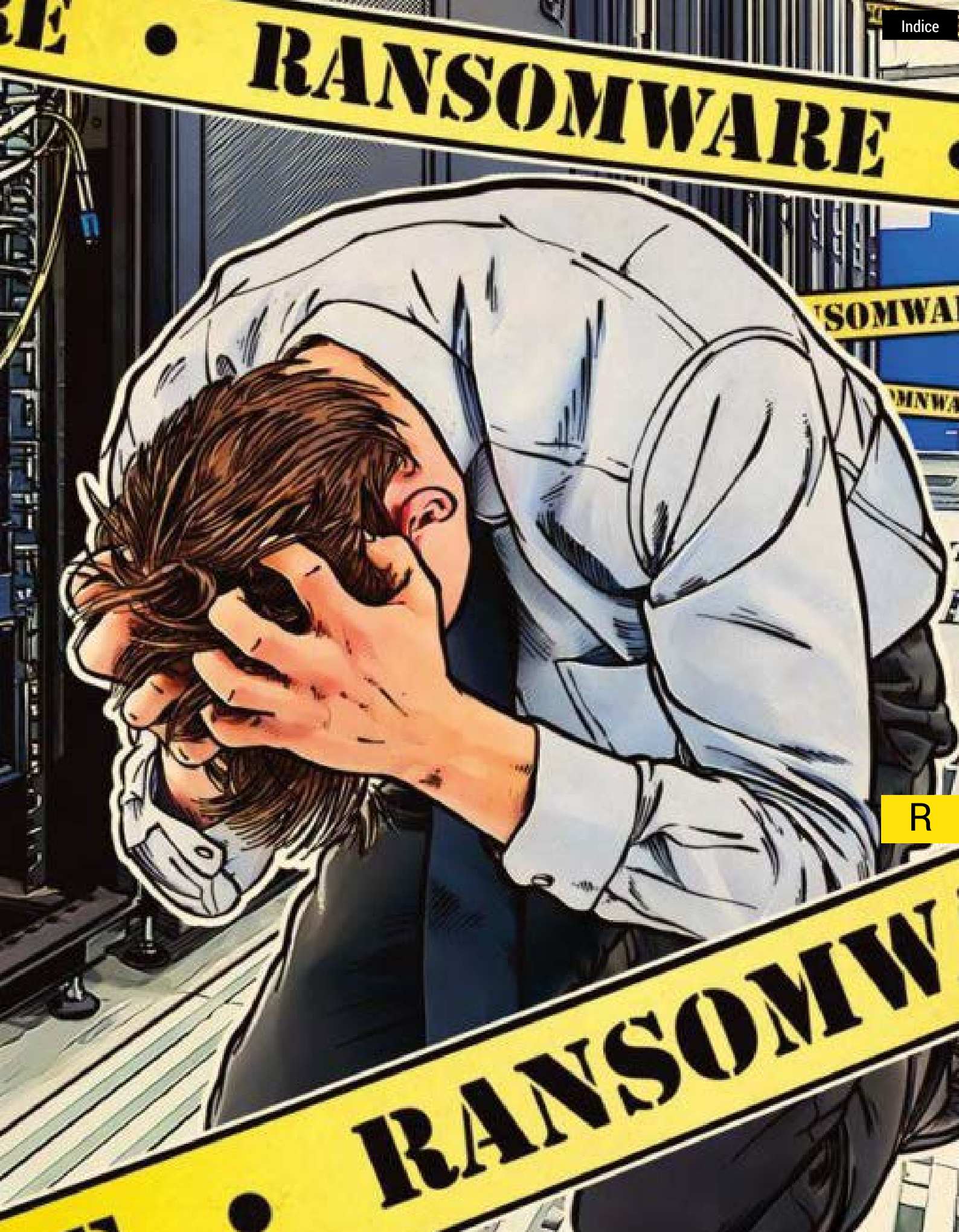
La campagna di *spamming* estorsivo segnalata in Italia dalla Polizia Postale è l'ultimo esempio di **sextortion** su cui si sono concentrati i media. La cosa funziona così: ignoti malfattori pretendono un riscatto in **bitcoin** per evitare la diffusione di video hackerati ai frequentatori di **siti porno** e per rendere credibile la minaccia chiamano la vittima per nome, gli mostrano una sua password e alludono a **strani gusti sessuali da divulgare** per rovinargli famiglia e carriera. Insomma, gli ingredienti per lanciare l'allarme ci sono tutti. La polizia però si è affrettata a chiarire che non c'è nulla da temere perché il ricatto è **infondato**: "Non si può attivare la webcam dalla posta elettronica, non si pagano mai i ricattatori e attenzione a **cambiare spesso la password**".

La campagna estorsiva tuttavia era **vecchia di tre mesi** e forse l'allarme andava dato prima. Ad accorgersene quasi subito i webmaster dell'Università Sapienza di Roma che già dal **25 luglio** scorso avevano segnalato queste stesse email ricattatorie. Solo che inizialmente erano in inglese.

Perché tanto scompiglio proprio adesso? Il primo motivo è che il **ricatto-truffa** è stato segnalato su Twitter da uno stimato ricercatore in **cybersecurity** che si fa chiamare **Odisseus**, il secondo è che a questo punto chi ha ricevuto l'email ha deciso di denunciare, ma soprattutto si è scoperto che nonostante tutto c'è qualcuno che ha ceduto al ricatto.

Quando è accaduto ci sono state decine di versamenti in bitcoin ai wallet, i portafogli, indicati dai ricattatori. E il **wallet** è stato segnalato per **abusi**.

Questo ci fa riflettere su alcune cose. La prima è che una grossa percentuale di utenti Internet frequenta **siti porno** e teme di essere stata pizzicata. Infatti l'email ricattatoria infatti dice così: "*Io*



R


RANSOMWARE
YOU HACKED
MWARE • RANSOM
SOMNWARE • RANSOM
RANSOM

rappresento un gruppo internazionale famoso di hacker. Nel periodo dal 22.07.2018 al 14.09.2018, su uno dei siti per adulti che hai visitato, hai preso un virus che avevamo creato noi. In questo momento noi abbiamo accesso a tutta la tua corrispondenza, reti sociali, messenger. Anzi, abbiamo i dump completi di questo tipo di informazioni. Siamo al corrente di tutti i tuoi "piccoli e grossi segreti", sì sì… Sembra che tu abbia tutta una vita segreta. Abbiamo visto e registrato come ti sei divertito visitando siti per adulti… Dio mio, che gusti, che passioni tu hai… :)".

Non è da escludere che sia accaduto per davvero. Nei mesi scorsi milioni di utenti di **Pornhub**, il più grande sito per adulti al mondo, sono stati bersagliati da un attacco di malvertising, pubblicità "pirata" che installava codice malevolo sui loro computer, mentre secondo le ricerche di B&B International e Kaspersky Lab sono centinaia i finti utenti dei siti di incontri (**dating online**) specializzati nella raccolta e profilazione dei dati personali dei frequentatori che cercano di estorcere dati finanziari dalle potenziali vittime.

Insomma, non si tratta di **una paura irrazionale**. Anche perché in alcuni casi è stato verificato che nelle email ricattatorie campeggiano password reali delle vittime: la "prova" che l'hacker criminale farebbe sul serio.

Però. Per avere quelle password "vere" non è necessario essere stati precedentemente vittime di un attacco informatico ben riuscito, ma che **nome**, **cognome**, **email** e **password siano stati pescati da uno qualunque dei databreach**, violazione di database, degli ultimi anni, senza alcun bisogno di installare fantomatici trojan.

Eppure, a guardare con più attenzione l'email truffaldina si dovrebbe capire subito che il mittente, per quanto possa spaventarci – visto che si presenta col nostro nome o quello dell'organizzazione che ci offre la posta elettronica – **è un mittente fasullo** che in molti casi è appoggiato a un provider di servizi Internet in Repubblica Ceca e in altri basato in Ungheria.

Comunque ha ragione la polizia postale: è importante proteggere le proprie password e cambiarle spesso, ma anche essere più attenti a fornire i propri dati in rete non guasta, neanche all'anima gemella dei siti di appuntamenti.

REVENGE PORN

SOCIAL E WEB, NIENTE SESSO SENZA CONSENSO

Revenge Porn, Sexting, Sextortion, Cyber-harassment e Cyber-stalking sono tutti fenomeni di aggressione criminale online riguardanti il sesso e la sessualità. E nella maggior parte dei casi riguardano le donne.

Il **Revenge porn**, la vendetta porno, ad esempio, indica la condivisione pubblica senza consenso via Internet di immagini intime e a sfondo sessuale per umiliare la vittima che ne è protagonista.

L'odiosa pratica è in genere originata da amanti delusi e colpisce più frequentemente le donne che gli uomini. Molto diffuso tra gli adolescenti, il fenomeno è all'origine di alcuni casi di cronaca che anche in Italia hanno portato al suicidio delle stesse vittime.

Il **Sexting** invece è la pratica di messaggiare qualcuno con contenuti sessuali non voluti mentre la **Sextortion** implica varie forme di ricatto, anche monetario, per non divulgare contenuti a sfondo erotico del bersaglio prescelto.

Cyber-harassment infine è il nome che si da alle molestie sessuali online assai frequenti nei social network sia nei profili pubblici dei malcapitati che attraverso le chat di quei servizi e che spesso si tramuta in **Cyber-stalking**, un insieme di condotte persecutorie che spesso riassumono tutti i casi precedenti.

A questi fenomeni generati da amanti gelosi o abbandonati si aggiungono i crimini informatici di chi ruba foto erotiche e di nudo di attrici e starlette per diffonderle sul web contando su un presunto anonimato, come è accaduto all'attrice Jennifer Lawrence e alla giornalista Diletta Leotta.

Questi fenomeni oltre a umiliare le vittime spesso le fanno sentire isolate e depresse, senza aiuto. Ma proprio per reagire a questa condizione è nato **50 Sfumature di silenzio**, un movimento globale che si batte contro le molestie online e il cyber-stalking e ha l'obiettivo di aiutare le vittime ad uscire dall'isolamento e a denunciare. I suoi promotori hanno lanciato un'app mobile per offrire strumenti e risorse alle vittime di questi comportamenti criminali. L'app fa parte di un più ampio progetto per porre fine al cyberbullismo, alla vendetta porno e alle molestie sessuali online, note anche come violenza domestica digitale, e contribuire a rendere giustizia e dare voce a milioni di persone in tutto il mondo vittime di questi abusi.

L'idea è di Darieth Chisolm, giornalista e autrice televisiva perseguitata un ex-fidanzato che aveva perfino costruito un sito web con meme molesti, foto e video di nudo che la ritraevano mentre dormiva. Era arrivato a minacciare di ucciderla se non fossero tornati insieme.

L'app per smartphone, integrata col sito www.50shadesofsilence.com, offre a vittime e sopravvissuti una piattaforma per condividere storie, accedere a risorse che insegnano le basi della sicurezza su Internet e altri materiali di empowerment.

Oltre all'app e al sito web, Darieth ha girato un documentario che esplora la crescente epidemia globale di cyber-molestie, cyberbullismo, cyber-rape, sexting e vendetta porno per denunciarne gli effetti sulla vita sociale e professionale delle vittime. Il documentario è finanziato dal pubblico in crowdfunding. L'idea è di supportare iniziative educative volte a combattere il problema, l'onere finanziario delle cause legali, e cambiare la mentalità sociopatica dei perpetratori. Ma anche per avere leggi più severe per i reati informatici di natura sessuale e chiedere alle aziende interessate di assumersi la loro parte di responsabilità restituendo dignità e rispetto alle vittime.

SMART WORKING

PERCHÉ IL PC VA TENUTO PULITO E AL SICURO DAI VIRUS INFORMATICI

Lavorare da casa ai tempi del Coronavirus implica il rispetto delle norme di Cyber Hygiene, ma anche delle policy aziendali.

Il Coronavirus cambia il modo di lavorare e le aziende si attrezzano per rispondere alla richiesta di farlo da casa. Almeno per le attività che lo consentono. Ma come si fa a mantenere gli stessi livelli di sicurezza previsti dalle policy aziendali quando computer e smartphone non sono più all'interno del perimetro aziendale?

Nei loro uffici i lavoratori hanno in genere una postazione con un computer collegato alla rete aziendale tipicamente protetta da software e hardware specifici per mantenere al sicuro progetti, dati sensibili, idee creative, proprietà intellettuale dell'azienda. Per proteggere reti e computer vengono usati firewall, proxy, limitazione della navigazione web, messaggistica ed email sicure, perfino controlli tramite sistemi anti-intrusione (IPS/IDS), ma a casa?

Per fare smart working in maniera sicura bisogna dotare i dipendenti di strumenti adeguati. E in Italia non tutte le aziende sono preparate a farlo.

Lo Smart Working o lavoro agile, consente di usare dispositivi propri se il lavoratore è d'accordo, ma gestire un dispositivo remoto presso il domicilio di un dipendente ha implicazioni di privacy e non solo. Perciò se il primo passo è mettere in sicurezza i dispositivi, ci vuole attenzione alle connessioni.

Non basta gestire in sicurezza i dispositivi, ma ogni strumento che permette di entrare nella rete aziendale. Una connessione cifrata, un firewall o una Vpn (Rete privata virtuale), in grado di segmentare il traffico domestico da quello aziendale potrebbero non bastare. Spesso chi lavora a casa ignora le norme applicate in azienda, a cominciare dalle regole minime di igiene cibernetica.

Per questo mentre occorre una chiara comunicazione ai propri dipendenti affinché siano consapevoli dei possibili rischi informatici in cui possono incorrere lavorando da casa, bisogna suggerire come fare per mettersi al sicuro. Sia perché un uso improprio degli strumenti può causare danni sia perché gli hacker criminali che cercano di sfruttare la situazione in questi giorni si nascondono dietro a finte comunicazioni aziendali per rifilare dei software dannosi ai lavoratori collegati in remoto.

PHISHING E TRUFFE

Aziende di cybersecurity come Sophos, d3Lab, Yoroi, hanno rilevato file dannosi che si presentavano come documenti pdf, mp4 e docx che avevano come oggetto

proprio il Coronavirus suggerendo che si trattasse di istruzioni e video su come proteggersi dal Coronavirus. I file contenevano diverse minacce informatiche in grado di interferire con il funzionamento dei computer o delle reti di computer ma anche di bloccare, modificare, copiare e distruggere dati preziosi.

Ci vuole buon senso e bisogna usare diversi accorgimenti relativi alla dotazione informatica: fornire una Vpn sicura ai dipendenti, limitare i diritti di accesso di chi si collega alla rete aziendale, proteggersi con software di sicurezza. Il motivo è facile da capire.

La remotizzazione delle attività e il massiccio impiego della rete hanno portato a una maggiore sofisticazione degli attacchi contro l'infrastruttura digitale in espansione, tra cui quelli guidati dall'intelligenza artificiale e dall'apprendimento automatico. Il consiglio degli esperti di cybersecurity è di usare soluzioni di software as a service, *cioè su richiesta*.

Adattarsi al lavoro agile significa però riorganizzare processi e modalità di team-working ed è plausibile che ci vorrà qualche tempo, perciò è utile guardare come proteggersi nell'immediato almeno quando si usano strumenti propri. Vediamo come.

Accorgimenti di sicurezza e cyber hygiene

Come è importante lavarsi le mani per tenere il nostro organismo in salute e al sicuro da ospiti indesiderati come i virus, è altrettanto importante seguire un insieme di norme di **igiene cibernetica** - sì, si chiama proprio così - per tenere i nostri computer protetti e funzionanti.

Prima di cominciare a lavorare da casa è bene sapere quali sono i file, i folder e gli altri strumenti necessari a farlo. Assicuratevi di avere una buona connessione a Internet. Controllate se i sistemi operativi in uso siano aggiornati. Scegliete con oculatezza i sistemi di lavoro collaborativo usandoli come un ufficio virtuale. Ma ricordate ai colleghi di non scambiarsi password in maniera insicura.

USATE PASSWORD INTELLIGENTI

Assicuratevi che per accedere a ogni dispositivo digitale dobbiate digitare una password. Molti servizi si accontentano di una password di otto caratteri, ma se la fate più lunga aumentate la sua robustezza. La password deve contenere lettere maiuscole e minuscole, numeri e simboli speciali combinati in una maniera tale che non risulti comprensibile a un estraneo: per capirci "pA$$w03d" non è sicura. Inoltre se una password è facile da ricordare probabilmente è un nome già presente in uno dei tanti dizionari online per attacchi di "enumerazione delle password".

Ma come si fa a ricordare una buona password? Sicuramente sono da preferire le password autogenerate dai sistemi a cui ci colleghiamo, e non è consigliato salvarle sul browser. E poi quando sono tante è difficile memorizzarle tutte senza confondersi. Il consiglio perciò è di usare un **password manager**, un'app che funziona da cassaforte digitale e che, grazie a una **master password**, sblocca tutte le password che ci servono. Altra raccomandazione utile è usare l'autenticazione multifattore, che presuppone l'invio di una seconda password per accedere ai servizi.

CAMBIATE IL NOME E LA PASSWORD DEL ROUTER

Per lavorare da remoto si usano spesso router casalinghi e portatili. Modificare il nome SSID (Set Service Identifier) predefinito del wi-fi domestico aumenta la sicurezza. Quando un pc cerca reti wireless nelle vicinanze, elenca tutte le reti visibili. Rinominarlo evitando di usare informazioni personali riduce le possibilità di essere individuati e hackerati. La maggior parte dei router che funziona da access point viene acquistata con una password di default uguale per tutti: cambiarla e crearne una nuova di almeno 20 caratteri è cosa buona e

giusta. Lo stesso vale per la crittografia del proprio network. In genere è del tipo **WPA2 encryption**: potete accontentarvi, ma assicuratevi che sia attivata e sopratutto verificate che il firmware del router sia aggiornato. In genere viene fatto automaticamente ma potete sempre farvi aiutare da chi ve lo ha venduto.

AGGIORNATE SOFTWARE E SISTEMA OPERATIVO

L'aggiornamento di software e sistema operativo risolve falle di funzionamento, errori nel codice e vulnerabilità presenti negli strumenti di produttività individuale. É la prima cosa da fare dopo aver verificato la sicurezza della vostra connessione.

INSTALLATE UN FIREWALL

Windows e Mac hanno già un firewall: controllate che sia attivo. Il firewall blocca il traffico non richiesto in entrata ed è capace di bloccare i virus e impedire che il pc cada in mano ai criminali che cercano di prenderne il controllo per farne i soldatini delle loro Botnet.

INSTALLATE, AGGIORNATE E LANCIATE UN ANTIVIRUS

Gli antivirus riconoscono la maggior parte delle minacce. Quelli gratuiti possono funzionare bene, ma la scelta dell'antivirus è proprio uno dei casi in cui è meglio spendere qualcosa per comprarne uno. Quelli a pagamento in genere hanno delle funzionalità aggiuntive per il riconoscimento di spyware, adware, malware e virus e la loro messa quarantena. Ricordate che se un computer è già compromesso, serviranno a poco le altre misure "igieniche", perciò prima di tutto fate una scansione del computer. Gli antivirus sono in grado di riconoscere buona parte dei software malevoli.

USATE UNA VPN PER COLLEGARVI

La Vpn o rete privata virtuale è una sorta di tunnel che crea un collegamento diretto tra voi e il computer a cui volete accedere, per collegarvi, ad esempio, al back-end di un servizio aziendale o del vostro blog. La Vpn cifra la connessione e impedisce a un eventuale spione di intercettare il traffico, compresi documenti sensibili, nascondendo la navigazione. Alcune aziende come Fortinet usano ad esempio reti private virtuali che si installano sul browser in maniera dinamica e temporanea.

FATE UNA COPIA DEI VOSTRI DATI

Se state lavorando a progetti sensibili, di lunga durata, fate un back up del lavoro svolto. Nella malaugurata eventualità in cui il computer si blocchi, si rompa o i suoi dati vengano persi e rubati ne avrete una copia di riserva. Il backup va fatto su un hard disk o una pennetta Usb da tenere scollegata dal computer con cui ci connettiamo in rete.

USATE UNA SANDBOX

Prima di aprire un file sospetto, proveniente da sconosciuti, magari allegato a una email sgrammaticata potete inviarlo a una ***sandbox***, *cioè a un servizio online come quello di Virus Total per farlo analizzare e assicurarvi che sia innocuo.*

Lavorare da casa significa spesso non sentire la pressione del gruppo o del datore di lavoro e si sarà tentati di passare più tempo sui social, soprattutto per capire come evolve l'epidemia del Coronavirus. I delinquenti lo sanno e per questo bisogna fare attenzione ai tentativi di phishing e di infezione informatica condotti con link che arrivano attraverso la versione desktop di WhatsApp e di Telegram attraverso cui viaggiano finti tutorial di ogni tipo.

Anche per questo bisogna fare attenzione a quale tipo di strumenti di messaggistica si ricorre per lavorare a distanza.

Scheda smart working

Il lavoro agile è il lavoro fatto da casa o da qualsiasi posto si trovi il lavoratore e ovviamente vale per la quasi totalità di forme di lavoro che richiedono un computer, un telefono e una connessione a Internet. Ed è regolato dalla legge. Non è una concessione dell'azienda, ma una modalità di esecuzione del rapporto di lavoro stabilita mediante accordo tra le parti (L.81 del 22/05/17), che prevede una serie di diritti e garanzie per il lavoro flessibile.

Potete decidere voi dove stare e come organizzare il vostro lavoro ma la prestazione è soggetta ai medesimi limiti di durata massima dell'orario di lavoro derivanti dalla legge e dal Contratto Collettivo Nazionale e non può essere un modo per farci lavorare di più. La scelta del luogo di lavoro deve inoltre rispettare i requisiti di riservatezza e senza controlli a distanza (art.4 stat. Lav.), a meno che non vi sia un diverso accordo sindacale o il consenso sottoscritto dal lavoratore. Con un'avvertenza: il datore di lavoro ha facoltà di controllare unicamente il risultato del lavoro e la sua organizzazione anche se il dispositivo che usa è stato fornito dall'azienda. E, come per il computer personale, non può obbligare il lavoratore a utilizzare il suo smartphone per ricevere le telefonate di lavoro. Può farlo solo sulla base del consenso informato e revocabile del lavoratore che può decidere se accettare di utilizzare i suoi mezzi oppure no. Ma non basta.

Il datore di lavoro è responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attività lavorativa e della loro gestione. La legge impone di cooperare con il datore di lavoro per garantire la sicurezza di dati, software e dispositivi in base alle policy di sicurezza IT aziendale.

SOCIAL NETWORK

ANTISEMITISMO E HATE SPEECH, UN VIZIO «SOCIAL»

"The Intercept", il giornale online fondato da Glenn Greenwald, Laura Poitras e Jeremy Scahill, ha dimostrato che Facebook vendeva pubblicità razziste e antisemite ai suoi utenti proprio nei giorni del massacro alla sinagoga di Pittsburgh (il 27 Ottobre 2018). L'autore dell'omicidio di 11 persone era convinto dell'esistenza di un complotto per decimare la «razza bianca», noto come «White genocide». Si tratta di una teoria complottista secondo la quale «i negri» cospirerebbero per cacciare i bianchi dalle loro terre.

Nonostante gli sforzi internazionali per smascherare la falsa tesi di un «Genocidio bianco», Facebook vendeva agli inserzionisti la teoria complottista a un «target dettagliato» costituito da un gruppo di interesse di 168.000 utenti che avevano espresso il favore per contenuti simili. L'azienda, contattata per un commento, ha eliminato la categoria di *targeting*, si è scusata e ha affermato che non avrebbe mai dovuto esistere. Quante pagine e quante inserzioni di questo tipo esistono ancora su Facebook?

Non ci piace ammetterlo, ma i social, non solo Facebook, sono diventati un brutto posto dove stare. Nati per i motivi più diversi, il loro modello di business si basa sulla vendita dei dati personali degli utenti e sulla capacità di indirizzare la loro attenzione verso specifici target pubblicitari. Più utenti hanno, maggiore è il volume di traffico che possono generare e maggiore il loro valore per gli inserzionisti. Maggiori gli utenti, maggiori i profitti, maggiore il valore delle azioni, maggiori i dividendi per gli azionisti.

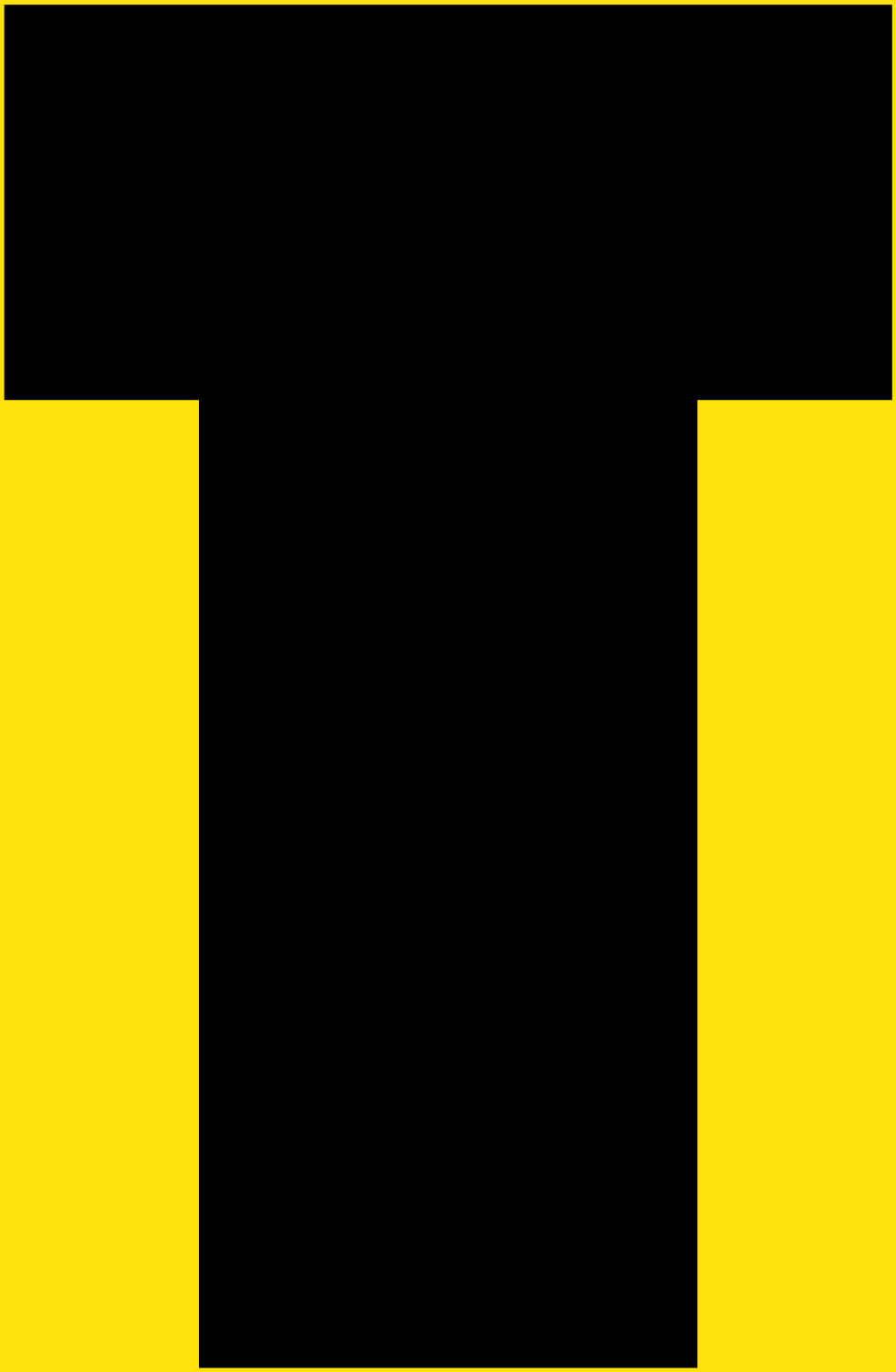
Per ampliare la platea degli iscritti ai social il primo obbiettivo è di renderli fruibili attraverso interfacce semplificate e sistemi di ricompensa. Gli stessi dispositivi digitali che usiamo per accedervi sono già predisposti per farlo grazie alle app, software dedicati a prova d'incapace. No, non offendetevi. Siti web, app, social e i dispositivi sono ingegnerizzati come i comandi di una lavatrice per essere usati senza capire come funzionano per davvero. Grazie alla logica del design centrato sull'utente, devono poter essere usati da tutti e perciò fanno leva su abilità umane comuni: coordinamento percettivo, linguaggio e memoria. Ma i social sono luoghi d'interazione che retroagiscono non solo su quelle abilità ma sui nostri «frame» comportamentali, modificandoli.

Ad esempio: perché sui social si litiga tanto? Perché l'assenza fisica dell'interlocutore elimina il timore di rappresaglie fisiche. Perché le opinioni sui social sono tanto polarizzate? Perché gli utenti possono approfittare dell'anonimato e si sentono meno responsabili di quello che pubblicano. Perché odiano tanto? Perché veniamo assegnati a categorie di utenti simili a noi che vedono e leggono le stesse

cose, rafforzando conformismo e *group thinking*.

Le piattaforme social non hanno ideologia se non quella del mercato. Non conta chi sei o come la pensi, contano i numeri che fai – like, fan, follower – insieme alla capacità di spesa nota dall'incrocio di fattori e informazioni anche esterne alla piattaforma. Per questo motivo le *policy* dei social mettono meno vincoli possibili al comportamento degli utenti, spesso sotto la bandiera di una presunta libertà d'espressione.

L'effetto è che persone che non avrebbero mai ammesso in pubblico di essere antisemite e razziste verso i neri, i gay, o altre «minoranze», lo fanno di frequente nei social. Se a questo aggiungiamo la rabbia sociale di una società bloccata come la nostra, quarta al mondo per analfabeti funzionali (OECD, 2017) capiamo il successo dell'odio online.



TIKTOK

L'IRRESISTIBILE ASCESA DI TIKTOK A RISCHIO PEDOFILIA

Il Garante italiano per la privacy Antonello Soro ha lanciato l'allarme TikTok. Il social network dei teenager che fanno video karaoke, gare di abilità e scherzi da caserma, non rispetterebbe le leggi sulla privacy. Già nel 2019 le autorità Usa avevano comminato una multa di sei milioni di dollari a ByteDance, la società cinese che controlla il social, perché non garantiva la sicurezza dei minori, possibili prede di pedofili e perversi sessuali.

All'inizio del 2020 il Garante italiano ha chiesto al Comitato europeo per la protezione dei dati personali di attivare una specifica task force per indagare eventuali comportamenti scorretti in seguito alla segnalazione di possibili vulnerabilità dell'app.

Nei mesi scorsi TikTok era stata accusata di obbedire alle leggi sulla censura che regolano gli altri social media cinesi come WeChat o Baidu e un gruppo di attivisti indiani l'aveva perfino accusata di incoraggiare pedofilia e pornografia, oltre che, negli Stati Uniti di raccogliere illegalmente informazioni sui bambini.

Interpellato, Antonello Soro ha dichiarato che «Il social network è da tempo all'attenzione del Garante, al quale peraltro sono giunte segnalazioni anche con riferimento ad un caso in cui un genitore ha scoperto che TikTok veniva usata da un pedofilo per contattare suo figlio» – aggiungendo che – «E' importante proteggere i nostri ragazzi ma è necessario anche far crescere in loro una sempre maggiore consapevolezza nell'uso delle app e dei social network».

Proprio a dicembre un rapporto dell'associazione tedesca per i diritti

digitali Netzpolitik.org accusava l'app cinese di aver discriminato utenti con disabilità fisiche e mentali dando istruzione ai suoi moderatori di limitare la diffusione dei loro post. Mentre il senatore democratico Chuck Schumer aveva esortato il suo governo a indagare su TikTok per il timore di interferenze nelle prossime elezioni statunitensi «in quanto potenziale minaccia di controspionaggio che non possiamo ignorare».

QUANTO VALE TIKTOK

Fondata nel 2017, anno dell'acquisizione di Musical.ly da parte di ByteDance per 800 milioni di dollari, e lanciata nel 2018 come TikTok, nome con cui è ora conosciuta in 150 paesi, in Italia oggi spopola tra i giovanissimi con 2,4 milioni gli utenti attivi che producono in media 236 video al minuto. Ma sono 12 milioni i video pubblicati ogni giorno sulla sua piattaforma, da ogni dove, e in più di 75 lingue.

Bytedance è inoltre la "startup" più finanziata al mondo. Dopo un accordo da 3 miliardi di dollari con il gruppo giapponese SoftBank, Kkr e General Atlantic, vale più di Uber, cioè oltre 7,5 miliardi di dollari.

Sembra una stima eccessiva per un'app dove i più giovani gareggiano a migliorare le coreografie inventate dai "*creators*" e *influencer* che la abitano per avere like e follower usando sia la simpatia che un pizzico di acerbo erotismo. Ma Bytedance non si occupa solo di piattaforme digitali quanto piuttosto di app basate su sistemi di machine learning per proporre contenuti su misura grazie a queste tecniche di intelligenza artificiale, come nel caso del suo un aggregatore di *news*, **Toutiao**, basato per l'appunto sulle preferenze e sui gusti degli utenti.

E probabilmente nascono lì i timori americani per questa sua ascesa anche quando si cita giustamente la discutibile *privacy policy* che gli è valsa una class action negli Usa per il presunto trasferimento di dati a Pechino. Cosa che ByteDance ha negato.

Adesso TikTok compete direttamente con Facebook e Instagram e mira a scalzarle. In uno studio di Ghost Data a nome di Andrea Stroppa, Bernardo Parrella e altri, risulta che, anche se Instagram genera più interazioni in generale, TikTok garantisce maggiore visibilità a contenuti di qualità.

Questo accadrebbe perché molti video che vengono visti milioni di volte in un breve periodo di tempo non sono per forza prodotti da marchi conosciuti o "influencer" ma da utenti comuni.

Grazie a una specifica funzionalità di TikTok: il suo algoritmo tende a premiare non solo gli utenti "autorevoli" (cioè verificati e con molti follower), ma favorisce la visibilità di qualsiasi contenuto originale che venga condiviso di frequente. Questa strategia (diversa da Instagram) potrebbe diventare una vera risorsa per il futuro di TikTok, potenzialmente permettendo a chiunque di diventare "famosi", il vero pallino dei nostri giovani costantemente a caccia di "popolarità".

Un obiettivo per cui sono pronti a fare di tutto, anche a dispetto della propria privacy.

TOR

TOR, THE ONION PROJECT CHE COS'È TOR E A CHE COSA SERVE

Immaginatevi il web come un iceberg. La sua punta è fatta dal web di superficie, quella dove troviamo Facebook, Twitter, i siti dell'università o del nostro giornale preferito. Sotto il pelo dell'acqua c'è il resto dell'iceberg, il Deep Web, cioè la porzione del web non indicizzata dai motori di ricerca e i cui siti non riusciremmo a trovare neppure con Google. E poi c'è una parte del deep web, più difficile da scoprire, il Dark web, che può essere raggiunta solo con speciali software come TOR, The Onion Router.

Tor è un software per navigare la rete in maniera anonima. Usato per garantire la privacy di giornalisti, whistleblower e dissidenti politici, Tor è anche il nome del network omonimo che protegge le proprie comunicazioni usando la crittografia.

Liberamente scaricabile dal web, il **Tor browser** ha l'aspetto di un semplice browser - è una versione modificata di Mozilla Firefox -, ma quando lo si usa riesce a schermare la connessione tra l'utente e la sua destinazione impedendo a uno spione di sapere chi sta guardando un certo sito o usando un certo servizio web.

Tor riesce ad anonimizzare i suoi utilizzatori perché impedisce l'analisi del traffico delle comunicazioni via internet, dal web surfing alle chat, attraverso una rete di computer intermedi tra il computer di partenza e quello di arrivo, i cosiddetti **onion router**, gestiti in parte dal Tor Project e in parte da volontari. Con Tor i dati trasmessi in rete sono protetti da strati successivi di crittografia, come gli strati di una cipolla: da qui il nome "onion" che in inglese vuol dire cipolla.

Con il browser Tor si può navigare qualsiasi sito in maniera anonima, ma il software blocca video e contenuti basati su Flash e Java ad esempio, e impedisce di aggiungere al browser funzionalità che potrebbero essere manipolate per rivelare l'indirizzo IP dell'utente, cioè per identificare la nostra "impronta digitale" quando ci connettiamo a Internet. Tor permette anche di creare dei siti nascosti con il suffisso ".onion" le cui comunicazioni sono protette sia in entrata che in uscita.

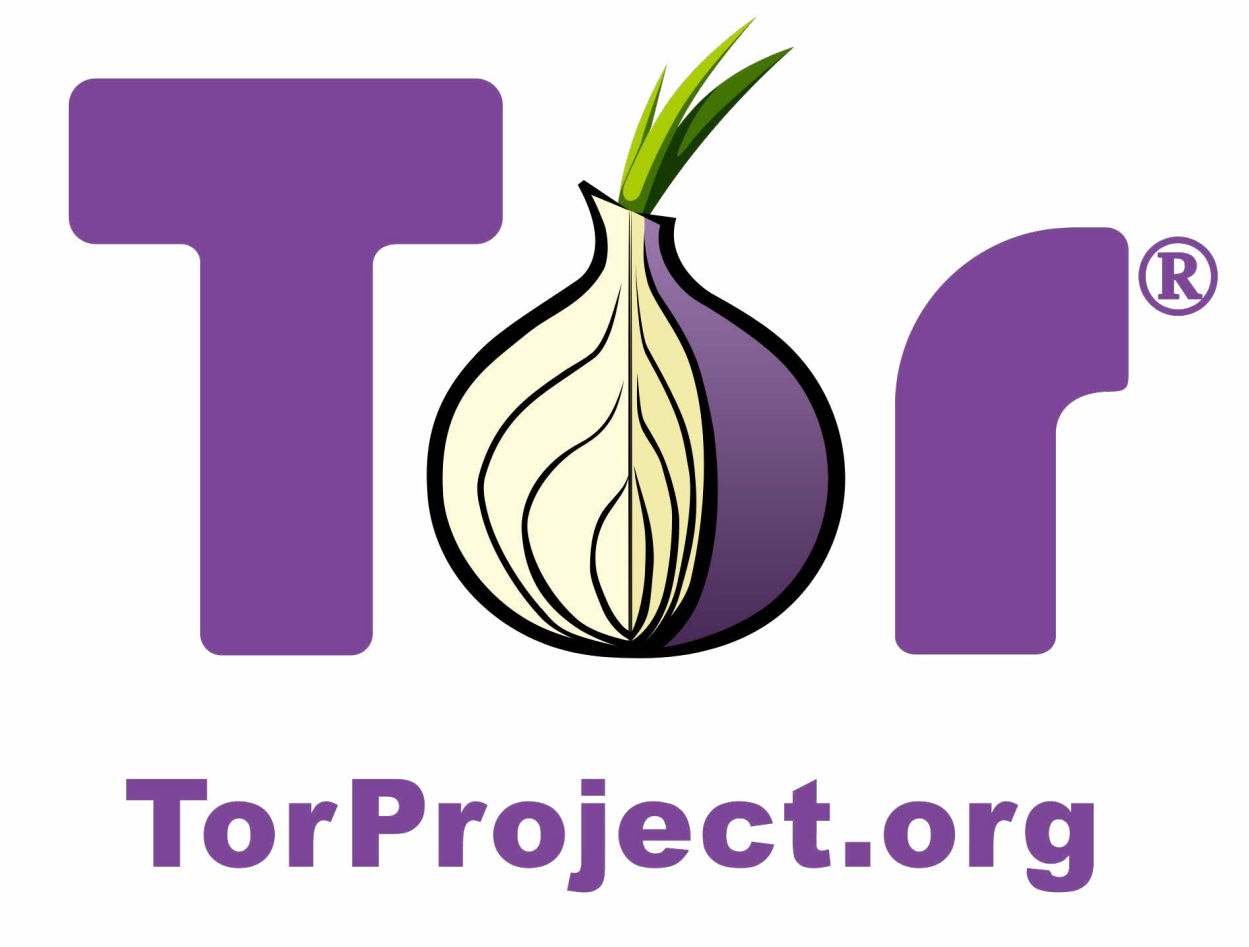
Nato per proteggere le comunicazioni della Marina militare americana, da oltre dieci anni il sistema viene sviluppato dal Tor Project, una fondazione finanziata dalla Electronic Frontier Foundation.

Nel tempo Tor è diventato il maggior alleato di chi in rete vuole comunicare, informarsi e collaborare senza farsi scoprire. Viene usato da persone che nelle scuole e nelle biblioteche cercano informazioni sensibili su AIDS e HIV,

sull'omosessualità e le dipendenze, oppure da chi in rete cerca consigli ai propri problemi e supporto psicologico come le vittime di abusi sessuali. Ma proprio perché garantisce la privacy delle comunicazioni è uno degli strumenti più usati dai criminali per fare affari nel Dark web.

E il Dark web è il nascondiglio preferito di cybertruffatori e blackmarket, siti di e-commerce che vendono droghe, armi, e materiale pedopornografico. Ma nel dark web ci sono anche i fedeli di religioni fuorilegge come i Falun Gong cinesi, giornalisti a caccia di prove e hacker governativi che si scambiano tool informatici e conoscenze di alto livello. É stato a lungo il luogo privilegiato per le transazioni in bitcoin.

Usare Tor rende difficile ma non impossibile determinare l'indirizzo IP di un utente e negli anni il network stesso dei suoi router è stato messo a dura prova da attacchi informatici e operazioni di polizia. Anche per questo il nuovo consiglio direttivo ha deciso di potenziare il network del progetto con l'obbiettivo di garantire un'efficace tutela dei diritti civili in rete.



TRACKER

ATTENTO, LA TUA TELEVISIONE TI SPIA

Il direttore generale del DIS che sovrintende ai nostri servizi segreti ha detto che tre o quattro compagnie sovranazionali hanno più informazioni sui cittadini di quante ne abbiano gli stati di appartenenza. Antonello Soro, Garante italiano della privacy la chiama *algocrazia*: il governo delle masse attraverso gli algoritmi che gestiscono i dati che le persone cedono, spesso inconsapevoli, alle grandi piattaforme digitali. Viviamo in una tale simbiosi con web e telefonino che non ci facciamo più caso.

Il motivo è facile da capire: tutti noi barattiamo qualche comodità con il controllo sociale esercitato dai big player della rete. I dati che noi produciamo non sono semplici dati, ma rimandano a dei comportamenti: dove siamo stati, con chi, per quanto tempo, con chi abbiamo parlato, cosa abbiamo comprato, quanta ginnastica abbiamo fatto. È così che attraverso l'analisi di questi dati è possibile anticipare quei comportamenti, manipolarli e modellarli come se fossero spontanei. Il dibattito pubblico su questi temi però è ancora a uno stadio larvale. La gran massa degli utenti se ne infischia a fronte della partecipazione gratuita al marketplace di Facebook, dell'uso gratuito della posta o delle mappe di Google, della possibilità di affossare un ristorante su TripAdvisor, o di celebrare il nostro autore preferito con una recensione su Amazon.

Per raccogliere i dati che gli interessano queste piattaforme ci inseguono, letteralmente. Lo fanno con dei software che si chiamano **tracker** che appunto tracciano i nostri comportamenti online. Per capirci, è come se qualcuno ci seguisse durante lo shopping e

annotasse i negozi che abbiamo visitato e quelli di cui abbiamo guardato solo la vetrina e mettesse il naso nella borsa degli acquisti.

La ribellione verso queste forme di sorveglianza commerciale, che diventa sorveglianza politica nei paesi autoritari, ha generato cause legali contro Facebook & Co. in UK, Belgio, Francia e Germania. Adesso sono molte di più le persone consapevoli di essere sorvegliate da siti, app e smartwatch da polso o dai rilevatori di frequenza cardiaca.

I più furbi modificano le impostazioni dei software usati e gli impediscono almeno la geolocalizzazione. Quelli ancora più furbi usano i software anti-tracciamento come Privacy Badger suggeriti dalla Electronic Frontier Foundation.

Ma che succede quando queste stesse tecnologie di sorveglianza ci entrano nella camera da letto o nel salotto di casa?

Il New York Times ha pubblicato un rapporto su Samba TV, che raccoglie dati su 13,5 milioni di telespettatori al fine di personalizzarne la visione. Samba ha firmato accordi con Sony, Sharp, Toshiba e altri, per installarci il suo software. Si chiama Automatic Content Recognition (ACR) e dovrebbe fornire "approfondimenti essenziali sulla tv".

Piazzata in salotto e accesa la tv, la prima schermata chiede di abilitare Samba Interactive. Il servizio promette consigli su cosa vedere e propone offerte speciali d'acquisto "riconoscendo abilmente i contenuti su schermo". Dal 2016 i dirigenti della società hanno affermato che oltre il 90% delle persone ha fatto clic sul pulsante di attivazione. Samba crea una "mappa del dispositivo" per abbinare i contenuti televisivi ai dispositivi che condividono la rete con la smart tv. Secondo Jeffrey Chester del Center for Digital Democracy, "l'azienda esce dal salotto per rintracciare gli utenti nel loro ufficio, in fila al ristorante e mentre viaggiano." Attento, anche la tua televisione ti spia.

V

VIDEOCHAT

VIDEOCHAT E TELEDIDATTICA GRATUITE CON IORESTOACASA.WORK, UN PROGETTO SOLIDALE E PARTECIPATIVO SVILUPPATO DALLA COMUNITÀ ITALIANA DEL SOFTWARE LIBERO

Zoom, Meet, Webex, GoToMeeting e gli altri: le piattaforme per videonferenza sono diventate un must ai tempi del Coronavirus. Compleanni, aperitivi, lezioni e riunioni a distanza saranno la norma per un po' e così i ricercatori italiani hanno deciso di dare il loro contributo col progetto iorestoacasa.work per offrire a tutti strumenti di videoconferenza gratuiti e open source.

Nato dall'inziativa di una rete di professionisti di Fabriano, Luca Ferroni, Riccardo Serafini, Francesco Coppola e Dawid Weglarz, *iorestoacasa* è una piattaforma tutta italiana per comunicare a distanza nei giorni dell'emergenza. A differenza delle altre piattaforme commerciali l'iniziativa solidale usa un sistema open source, **Jitsi Meet**, che permette agli utenti di effettuare videochiamate in modo immediato, semplice e gratuito. Per accedere alle "stanze" di discussione basta cliccare un link dal browser, senza installare programmi o registrarsi nome e cognome, e si comincia a parlare.

Il software, simile a quelli commerciali più famosi, permette di vedersi, chattare, condividere lo schermo e realizzare una diretta streaming su Youtube. Per questo è adatto sia per i consueti meeting di lavoro che per impartire lezioni a distanza.

Risultato di un'attività decennale legata alla diffusione del software libero nel proprio territorio, l'idea dei suoi creatori, "linuxari" doc (utilizzatori del sistema operativo GNU/Linux e dei programmi correlati), era proprio quella di sviluppare un prodotto socialmente utile sia per le persone che per le imprese, ma adesso l'obbiettivo è di usarlo anche per la teledidattica.

Proprio per questo il Garr, Gruppo armonizzazione delle reti di ricerca, che gestisce le reti di comunicazione della ricerca e dell'Università italiane, è stata tra le prime realtà a volere aderire mettendo a disposizione un proprio server. Si chiama open.meet.Garr.it e consente di offrire un'opportunità alle scuole che hanno attualmente minori risorse. In questo riescono a offrire una soluzione semplice e gratuita da usare con una normale connessione ad Internet.

La piattaforma non è diversa da altri sistemi, ma è gratuita e open source e tutti possono collaborare alla sua crescita unendosi al gruppo Telegram dove si ritrovano una sessantina di sviluppatori e sistemisti. Dai due server iniziali messi a disposizione adesso sono cinquantasette gli hub che consentono di lavorare a distanza

V

Immagine tratta da: https://iorestoacasa.work/


Esc
Insert
PrtSc
Delete
Home
End
PgUp
Num Lock
Q
W
E
R
T
Z
U
O
P
G
H
J
V
B
N
7
Home
8
9
PgUp
1
End
3
PgDn
0
Ins
Del

e alleggerire così il congestionamento della rete italiana provocato dalla quarantena e dalla remotizzazione del lavoro e della didattica. E con un valore aggiunto: i server si trovano in Italia, i dati rimangono in Italia e le sessioni sono illimitate. Con un'interfaccia semplice e intuitiva si può utilizzare anche da cellulare. Insomma, anche nel design non ha niente da invidiare ai sistemi di videocall più famosi.

Per capirci, **Google Hangouts Meet**, il software di videoconferenza aziendale di Google che supporta fino a 250 partecipanti e 100.000 visualizzatori di streaming live è stato a pagamento fino a qualche settimana fa. Google ha promesso di rendere gratutito il servizio fino a settembre 2020. Anche Google Meet permette di condividere lo schermo e chattare coi partecipanti.

Stesse funzioni per **Zoom**, il software omonimo dell'azienda unicorno fondata nel 2014 in California dal cinese Eric Yuan dopo dieci anni passati alla guida di Webex, l'applicazione per videoconferenze di Cisco. Come iniziativa solidale l'accesso alla piattaforma è gratuito in queste settimane e può essere usata direttamente dal browser o scaricando l'app per iOS e Android. Rispetto alla versione aziendale, la versione gratuita di Zoom però connette fino a 100 persone per 40 minuti, seguendo un link di invito tramite email o messaggistica. La videochat permette di condividere documenti, video e foto, chattare, registrare la sessione e la versione a pagamento consente l'accesso a 1.000 partecipanti per un tempo illimitato.

Anche se adesso il padrone di Zoom ha reso l'applicazione disponibile gratuitamente si tratta comunque di un progetto commerciale che deve produrre utili. Al contrario il progetto della piattaforma italiana è non-profit, basato su un approccio solidale e collaborativo in cui più organizzazioni possono partecipare mettendo in comune i propri server. È così che ai primi due server si sono aggiunti gli altri messi a disposizione da aziende come BeFair, IFInet e Seeweb, associazioni come l'Italian Linux Society, istituzioni come il Garr e il Cnr, appunto, con l'Istituto di metodologie per l'analisi ambientale, Imaa.

Come ha spiegato uno dei suoi creatori, Riccardo Serafini, la community di progetto agisce in maniera coordinata riuscendo a monitorare le metriche dell'uso della piattaforma. Gran parte del lavoro è stato proprio adattare il software agli utenti italiani e renderne facile l'utilizzo. Si crea una stanza, si genera un link, si condivide una password affinché solo gli invitati possano partecipare. E poi, se serve, si può fare una diretta streaming pigiando un pulsante. I servizi disponibili sono visibili sul web e di volta in volta si può scegliere quale usare per un risultato ottimale.

Frutto di un percorso fatto da appassionati di software libero non c'è un grande attore che profila gli utenti e incamera i loro dati. Inoltre il software open source è su Github (una sorta di biblioteca di progetti software) e chiunque può verificare il codice per essere sicuri che non faccia cose strane di nascosto. Insomma se una scuola vuole usare i server di iorestoacasa.work per le lezioni in videopresenza lo può fare.

VIRALITÀ

QUANDO LA CONDIVISIONE FA MALE

Victoria Grand, vicepresidente di WhatsApp, durante una conferenza stampa in Indonesia ha dichiarato: «Abbiamo introdotto un limite di cinque inoltri valido in tutto il mondo a partire da oggi». La decisione, attesa da tempo, dovrebbe contribuire ad arginare la diffusione di «fake news» attraverso la popolare applicazione di messaggistica, considerata responsabile sia di linciaggi e uccisioni in India sia di interferenze nelle elezioni che hanno portato Jair Bolsonaro alla presidenza del Brasile.

Tra aprile e luglio 2018, infatti, 18 persone accusate di pedofilia e rapimenti di bambini in India sono state uccise in seguito alla diffusione di messaggi fasulli divenuti virali grazie alla possibilità di inoltrarne un gran numero e gratis.

Per quanto riguarda il Brasile, invece, secondo i cacciatori di bufale di «Aos Fatos», Whatsapp è stato il veicolo di milioni di messaggi pagati dai sostenitori di Bolsonaro contro lo sfidante Haddad, violando le norme elettorali e producendo uno spostamento dell'elettorato pari al 20% di voti.

Gli utenti di questa app - *acquistata da Facebook* - nel mondo sono un miliardo e mezzo ed è probabilmente per il suo successo che, nonostante l'uso del teatro di strada, la pubblicazione di materiali informativi e corsi ad hoc per alfabetizzare le persone sugli effetti delle fake news, WhatsApp ha deciso questa misura radicale ma che probabilmente non funzionerà.

Per un motivo semplice: con la crisi del giornalismo tradizionale le notizie false che provengono da familiari e amici appaiono più plausibili. Ma anche perché le notizie via WhatsApp, come ha notato una giornalista di «Aos Fatos», Tai Nalon, sono gratuite, mentre confrontarle e risalire alla fonte non lo è.

Per intervenire sui pericoli generati dalla viralità dei contenuti digitali anche Youtube ha deciso di limitare i «forward». La funzione che permette ai creatori di contenuti di condividere i propri video automaticamente nei principali social network.

Questa decisione segue a un'altra per la quale la popolare piattaforma ha deciso di rimuovere 8 milioni di video controversi dal sito negli ultimi mesi del 2018. L'operazione, cominciata con la rimozione di filmati che promuovono il gioco d'azzardo, si è estesa fino a bandire tutti i video con scherzi pericolosi o comportamenti al limite della pornografia.

A Gennaio 2019 Google ha infatti annunciato di aver aggiornato le proprie regole per postare i video, con l'intento di bloccare tutti quelli relativi a scherzi pericolosi e sfide estreme come versarsi liquidi infiammabili sulla pelle e darsi fuoco, fino alle gare in cui vince chi ingoia

il maggior numero di pasticche per la lavatrice.

Nel passato aveva destato molto scalpore il video di una donna che sparava al compagno per dimostrare che una pesante enciclopedia fosse in grado di fermare un colpo di pistola diretto al petto. L'uomo, Pablo Ruiz III, uno «youtuber» famoso per i suoi scherzi virali, era morto e la donna condannata.

D'ora in poi questi «scherzi», filmati e diffusi su YouTube, in seguito alle segnalazioni di persone rimaste ferite e uccise, non potranno essere più pubblicati.

W

WANNACRY

Nel 2017 un gruppo di hacker noto come Shadow Brokers informa un tale Jake Williams di essere in possesso di tutte le informazioni che lo riguardano.

Jake non è una persona qualsiasi, fa parte della *hacking unit* della National Security Agency, l'agenzia per lo spionaggio elettronico del governo americano.

Per dimostrargli che dicono la verità pubblicano sul suo stesso blog ogni riga del codice usato da Williams per attaccare i bersagli degli Stati Uniti e poi decidono di divulgare le sue pericolose cyber-armi.

Tra queste ce n'è una alla base del più grande attacco ransomware della storia, l'*exploit EternalBlue*, usato per bloccare i computer di mezzo mondo e farsi pagare un riscatto (ransom) per sbloccarli.

Secondo il glossario del CERT Nazionale **un 'exploit' è un "codice che sfrutta la vulnerabilità di un sistema permettendo l'esecuzione di codice malevolo, generalmente con lo scopo di acquisire i privilegi di amministratore della macchina colpita**." Ecco, questo exploit EternalBlue sfrutta una vulnerabilità di sistema delle macchine Windows non aggiornate, senza manutenzione, spesso quelle in uso alla Pubblica Amministrazione come scuole e ospedali, mentre a quelle nuove e ben tenute gli fa un baffo. E infatti è riuscito a bloccare ambulanze e pronto soccorsi inglesi, ferrovie russe e porti baltici.

EternalBlue viene utilizzato per installare la backdoor 'DoublePulsar' e prendere possesso del singolo pc che infetta ma

anche di prendere in ostaggio la rete in cui si trova. È così che nel 2017 circa 300mila computer in 150 paesi sono stati bloccati dal ransomware Wannacry.

ESET, azienda di sicurezza slovacca con sede anche in Italia, ci dice che EternalBlue nel 2018 è tornato a impazzare sulle macchine Windows non protette. Secondo l'agenzia di stampa AskaNews l'ultimo picco di infezione era coinciso con la campagna ransomware 'Satan' ma EternalBlue aveva permesso di continuare molti attacchi informatici di alto profilo nei mesi a seguire. Oltre a WannaCryptor, Petya, NotPetya ed ExPetya aveva favorito la diffusione del ransomware BadRabbit prima di Natale. E sempre secondo ESET è stato anche usato dal gruppo di cyberspionaggio Sednit - noto anche come Fancy Bear e Sofacy - per attaccare le reti Wi-Fi negli hotel europei.

Adesso si scopre che lo stesso exploit è stato utilizzato per diffondere crypto miner maligni.

I ricercatori di AlienVault hanno identificato una nuova famiglia di malware per l'*estrazione* fraudolenta di cryptovalute, battezzata **MassMiner**. A partire da una macchina Windows infetta, MassMiner si diffonde inizialmente sulla rete locale prima di tentare di propagarsi attraverso Internet. MassMiner include una variante (*fork*) di MassScan, strumento in grado di eseguire la scansione Internet di server vulnerabili sui quali diffondersi in pochissimo tempo. Anche MassScan usa EternalBlue.

E questo è uno dei motivi per cui le associazioni a difesa della privacy e dei diritti digitali come Access Now hanno chiesto a più riprese al governo americano di non accumulare e di non tenere nascoste queste che sono vere e proprie cyber-armi, ma di avvisare subito chi può renderle innocue, le agenzie pubbliche e le aziende di informatica, per impedirne un uso incontrollato.

WEB

BUON COMPLEANNO AL WEB

W come Web. WWW come World Wide Web. Il Web, La Ragnatela mondiale. Il 12 marzo del 1989 uno scienziato inglese, Tim Berners Lee, presenta il progetto di un sistema di condivisione di documenti elettronici per facilitare la comunicazione e la cooperazione scientifica tra i suoi colleghi del centro di ricerche nucleari

di Ginevra, il CERN, quello del Bosone di Higgs, per intenderci. La sua idea era la stessa vagheggiata dallo psicologo Joseph Robnett Licklider che sviluppò a fini civili il primo progetto per Internet, cioè creare una biblioteca universale di documenti elettronici. Tim Berners Lee però fece di più: insieme al collega belga Robert Cailliau avviò lo sviluppo di un linguaggio per visualizzare sullo schermo di un computer questi documenti, l'HTML, Hyper Text Markup Language, e collegarli tra di loro tramite l'HTTP, Hyper Text Transfer Protocol.

È solo dal 1991 che però celebriamo la nascita del web poiché il 6 agosto dello stesso anno Berners Lee mise online il primo sito web del CERN.

Tim Berners Lee negli ultimi anni è diventato molto critico con la sua creatura dicendo che a causa del web abbiamo perso il controllo dei nostri dati; che è troppo facile spargere disinformazione e bufale sul web; che la propaganda politica online andrebbe regolata e resa trasparente, altrimenti il web sarà sempre di più uno strumento di manipolazione e di controllo dei suoi utilizzatori.

In occasione del 29esimo anniversario della sua "invenzione", Tim Berners Lee ha lanciato un nuovo allarme dalle pagine del giornale inglese The Guardian: "Le piattaforme web sono diventate un'arma". Vuol dire che Facebook, Twitter, Google e Co. non sono più strumenti di emancipazione, ma di controllo delle idee e delle opinioni che attraverso di essi vengono condivise.

In effetti Google gestisce quai il 90% delle ricerche online mondiali, Facebook è la nazione più grande del pianeta coi suoi 2,2 miliardi di utenti attivi mensilmente e, come dice il Guardian, le due società, con le loro controllate, YouTube e Instagram, assorbono più del 60% della spesa pubblicitaria digitale in tutto il mondo. Motivo questo degli enormi profitti che le aziende capofila cercano di non farsi tassare nei paesi dove li producono bensì dove hanno agevolazioni fiscali come l'Irlanda o il Belgio.

Queste piattaforme sono responsabili della distruzione della biodiversità del web, quella rappresentata da siti e blog indipendenti.

Ma è vera anche un'altra cosa: il web così come lo conosciamo e usiamo è solo un quarto di tutto il web. Pensatelo come un iceberg. La punta è fatta dal Clear Web o Surface Web, quello dove troviamo Twitter, Microsoft, le università, i siti dei cantanti preferiti. Sotto il pelo dell'acqua c'è il Deep web, il web profondo, che per definizione è la parte del web non indicizzata dai motori di ricerca e che quindi non compare nei risultati di Google se la cerchiamo con delle parole chiave, le "keyword". Nel Deep Web ci sono database scientifici a pagamento e i contenuti che richiedono login e password. All'interno del Deep Web troviamo il Dark Web, il web oscuro che è accessibile solo con software specifici come TOR, usato da spioni e criminali, ma anche da attivisti, hacker e perseguitati politici che non vogliono essere trovati. Nel Surface, Deep e Dark Web troviamo allo stesso modo contenuti che sono legali e illegali, morali o immorali, sicuri o insicuri. Il Dark Web si chiama così solo perché è più difficile da trovare non perché sia più pericoloso.

Z

ZERO DAY

LA FALLA DI TELEGRAM PRODUCE CRYPTOMONETE

Z come zero day. Uno "zero day" è un tipo di vulnerabilità del software sconosciuta agli stessi produttori che, se sfruttata, è in grado di offrire su un piatto d'argento a malintenzionati e centrali criminali il controllo di computer, tablet e smartphone di vittime ignare.

È successo anche a Telegram. I ricercatori di Kaspersky Lab, azienda russa di sicurezza informatica, hanno scoperto una di queste falle, il così detto zero day, all'interno del programma di messaggistica creato dai fratelli Durov, russi anch'essi. Telegram è un software per le comunicazioni riservate che consente comunicazioni cifrate dall'emittente al destinatario (la famosa cifratura end-to-end), ma anche di inviare file pesanti, video e testuali, con un buon livello di protezione, motivo per cui è stato spesso usato dai terroristi dell'isis per scambiarsi istruzioni e diffondere video di propaganda. Telegram, nato come software libertario e anti-spioni nell'autoritaria Russia come atto di ribellione e manifesto pro-privacy, è diventata da qualche anno una delle app di chat e messaggistica più diffuse al mondo, per un volume di 15 miliardi di messaggi giornalieri, proprio grazie alla robustezza del suo software crittografico. E per questo in molti, comuni mortali, la usano ritenendosi al riparo da intercettazioni e spioni. Ma la scoperta di questa falla dimostra che anche Telegram può avere dei problemi.

Non è la prima volta che capita con queste app di messaggistica che invece di nasconderli, svelano i segreti che gli vengono affidati. Pochi mesi fa la stessa Kaspersky aveva individuato un malware, un software maligno di tipo Trojan, in grado di rubare i messaggi di WhatsApp, dal nome SkyGoFree.

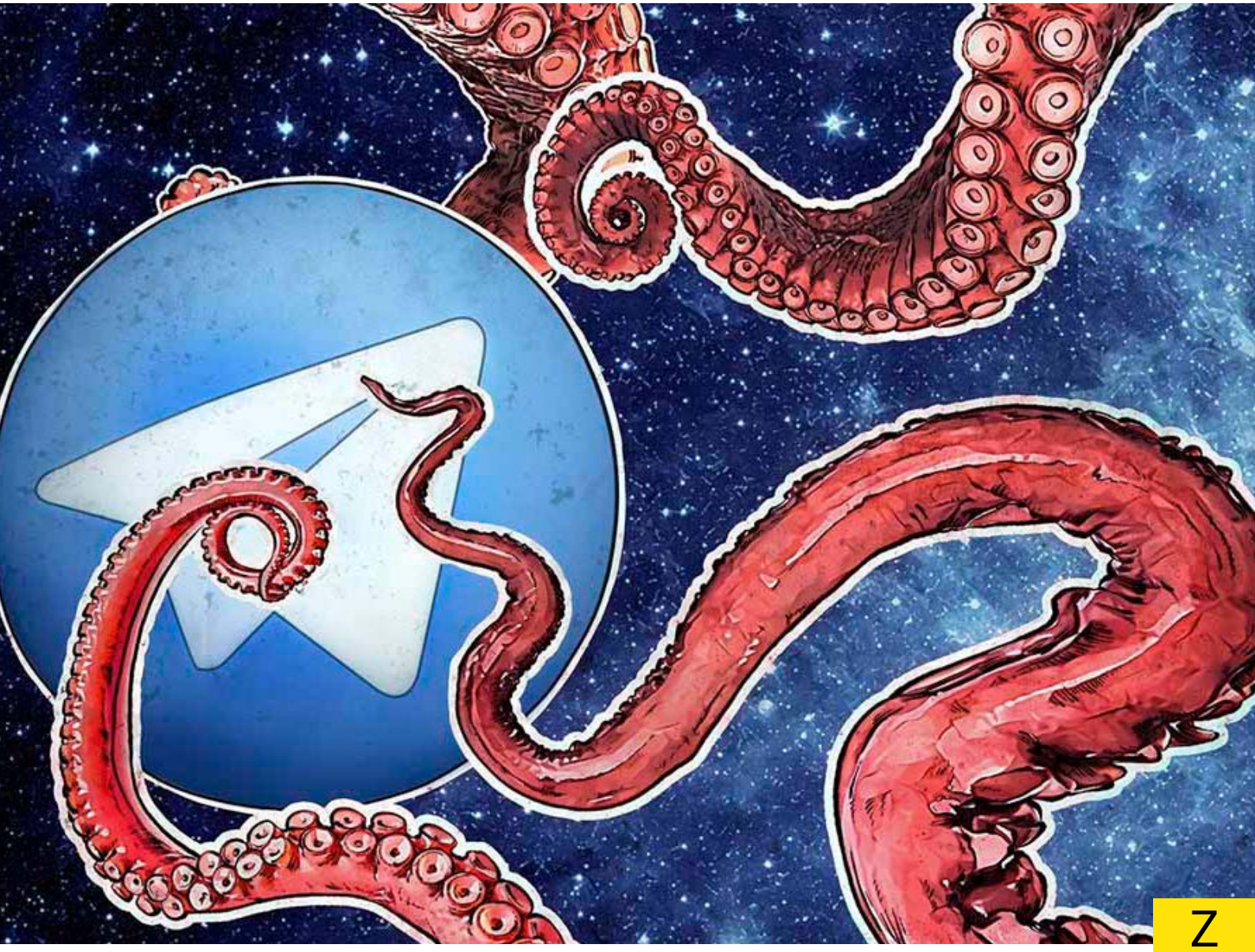
La vulnerabilità individuata in Telegram dai ricercatori stavolta però fa una cosa diversa: permette di controllare da remoto il computer su cui è installata la versione desktop del software per "minare" delle cryptomonete, le monete elettroniche cifrate tipo Bitcoin. Come? Utilizzando la potenza di calcolo dei computer su cui è installato il software bacato e, all'insaputa del proprietario, risolvere complessi algoritmi matematici la cui soluzione viene remunerata in monete digitali da spendere come tali o da cambiare in moneta sonante (in Islanda ci paghi anche il caffè).

La valuta digitale più famosa interessata dalla falla di Telegram si chiama Monero, un cryptovaluta già coinvolta nella vicenda di Wannacry, il ransomware che nell'estate 2017 bloccò l'accesso a 300 mila computer in tutto il mondo.

La falla, segnalata dai ricercatori è già stata corretta. E tuttavia, se possiamo ancora fidarci di tutte queste app per comunicare in privato da smartphone e pc, perché basate sulla crittografia, bisogna ricordare che le app stesse

vanno costantemente aggiornate, ma se il computer o il telefonino è già compromesso, con uno spyware, ad esempio, cioè a causa di un software spia installato da un marito geloso, un agente segreto o un ladro di segreti commerciali, non servono a niente.

La raccomandazione è sempre quella di aprire messaggi e allegati di persone di cui ci fidiamo e avere un antivirus sul proprio dispositivo in grado di intercettare contenuti dannosi. L'abitudine di mandarsi file video o .pdf sul telefono via app sta infatti diventando una vera e propria piaga visto che sempre più spesso contengono codice malevolo in grado di impossessarsi del telefono e acquisire da remoto il controllo di microfono, telecamere e, ciliegina sulla torta, rubarci i messaggi e la rubrica dei contatti.



ZOMBIE

COME SOPRAVVIVERE ALL'APOCALISSE DEGLI ZOMBIE ONLINE, LA CHECKLIST

Halloween è passato da un po' ma gli zombie non sono tornati nelle tombe. Stanno lì fuori ad aspettare che ti distrai per azzannare i tuoi dispositivi, quegli oggetti intelligenti che ti permettono di programmare l'ora in cui si accende il riscaldamento, l'apertura del garage, lo smartwatch che registra le tue sessioni di fitness. Ma anche la stampante dell'ufficio e la webcam con cui si controllano bambini e babysitter.

"Gli zombie online non hanno bisogno di mordere fisicamente te o il tuo dispositivo per causare dolore. Gli basta sedere al tuo stesso ristorante, accedere al router Wi-Fi o essere gli amministratori di rete del tuo hotel. Questo è tutto ciò di cui hanno bisogno per rubare i dettagli della tua vita privata o scoprire informazioni sulle tue operazioni finanziarie. E a te non rimane che sperare che non si approprino dei tuoi dati o ne facciano cattivo uso."

La metafora di **Avira**, una società che produce antivirus contro i malware, i software maligni che prendono possesso dei computer e degli smart device connessi in rete con un numero di IP (Internet Protocol), è efficace e non è troppo lontana dalla realtà: i computer zombie esistono per davvero. Sono i pc infetti che possono essere resuscitati a comando per trasferire i tuoi dati a terzi, rubare cartelle cliniche e dati bancari, e possono essere utilizzati per attacchi Internet su larga scala, i DDoS, i Distributed Denial of Service. I DDoS sono le negazioni di servizio che si verificano quando un numero elevato di richieste viene rivolto contemporaneamente a uno stesso servizio Internet, facendo collassare il server che non riesce a soddisfarle tutte. Per capirci, è come una folla di gente che si catapulta dentro un concerto da una porticina secondaria: la porta non sarà abbastanza grande per far passare tutti e potrebbe finire in frantumi.

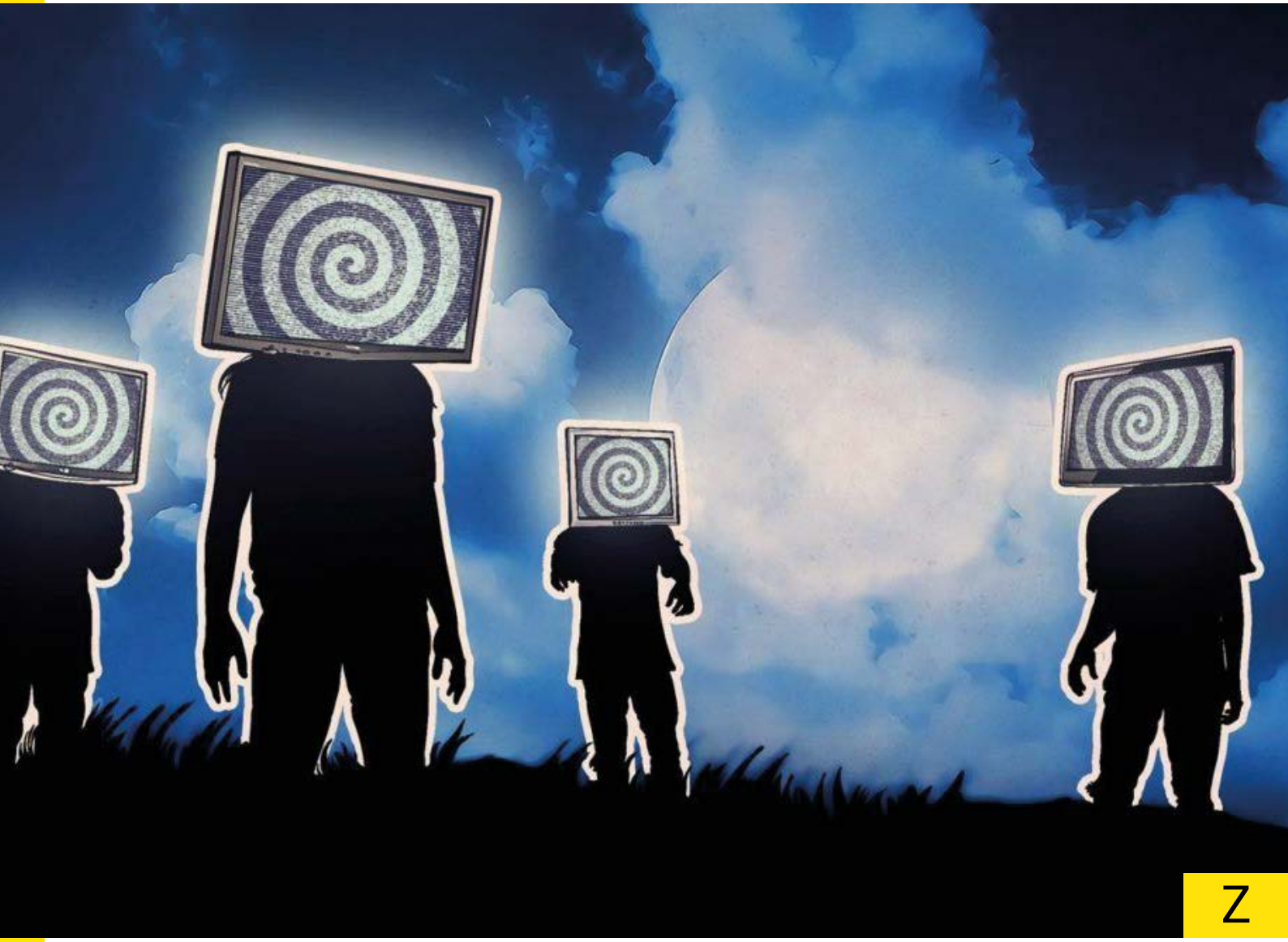
Qualcosa di simile è successo il 21 ottobre 2016 quando un attacco DDoS ha preso di mira un DNS provider, Dyn, con il compito di smistare il traffico Internet verso servizi come Amazon, Netflix, Twitter e altri. L'attacco, portato da una rete di computer zombie, una botnet infettata dal software Mirai, ha creato un disservizio per milioni di utenti. Oggi sappiamo che lo stesso tipo di tecnica, con una variante dello stesso tipo di botnet, la Botnet #14, ha preso di mira un paese africano di nome Liberia.

Come gli esperti avevano preconizzato, non si trattava probabilmente di un golpe verso quel paese ma di un test: i criminali volevano testare la capacità di tenuta di Internet quale infrastruttura di trasporto dei dati digitali. E lo hanno fatto reclutando computer zombie da aggiungere all'esercito di botnet che non sono solo i nostri computer dell'ufficio ma

telecamere, videoregistratori e stampanti che popolano case, scuole e università.

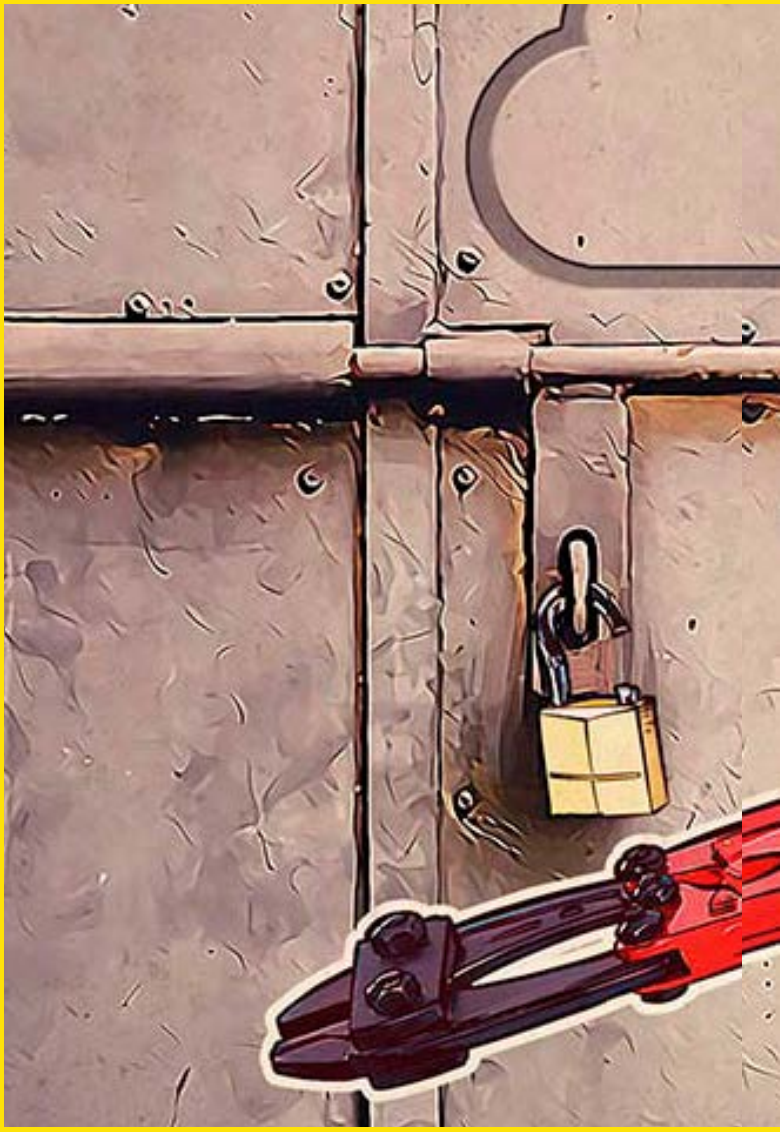
Ironia della sorte è che ci riescono per un errore banale: gli oggetti intelligenti connessi alla rete non sono protetti da password adeguate e i venditori di questi oggetti non se ne preoccupano di avvertircene.

Non basta allargare le porte dei servizi che usiamo sul web per impedire che i server che ci danno quello che cerchiamo in rete collassino. Forse potremmo nascondere l'IP di questi dispositivi, oppure crittografarli, oppure usare una *Virtual Private Network* che da internet non sia visibile, oppure seguire i consigli di OTA, la Online Trust **Alliance**, che ha rilasciato delle **linee guida** per rendere sicuro ogni router, telefonino, automobile e televisore intelligente e impedire che un malvivente possa introdursi nella nostra quotidianità, impossessarsi dei nostri dati personali o peggio, con effetti a cascata sulle nostre vite (https://otalliance.org).



10 COSE DA FARE PER METTERE AL SICURO CASA, DATI E UFFICIO

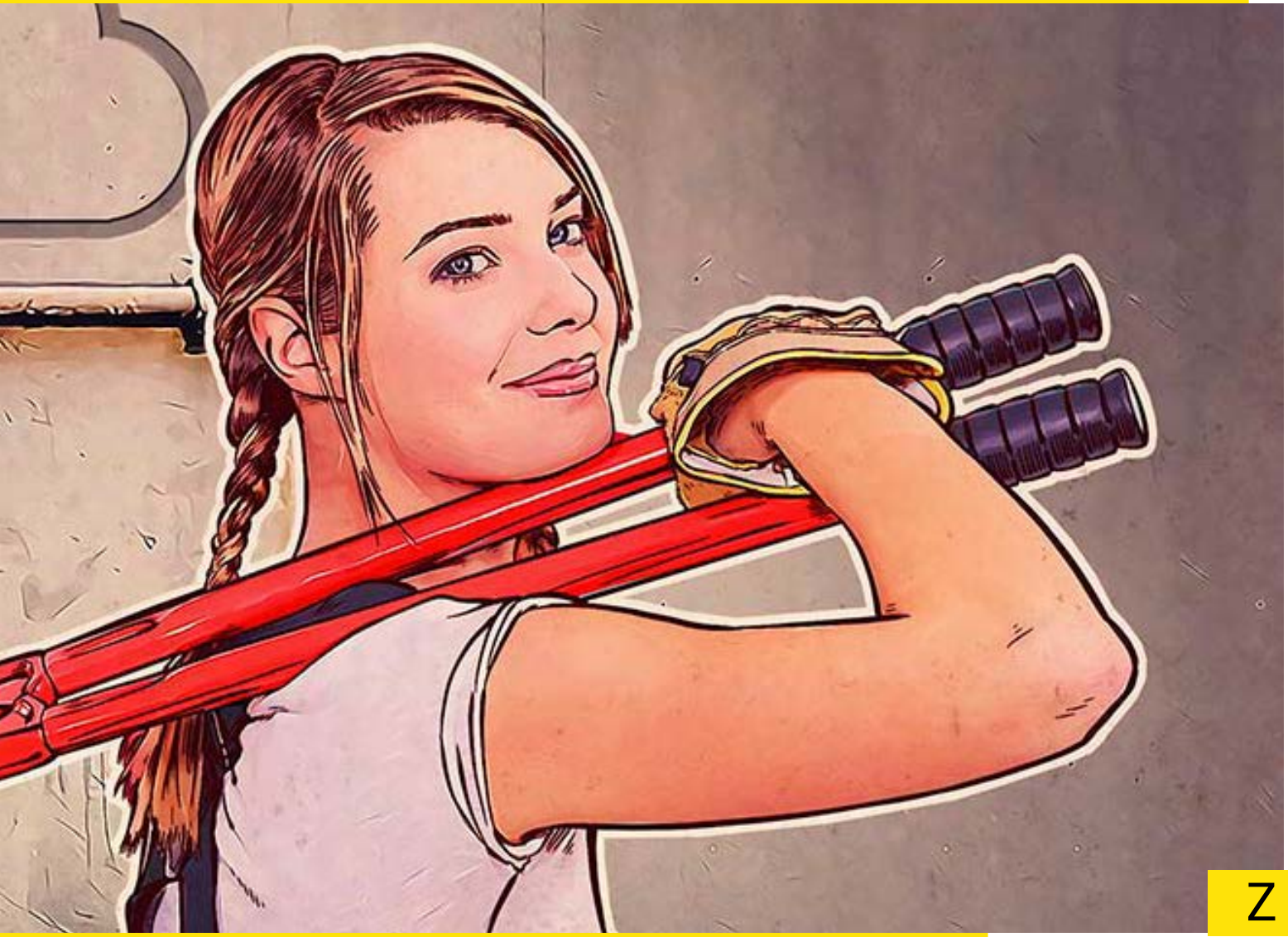
1. **Fai un inventario** di tutti i dispositivi casalinghi e dell'ufficio connessi a Internet o altre reti. Controlla lo stato dei router e disabilita TUTTI i dispositivi sconosciuti.
2. **Contatta il tuo Internet Service Provider** (ISP) per aggiornare router e modem agli standard di sicurezza attuali. Cambia il nome del tuo SSID in maniera che non identifichi te stesso o la tua famiglia.
3. **Verifica le informazioni di contatto** di ogni dispositivo inclusa una email dove ricevere aggiornamenti di sicurezza ed eventuali notifiche.
4. **Assicurati** che ciascun dispositivo e la relativa app **ricevano aggiornamenti di protezione in maniera automatica** e controlla i siti loro relativi per eventuali aggiornamenti di correzione del firmware.
5. **Controlla tutte le password e gli account utente** ed evita di usare la stessa password per dispositivi diversi. Cancella tutti i guest code che non usi più. Dove possibile attiva la doppia autenticazione per ridurre il rischio che i tuoi account possano essere violati. Questo metodo permette solo a te di accedere l'account e non a qualcuno che conosce la tua password.
6. **Rivedi le tue abitudini** e le preferenze relative alla privacy e l'uso che fai dei tuoi dispositivi, compreso l'immagazzinamento di dati e la loro condivisione con altri. I tuoi setting possono essere cambiati inavvertitamente durante gli aggiornamenti. Resettali affinché rispettino le tue preferenze.
7. **Controlla la garanzia di ogni dispositivo** e le indicazioni sull'assistenza. Se un prodotto non viene più supportato per gli aggiornamenti smetti di usarlo o disconnettilo dalla rete.

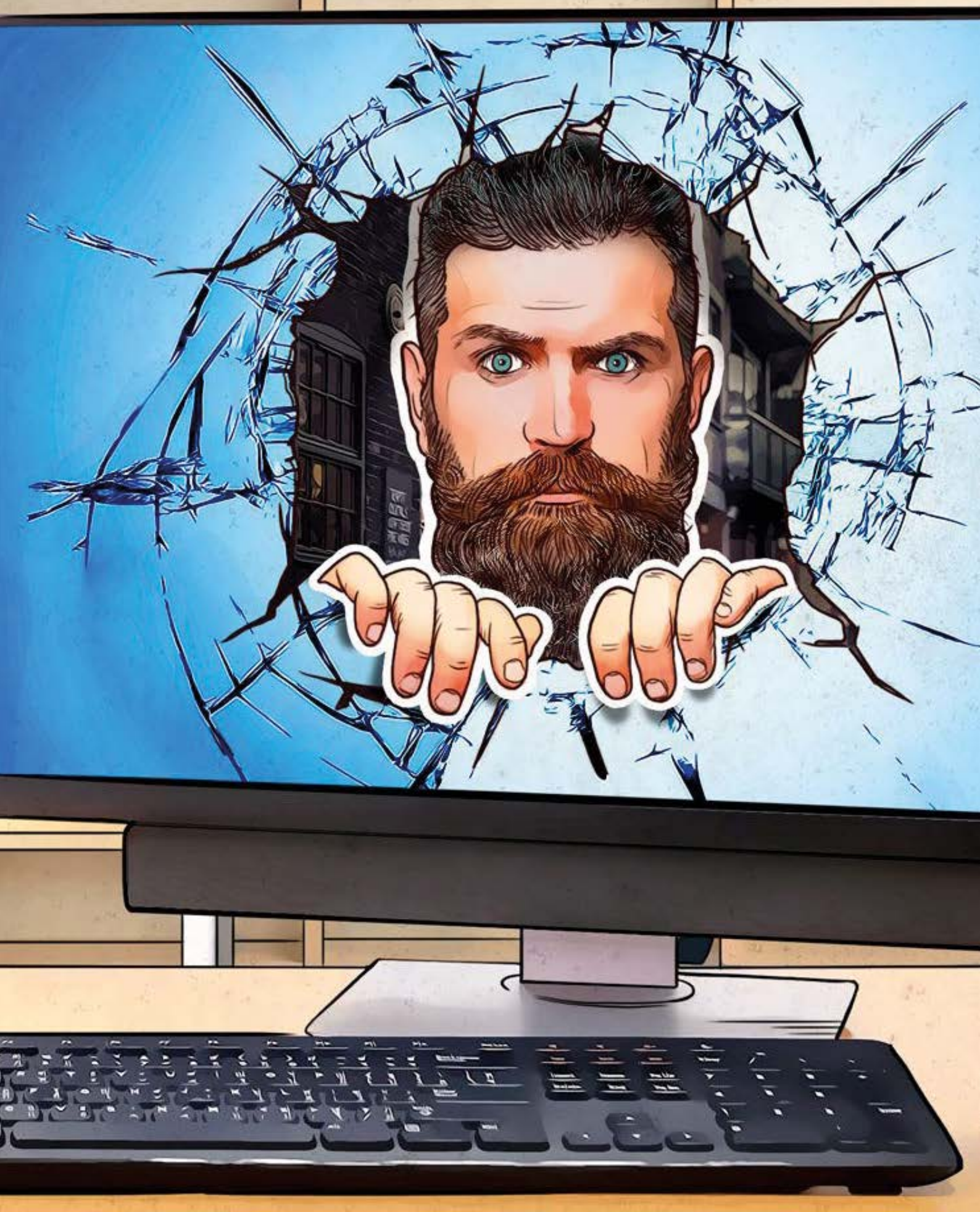


8. Prima di smettere di usare un qualsiasi dispositivo, di mandarlo indietro o di rivenderlo, **ricordati di cancellare ogni dato che ti riguarda e ristora i setting originali.** Disabilitane l'account online e cancellane i dati.

9. **Controlla i privacy setting del telefonino** compresa la geolocalizzazione, i cookies, i contatti, il Bluetooth, il microfono e tutte le altre impostazioni e preferenze. Imposta questi ultimi in maniera che ogni applicazione ti chieda cosa vuoi fare prima di avviarla e di condividere dei dati.

10. **Fai un Back up di tutti i documenti personali** e delle fotografie e memorizzali in dispositivi che non siano sempre connessi a Internet. c'è bisogno di fare tutto in una volta, ma l'importante è farlo asap (as soon as possible).





Un computer sicuro non è un computer spento

Negli ultimi mesi le incursioni dei malfattori digitali hanno fatto registrare una paurosa impennata di attacchi e solo quelli più gravi sono stati trattati dai giornali.

Nell'ottobre del 2018 criminali ancora sconosciuti sono entrati in possesso di nomi, cognomi, codici fiscali e codici identificativi di 731.519 clienti della banca Unicredit individuando le password di 6.859 utenze, alle quali la banca ha bloccato l'accesso una volta scoperta l'intrusione.

A novembre c'è stato il furto di 500mila identificativi delle caselle di Posta Elettronica Certificata (PEC) di ministeri, militari e forze dell'ordine, banche e aziende.

A causa della gravità del fatto molti tribunali che hanno adottato il processo telematico hanno interrotto le attività in via precauzionale da uno a tre giorni. Con la Pec infatti vengono notificati atti giudiziari, circolari ministeriali e documenti amministrativi. In questo caso gli inquirenti hanno parlato dell'attacco di attori stranieri organizzati.

Nei mesi di novembre, dicembre e gennaio i tre collettivi di hacker attivisti più famosi d'Italia, LulzSecIta, InfosecIta e Anonymous Italia hanno scorrazzato liberamente nei database dei ministeri dello Sviluppo Economico, della Difesa e dell'Università; hanno racimolato indirizzi, nomi e cognomi di iscritti alla Lega Nord, al Partito Democratico e a Fratelli d'Italia di cui hanno spesso cambiato la homepage defacciandola e messo in crisi associazioni industriali.

Nel caso degli Anonymous si è trattato di azioni dimostrative per denunciare la scarsa protezione dei dati personali di cittadini, clienti, elettori, ma le ultime azioni sono state dirette a protestare contro le morti bianche – più 10% nel 2018 – di chi un lavoro malpagato ce l'ha ma da precario.

A gennaio 2019 è stata resa nota la notizia dell'esistenza di un archivio di 773 milioni di email rubate. Dalle analisi effettuate 10 milioni di password associate a queste erano "nuove", cioè mai finite prima in un dataleak intercettato dagli esperti. Tutto in vendita online a 45 dollari.

L'archivio, denominato Collection #1 era solo il primo di altri quattro, dal peso di 1 terabyte (lo spazio necessario a riempire 1400 compact disc).

In queste 'collection' i ricercatori di cybersecurity hanno trovato migliaia di indirizzi italiani, compresi quelli di Bankitalia, Corte dei Conti, e quelli che i Servizi Segreti usano per fare attività d'intelligence su fonti aperte, blog, forum, social network. Al loro interno un insieme di credenziali illegali che comprendono *databreach* precedenti come Exploit. in dove negli anni scorsi erano finiti 1.500 account universitari, 1.200 di giornalisti e 900 di parlamentari.

Il rischio rappresentato da questi furti di credenziali è grave.

Con email e password della vittima, lo ripetiamo, si possono rubare l'accesso ai social, chiedere un rimborso non dovuto, ordinare acquisti, leggerne la corrispondenza, prenderne il posto con un furto di identità vero e proprio. Non è una prospettiva allettante.

CHE FARE ALLORA?

Hai installato l'antivirus, messo dei filtri alla posta elettronica, aggiornato il sistema operativo ma sei lo stesso diventato preda di un cybercriminale. Forse sei stato convinto ad usare un'app o ad accedere a un sito truffaldino, e così qualcuno ha preso il controllo del tuo account, qualcuno che non vuole infettarti il computer o rubarti il numero della carta di credito ma solo introdursi all'interno della tua vita, e rimanerci il più a lungo possibile. E l'unica cosa che gli preme è evitare di essere individuato. Sarebbe un bel guaio, visto che gli attacchi distruttivi e le frodi prima o poi finiscono sui giornali mentre un account compromesso lo rimane per mesi o anni.

A dispetto del fatto che stiamo attenti a non cliccare su allegati sospetti e che usiamo buoni antivirus per la posta elettronica, gli attaccanti usano tecniche sempre più sofisticate e gli attacchi sono oggi così ingegnosi che queste attenzioni non bastano più, anche perché molte organizzazioni abbandonano l'email per coordinarsi e gli preferiscono *Slack* e altre piattaforme per la collaborazione interna. Chi non cliccherebbe sul messaggio di un utente "fidato" nella chat interna dell'ufficio? Ma questi strumenti non hanno in genere nessuna protezione da phishing e malware.

E poi, pensiamoci. Sebbene i messaggi di phishing siano il modo più comune per i malfattori di accedere a un account, non sono l'unico strumento. I databreach degli ultimi mesi hanno creato un mercato fiorente per scambiarsi o vendere password rubate. Anche la violazione di un database che non include nome utente e password email, potrebbe offrire informazioni personali (indirizzo, scuola, nome da nubile della madre) che consentono agli aggressori di ottenere un accesso temporaneo richiedendo una modifica della password.

Di fronte a un dataleak, la diffusione non autorizzata di dati personali, si consiglia sempre di cambiare la password se il proprio account è stato compromesso e tuttavia il primo passo nella maggior parte degli attacchi che lo precedono include la creazione di una "backdoor" secondaria che non utilizza l'accesso principale. Ad esempio, gli attaccanti possono usare applicazioni cloud malevole e *token*, profili di accesso permanenti e non revocati, o specifiche regole di posta elettronica per inoltrare e reindirizzare i messaggi dell'account violato senza la necessità di accedervi nuovamente.

Questo è un grosso pericolo perché oggi sia i cybercriminali che gli hacker pagati dagli stati non solo attaccano le infrastrutture critiche (centrali elettriche, dighe ed aeroporti), ma rubano tecnologia militare e seminano discordia con notizie false e attaccano obiettivi "civili" come scuole, università, assicurazioni e ospedali, attraverso i loro dipendenti. E se non ci riescono, prendono di mira i famigliari e il circuito di relazioni che gli girano intorno.

L'obiettivo degli attaccanti è utilizzare i dati raccolti come punto di partenza per la raccolta di informazioni ancora più importanti: un progetto governativo, una fusione aziendale, un nuovo prodotto commerciale. E attaccano i singoli perché è più facile di hackerare un'università o un'agenzia governativa. Attaccano i figli per colpire i padri, il contabile per arrivare all'amministratore delegato, lo studente per arrivare al rettore. Un account compromesso oggi potrà essere usato domani per raccogliere informazioni strategiche in campo economico e industriale, militare e di sicurezza nazionale.

Si è detto tante volte che l'unico computer sicuro è un computer spento. Non ci sembra la strada giusta.

Perciò è tanto importante proteggere i dati privati e i database che li contengono e sviluppare una cultura della sicurezza trasversale a ogni settore della società.

Perciò abbiamo realizzato questo libro, nella speranza che vi torni utile.


DATA ACQUISITION
DATA ANALYSIS
VERDICT
Search

Scheda

LA VERA STORIA DI INTERNET. ATTENZIONE: NON NACQUE COME PROGETTO MILITARE

Internet non è nata come progetto militare. Levatevelo dalla testa. Internet è nata per battere i sovietici nella corsa allo spazio. Come? Collegando fra di loro i migliori scienziati americani e facilitando lo scambio dei dati fra i centri di supercalcolo sparsi negli Stati Uniti.

L'idea fu di Dwight David "Ike" Eisenhower, il presidente americano che da generale aveva guidato lo sbarco in Normandia per sconfiggere i nazisti di Hitler. Il presidente, preoccupato che l'America perdesse la propria egemonia scientifica, tecnologica, economica e militare dopo il lancio nello spazio dello Sputnik sovietico nel 1957, riunì attorno a sé i migliori cervelli dell'epoca e nominò il rettore del MIT James Killian a capo dell'Arpa, Advanced Project, Research Agency (Agenzia per i progetti di ricerca avanzata) per contrastare il milione di scienziati messi in campo dalla Russia.

Pochi anni dopo, ma prima che nel 1972 l'Arpa assumesse compiti militari diventando DARPA (Defense Advanced Project, Research Agency), la rete Arpanet, progenitrice di Internet, era già nata.

LO SFORZO CONGIUNTO DI MILITARI E ACCADEMICI

Lo sforzo di creare una rete per migliorare l'allocazione delle risorse umane e finanziare dedicate alla ricerca scientifica richiedeva un alto grado di collaborazione a tutti i livelli, tra aziende, militari e accademici, ma furono questi ultimi a teorizzare la rete delle reti e a svilupparne la tecnologia.

Divenuto capo dell'ufficio dedicato al progetto, un giovane psicologo, **Joseph Robnett Licklide**r, teorizzò l'Intergalactic Computer Network a partire da una sua idea di come dovessero essere le biblioteche nel futuro, consultabili da chiunque a da qualsiasi posto. Ma fu il suo successore, **Larry Roberts**, brillante ingegnere, che sviluppò l'idea dell'Arpa Net, il network di computer dell'agenzia. Era il 1967.

L'idea semplice, quasi banale di Roberts era di creare una rete distribuita di computer per evitare gli spostamenti umani e usare le risorse di calcolo laddove c'erano già, ma doveva risolvere il problema di far parlare i computer tra di loro.

Certo dovevano essere collegati attraverso una normale linea telefonica, magari dedicata, ma come tradurre il linguaggio di macchine eterogenee e far viaggiare i bit senza perderli? Gli vennero allora in aiuto le ricerche quasi contemporanee di **Leonard Kleinrock**, **Paul Baran** e **Donald Davies**, che intorno al 1965 erano arrivati a teorizzare la trasmissione dei dati con la commutazione di pacchetto: per dirla in parole semplici i dati avrebbero dovuto viaggiare linearmente e in sequenza come i vagoni di un trenino con dentro le istruzioni (i metadati) aggiuntive sul viaggio che dovevano fare.

Ma questa geniale intuizione non risolveva il problema di come far parlare computer di reti diverse e allora Roberts usò gli studi di **Wes Clark** sugli Interface Message Processor (IMP). Gli IMP, costruiti poi dalla Bolt Beranek e Newman nel 1969, erano computer intermedi tra i nodi host, instradavano il traffico tra le macchine, non sovraccaricavano i mainframe dedicati ai calcoli e standardizzavano il traffico. Facevano più o meno quello che fanno gli odierni router.

LA NASCITA DI ARPANET

Così, definite le regole di comunicazione tra host e IMP grazie a una Rfc (Request for comments) di Stephen Crocker, nel 1969 venne realizzato il primo collegamento tra i computer dell'Università della California Los Angeles (Ucla) e lo Stanford Research Institute di Palo Alto. Era il 29 Ottobre. Altri due nodi vennero aggiunti entro dicembre, l'Università della California Santa Barbara (UCSB) e quella dello Utah: era nata Arpanet.

Gli studi successivi di **Vinton Cerf** e **Bob Kahn** risolsero il problema di non perdere pezzi di informazione. Nel primo collegamento infatti, la parola da trasmettere, Login, arrivò solo in due lettere "LO", che pure diceva che l'esperimento aveva funzionato. Ma con la definizione del TCP/IP (Transmission Control Protocol/Internet Protocol), i dati non venivano più persi perché l'IP gli dice dove devono andare e il TCP come si devono comportare i computer che comunicano tra di loro. Era il 1973, e fu Bob Kahn a usare il termine Internet per le reti che si fossero scambiati i dati via TCP/IP, riservando il nome internet con la i minuscola alle sole tecnologie che consentivano di farlo.

Prima che Arpanet diventasse Internet, però passò altro tempo.

Nel 1983 il TCP/IP divenne lo standard di comunicazione di Arpanet e la parte della rete dedicata alle comunicazioni militari divenne Milnet. Quando altre reti cominciarono a scambiarsi permanentemente i dati con quei protocolli cominciò ad affermarsi il termine Internet per la rete Arpanet.

L'AVVENTO DEL WEB E L'ITALIAN INTERNET DAY

Il resto è storia recente. Nel 1985 nasce NSFNet, la rete della Fondazione americana per la scienza (National Science Foundation), che doveva collegare i centri di supercomputing americani con delle dorsali di trasmissione dedicate (backbone). Nel 1990 Arpanet fu

chiusa e la rete della NSF andò incontro a un processo di evoluzione in cui ai sussidi federali si affiancarono quelli di molte aziende private come Mci. NsfNet chiuderà nel 1995. Ma nel frattempo non smettevano di moltiplicarsi i computer privati collegati in rete e accessibili dai cittadini. Perché?

Nel 1991 era nato il World Wide Web (Ragnatela attorno al mondo) che permetteva di sfruttare agevolmente la capacità trasmissiva della rete basata su TCP/IP. Ed era nato dall'idea di uno scienziato inglese che aveva progettato un sistema di relazione ipertestuale tra documenti elettronici, l'HTML (Hypertext markup Language), ancora una volta, per facilitare il lavoro degli scienziati delle alte energie, stavolta però accadeva in Europa, al CERN di Ginevra.

Insieme all'Http (Hyper Text Transfer Protocol) e al sistema degli Url (Uniform Resource Locator) che costituirono il primo nucleo del web, Internet uscì fuori dai laboratori di ricerca e hacker e appassionati ne svilupparono i programmi che usiamo ancora oggi, come il browser Mosaic che permetteva di accedere i documenti elettronici e ipertestuali residenti sui computer collegati via Internet e anche di "leggere" i primi siti web.

Intanto però era successa una cosa che ci riguarda da vicino: il 30 aprile 1986 dall'Italia e precisamente da Pisa, era partito un pacchetto di bit verso il Telespazio in Abruzzo: sparato al satellite Intelsat V era atterrato in un battibaleno a Roaring Creek in Pennsylvania (Usa).

Anche l'Italia era collegata a Internet, ops, Arpanet.

MANUALE DI AUTODIFESA

ASSISTENTI VIRTUALI/SMART SPEAKER

Hey, Google, mi cerchi questa strada? Alexa, mi ordini la pizza? Gli assistenti virtuali comandati attraverso gli Smart Speaker che ci mettiamo anche in cucina lavorano al posto nostro e sembrano capire sempre quello che vogliamo. Ma non è proprio così.

Il funzionamento di questi dispositivi è semplice: il consumatore "risveglia" l'assistente con una wake-up word, cioè una "parola d'ordine" come "Alexa", "Hey, Siri", e impartisce dei comandi. L'audio, spedito a un servizio online (in cloud) viene analizzato per capire l'ordine e procedere all'esecuzione basata su una libreria di richieste già pronte che tiene traccia di quelle precedenti.

Gli assistenti virtuali riescono a rispondere ai comandi vocali, inviare messaggi di testo, effettuare telefonate, impostare un promemoria e tra breve, secondo i ricercatori, potranno discutere con noi come fanno i membri di una famiglia vera. Qualsiasi cosa si possa fare con un cellulare, si può anche chiedere che venga fatta dall'assistente virtuale. Ma già oggi possono rispondere a domande, raccontare barzellette, riprodurre brani musicali e controllare oggetti domestici come luci, termostati, serrature e dispositivi per la casa intelligente (smart home).

Gli stessi smart speaker che ci mettiamo in casa sono "sempre" connessi a Internet e ad altri oggetti intelligenti e possono essere attivati da lontano, tramite cellulare, smartwatch, o altri apparecchi diventando il punto di accesso a una rete aziendale o domestica e per questo sono una preda ambita dai delinquenti.

- **FARE UNA LISTA DEI DISPOSITIVI INTELLIGENTI CHE ABBIAMO IN CASA.**
- **CAMBIARE SUBITO LA LOGIN E LA PASSWORD DEL DISPOSITIVO.**
- **RICORDARE CHE L'ASSISTENTE È SEMPRE IN ASCOLTO.**
- **SPEGNERLO QUANDO DECIDIAMO CHE NON CI SERVE.**

BEC - BUSINESS EMAIL COMPROMISE

Avete mai ricevuto un'email che vi chiede di pagare una fattura per qualcosa che non avete comprato? Avete ricevuto la conferma di un acquisto ordinato in rete, o di un affare da completare? Probabilmente sì, e se non gli avete dato seguito avete fatto bene.

In genere queste richieste sono fasulle e rappresentano un tipo di truffa online che gli esperti chiamano *Business Email Compromise* (Bec) perché usano account email rubati ai legittimi proprietari.

In questo tipo di truffe i malfattori si presentano via email come il datore di lavoro, un fornitore o un collega, e chiedono alla vittima di inviare denaro tramite bonifico bancario. Lo fanno imitando l'identità del possessore della casella di posta compromessa per frodare l'azienda, i suoi dipendenti, clienti e partner. In molti casi i truffatori concentrano i loro sforzi sui contabili o gli impiegati delle risorse umane.

Capita anche che il criminale provi a stabilire un rapporto con la vittima avviando una conversazione e chiedendole se è disponibile per un affare urgente o se è pronta ad accettare un incarico professionale e dopo la prima email di risposta ci chiede di effettuare un pagamento, da non fare mai.

COME DIFENDERSI

- **CONTROLLARE SEMPRE LA CORRETTEZZA DELL'INDIRIZZO DI POSTA ELETTRONICA DA CUI PROVIENE LA COMUNICAZIONE.**
- **VERIFICARE LA VERIDICITÀ DELLA RICHIESTA CON UNA TELEFONATA AL MITTENTE O AL COLLEGA D'UFFICIO.**
- **OTTENERE INFORMAZIONI DIRETTAMENTE DALLA BANCA DI DESTINAZIONE DEL BONIFICO.**

CRITTOGRAFIA

La Crittografia permette di creare messaggi in codice che solo gli interlocutori che lo conoscono riescono a interpretare.

Mentre prima si usavano buste chiuse, scrigni e casseforti, adesso la segretezza delle informazioni viene protetta da algoritmi elettronici.

In un mondo interconnesso dagli apparati di comunicazione digitale, la crittografia è una componente fondamentale della vita quotidiana anche se non ce ne rendiamo conto: quando usiamo un bancomat o guardiamo la pay-tv, quando ci colleghiamo a un sito web per le operazioni bancarie o compriamo qualcosa su Internet, quando parliamo al telefono cellulare.

Ma possiamo decidere noi stessi di cifrare un messaggio. Ormai tutti i sistemi operativi consentono di cifrare l'hard disk o singoli file, perfino la posta elettronica, cliccando un pulsante. Ed è una buona abitudine da sviluppare per proteggere quei dati "molto personali" che teniamo sul computer o spediamo in rete.

- **CONTROLLA SE L'INDIRIZZO DEL SITO A CUI TI COLLEGHI; SE COMINCIA CON HTTPS VUOL DIRE CHE È SICURO.**
- **USA I SOFTWARE PER LA CIFRATURA DI FILE E MESSAGGI.**
- **SCEGLI UN CLIENT PER LA POSTA CRITTOGRAFATA.**

CYBERBULLISMO

A chi non è mai capitato di essere preso in giro o insultato per il proprio aspetto, una parola detta al bar o per la sua appartenenza etnica e religiosa? Quando questi comportamenti sono ripetuti e organizzati si parla di bullismo.

I bulli spesso agiscono in branco: c'è un leader e un gruppo che lo sostiene. Si scagliano contro le vittima designata che in genere è una persona debole o in difficoltà, sensibile, che fatica a reagire. Il bullismo diventa cyberbullismo quando queste stesse azioni vengono innescate online da un post su Facebook un commento nella chat della scuola o una fotografia pubblicata online. Il fenomeno delle molestie in rete, via app, messenger, social network, tipico dei contesti giovanili, riguarda anche gli adulti che deridono, spaventano, aggrediscono altri adulti con i loro messaggi.

I bulli si approfittano delle nostre incertezze e delle nostre fragilità, facendoci sentire strani, diversi o inadeguati per il nostro aspetto o per i comportamenti che esibiamo, a scuola, nello sport o all'oratorio. Qualche volta i bulli usano violenze verbali per insultare la nostra religione, il paese di appartenenza, la squadra del cuore o le idee politiche. E in questo caso parliamo di Hate Speech, il linguaggio dell'odio. La legge persegue questi comportamenti che possono essere denunciati alla Polizia, però la forza del bullo dipende sempre dalla capacità di reazione della vittima e di chi gli sta intorno.

Jude Milhon, hacker americana diceva: “Pietre e bastoni possono farmi male, ma le parole sopra uno schermo possono nuocermi solo se, e fino a che, io glielo permetto."

COME DIFENDERSI DAI BULLI

- **PARLARNE IN FAMIGLIA E CHIEDERE CONSIGLIO AI PIÙ GRANDI; RIVOLGERSI A UNO PSICOLOGO O AD UN’ASSOCIAZIONE DI SETTORE.**
- **CONTATTARE I SOCIAL NETWORK CHE OFFRONO SISTEMI DI SEGNALAZIONE PER DENUNCIARE COMPORTAMENTI INAPPROPRIATI. È ANCHE POSSIBILE SCRIVERE AL GARANTE PER LA PRIVACY.**
- **RIPETUTI ATTI DI BULLISMO, MINACCE E VIOLENZE VERBALI POSSONO ESSERE DENUNCIATI SUL SITO ONLINE DELLA POLIZIA DI STATO. SE PENSI DI ESSERE IN PERICOLO CHIAMA SUBITO LA POLIZIA.**

DEEP WEB E DARK WEB

In alcune biblioteche americane i cittadini hanno preteso e ottenuto di poter navigare nel Dark Web con software speciali. Ma perché? Per non lasciare traccia delle proprie ricerche a proposito di argomenti delicati come Hiv, omosessualità, droghe e abusi famigliari, ma anche per dialogare in sicurezza con esponenti politici e religiosi che non possono professare apertamente le loro idee.

MA CHE COS'È IL DARK WEB?

Se immaginiamo il web come la punta di un iceberg che emerge dall'oceano di Internet, sotto il pelo dell'acqua potremo trovarne una parte più grande: il Deep Web o Web profondo, quella parte del web non indicizzata dai motori di ricerca. I motori di ricerca infatti funzionano raccogliendo i link relativi alle risorse accessibili in rete, ma è possibile che non siano in grado di ispezionarli tutti per limiti propri dei software che li raccolgono o perché il proprietario del sito web non vuole che accada, usando uno speciale comando: robots.txt. Chi cerca i siti nel deep web dovrà conoscerne in anticipo l'"indirizzo web" perché il motore di ricerca non è in grado di farcelo trovare. Questo è il caso di molti servizi web a pagamento nel Deep Web: biblioteche online, database, e siti, anche illegali, che aprono e chiudono nel volgere di una notte. All'interno del Deep Web possiamo individuarne una parte ancora più nascosta da esplorare che è chiamata **Dark Web**, il web oscuro. Il nome viene dalle darknet, le reti all'epoca separate da Darpanet, la "nonna" di Internet. Il Dark web è quella parte di Internet che non viene indicizzata dai motori di ricerca e in aggiunta necessita di software speciali per accedervi. Tor è uno di questi. Siccome i criminali vendono le loro merci nei negozi di e-commerce del web oscuro questo fa paura. Luoghi di incontro sicuri o pericolosi, contenuti morali e immorali, attività legali e illegali si trovano però ovunque ad ogni livello, nel Surface Web, nel Deep Web o nel Dark Web. Il dark web si chiama così perché è più difficile da trovare e non perché fa paura.

- **SURFACE WEB O WEB DI SUPERFICIE CONTIENE I SITI CHE VISITIAMO OGNI GIORNO COME UNILINK.IT.**
- **DEEP WEB È IL WEB NON INDICIZZATO DAI MOTORI DI RICERCA.**
- **IL DARK WEB È UNA PORZIONE DEL WEB CHE SI PUÒ ESPLORARE SOLO CON SOFTWARE SPECIALI.**

FAKE NEWS

"Attenzione! Scoperta la pillola per sconfigere il Coronavirus!" La notizia, pubblicata da un sito web parla di un evento eccezionale, ma è una **fake news**. Le fake news sono le notizie false diffuse in rete intenzionalmente per manipolare l'opinione pubblica, delegittimare personalità e istituzioni e inquinare il dibattito scientifico. A differenza della satira, delle opinioni personali, del diritto di critica, e degli errori giornalistici, le fake news sono pensate per imbrogliarci con notizie che sembrano vere, costruite con verità parziali e fatti non verificabili. La maggior parte delle persone non è capace di riconoscere le notizie vere da quelle false proprio perché le fake news sono notizie verosimili, talvolta romanzate, e condite da particolari curiosi o singolari. È facile credere alle notizie false quando confermano i pregiudizi, consentono di spiegare fatti complessi senza sforzo, giustificano delle scelte precedenti o producono un vantaggio nel gruppo di appartenenza. Ci sono però diversi modi per stabilire quando ci troviamo di fronte a una fake news.

COME RICONOSCERE LE FAKE NEWS

- **ATTENTI AI TITOLI.** Le fake news hanno spesso dei titoli "strillati" costruiti per causare rabbia e indignazione. Chi scrive le bufale conta proprio sulla reazione emotiva di chi legge, guarda, ascolta.
- **CONTROLLATE ALTRE FONTI.** Se vedete una storia che vi sembra incredibile o scioccante, meglio controllare se altre fonti accreditate la riportano. Fate una piccola verifica sul nome dell'autore dell'articolo.
- **VERIFICATE IL SITO DI PUBBLICAZIONE.** Se un sito vi insospettisce controllate che non sia un sito parodia e se viene menzionato in altri contesti. Se la grafica e il layout del sito non sembrano professionali e se i titoli sono gridati, scritti tutti in maiuscolo, col punto esclamativo, diffidate sempre.
- **LA DATA È IMPORTANTE.** Controllate se il fatto narrato è davvero accaduto con una veloce ricerca online. Spesso si spacciano per nuove notizie vecchie che, in un contesto diverso, assumono un altro significato.
- **NON FERMATEVI ALLE APPARENZE.** Spesso ci si sofferma solo al titolo-bomba da condividere immediatamente. Meglio però leggere tutto l'articolo. A volte ci si accorge che il testo non ha nulla a che fare con il titolo o che la storia è falsa e non esistono prove per dimostrarla.
- **IMMAGINI DUBBIE.** È facile scambiare una foto per un'altra. Basta dire che è stata scattata a un dato evento quando invece appartiene a tutt'altro contesto. Per verificare le immagini possiamo usare un motore di ricerca e fare il "reverse engineering" della foto.

HACKER

Avete paura degli hacker? Beh, forse non dovreste. Avrete sicuramente sentito di hacker che si sono intrufolati nei conti di una banca, che hanno manomesso server e computer o cambiato i connotati a una pagina web, ma gli hacker non sono tutti uguali.

Gli hacker per definizione sono programmatori informatici esperti di computer e reti di comunicazione che rispettano l'etica della condivisione delle informazioni. Quelli che "bucano" i sistemi informatici altrui senza permesso sono chiamati **cracker** o black hat hacker.

Agli albori dell'informatica moderna **hacker** vennero chiamati quelli che con un **hack**, una soluzione rozza ma efficace, riuscivano a migliorare le prestazioni dei computer e risparmiare tempo e fatica agli umani che li usavano.

Per i criminologi esistono tre tipi di hacker: i white hat hacker, i gray hat hacker e i black hat hacker, cioè gli hacker col cappello bianco, che sono i buoni; quelli col cappello nero che sono i cattivi; e quelli col cappello grigio che possono diventare buoni o cattivi.

In realtà esistono molti tipi di hacker, ne elenchiamo alcuni:

- **HACKER ETICI (ETHICAL HACKER):** scrivono, migliorano e condividono il software; sono programmatori e divulgatori informatici.
- **GLI HACKER DEI DATI (DATA HACKER):** informatici esperti, analizzano i big data per trovare soluzioni a problemi complessi.
- **GLI HACKER ATTIVISTI (HACKTIVIST):** sono attivisti digitali con una forti motivazioni etiche e sociali.
- **I BIOHACKER:** sono informatici e scienziati che modificano molecole biologiche e farmaci per trovare nuove cure alle malattie.
- **I NINJA HACKER:** sono programmatori esperti al soldo di criminali che attaccano e distruggono sistemi informatici a pagamento.
- **GLI HACKER SOLDATI (CYBERSOLDIER):** lavorano per gli Stati o per le agenzie di sicurezza per proteggere o attaccare i sistemi economici e militari avversari.

IGIENE CIBERNETICA

Come ci laviamo le mani per evitare un'infezione, così dobbiamo tenere il computer e i dispositivi “puliti” e “al sicuro” da ospiti indesiderati come i virus informatici. Il concetto di Igiene Cibernetica, nato in ambito aziendale, può essere anche immaginato come una serie di principi per minimizzare i rischi dovuti a un uso poco accorto degli apparecchi informatici.

- Il nostro computer è come in un organismo vivente e la prima regola è mantenerlo in salute. Perciò è importante tenere sempre aggiornato il suo **SISTEMA OPERATIVO**, che è il suo software di base. Gli aggiornamenti risolvono errori del codice, falle e vulnerabilità scoperte dopo l'acquisto. L'antivirus è come un antibiotico. Nella maggior parte dei casi è in grado di rendere innocuo il virus che l'ha colpito.
- La prima linea di difesa è però sempre costituita dalla **PASSWORD**, che deve essere robusta e complessa, per avere il permesso di usare un certo dispositivo, si tratti di un computer, un tablet o un telefono di ultima generazione.
- Bisogna poi fare molta attenzione a come usiamo la **POSTA ELETTRONICA**, uno dei vettori più frequenti per le infezioni. Anche per questo non bisogna cliccare su link sospetti e verificare il mittente prima di scaricare un allegato di posta elettronica. Anche la posta va protetta con una password, soprattutto se la leggiamo sul web.
- È meglio non usare il nostro **ACCOUNT DI LAVORO** per le attività ludiche. E lo stesso vale per computer e telefoni. Alcuni siti web che visitiamo possono contenere codice malevolo. Anche per questo è importante non lasciarlo nelle mani dei familiari o dei bambini che potrebbero cliccare su un link infetto o installare software malevolo senza che ce ne accorgiamo.
- Infine, è bene duplicare i dati rilevanti e tenerli su un hard disk separato e non collegato alla rete. La procedura di duplicazione si chiama **BACKUP** e serve ad avere una copia di riserva dei dati che riteniamo più importanti: la tesi di laurea, la contabilità o l'elenco dei fornitori.
- Se siamo già un poco esperti potremo proteggere quei dati con la **CRITTOGRAFIA**.

INTERNET

Internet non è il web e il web non è Internet. Lo sapevate? Anche se a volte usiamo i due termini in maniera interscambiabile stiamo parlando di due cose diverse.

Internet è l'autostrada, il **web** è uno dei servizi che troviamo su questa autostrada: come l'autogrill, il parcheggio e il benzinaio dove ci fermiamo quando viaggiamo in automobile. E infatti all'inizio della sua diffusione di massa si parlava di Internet come di una "autostrada elettronica" (definizione di Al Gore).

Nata nel 1969 negli Stati Uniti, prima di chiamarsi così ha cambiato diversi nomi. **Arpanet**, la nonna di Internet, è stata la rete di poche centinaia di computer che ha dato vita a questo strumento che ha rivoluzionato il nostro modo di comunicare, divertirci e lavorare.

Il suo compito dagli inizi era uno ed uno solo: "far parlare" tra di loro computer diversi appartenenti a reti diverse (eterogenee, si dice). **Perché i computer, come gli umani, devono darsi la mano e salutarsi prima di decidere in quale lingua possono capirsi.**

Per risolvere questo problema di comunicazione due ingegneri, **Bob Kahn** e **Vinton Cerf**, inventeranno il protocollo di tramissione TCP/IP (Transmission Control Protocol/ Internet Protocol), cioè un insieme di "regole di comunicazione" fra computer in modo da "farli parlare" tra di loro. Questo protocollo diventerà lo **standard** ufficiale di Arpanet il primo gennaio del **1983** e solo allora la rete comincerà ad essere chiamata Internet, con la I maiuscola.

- **1958:** Nasce l'Arpa. Nei suoi uffici viene progettata la rete di computer Arpa Net.
- **1969:** Data della prima connessione tra due computer universitari tramite Arpanet.
- **1983:** Il TCP/IP diventa lo standard di comunicazione per la rete. Si comincia a parlare di Internet.
- **1986:** L'Italia si collega per la prima volta a Internet dal CNR di Pisa. É il quarto paese a farlo dopo Usa, Inghilterra, Francia, insieme alla Germania.
- **1990:** Tim Berners Lee e Robert Cailliau presentano il progetto di una rete di documenti elettronici ipertestuali e gli danno il nome: World Wide Web o Web.
- **1991:** Il Centro di ricerche nucleari di Ginevra pubblica il primo sito web.

PASSWORD

Vi ricordare la parola magica della taverna di Alì Babà e i 40 ladroni? Era “sesamo” e funzionava esattamente come la password di un computer.

La Password, la chiave d'accesso, serve a proteggere i nostri dispositivi digitali, i servizi web e i profili online che usiamo per lavorare, comunicare e postare sui social.

La password è la prima linea di difesa contro gli hacker criminali.

Per questo deve essere lunga, robusta e complessa e non deve avere un significato compiuto che può essere ricostruito da un potenziale attaccante. Insomma deve essere complicata, perché se la ricordate senza sforzo non è proprio una buona password.

Ma come si fa a scegliere una buona password?

- **UNA BUONA PASSWORD È LUNGA ALMENO OTTO CARATTERI, MA SE È PIÙ LUNGA È MEGLIO.**
- **È COMPOSTA DA: NUMERI, LETTERE MAIUSCOLE, LETTERE MINUSCOLE, CARATTERI SPECIALI (PUNTEGGIATURA E SIMBOLI).**
- **NON DEVE CONTENERE RIFERIMENTI PERSONALI (IL NOME DEL GATTO, DEI FAMILIARI, IL TIPO DI LAVORO, LE DATE IMPORTANTI DELLA VITA).**
- **LA PASSWORD DEVE ESSERE DIVERSA PER OGNI SERVIZIO USATO (DAI SOCIAL ALLA POSTA ELETTRONICA).**
- **VA CAMBIATA PERIODICAMENTE (MEGLIO SE VIENE AUTOGENERATA DAL SERVIZIO IN USO).**
- **LA PASSWORD VA CONSERVATA CON CURA (NON DEVE ESSERE SCRITTA SU FOGLIETTI VOLANTI O CONSERVATA NEL PROPRIO COMPUTER NON PROTETTA), MAGARI CON UN PASSWORD MANAGER.**

PHISHING

“La tua carta di credito è stata bloccata. Per sbloccarla cambiare la password andando sul sito." Presi dall'urgenza e dal panico di non poter accedere ai propri risparmi potremmo essere tentati di farlo, ma si tratta di una truffa e in questo caso prende il nome di **Phishing**.

Il Phishing è la pesca a strascico dei dati finanziari e dei codici di accesso in rete. Si tratta di una tecnica fraudolenta che usa false email per per carpire la nostra fiducia e farci fare qualcosa che non faremmo di nostra iniziativa: inserire i propri dati su un sito fasullo, cliccare su un link infetto o scaricare un allegato contenente un virus.

In genere queste email fasulle prendono la forma di un'offerta irrinunciabile, di un regalo o di una promozione. Altre volte si presentano come finte fatture da pagare, bollette della luce, questionari aziendali.

I cybercriminali ne spediscono milioni ogni giorno e c'è sempre qualcuno che abbocca.

La tecnica può essere personalizzata e in questo caso si chiama “**Spear phishing**", la “pesca con la fiocina". In questo caso riceverete una email con il vostro nome e qualche informazione che vi riguarda.

Sono le più pericolose perché vi chiedono di andare su siti fasulli dove inserire le credenziali, rubandole, per entrate nel nostro conto in banca o nella casella di posta elettronica.

VERIFICATE SEMPRE I LINK CHE AVETE INTENZIONE DI APRIRE:

- Se individuate qualche errore di battitura nell'email, potrebbe trattarsi di tentativo di truffa.
- Meglio non cliccare subito sul link ricevuto via mail ma fare una verifica sul mittente, l'azienda, il dominio web.

DIGITATE USERNAME E PASSWORD SOLO SE SIETE SICURI DI FARLO:

- Controllate con attenzione il sito su cui vi trovate.
- Verificate di utilizzare una connessione sicura preceduta da “https" (la “s" indica una connessione cifrata) ed evitate i wi-fi pubblici e non protetti.

ATTENTI A CHI VI SCRIVE:

Anche se un messaggio o un'email proviene da uno dei vostri migliori amici, ricordate che i loro account potrebbero essere stati hackerati. Lo stesso vale per email ricevute da banche, fisco, negozi online, agenzie di viaggi, compagnie aeree. Attenzione persino alle mail provenienti dal vostro stesso ufficio. Non è difficile creare un'email falsa simile in tutto e per tutto a una ufficiale.

PRIVACY

La privacy si riferisce alla tutela delle informazioni che ci identificano di volta in volta come cittadini, elettori, lavoratori e consumatori.

Indicava originariamente il diritto a non subire intrusioni nella propria vita privata, oggi invece si riferisce all'autodeterminazione informativa, cioè al diritto di decidere l'uso delle informazioni che ci riguardano e che ci definiscono come persone nel mondo fisico e digitale.

Questo è necessario perché ogni volta che usiamo un dispositivo elettronico lasciamo una traccia del suo utilizzo, e quei dati, incrociati fra di loro, contribuiscono a creare un'immagine digitale della persona che naviga sul web, usa il cellulare o la carta degli sconti del supermercato.

Poiché quei dati possono essere usati in maniera difforme dai nostri interessi, la privacy protegge ogni informazione che permette di identificarci e classificarci a cominciare dal nome personale.

- La privacy protegge **DATI COMUNI** come nome, cognome, partita IVA, codice fiscale, indirizzo, numeri di telefono, o patente, che consentono di identificare una persona fisica o giuridica.
- La privacy protegge **DATI GIUDIZIARI** relativi a reati, accuse pendenti e sanzioni amministrative.
- La privacy protegge **DATI SENSIBILI** che permettono di rivelare l'origine etnica, le convinzioni religiose, le opinioni politiche, l'appartenenza a partiti, sindacati, associazioni e i dati personali idonei a rivelare la salute e la vita sessuale.
- La privacy protegge **DATI SEMI-SENSIBILI** il cui trattamento può causare danni all'interessato, ad esempio i dati relativi alla sua situazione finanziaria.

RANSOMWARE

Il computer non funziona e sullo schermo compare una scritta minacciosa. “Il tuo computer è stato bloccato. Per sbloccarlo invia una email a questo indirizzo".

Quando succede qualcosa del genere è possibile che siate stati vittima di un ransomware.

Questo tipo software malevolo si chiama proprio così perché una volta che ha infettato il nostro dispositivo lo rende inutilizzabile fino al pagamento di un riscatto (ransom).

Sono molte le aziende che hanno subito attacchi ransomware provocando danni per miliardi di euro, tra questi gli ospedali che non sono più riusciti ad accedere alle cartelle cliniche dei pazienti e i comuni che non hanno potuto pagare gli stipendi.

Due sono le varianti principali dei ransomware:

- I **cryptor** o **cryptolocker**, che cifrano il contenuto del dispositivo
- I **blocker** che bloccano l'uso del dispositivo

La richiesta di pagamento appare in una finestra del computer. Se non si paga, il blocco diviene permanente. Se si paga al malfattore è possibile sbloccare file e dispositivi, inviandovi un codice di sblocco, ma senza la garanzia che non accada di nuovo.

Se si paga è facile diventare vittime seriali:

- Non si ricevono i codici di sblocco
- Si viene infettati da un secondo malware
- Si finisce in “liste di pagatori"

La cosa migliore da fare è avere sempre a disposizione una copia aggiornata dei dati presenti su server e computer e per evitare che accada, proteggere le password, evitare link e allegati sospetti ed essere dotati di un buon antivirus.

WEB

Il **Web**, nato nel 1991, è il modo in cui i computer rappresentano le informazioni che viaggiano su Internet prendendo la forma di "pagine web" grazie a un linguaggio inventato da un hacker e ingegnere inglese al Centro di ricerche nucleari di Ginevra: **Tim Berners Lee**. Grazie a questo linguaggio, l'HyperText MarkUp Language, i "browser" dei nostri computer, Chrome, Firefox, eccetera, possono mostrarci le informazioni digitali residenti sui computer lontani chilometri, nella forma di una schermata grafica, interattiva e multimediale.

Il Web, nomignolo di World Wide Web (la "Ragnatela mondiale") come Tim Berners Lee e il suo collega Robert Cailliau avevano deciso di chiamarla nel 1990, dava abbastanza bene l'idea di una ragnatela di documenti digitali raggiungibili da una delle tante reti di computer collegati fra di loro tramite Internet. Ma per far che cosa? Permettere agli scienziati, e a chiunque altro, di accedere alla biblioteca universale dei documenti elettronici presenti nei computer collegati alla rete.

Oggi è possibile usare Internet anche con lo **smartphone** e con questo "telefono intelligente" possiamo collegarci alla rete e usare i suoi servizi come il web o la posta elettronica. Senza bisogno di stare seduti a una scrivania davanti a uno schermo collegato a tanti cavi penzolanti. I programmi per farlo oggi li chiamiamo app quando li scarichiamo sul telefonino, ma il risultato non cambia: ci permettono di collegarci al social network preferito, di ascoltare la musica online e di spedire email anche mentre camminiamo.

L'importante è che ci sia il wi-fi, la rete senza fili. Ma questa è un'altra storia.

- **IL 12 MARZO 1989 TIM BERNERS LEE PRESENTA AL SUO CAPO UN PROGETTO PER LA GESTIONE DI DOCUMENTI ELETTRONICI CHE USA GLI IPERTESTI.**
- **IL 12 NOVEMBRE 1990 LA PROPOSTA CONGIUNTA TIM BERNERS-LEE E ROBERT CAILLIAU, DIVENTA DEFINITIVA COL NOME DI WORL WIDE WEB.**
- **IL 6 AGOSTO 1991 TIM BERNERS LEE PUBBLICA IL PRIMO SITO WEB DEL CERN.**

BIBLIOGRAFIA ESSENZIALE

ANONYMOUS

Antonella Beccaria, *Anonymous. Noi siamo legione*, Aliberti Editore, 2012 ISBN 978-88-7424-928-2

Arturo Di Corinto, *Un dizionario hacker*, Manni Editori 2014, ISBN 978-88-6266-516-2

Carola Frediani, *Dentro Anonymous. Viaggio nelle legioni dei cyberattivisti*, Informant, 2012, ISBN 978-88-907232-5-4

Parmy Olson, *Noi siamo ANonymous*. Piemme, 2013, ISBN 978-88-566-2957-6

CYBERSECURITY

ISACA, CSX Cybersecurity Fundamentals, 2015, ISBN 978-1-60420-594-7 R. Baldoni, R. De Nicola, *Il Futuro della Cybersecurity in Italia*, Consorzio Cini, 2015, ISBN 9788894137309

R. Baldoni, L. Montanari, *2015 Italian Cybersecurity Report. Un Framework Nazionale per la Cybersecurity*, 2017, Research Center of Cyber Intelligence and Information Security - Sapienza Università di Roma ISBN: 9788894137316

R. Baldoni, L. Montanari, L. Querzoni, *2016 Italian Cybersecurity Report. Controlli essenziali di Cybersecurity*, 2017, Research Center of Cyber Intelligence and Information Security - Sapienza Università di Roma ISBN: 978-88-941-3732-3

R. Marchetti, R. Mulas, *Cyber security. Hacker, terroristi, spie e le nuove minacce del web*, 2017, Luiss University Press, ISBN: 9788861052666

R. Baldoni, R. De Nicola, P. Prinetto, *Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici*, 2018, ISBN 9788894137330

V. De Luca, G. Terzi di Sant'Agata, F. Voce, *Il ruolo dell'Italia nella sicurezza cibernetica. Minacce, sfide e opportunità*, 2018, Franco Angeli, ISBN 9788891768049

HACKER

Steven Levy, Hackers. *Gli eroi della rivoluzione informatica*, Milano, Shake Editore, 1997, ISBN 88-86926-02-2

Stefano Chiccarelli, Andrea Monti, *Spaghetti hacker*, 1997, Apogeo Editore, ISBN 88-7303-359-8

Steven Levy, *Crypto, i ribelli del codice in difesa della privacy*, 2002, Shake Editore, ISBN 88-86926-81-2

Arturo Di Corinto, Tommaso Tozzi, *Hacktivism. La libertà nelle maglie della rete*, Manifestolibri, 2002, ISBN 88-7285-249-8

Sam Williams, *Codice libero*, 2002, ISBN 88-503-2108-2

Pekka Himanen, *L'etica hacker e lo spirito dell'età dell'informazione*, 2003, Feltrinelli, ISBN 88-07-81745-4

McKenzie Wark, *Un manifesto hacker*, 2005, Feltrinelli, ISBN 88-07-17108-2

Carlo Gubitosa, *Hacker, scienziati e pionieri. Storia sociale del ciberspazio e della comunicazione elettronica*, Viterbo, Stampa Alternativa, 2007, ISBN 978-88-7226-973-2

Giovanni Ziccardi, *Hacker. Il richiamo della libertà*, Marsilio Editori, 2011. ISBN 978-88-317-0925-5

Arturo Di Corinto, *Un dizionario hacker*, S. Cesario di Lecce, Manni Editori, 2014, ISBN 978-88-6266-516-2

FAKE NEWS

N. Chomsky, *Le dieci leggi del potere. Requiem per il sogno americano*, Ponte alle Grazie, 2017

M. Ferraris. *Postverità e altri enigmi*, Il Mulino, 2017

L.S. Germani, *Disinformazione e manipolazione delle percezioni. Una nuova minaccia al sistema-paese*, Eurilink, 2017

J. Lanier, *Dieci ragioni per cancellare subito i tuoi account social*, Il Saggiatore, 2018

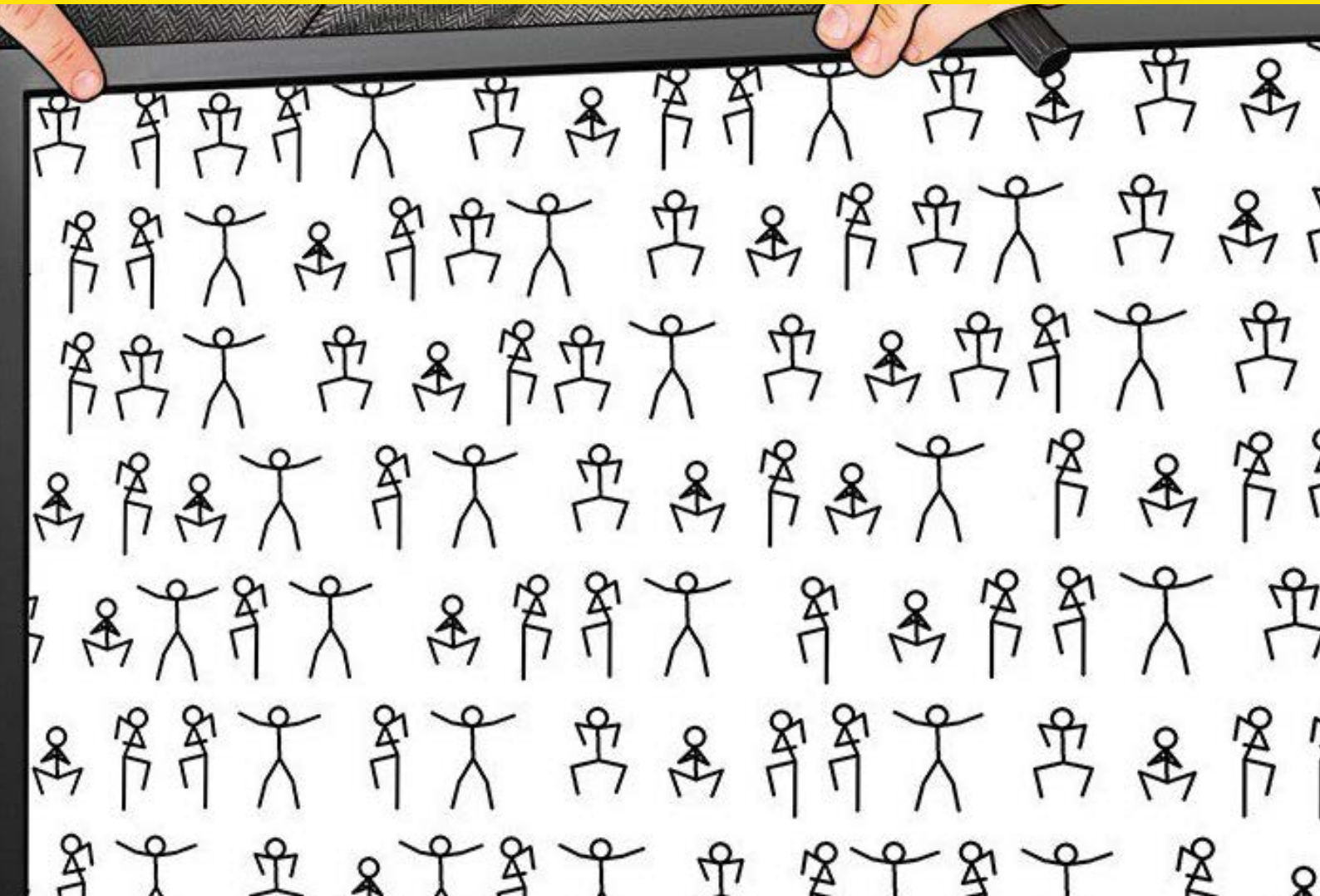
P. Messa, *L'era dello sharp power. La guerra (cyber) al potere*, Università Bocconi Editore, 2018

Francesco Nicodemo, *Disinformazia. La comunicazione al tempo dei social*, Marsilio, 2017

P. Sordi, *La macchina dello storytelling. Facebook e il potere di narrazione dell'era dei social media*, Bordeaux Edizioni, 2018


PRESS ANY KEY!

GLOSSARIO



AI: Abbreviazione di Artificial Intelligence (Intelligenza Artificiale), disciplina che si occupa dello studio di funzioni tipiche dell'intelligenza umana e della loro possibile replicazione mediante metodi e strumenti informatici.

ALGOCRAZIA: il governo delle masse attraverso gli algoritmi che gestiscono i dati che le persone cedono, spesso inconsapevoli, alle grandi piattaforme digitali.

ALGORITMO: Procedimento che consente la risoluzione di problemi di carattere logico e matematico, o pratico.

ANONYMOUS: Vasto ed eterogeneo gruppo di attivisti telematici aggregatosi inizialmente intorno al forum americano 4chan. Noti dal 2008 per gli attacchi informatici alla setta di Scientology, sono diventati famosi con l'operazione Payback, per rivendicare l'inutilità del copyright e le sentenze contro chi scarica materiali coperti da diritto d'autore.

ANTIVIRUS: Software che riconosce la presenza di virus informatici nei file e nelle memorie di massa e cerca di rimuoverli o di neutralizzarli

APT (Advanced Persistent Threat): 'Minaccia persistente avanzata', rappresentata da hacker spesso provenienti dai ranghi dell'esercito e dell'intelligence, finanziati a livello statale, il cui obiettivo è colpire un sistema tramite una serie di attacchi mirati per acquisire e mantenere il controllo del sistema stesso per periodi di tempo anche molto lunghi.

BACKDOOR: Metodo per aggirare la normale autenticazione in un sistema informatico e accedervi in remoto per prenderne il completo o parziale controllo.
Backdoor possono essere nascoste all'interno di programmi di sistema, di applicazioni software o di componenti hardware e possono essere introdotte da un programmatore, da un progettista o da un compilatore.
Una backdoor può essere anche di tipo matematico all'interno di sistemi crittografici per poter decifrare flussi di dati. Tipicamente chi scopre una backdoor è in grado di sfruttarla, mentre una backdoor matematica può essere utilizzata esclusivamente solo da chi l'ha introdotta.

BACKUP: È la procedura di duplicazione, totale o parziale, dei contenuti di una memoria informatica.

BITCOIN: Il nome Bitcoin si riferisce sia alla moneta (ma con la b minuscola) sia al software open source progettato per implementare il protocollo di comunicazione e la rete peer-to-peer che ne consente lo scambio (con la B maiuscola) e rende concreta la possibilità di evitare il ricorso a un ente centrale grazie a un database distribuito tra i nodi della rete che tengono traccia di tutte le transazioni.

BLOGGER: Autore o curatore di un blog. Il blog, crasi di web-log, è un diario personale online sul web basato su tecnologie di open publishing. Nel tempo i blog sono diventati veri e propri siti personali o aziendali, mentre molti blogger si sono trasformati in citizen journalist.

BOT: Applicazione software, chiamata anche robot Web, che esegue attività automatizzate. Esempi di uso corretto dei bot sono la generazione automatica di contenuti e risposte automatizzate. Questi programmi sono in grado di riprodurre il comportamento umano on-line come, ad esempio, popolare un profilo social ed inviare messaggi in una chat. Esempi di uso improprio dei social bot sono relativi alla sottrazione di dati personali, allo spamming e alla diffusione di informazioni fasulle nei social network.

BOTNET: Rete composta da dispositivi infettati da malware specializzati (bot malevoli) e controllata da un cosiddetto botmaster il quale, da remoto, può lanciare attacchi di tipo Distributed Denial of Service (DDoS) contro altri sistemi o compiere operazioni illecite, anche su commissione di organizzazioni criminali.

BUG: Il 'baco' è un errore di programmazione o progettazione. Può essere di tipo hardware e software. A causa del baco il dispositivo che ne è interessato, pur "funzionando" correttamente, presenta delle vulnerabilità che possono essere sfruttate da malintezionati.

CENSURA: La censura è l'insieme di metodi, pratiche e interventi autoritari che limitano o vietano la circolazione di informazioni.

CITIZEN JOURNALISM: Forma di giornalismo partecipativo praticato da giornalisti non professionisti che utilizzano gli strumenti di open publishing offerti da Internet per rivolgersi alla propria comunità di riferimento o a una audience globale.

COPYRIGHT: Il diritto d'autore riguarda la facoltà esclusiva di diffusione e di sfruttamento di un'opera creativa, quale riconoscimento del lavoro intellettuale del suo autore.

CREATIVE COMMONS: Indica un set di licenze che specifica i diritti legali attinenti a un'opera creativa precedentemente definiti dal suo autore. Tale specificazione si fonda su una peculiare combinazione di simboli e descrizioni per indicare ex ante il tipo di utilizzo dell'opera concesso in regime di diritto d'autore. Creative commons è anche il nome dell'organizzazione non-profit fondata nel 2001 da Lawrence Lessig per promuovere le licenze creative commons con l'obiettivo di facilitare la più ampia condivisione delle opere creative in contrasto alle rigidità del copyright tradizionale.

CRITTOGRAFIA: Tecnica che permette di nascondere il contenuto di un messaggio in modo che possa essere correttamente compreso solo da chi ne possiede la chiave di decifrazione.

CROWDSOURCING: Con questa parola si indica l'esternalizzazione dell'attività di un ente o di un'azienda a una moltitudine di persone attraverso una open call. Il termine Crowdsourcing è stato coniato nel 2006 da Jeff Howe. **Crowdcreation** è un neologismo che descrive abbastanza bene quello che fanno i redattori di Wikipedia. **Crowdfunding** è invece il termine che indica il finanziamento distribuito di un'opera per consentire al suo autore di realizzarla.

CRYPTOMINER: Software malevoli che generano bitcoin e altre criptovalute sfruttando la potenza computazionale di computer e smartphone.

CYBERATTACCO: Un attacco informatico che ha la finalità di accedere, modificare, distruggere o esfiltrare (rubare) dati e informazioni.

CYBERCRIME: Qualsiasi reato o comportamento delittuoso svolto nel cyberspace oppure ai danni di un sistema informatico per trarne profitto.

CYBERSECURITY: Si riferisce alla sicurezza fisica, cyberfisica, logica e proedurale dei sistemi informativi o degli asset informatici di singoli, aziende, organizzazioni e governi.

CYBERSPACE: La stratificazione di reti, programmi software e protocolli sviluppati negli ultimi quaranta anni. Questa complessità è generatrice di vulnerabilità (errori software, errate configurazioni e debolezze nei protocolli) che vengono sfruttate dai cyber-criminali per sottrarre dati o arrecare danni.

CYBERSQUATTING: Registrazione abusiva di un dominio Internet. In generale qualsiasi operazione di registrazione, commercio e utilizzo di un nome di dominio al fine di trarne profitto o per procurare un danno d'immagine al legittimo proprietario.

CYPHERPUNK: Attivista informatico che sostiene l'uso intensivo della crittografia informatica per proteggere la privacy e cambiare la società. Parte di un movimento attivo dalla fine degli anni '80, con influenze della cultura punk.

DATA BREACH: Evento che mette a rischio, rendendoli accessibili o pubblici, i dati personali di un individuo, quali, ad esempio, dati anagrafici, informazioni medico/sanitarie o finanziarie, copie di documenti di identità, dati relativi alle carte di credito, eccetera. Le cause principali di un Data Breach sono tipicamente ascrivibili ad attacchi cyber, a vulnerabilità presenti nei sistemi e/o a errori umani.

DDOS (Distributed Denial Of Service): È la pratica di bloccare un servizio online, in genere un sito sul web pubblico, inondandolo di richieste di accesso. L'attacco DDoS può essere realizzato da agenti umani, una rete di botnet e/o software creati ad hoc come il LOIC di Anonymous e hanno l'effetto di sovraccaricare il servizio determinandone il collasso. Discendente di pratiche pre-web come il *flooding* e il *netstrike* si afferma come

tecnica di protesta nel mondo hacktivist verso aziende e governi e successivamente è stato usato anche da organizzazioni criminali con l'intento di ricattare soggetti commerciali.

DEEP WEB - DARK WEB: Parti del web contenenti dati non pubblicamente indicizzati o il cui accesso è protetto attraverso reti di anonimizzazione. Si ritiene che circa l'80% dei contenuti oggi presenti sul world wide web siano "nascosti" in queste parti.

DEFACEMENT: Indica la sostituzione della homepage e delle pagine interne di siti pubblici di enti governativi, aziende e avversari politici con un messaggio difforme, ironico o minaccioso verso gli owner della pagina.

DLT - DISTRIBUTED LEDGER TECHNOLOGY: Tecnologia basata su un database distribuito chiamato blockchain, che contiene blocchi di transazioni. Grazie a crittografia a chiave pubblica e algoritmi di consenso, è in grado di garantire la sua irreversibilità e integrità (nel tempo).
L'approccio è naturalmente decentralizzato e non necessita di intermediari che convalidino o autentichino le transazioni. Ogni nodo nella rete mantiene la propria copia di tutte le transazioni e i nodi lavorano per verificare la validità di una nuova transazione attraverso un processo chiamato consenso. Ognuna di queste transazioni viene inviata a tutti i nodi della rete per essere verificata e raggruppata in blocchi di transazioni marcati con un timestamp.
Vi sono due categorie principali di piattaforme DLT: unpermissioned (aperta) e permissioned (regolata). La prima è mantenuta da nodi pubblici ed è accessibile a chiunque (Bitcoin ne e il più noto esempio). La seconda (per esempio, la piattaforma Corda), coinvolge solo nodi autorizzati e quindi facilita transazioni più veloci, più sicure e più convenienti.

ECHO-CHAMBER: Luogo digitale dove si finisce per parlare solo all'interno di gruppi che hanno idee omogenee, con meccanismi che si autoalimentano. La comunicazione all'interno di tali gruppo tende a rinforzare gli elementi comuni e ad attenuare, se non a eliminare, quelli dissonanti.

EXPLOIT: Azione che mira a prendere il controllo di una risorsa informatica o a danneggiarla. Il termine indica anche un pezzo di software, una stringa di comandi o a un codice che sfruttando una vulnerabilità o un bug presente nel sistema attaccato, punta ad acquisirne il controllo fino al livello di amministrazione ("root").
Le tecniche e i tool di exploit sono molteplici e la loro classificazione viene fatta in base al tipo di vulnerabilità sfruttata. Gli exploit più noti sono il buffer overflow, la SQL injection, il format string attack ed altri. Uno degli utilizzi più frequenti di tali tool e tecniche mira a determinare un "diniego di servizio" ("denial of service") da parte di uno o più computer server o a prenderne possesso per creare una botnet. Dall'inglese "to exploit" ("sfruttare").

GDPR (GENERAL DATA PROTECTION REGULATION): Regolamento europeo relativo alla protezione dei dati personali in vigore in Italia dal 25 maggio 2018 in base al regolamento Ue 2016/679.

HACKER: Esperto di programmazione informatica e di reti telematiche. La parola inglese hacker viene dal verbo "to hack", che significa "tagliare", "spezzare", "sfrondare", "sminuzzare", "aprirsi un varco". Hacker sono storicamente i programmatori capaci di ridurre il numero di istruzioni dei programmi informatici attraverso un "hack", cioè una scorciatoia per risparmiare tempo di elaborazione ai computer e lunghe attese agli operatori umani.

HACKING: L'azione di compiere un hack. Esplorazione non finalizzata, ricerca di soluzioni creative, modifica di ambienti e situazioni o di sistemi elettronici. In informatica il termine hacking indica lo studio di reti di comunicazione, hardware e software e delle tecniche per modificarne il funzionamento. In questa accezione l'hacking rimanda all'etica hacker e alla pratica dell'imperativo "hands on" ("metterci le mani sopra") e si connota ideologicamente come il tentativo di migliorare le prestazioni di un sistema dato. Le tecniche di hacking sono diverse e molteplici e assumono valenza diversa in relazione ai contesti in cui sono praticate. In genere ha una connotazione positiva e augurale ("happy hacking"), ma può riferirsi a un'intrusione o a una modifica non autorizzata di macchine, software e sistemi.

HACKTIVISM: L'espressione deriva dall'unione di due parole: **hacking** e **activism**. In questa accezione l'hacking è un modo creativo, irriverente e giocoso, di accostarsi ai computer, activism, indica le forme dell'azione politica diretta proprie di chi vuole modificare uno stato di cose senza delegarne a nessuno la responsabilità. La parola hacktivism indica differenti modalità di azione diretta attraverso la rete Internet.

IOT (INTERNET OF THINGS): Espressione che fa riferimento alla moltitudine di "cose", o "oggetti" che, connessi in rete e identificati in modo univoco, sono in grado di comunicare tra di loro, o con altri sistemi, senza richiedere l'intervento umano. Gli "oggetti" possono essere dispositivi, apparecchiature, impianti e sistemi, macchine e attrezzature, nei campi più disparati della nostra vita quotidiana.

MALWARE: Qualsiasi programma usato per disturbare le operazioni svolte da un computer, rubare informazioni sensibili, accedere a sistemi informatici privati, o mostrare pubblicità indesiderata. Il principale modo di propagazione del malware è quello di generare frammenti di software parassiti che si inseriscono all'interno di un codice eseguibile già esistente.

PHISHING: Truffa via Internet in cui l'aggressore cerca di ingannare la vittima inducendola a fornire informazioni personali, come ad esempio credenziali d'accesso, dettagli sul conto corrente bancario e sulle carte di credito. Si realizza tipicamente tramite

l'invio di email che imitano nella grafica e nelle impostazioni siti bancari o postali con le quali si richiede di inviare dati personali.

POLARIZZAZIONE: Tendenza a separarsi in echo-chamber distinte e basate su sistemi di credenze contrapposti e contrastanti; tali echo-chamber tendono a rigettare a priori informazioni esterne.

RANSOMWARE: Malware che introduce limitazioni nell'uso di un dispositivo, ad esempio criptando i dati o impedendo l'accesso al dispositivo stesso.

SOCIAL ENGINEERING: Insieme di tecniche atte a raggirare una persona al fine di ottenerne informazioni riservate. Queste possono essere poi utilizzate in modo fraudolento per portare a termine un attacco, utilizzando strumenti e tecnologie diverse.

SPEAR PHISHING: Tipo particolare di phishing realizzato mediante l'invio di email fraudolente a una specifica organizzazione o persona. Lo scopo di questi attacchi è tipicamente quello di ottenere accesso a informazioni riservate di tipo finanziario, a segreti industriali, di stato o militari.

VULNERABILITÀ: Debolezza presente in un elemento software o hardware di un sistema che può essere sfruttato da un attaccante per condurre un attacco contro il sistema stesso.

WHITE HACKING: Attività di esperti informatici, chiamati anche **hacker etici** o **white hat**, che si oppongono all'uso criminale dei sistemi informatici. Questi esperti sono specializzati nel penetration testing e in tutte le metodologie per testare la sicurezza dei sistemi, essi si differenziano dai **black hat** per le loro finalità positive e altruistiche.

WIKILEAKS: Sito protrasparenza e anticorruzione fondato da un gruppo di attivisti e giornalisti coordinati dal giornalista, crittografo e hacker Julian Assange. Il sito consente la comunicazione anonima e protetta, attraverso la crittografia, di documenti riservati per denunciare corruttele, malversazioni e abusi del diritto internazionale.

ZERO-DAY: Vulnerabilità del software non nota ai gestori di un sistema interessati a difenderlo da attacchi, ma nota a eventuali attaccanti. Fino a quando la vulnerabilità non viene resa nota, gli attaccanti possono sfruttarla per compromettere il sistema stesso o altri sistemi. Un attacco che sfrutta una vulnerabilità zero-day è chiamato **exploit zero-day**.

Università degli studi Link Campus University
Via del Casale di San Pio V, 44 - 00165 Roma
Tel. 0694802270 - email: info@unilink.it
unilink.it