SICUREZZA IN RETE

Come proteggere i vostri dispositivi e i vostri dati

Tutto ciò che dovete sapere sulla sicurezza informatica

INDICE

1.	**Che cos'è la sicurezza informatica e come si è evoluta nel tempo**	**5**
1.1.	Sicurezza informatica, guida all'uso	7
1.2.	Storia della sicurezza informatica	9
1.3.	Sicurezza informatica: perché dovresti interessartene (prima che sia troppo tardi)	15
1.4.	Sicurezza informatica: i settori principali	18
2.	**Sicurezza informatica per PC: i rischi, le soluzioni**	**20**
2.1.	Sicurezza informatica per PC: le basi	22
2.2.	Hacker, cracker e hacktivist: chi sono e cosa fanno	24
2.3.	Le famiglie malware: cosa sono e quali rischi si corrono	26
	Virus	*27*
	Worms	*28*
	Trojan Horse	*28*
	Adware	*28*
	Spyware	*29*
	Ransomware	*29*
	Backdoor	*29*
	Bot	*30*
	Rootkit	*30*
	Keylogger	*30*
2.4.	Sicurezza informatica per PC: cosa serve	31
2.4.1.	Cosa sono gli antivirus e come funzionano	32
2.4.2.	Come scegliere l'antivirus	34

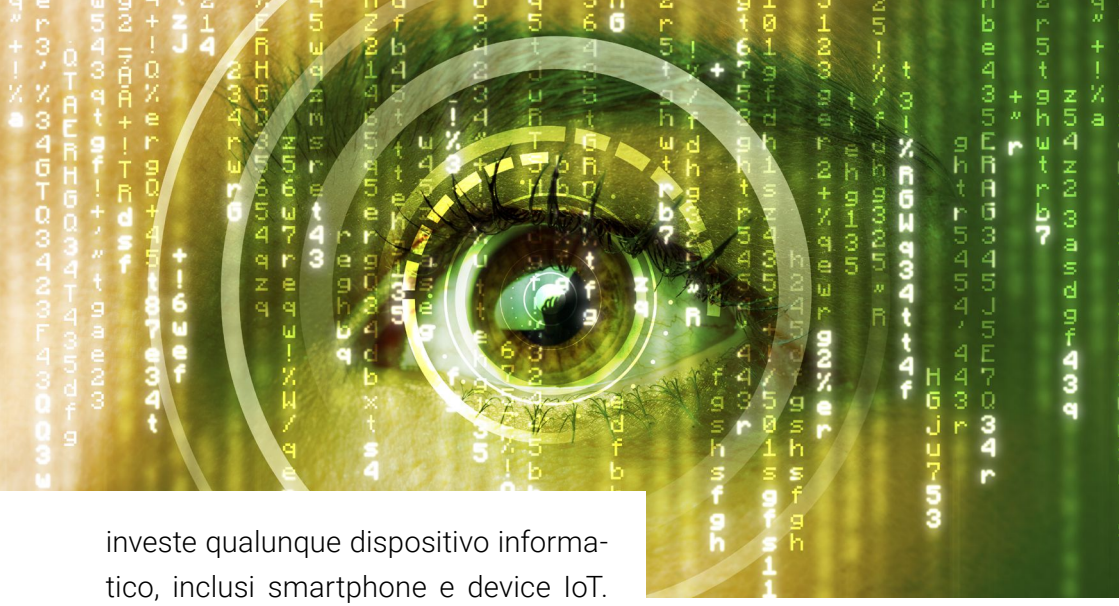
2.4.3.	Cosa sono gli antimalware	36
2.4.4.	Gli altri tool per difendersi da attacchi informatici	37
2.5.	Sicurezza informatica: differenze tra Windows e macOS	39
2.6.	Le distro Linux per la sicurezza informatica	40
3.	**Smartphone sotto attacco: nuovo fronte per la sicurezza informatica**	**42**
3.1.	Sicurezza degli smartphone, cosa bisogna sapere	43
3.2.	Malware per smartphone: i più diffusi	46
	Trojan	*47*
	Spyware	*47*
	Adware	*47*
3.3.	Come difendere lo smartphone dai cybercriminali	48
3.4.	Antivirus Android, quali sono e la loro efficacia	52
3.5.	Sicurezza iPhone: iOS è (davvero) a prova di virus?	54
3.6.	Truffe telefoniche, come riconoscerle e come difendersi	56
	SIM Swap	*57*
	Smishing	*58*
	Vishing	*58*
	Wangiri	*58*
4.	**Sicurezza informatica, il pericolo viene dal web**	**59**
4.1.	Sicurezza online, attenzione doppia	61
4.2.	Cos'è e come riconoscere un attacco phishing	62
4.3.	Cos'è e come riconoscere il social engineering	65
4.4.	Cos'è e a cosa serve la crittografia nel web	68
4.4.1.	Che cos'è la crittografia e a che cosa serve	69

4.4.2.	Come funziona la crittografia	70
4.5.	Sicurezza WhatsApp: i pericoli delle chat	72
4.5.1.	Attivare l'autenticazione a due fattori	74
4.5.2.	Controllare le impostazioni della privacy	75
4.5.3.	Privacy dei gruppi	76
4.5.4.	Attivare lo sblocco con impronta digitale	77
4.6.	Come gestire la privacy sui social network	78
4.7.	Come proteggere gli account online	81
4.7.1.	Come verificare se la propria email è stata rubata	83
4.7.2.	Creare una password sicura	83
4.7.3.	Attivare l'autenticazione a due passaggi	84
4.7.4.	Usare i password manager	85
4.8.	Acquisti online, come farli in sicurezza	85
4.8.1.	Come riconoscere un e-commerce affidabile	86
4.8.2.	Pagare online, come evitare di farsi rubare i soldi	87
4.8.3.	Cosa fare in caso di truffa online	89
5.	**Sicurezza informatica, cosa aspettarsi**	**90**
5.1.	L'evoluzione della sicurezza informatica	91
5.2.	Sicurezza informatica e intelligenza artificiale, rapporto complesso	93
5.3.	Sicurezza informatica: cosa aspettarsi	97
	GLOSSARIO	**101**

1. Che cos'è la sicurezza informatica e come si è evoluta nel tempo

Fino a non più di 10 anni fa, chi si interessava di sicurezza informatica era considerato un geek. Uno **smanettone**, detto in maniera confidenziale. Oggi, invece, **tutti siamo tenuti a interessarci di sicurezza informatica**. Se così non dovesse essere, saranno gli hacker a interessarsi di voi, e in particolare dei dati e delle informazioni contenute nella memoria dei vostri dispositivi. Qualche esempio? Se non proteggete adeguatamente lo smartphone, qualcuno potrebbe approfittarne per trafugare foto e altri dati presenti al suo interno, come email o SMS.

Per essere in grado di farlo, però, è necessario partire dalle basi. Ossia, si dovrà rispondere prima di tutto alla domanda **cosa si intende per sicurezza informatica?** Un quesito meno ovvio di quanto si possa pensare. Nel corso degli anni, il settore della cybersecurity è andato incontro a una continua evoluzione, che ne ha ampliato in maniera considerevole il "campo d'azione": se inizialmente erano i computer (aziendali, nella gran parte dei casi) a correre i pericoli maggiori, oggi la cybersecurity



investe qualunque dispositivo informatico, inclusi smartphone e device IoT. Va da sé che l'esperto di sicurezza informatica ha oggi un bagaglio di conoscenze trasversali e di gran lunga superiori a quelle possedute da un suo "omologo" qualche anno fa.

Ovviamente, un normale utente non può – e, diciamolo francamente, non deve – avere le stesse conoscenze di un esperto. Ma **non può neanche ignorare completamente l'argomento**: anche utilizzando smartphone o PC solo per svago o divertimento, all'interno della memoria sono presenti comunque informazioni che potrebbero fare gola a un hacker. Non siete convinti? Dalla sola cronologia del browser, ad esempio, un cybercriminale potrebbe ricavare informazioni utili per ricattarvi o rubare la vostra identità online.

Insomma, **non bisogna mai e poi mai abbassare la guardia**. E, soprattutto, bisogna cercare di restare quanto più possibile al passo con i tempi. Questo e-book nasce proprio con questa intenzione: offrire ai lettori di Fastweb un **piccolo "manuale" sulla sicurezza informatica**, grazie al quale potersi orientare all'interno di un settore sempre più ampio e complesso.

1.1 Sicurezza informatica, guida all'uso

Partiamo da due domande che, a nostro avviso, sono fondamentali per orientarsi nel settore: **cosa si intende per sicurezza informatica** e "come si fa" sicurezza informatica al giorno d'oggi? Vediamolo insieme.

In breve, quando parliamo di sicurezza informatica ci riferiamo a **tutte quelle tecniche e a quegli strumenti utilizzati per proteggere dispositivi elettronici da tentativi di attacco**. I device possono essere di qualunque genere: server e reti di computer, ma anche PC, smartphone e addirittura le lampadine smart che illuminano il salone di casa o la telecamera di sicurezza IP che permette di sorvegliare l'abitazione quando non ci siete.

Ovviamente, a seconda del dispositivo attaccato e degli obiettivi dell'hacker, cambierà anche **tipologia di minaccia informatica**. Se il cybercriminale vuole prendere possesso del nostro dispositivo utilizzerà un malware di tipo Trojan Horse; se, invece, è intenzionato a rubare la nostra identità online dovrà utilizzare tecniche di social engineering. Nel caso in cui l'obiettivo sia quello di creare una botnet, invece, andrà alla ricerca di vulnerabilità nel firmware di dispositivi IoT[1].

1. Non preoccupatevi se alcuni termini di questo paragrafo vi risultano oscuri, verranno "tradotti" in un linguaggio più semplice e alla portata di tutti nei prossimi capitoli e paragrafi (e, se non doveste trovarli, a fine e-book troverete un comodo glossario).

Un ipotetico **corso di sicurezza informatica**, dunque, dovrebbe passare in rassegna sia le tecniche che consentono di proteggere dati e dispositivi, spiegandone il funzionamento e l'efficacia, sia analizzare gli strumenti più idonei per mettere in pratica queste tecniche. Solo in questo modo, infatti, si potrà prendere coscienza di **quali sono i reali rischi che si corrono** e quali le possibili risposte a tentativi (riusciti o meno) di attacco.

Quando si pensa a come fare sicurezza informatica, però, c'è un altro elemento da tenere in considerazione. Secondo diversi esperti di cybersecurity, infatti, **il "fattore umano" è il proverbiale anello debole della catena**. Ossia, sempre più attacchi cibernetici puntano sulle "vulnerabilità" dell'utente in carne e ossa anziché su quelle presenti nei software. Per questo motivo la sicurezza informatica non si fa solo attraverso software sviluppati appositamente (come antivirus e antimalware): se non si pone la giusta attenzione, gli hacker avranno vita facile ad aggirare le misure di sicurezza approntate e accedere così alle informazioni presenti nel computer e nello smartphone.

Va detto che **non sempre sarà possibile arginare tentativi di attacco** né sarà possibile trovare una soluzione semplice e immediata. Questo, però, non significa che dovremmo desistere alle prime difficoltà: la sicurezza informatica è paragonabile a una "gara di regolarità" e come tale va affrontata. Dovrete continuamente **affinare e aggiornare sia le difese dei vostri dispositivi sia il modo**, così da evitare di esporvi a inutili rischi.

Prima di procedere, però, **sarà il caso di studiare un po' di storia** (della sicurezza informatica, ovviamente). Ciò aiuterà a capire cosa è successo in passato, come si sono evolute le minacce informatiche e le misure di sicurezza adottate e come è stato possibile arginare attacchi che avrebbero potuto essere catastrofici. Insomma, apprendere dal passato per evitare di ripetere gli stessi errori.

1.2 Storia della sicurezza informatica

In principio c'era il ***creeper***. Il primo virus informatico della storia – anche se in una forma estremamente primitiva – aveva infatti questo nome. Venne creato all'inizio degli Anni '70 da **Bob Thomas**, un ricercatore statunitense che contribuì allo sviluppo della prima rete informatica geografica del mondo occidentale. A voler essere estremamente precisi, però, ***creeper* non è affatto un virus come lo intendiamo oggi**: era sì in grado di diffondersi all'interno di una rete di PC ma non di autoreplicarsi, e il suo potenziale distruttivo era praticamente nullo.

Creeper, piuttosto, è stato utile per **mettere a nudo le criticità e le vulnerabilità insite in ogni network di dispositivi elettronici**. Il primo "virus" della storia, infatti, si diffuse tra i nodi di Arpanet (la rete informatica creata da ARPA, l'agenzia di ricerca militare della Difesa statunitense) non creando danni, ma lasciando una sorta di biglietto da visita che avvisava il gestore del nodo – o del PC – del suo passaggio[2]. Dopo aver

lasciato il messaggio, *creeper* passava al nodo successivo. E così via sino a non aver visitato tutti i computer, server e mainframe della rete.

Non bisognò attendere molto tempo, comunque, per assistere alla comparsa del primo **"software autoreplicante"**. Ossia, un programma che somiglia maggiormente a un virus moderno. Venne creato da Ray Tomlison – ricercatore che, tra le altre cose, ha inventato anche la posta elettronica – e venne considerato come l'evoluzione di *creeper*. Questo nuovo programma, a differenza del predecessore, era in grado di "invadere"

2. Il messaggio recitava "*Catch me, if you can*", "Prova a prendermi" in italiano.

un nodo informatico e autoreplicarsi, restando così registrato nella memoria della macchina. Oggi lo definiremmo un **worm**, una categoria di malware che dominerà la scena nei primi decenni dell'informatica.

Anche se *creeper* e il suo successore non hanno di fatto provocato danni di rilievo alle reti attaccate, hanno comunque svolto un **ruolo di primissimo piano nell'evoluzione del settore**. Di fatto, hanno dimostrato che le reti informatiche erano vulnerabili e potevano essere utilizzate per diffondere in maniera autonoma software di qualunque genere. Sono stati, dunque, il *proof of concept* che sarebbe stato possibile creare programmi da utilizzare non più per scopi didattici o "dimostrativi", ma per ricattare organizzazioni governative, aziende e privati.

A metà Anni '80 ci fu il primo vero boom di attacchi informatici "propriamente detti". In piena Guerra Fredda, **un informatico tedesco riuscì ad hackerare un nodo della neonata Internet** e, da lì, non ebbe difficoltà a trafugare informazioni e dati sensibili da 400 computer del Pentagono. A fine 1988, invece, un informatico statunitense creò un software autoreplicante per "misurare" la grandezza della Rete delle reti. Nella mente di Robert Morris – questo il nome dello sviluppatore – si trattava di un'idea piuttosto semplice: creare un programma che navigasse di computer in computer, autoriproducendosi, e "portasse il conto" delle macchine visitate.

Il software, però, andò ben oltre le aspettative del suo creatore e si diffuse così in fretta da **mettere a rischio la stessa sopravvivenza della Rete**, sovraccaricandola di lavoro. Il Morris Worm – questo il nome dato al virus – infettò diverse migliaia di computer e server in tutto il mondo, provocando danni economici stimati tra i 100 mila e i 10 milioni di dollari.

Se, da un lato, il Morris Worm fece da apripista a malware (letteralmente "software malevoli") sempre più aggressivi e pericolosi, dall'altro fece nascere la consapevolezza che bisognasse scendere in campo per **creare delle misure di sicurezza** che consentissero di arginare il fenomeno. Tra la fine degli Anni '80 e l'inizio degli Anni '90 si assistette così allo sviluppo di **software di sicurezza informatica sempre più efficaci**.

Comparvero in questo periodo **i primi firewall** (software che proteggono i computer da tentativi di accesso remoto), mentre gli **antivirus** adottarono tecniche difensive sempre più raffinate, basate su una protezione continuativa e sul **metodo delle "signatures"**. Quest'ultimo prevedeva che tutti i file presenti sul disco rigido di un computer dovessero essere confrontati con le "firme" di tutti i malware conosciuti e, in caso di corrispondenza, essere eliminati dalla memoria (o messi in quarantena).

Nella seconda metà degli Anni '90, però, questa tecnica iniziò a mostrare tutti i suoi limiti: il numero di malware crebbe in maniera esponenziale, passando dalle poche decine di migliaia comparsi negli anni precedenti ai **5 milioni di nuovi esemplari creati ogni anno a inizio XXI secolo**. Riuscire a controllarli tutti, insomma, era diventato impossibile.

Negli anni successivi la situazione si fece ancora più complessa: si stima, ad esempio, che ogni giorno comparivano sul web centinaia di migliaia di

nuovi malware, in grado di compromettere anche i sistemi di cybersecurity più avanzati. I sistemi "Signature" vennero così sostituiti da **motori a scansione euristica**, capaci di riconoscere anche nuove famiglie malware dal loro comportamento.

La diffusione di Internet e del web, poi, non ha fatto altro che complicare ulteriormente la situazione. **Diffondere nuovi virus è diventato sempre più semplice**: basta che la vittima visiti un sito web compromesso o apra l'allegato di una mail per indurla a scaricare un malware (senza che se ne accorga, nella stragrande maggioranza dei casi). Con l'inizio del nuovo millennio, ad esempio, diventano sempre più frequenti i casi di virus diffusi via posta elettronica: è il caso di **ILOVEYOU**, **Pikachu** e **Anna Kournikova**, che imperversano online a cavallo tra 2000 e 2001.

Ma è dal 2010 in poi che **la situazione inizia a precipitare**. Le tecniche sviluppate da hacker e cybercriminali – in molti casi alle dipendenze di stati, come fossero delle unità militari – diventano sempre più raffinate e pericolose. Con la **diffusione di massa di smartphone e PC** e la presenza "ubiqua" di Internet, anche la portata degli attacchi informatici diventa sempre più ampia.

Nel **2013** Edward Snowden rivela l'esistenza di decine di strumenti creati dall'NSA (acronimo di *National Security Agency*, l'agenzia per la sicurezza nazionale statunitense) per spiare cittadini statunitensi e non tramite la Rete. In quello stesso anno, i **server Yahoo! vengono ripetutamente attaccati**, causando così uno dei più grandi *data breach* della storia: gli hacker hanno accesso alle informazioni contenute nei 3 miliardi di caselle di posta elettronica dell'azienda statunitense, e successivamente resi disponibili online.

Tra la fine del 2016 e l'inizio del 2017 si assiste probabilmente al picco dell'offensiva informatica "pubblica". Nell'ottobre 2016 una serie di **attacchi DDoS**[3] ha messo KO una larga fetta di Internet: per diverse decine di minuti portali come Twitter, Amazon, eBay, Airbnb, Spotify e SoundCloud risultano irraggiungibili in buona parte del mondo, Italia inclusa. Nel maggio 2017, invece, il mondo fa conoscenza con i **ransomware** (letteralmente "Software del ricatto"). Questa particolare tipologia di malware si diffonde via web, blocca con la crittografia tutti i dati presenti nella memoria del computer e chiede un riscatto per poterli sbloccare.

Nel giro di poche settimane, parole come **WannaCry** e **notPetya** diventano di dominio comune: sono i nomi dei ransomware più conosciuti e diffusi, capaci di **provocare danni per miliardi di dollari** nel giro di pochi minuti. WannaCry, ad esempio, colpì la rete del Sistema Sanitario Nazionale britannico (lo NHS) e quella di Maersk (principale società armatrice al mondo), bloccando decine di migliaia di computer e costringendo le due realtà a stoppare le loro attività.

3. Acronimo di Distributed Denial of Service, "Interruzione distribuita del servizio" in italiano, è un attacco che mira a rendere irraggiungibili alcune risorse altrimenti disponibili online.

1.3 Sicurezza informatica: perché dovresti interessartene (prima che sia troppo tardi)

Da questo rapido excursus storiografico appare chiaro che **è diventato ormai impossibile ignorare le minacce di sicurezza informatica** che ci circondano. E che, ogni giorno che passa, diventano sempre più inquietanti. Che si utilizzino smartphone e PC per semplice svago o per lavoro fa ben poca differenza: i nostri dispositivi e i nostri dati personali sono **costantemente esposti a rischi di ogni genere**, spesso e volentieri senza alcuna forma di protezione.

Ignorare i pericoli legati agli attacchi informatici non fa che aumentare le probabilità di finire nella rete di un hacker, pronto ad approfittare di ogni nostra minima incertezza. La tattica dello struzzo (nascondere la testa sotto la sabbia e fare finta che non stia accadendo nulla) non è dunque una soluzione accettabile: come dimostrano i **dati del Rapporto Clusit 2020**, nel nostro Paese si assiste a un'evoluzione quantitativa e qualitativa del rischio informatico. Non solo aumentano il numero di attacchi, ma questi diventano sempre più efficaci e complessi, messi a punto da veri e propri professionisti del settore.

Cresce il numero di attacchi considerati gravi (il 54% di quelli registrati), mentre il **Cybercrime** a scopo estorsivo diventa la principale minaccia per gli utenti italiani. La tendenza è quella di **utilizzare tecniche apparentemente semplici**, ma declinate in moltissime varianti, in modo

che gli utenti vengano tratti in inganno. A farla da padrone sono gli **attacchi via malware** (44% dei casi registrati dagli strumenti Clusit), seguiti da quelli phishing e di social engineering. Dai dati del Security Operation Center di Fastweb emerge che solamente nel nostro Paese viene registrato più di un evento di sicurezza al secondo (**43 milioni nel 2019**), con **almeno una vittima di attacco informatico al secondo**. Appare piuttosto chiaro, dunque, che la sicurezza informatica è una tematica che riguarda da vicino ognuno di noi, che ci piaccia o no. Necessario rendersi conto, dunque, che la protezione dei nostri dati personali e dei nostri dispositivi passa, prima di tutto, attraverso un **atteggiamento proattivo**. Come detto, infatti, strumenti e software di sicurezza informatica, da soli, non bastano a difendersi da tentativi di attacco o intrusione.

> **Viviamo ed operiamo in una situazione di inaudita gravità in termini di rischi cyber, che mette a repentaglio tutti i presupposti sui quali si basa il buon funzionamento dell'Internet commerciale e di tutti i servizi, online e offline, che su di essa fanno affidamento.**
>
> *Andrea Zapparoli Manzoni, Comitato Direttivo Clusit*

L'utente gioca infatti un ruolo di primaria importanza: continuare ad aprire email e allegati provenienti da mittenti sconosciuti o scaricare software e applicazioni da siti e store poco affidabili non farà altro che aumentare le probabilità di essere infettati da qualche malware (o diventare vittima di una truffa online). Affinché gli strumenti possano essere realmente

efficaci, dunque, sarà necessaria la nostra collaborazione: dovremmo fare attenzione ai siti che visitiamo, ai link sui quali clicchiamo, alle app scaricate e ai messaggi (di posta elettronica o delle app di messaggistica) che riceviamo e leggiamo. Certo, per alcuni versi **potrà sembrare anche un atteggiamento eccessivamente prudente**, ma ne va della sicurezza dei nostri dati personali, con tutto ciò che ne può conseguire.

RAPPORTO CLUSIT 2020: LE CIFRE IN BREVE

43 MILIONI

di eventi di sicurezza registrati dal Security Operation Center di Fastweb

1.670 ATTACCHI GRAVI

registrati nel corso del 2019

83% DEGLI ATTACCHI

è di tipo "Cybercrime" a scopo estorsivo

44% DEGLI ATTACCHI

viene condotto tramite malware (di questi, il 46% è rappresentato da attacchi ransomware)

17% DEGLI ATTACCHI

viene condotto con tecniche di phishing o ingegneria sociale (in crescita dell'82% rispetto ai dati del 2018)

14 Sicurezza informatica: i settori principali

Per comprendere a pieno che cos'è la sicurezza informatica, però, è necessario conoscere anche i settori nei quali questa si articola. Come detto, infatti, sono lontani i tempi nei quali le minacce riguardavano solo ed esclusivamente PC o nodi di reti di computer. **Il panorama dell'informatica, e con esso quello della cybersecurity, è diventato molto più complesso rispetto al passato.** Oggi, al fianco dei PC troviamo decine di altri possibili obiettivi per hacker e cybercriminali. Tra questi, però, solo alcuni interessano direttamente gli utenti "comuni", mentre molti altri sono relativi ad ambiti professionali e industriali. Vediamo in dettaglio quali sono le **minacce informatiche che possono riguardarci più direttamente**.

- **COMPUTER** - Nonostante il tempo passi, la sicurezza informatica resta strettamente legata al mondo dei computer. Le minacce per PC spaziano dalle infezioni malware alle truffe online, passando per furto di credenziali o identità digitale e tentativi di accesso alle informazioni archiviate all'interno della memoria del computer.

- **SMARTPHONE** - Con il passare degli anni, gli smartphone hanno assunto un'importanza sempre maggiore all'interno della nostra quotidianità. Oggi li utilizziamo per chiamare e inviare SMS (ovviamente), ma anche per controllare posta elettronica e profili social; per accedere al conto corrente con le app di mobile

banking; per inviare messaggi multimediali con le app di messaggistica; per archiviare foto e video sul cloud e per lavorare. Va da sé che facciano sempre più gola ad hacker e cybercriminali vari, che sperano di poter mettere le mani su una mole impressionante di dati. Diverse le tattiche messe in atto per riuscire in questa "impresa": infezioni malware, messaggi "truffa" su app di messaggistica istantanea, app contraffatte, tecniche di ingegneria sociale via social network e non solo.

• **DISPOSITIVI IOT** - Anche le telecamere di sicurezza, le lampadine smart e gli altri dispositivi della casa intelligente (ma non solo) sono a forte rischio di attacchi informatici. Anzi, per alcuni versi sono i dispositivi maggiormente esposti a rischi di questo genere: a oggi, infatti, non esistono "antivirus" o strumenti di sicurezza pensati per difenderli. Inoltre, accade con una frequenza preoccupante che i firmware dei dispositivi dell'Internet of Things contengano vulnerabilità non risolte, che consentono ai criminali informatici di prendere il controllo del device. I rischi? Che le nostre lampadine smart giochino (inconsapevolmente) un ruolo fondamentale in un attacco DDoS di grande portata o che qualcuno sfrutti la telecamera IP per spiare ciò che facciamo in casa.

• **CLOUD** - Tra i settori della sicurezza informatica, è quello meno "tangibile". Ma ciò non vuol dire che sia meno importante. Anzi: il cloud è diventato parte integrante della nostra "esperienza d'uso" di PC e smartphone. Basti pensare, ad esempio, a foto, documenti e file in genere che archiviamo sui servizi di cloud storage. Per questo, nell'immediato futuro diventerà indispensabile adottare tattiche di difesa anche della "nostra" porzione di nuvola.

2.2 Sicurezza informatica per PC: i rischi, le soluzioni

Per un lungo periodo (e fino a non molto tempo fa), il termine "sicurezza informatica" era legato esclusivamente al **mondo del computer**. Oggi, però, la sicurezza informatica abbraccia un numero di settori e dispositivi di gran lunga più ampio: complice l'evoluzione e "l'espansione" dell'universo dell'elettronica, si parla di cybersecurity anche in riferimento alla navigazione online e alla protezione dei dati personali, agli smartphone e ai dispositivi della casa smart.

È inutile negare, però, che il rapporto tra la cybersecurity e il mondo dei computer è particolarmente stretto. Ancora oggi, investimenti e ricerche sono concentrati sul settore **della sicurezza informatica per PC**. Gran parte delle minacce, infatti, riguarda ancora i computer, in tutte le loro varie "forme e declinazioni". Merito del fatto (se di merito si può parlare, visto l'argomento) che negli ambienti lavorativi i PC sono i dispositivi più utilizzati. E, fino a quando questa tendenza non cambierà, i computer resteranno il bersaglio preferito di nuove minacce informatiche.

Per un cybercriminale i dati legati alla sfera lavorativa hanno un valore più elevato rispetto a quelli della sfera privata. Che si tratti di un "furto su commissione" o di un'iniziativa personale poco cambia: **riuscire a impossessarsi di segreti industriali o, più genericamente, documenti di lavoro** di una grande azienda consente di avere tra le mani del materiale che può essere rivenduto ad "avversari" o per ricattare la stessa azienda. Gli hacker hanno quindi tutto l'interesse a sviluppare, anche con cadenza quotidiana, **nuove minacce, nuovi malware e nuove tecniche** per aggirare sistemi di sicurezza sempre più complessi e avanzati.

Queste stesse tecniche di attacco e questi stessi malware **possono poi essere utilizzati anche contro utenti "normali" e non solo contro aziende e professionisti**. Una volta che sono diventati di pubblico dominio, infatti, nulla vieta che criminali informatici con poca esperienza (e senza molti scrupoli) traggano vantaggio dal lavoro di colleghi più navigati, "riciclando" malware e minacce sviluppati per altri scopi. La storia dell'informatica, d'altronde, è piena di esempi di questo genere: si pensi alle decine di tool sviluppati da agenzie governative per compiti di spionaggio (quelli della NSA statunitense, ad esempio) che oggi sono utilizzati per bypassare le difese di un qualunque PC connesso a Internet.

Insomma, anche se riteniamo che il nostro PC non contenga nulla di troppo interessante, **non possiamo permetterci il lusso di abbassare la guardia**. I nostri computer, e i dati contenuti al loro interno, sono costantemente sotto attacco: indipendentemente dal sistema operativo che utilizziamo, dobbiamo essere in grado di proteggere il nostro dispositivo da tentativi di infezione e intrusione vari. Necessario, dunque, approntare una "strategia di difesa", che consenta di non farsi trovare impreparati in caso di attacco.

2.1 Sicurezza informatica per PC: le basi

Per "sconfiggere" il nemico, si deve innanzitutto conoscerlo. Quindi, nel gettare le basi per una strategia di sicurezza informatica si parte **dall'analisi di quegli "elementi" che mettono maggiormente a rischio integrità e funzionamento del computer**. Affinché la propria strategia sia efficace ed efficiente, dunque, è necessario sapere cosa sono i malware, quali sono le famiglie malware, come agiscono e quali gli strumenti di difesa.

Questi ultimi, ovviamente, giocano un ruolo fondamentale in una qualunque strategia di sicurezza informatica, anche la più basilare ed elementare. Senza dotarsi di strumenti adeguati **sarà di fatto impossibile pensare di difendersi da qualunque tipo di minaccia**. È vero, come abbiamo sottolineato nell'introduzione, che il comportamento dell'utente

è fondamentale nel prevenire attacchi diretti e difendere al meglio il proprio dispositivo. Ma è altrettanto vero che, senza ricorrere a software e applicativi di sicurezza informatica, saremo esposti a qualunque tipologia di "attacco indiretto". Moltissime minacce, infatti, sono **invisibili anche agli occhi degli utenti più attenti ed esperti**: in casi come questi la scelta dei programmi di cybersecurity avrà un peso preponderante nel determinare l'inviolabilità del sistema informatico o la facilità con la quale un cybercriminale (magari anche alle prime armi) avrà accesso alle risorse del nostro computer.

Prima, però, è necessario conoscere chi siano i protagonisti del settore. Ossia, **chi si nasconde dietro la creazione di nuove minacce e nuovi malware** e chi, dall'altra parte, studia per arginare gli attacchi e studiare nuovi strumenti e nuove metodologie di difesa.

Di fatto, per quanto ampio sia il settore e per quanto variegate siano le tecniche di attacco e le minacce informatiche oggi esistenti, **il mondo della sicurezza informatica si regge su questi tre "pilastri"**. Analizzandoli a fondo, dunque, sarà possibile comprendere meglio chi e perché sviluppa virus (o chi, al contrario, è impegnato sul fronte opposto e cerca soluzioni alle minacce più gravi), quali sono le famiglie malware più pericolose e gli strumenti che è possibile utilizzare per proteggere il proprio PC.

2.2 Hacker, cracker e hacktivist: chi sono e cosa fanno

Di sicurezza informatica se ne parla da decenni. A esser precisi, **se ne discute sin dagli Anni '70**, quando l'informatica stava uscendo da laboratori militari e dalle università per entrare all'interno di uffici e abitazioni. Come abbiamo visto, in questo periodo cominciarono a comparire i primi malware e virus (molto rudimentali e molto poco pericolosi, se confrontati con la controparte moderna) e i primi tentativi di incursione all'interno di rete informatiche aziendali e militari.

Quasi a mo' di "riflesso condizionato", **sono comparsi anche i primi esperti di sicurezza informatica**: si trattava solitamente di esperti di programmazione che, per far fronte all'emergenza, iniziarono ad analizzare il codice sorgente dei software alla ricerca di eventuali errori, falle e vulnerabilità. Con il passare del tempo la strada del programmatore e quella dell'esperto di cybersecurity si divisero e divennero due figure professionali distinte. Nonostante ciò, il "nomignolo" utilizzato negli Anni '70 e negli Anni '80 per descrivere i programmatori/esperti di sicurezza informatica viene utilizzato ancora oggi per identificarli.

Il **termine hacker** nasce proprio in questo contesto, anche se il suo significato iniziale non era lo stesso con cui viene utilizzato ai nostri giorni. A volerla dire tutta, però, un'eccessiva semplificazione ha portato a "restringere" sin troppo il significato, identificando l'hacker con un criminale informatico. La verità è che gli esperti di sicurezza informatica

si dividono in tre categorie: i cybercriminali, i ricercatori di soluzioni per la protezione dei PC e chi si occupa di sicurezza informatica per scopi "etici". Vediamo chi sono.

- **CHI SONO GLI HACKER** - Si tratta degli esperti di sicurezza informatica "propriamente detti", grandi conoscitori di materie come crittografia, programmazione e con grandi capacità di ragionamento logico-deduttivo. Mettono a frutto le loro conoscenze per sviluppare tecniche e tecnologie atte a proteggere computer, reti di computer e le informazioni archiviate all'interno dei loro dischi rigidi.

- **CHI SONO I CRACKER** - Detti anche Black-hat hacker, i cracker sono un po' la nemesi degli hacker. Come i primi, anche loro hanno grandi conoscenze nel campo della programmazione e della crittografia, e un ampio bagaglio di competenze nel settore della sicurezza informatica. La differenza maggiore sta nell'utilizzo che fanno di queste conoscenze: i cracker, infatti, sono i cybercriminali che sfruttano le loro capacità per penetrare all'interno di sistemi informatici (spesso e volentieri dietro compenso di un committente) e ottenere informazioni riservate o guadagnare i diritti

di amministratore, così da poterli controllare a distanza. Rientrano poi in questa categoria tutti quei programmatori che utilizzano le loro conoscenze per sviluppare malware di ogni genere, dai virus ai ransomware.

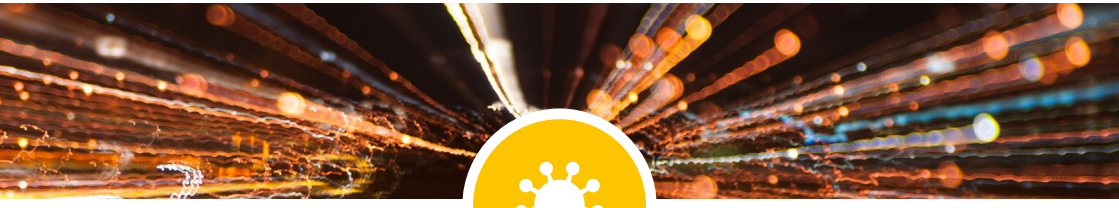
- **CHI SONO GLI HACKTIVIST** - Detti anche White-hat hacker o hacker etici, si tratta di professionisti della sicurezza informatica che scovano falle e vulnerabilità all'interno di reti di computer, software e sistemi operativi per poi informare produttori di dispositivi o software house. In questo modo questi ultimi possono risolvere il problema di sicurezza rilasciando delle patch prima che il bug venga utilizzato da qualche Black-hat hacker per scopi malevoli.

2.3 Le famiglie malware: cosa sono e quali rischi si corrono

La principale minaccia che i possessori di PC si trovano ad affrontare è rappresentata dalle varie famiglie di malware oggi esistenti. Infatti, indipendentemente dalla tecnica che i cybercriminali adottano per diffonderli, **l'attacco vero e proprio viene condotto dal software malevolo** sviluppato da un cracker. E, a seconda della tipologia di malware – o famiglia, come detto in gergo tecnico – saranno differenti anche gli effetti e le tipologie di contromisure da adottare. Prima di vedere quali sono le famiglie malware più comuni e pericolose, però, vale la pena partire da una definizione: quella di malware. Troppo spesso, infatti,

si fa confusione su **cosa significa malware** e si finisce con il confondere questo termine con una tipologia di software malevolo in particolare. Il malware, invece, è un "nome collettivo" che sta a indicare la totalità di minacce informatiche che si palesano sotto forma di software. **Malware, infatti, altro non è che l'unione dei termini inglesi *"malicious"* e "software"**, ossia software malevolo.

Di software malevolo, oggi, ne esiste di ogni tipo. Vengono create **decine di migliaia di malware**, anche se nella gran parte dei casi si tratta di semplici "variazioni sul tema". Nel complesso, infatti, tutti i software che tentano di infiltrarsi sono parte di una decina di "macrocategorie" (le famiglie malware, per l'appunto) che condividono "metodologia" di attacco, tipologia di danni provocati al sistema informatico oppure gli "obiettivi" da raggiungere. Ecco le più pericolose.



VIRUS

Si tratta della forma forse più "comune" di malware. I virus informatici, come quelli biologici, infettano un corpo per replicarsi e danneggiare il sistema che li ospita. Un virus può sfruttare diversi vettori per infettare un PC: da un file già infetto scaricato da Internet a un allegato di posta elettronica corrotto, passando per chiavette USB o hard disk esterni infettati o un nodo di una rete locale compromesso. Una volta all'interno della macchina, il virus entra in azione in maniera silenziosa, distruggendo file, corrompendo intere porzioni di memoria e, nei casi più gravi, rendendo del tutto inutilizzabile il computer.

WORMS

Come i virus, anche i worms sono caratterizzati dalla capacità di autoriprodursi ma, a differenza dei primi, sanno anche diffondersi autonomamente. Solitamente, infatti, i worms sfruttano strumenti come la posta elettronica per trasmettersi all'intera lista dei contatti e infettare il numero maggiore possibile di altre macchine. Il worms in sé e per sé non è pericoloso ma, solitamente, fa da apripista per altre tipologie di infezioni: può portare con sé carichi (*payload* in gergo tecnico) piuttosto pericolosi, causando danni non indifferenti al sistema informatico.

TROJAN HORSE

Letteralmente vuol dire "Cavallo di Troia", un nome tutt'altro che casuale. I Trojan Horse, infatti, infettano i PC per creare delle aperture nelle difese del sistema informatico. Un Trojan, ad esempio, può aprire delle porte di comunicazione in modo da "sifonare" il traffico del PC e inviarlo verso un server spia appositamente configurato; o, attraverso quella stessa porta di comunicazione, un cybercriminale può prendere possesso del computer infetto e controllarlo da remoto ogni volta che vuole.

ADWARE

Tra le varie famiglie di malware, gli adware sono tra i meno pericolosi per la stabilità del sistema, ma forse sono tra i più fastidiosi. Si tratta, infatti, di "virus pubblicitari", che mostrano banner e annunci pubblicitari mentre navighiamo online o mentre lavoriamo con il PC.

In questo modo, i cracker che li hanno creati possono guadagnare denaro dalle visualizzazioni della pubblicità da parte di utenti inconsapevoli.

SPYWARE

Come dice il nome, si tratta di software spia che, una volta installati, sottraggono informazioni di ogni tipo dal dispositivo infetto. Può rubare file e documenti archiviati sul disco rigido e inviarli a server controllati da remoto; accedere alle immagini della webcam e all'audio del microfono. Insomma, qualunque cosa l'utente fa con il PC, il cracker lo viene sicuramente a sapere.

RANSOMWARE

Tra le famiglie malware più recenti, sono anche una delle più pericolose. I ransomware, detti anche software del riscatto, sono tanto semplici nel loro funzionamento quanto efficaci nel provocare danni. Dopo aver infettato un dispositivo, il ransomware crittografa tutti i danni presenti nella memoria e riavvia il PC. Una volta che il processo viene completato, l'utente non può più accedere ai propri documenti e foto: se vuole farlo, deve ottenere la chiave di sblocco dal cracker che ha realizzato il malware, pagandogli un riscatto (*ransom*, in inglese) in Bitcoin. I ransomware, inoltre, sono anche piuttosto veloci nel replicarsi e diffondersi: se dovessero infettare una rete aziendale, sarebbero in grado di autoreplicarsi su tutti i nodi della rete (pc, datacenter, server) e renderla inutilizzabile nel giro di una manciata di secondi.

BACKDOOR

Letteralmente "porta di servizio", di per sé una backdoor non è un malware o una minaccia informatica. Però, in alcune occasioni, può trasformarsi in uno dei peggiori incubi per la privacy degli utenti. In ambito informatico, una backdoor è un software (o una porzione di un software o del sistema operativo) che permette all'amministratore di sistema di accedere al PC o al server per effettuare operazioni di manutenzione da remoto. A volte, però, le backdoor possono essere utilizzate anche da cracker con l'obiettivo di accedere al sistema e utilizzarlo a proprio piacimento. Ad esempio, tramite una backdoor è possibile installare uno spyware e far filtrare informazioni su tutte le attività dell'utente; oppure accedere ai dati presenti nel disco rigido e trafugarli.

BOT

Anche se la parola "bot" ha visto espandere notevolmente il proprio *range* di significati (si pensi, ad esempio, alle chatbot tanto in voga), quando viene utilizzata in ambito di sicurezza informatica ci si riferisce a computer infetti da software in grado di "prenderne il controllo" in un qualunque momento. Detti anche "computer zombie", i bot sono solitamente utilizzati per attacchi DDoS di grande portata: nel momento in cui i cracker devono lanciare l'attacco, "risvegliano" i bot dormienti comandandoli da remoto e li forzano a creare un immenso flusso di traffico dati verso un unico sito web o un gestore di reti di distribuzione dei contenuti (dette CDN, *Content Delivery Network*).

ROOTKIT

Tra le varie famiglie malware, quella dei rootkit è una delle più pericolose. Si tratta di kit, quindi di un insieme di strumenti, che consentono a un hacker di ottenere i permessi di root del dispositivo. Di fatto, l'hacker diventerà amministratore di sistema e potrà disporre del nostro PC nella maniera che preferisce: potrà installare e disinstallare programmi; potrà cancellare file a piacimento e spiarci dalla webcam. Insomma, avrà il controllo totale del PC e potrà gestirlo da remoto nella maniera che più preferisce.

KEYLOGGER

Altra tipologia di software spia indicato principalmente per trafugare dati sensibili come nome utente, password e altri codici di accesso. I keylogger, una volta installati in un computer, iniziano a registrare tutte le parole che l'utente digita sulla tastiera e le invia a un server remoto, controllato da chi ha creato il malware. In questo modo potrà recuperare tutti i dati e le informazioni di cui ha bisogno.

2.4 Sicurezza informatica per PC: cosa serve

Ora che sappiamo da chi e da cosa dobbiamo difenderci, possiamo passare ad analizzare **quali sono gli strumenti più idonei per proteggere il nostro sistema informatico**. Com'è semplice immaginare, di fronte a uno scenario così complesso e frammentato, si dovrà necessariamente fare ricorso a dei software che offrano uno scudo dalle varie minacce che incombono sui nostri dispositivi. Anche l'utente più attento e accurato di questo mondo, infatti, può restare vittima di un cyberattacco di qualunque genere.

Per questo motivo è necessario conoscere **quali siano gli strumenti di sicurezza informatica da installare sul PC** e quale sia il loro funzionamento. Solo in questo modo, infatti, sarà possibile scegliere l'opzione che meglio si adatta alle proprie necessità e alle proprie esigenze. Un'operazione che richiede un po' di impegno e un po' di tempo a disposizione, ma che permetterà di risparmiarne molto di più nel caso in cui un virus o un cybercriminale dovesse riuscire a installare qualche software malevolo nella memoria del nostro dispositivo.

2.4.1

Cosa sono gli antivirus e come funzionano

Come dice anche il nome, gli antivirus sono software pensati e sviluppati per individuare e neutralizzare virus all'interno della memoria del computer di casa o dell'ufficio. Questa, almeno, era la loro funzione iniziale: oggi, infatti, con questo stesso nome vengono identificati **software molto più complessi e capaci di offrire protezione contro un numero di software malevoli molto più ampio** e in tempo reale.

Questo vuol dire che il software non individuerà solamente virus, ma anche moltissime altre famiglie malware e minacce di ogni tipo. Inoltre, lo "schermo" contro i malware funzionerà anche per prevenire eventuali infezioni e non solo per rimuoverle una volta che sono già entrate all'interno della macchina. Questo garantirà un livello di sicurezza più elevato, facendo sì che le informazioni presenti all'interno del disco rigido siano schermate da eventuali tentativi di incursione di software malevolo.

Per riuscirci, i software antivirus utilizzano una serie di tecniche e tecnologie in continua evoluzione. Di fatto, il funzionamento degli antivirus si basano su una combinazione di due tecniche che, nel corso degli anni, si sono dimostrate particolarmente efficaci: **la scansione "signature based" e la scansione euristica**. La prima è quella più "datata" e che, nel corso degli ultimi tempi, ha mostrato qualche segno di cedimento; la seconda, invece, è quella sviluppata più recentemente e dalle "capacità" di analisi decisamente maggiori. Vediamo come funzionano.

• **ANTIVIRUS CON ANALISI "SIGNATURE BASED"** - I primi antivirus sviluppati a cavallo tra la fine degli Anni '70 e l'inizio degli Anni '80 utilizzavano l'analisi "signature based" per poter riconoscere eventuali minacce. Questa tipologia di scansione si basa su un database interno al programma nel quale sono archiviate delle "firme" (*signature* in inglese) dei software malevoli conosciuti. Per ogni nuovo file che viene salvato sul disco rigido, l'antivirus confronta le firme a sua disposizione con il codice sorgente del file: in caso di corrispondenza, verrà messo in quarantena oppure eliminato. Un metodo che si è dimostrato efficace nei primissimi anni, quando il numero di virus e malware non era troppo elevato. Ora che compaiono decine di migliaia di nuove minacce a cadenza quasi quotidiana, questa metodologia di analisi mostra qualche crepa: per monitorare una mole così elevata, sarebbero necessarie risorse informatiche non indifferenti, rallentando non poco il funzionamento del computer.

• **ANTIVIRUS CON ANALISI EURISTICA** - Entra quindi in gioco l'analisi euristica, che permette di individuare anche minacce non ancora conosciute e alleggerire il carico di lavoro della CPU. Questa metodologia non si basa su database prestabiliti o firme, ma studia il comportamento dei malware e lo confronta con quello dei nuovi file archiviati in memoria. Se ci sono delle analogie il file viene messo in quarantena in attesa di un'analisi più approfondita. Questa tipologia di scansione consente di effettuare verifiche più veloci e con un minor consumo di risorse: vuol dire che l'antivirus utilizzerà meno potenza di calcolo del processore e occuperà una quantità di memoria RAM inferiore rispetto a un software analogo "signature based".

2.4.2 Come scegliere l'antivirus

Come accennato qualche rigo sopra, gli antivirus installati sui nostri computer sono solo lontani parenti di quelli che fecero il loro esordio nel mondo dell'informatica circa 40 anni fa. Oggi sono delle suite di sicurezza che comprendono diversi strumenti e rivolte a minacce di tipologie differenti. **Scegliere un antivirus**, dunque, non è così semplice come poteva essere fino a qualche anno fa: i fattori da tenere in considerazione sono molteplici e non sempre è possibile fare un confronto immediato e diretto tra le varie soluzioni di sicurezza informatica.

Alcuni elementi più di altri, però, determinano il "successo" di una suite antivirus rispetto alle altre. Vediamo quali saranno di aiuto per scegliere il miglior antivirus per il PC.

• **SCEGLIERE UN SOFTWARE CON UN'ELEVATA PERCENTUALE DI RILEVAMENTO DEI MALWARE** - Il compito principale di un antivirus è quello di rilevare potenziali file pericolosi. Quindi, la scelta deve essere guidata principalmente da questo aspetto. Per fortuna, cercare un antivirus con un'alta percentuale di rilevamento dei malware non è troppo complesso: grazie a laboratori come AV-Test e AV-Comparatives si hanno a disposizione test sempre aggiornati sull'efficienza dei motori di scansione dei vari software antivirus, così da scegliere quello più adatto alle proprie esigenze.

• **CONTROLLARE LE RISORSE UTILIZZATE** - Altro aspetto da tenere in considerazione è quello della "pesantezza" del software. Anche se, probabilmente, non interagiremo mai con un antivirus, questo continuerà a funzionare in background e "consumare" risorse del sistema. Valutate, quindi, quale sia quello che ha il minor impatto sul sistema e che lo rallenti il meno possibile.

• **PROVA PRIMA DI COMPRARE** - La gran parte delle case sviluppatrici offre delle versioni gratuite dei loro antivirus, in modo che gli utenti possano testarli prima, magari, di comprare una licenza. Solitamente ci sono molte meno funzionalità rispetto alla versione a pagamento, ma sono comunque un ottimo banco di prova per testarne interfaccia, funzionamento e "pesantezza".

• **PROTEZIONE INTERNET** - Come accennato, oggi un antivirus non è solo un antivirus, ma offre decine di strumenti in più capaci di garantire un grado di sicurezza più elevato che in passato.

Potrebbe essere quindi una saggia decisione quella di scegliere un antivirus che offra anche protezione da minacce web, come allegati infetti e siti web corrotti.

- **NON PAGATE PIÙ DI QUELLO CHE UTILIZZERETE** - Questo, ovviamente, non vuol dire che dovrete esagerare. Valutate sempre per bene se le funzionalità extra offerte da un antivirus siano realmente necessarie o se, alla fine dei conti, non le utilizzerete mai. Anche perché maggiori saranno le funzionalità e maggiore sarà il consumo di risorse da parte dell'antivirus.

2.4.3

Cosa sono gli antimalware

Gli antivirus da soli, però, potrebbero non essere sufficienti per garantire una protezione più ampia possibile del proprio sistema informatico. Per questo è più che raccomandabile **installare e utilizzare anche degli antimalware**, software specializzati nella "ricerca&rimozione" di software malevoli di nicchia, ma non per questo meno pericolosi.

La **maggiore differenza tra antivirus e antimalware**, infatti, sta proprio nelle categorie di malware che i motori di scansione sono in grado di trovare. Solitamente, gli antivirus sono specializzati nell'individuazione di famiglie malware più conosciute e "ampie"; gli antimalware, invece, hanno motori specializzati nell'individuare famiglie malware meno note ma, in alcune occasioni, più pericolose di altre.

2.4.4

Gli altri tool per difendersi da attacchi informatici

Antivirus e antimalware, però, non sono i soli strumenti che possono essere utilizzati per mettersi al riparo da minacce informatiche di ogni genere. Ad esempio, alcuni tool possono tornare molto utili per proteggere "il perimetro" del proprio sistema informatico mentre si naviga online. Altri ancora aiutano a individuare file infetti ed eliminarli prima che possano causare dei danni al proprio PC. Insomma, un panorama vasto e variegato che è quanto meno utile conoscere in caso se ne avesse la necessità.

• **FIREWALL** - Anche se non ce ne accorgiamo, i nostri PC sono costantemente esposti ad attacchi da parte di cracker. In molti casi, questi attacchi si concretizzano in tentativi di intrusione nel sistema informatico, utilizzando una delle "porte informatiche" presenti nel sistema operativo. Per evitare che ciò accada è utile installare un firewall, software che monitora il traffico in entrata e in uscita dal PC e, basandosi su determinate regole di sicurezza, blocca sul nascere prove di intrusione non autorizzate.

• **VIRUS TOTAL** - Rispetto ad altri strumenti di sicurezza, Virus Total offre protezione "on demand" e non in tempo reale. Si tratta di un sito web (acquistato qualche anno fa da Google) che mette insieme 40 differenti motori di scansione e consente di verificare se un file (grandi fino a 20 megabyte), un indirizzo web o un intero sito siano compromessi e infetti.

• **AGGIORNAMENTI SOFTWARE** - Potrà sembrare un elemento anomalo, nell'ambito della sicurezza informatica, ma gli aggiornamenti software sono importantissimi nell'ottica di proteggere il proprio sistema. Nella stragrande maggioranza dei casi, infatti, tutti gli aggiornamenti software e di sistema operativo contengono patch per vulnerabilità e bug del codice sorgente che potrebbero consentire a cybercriminali e cracker di accedere al nostro PC e ai dati che contiene.

2.5 Sicurezza informatica: differenze tra Windows e macOS

Per decenni, si è ritenuto che **i sistemi Apple fossero più sicuri rispetto a quelli di Microsoft**. E, tutto sommato, un fondo di verità in questa supposizione c'è. Complice la maggiore diffusione di computer con sistema operativo Windows, per lungo tempo i cracker e cybercriminali vari si sono concentrati nello sviluppo di software malevoli (e altre minacce informatiche) per l'ecosistema Microsoft.

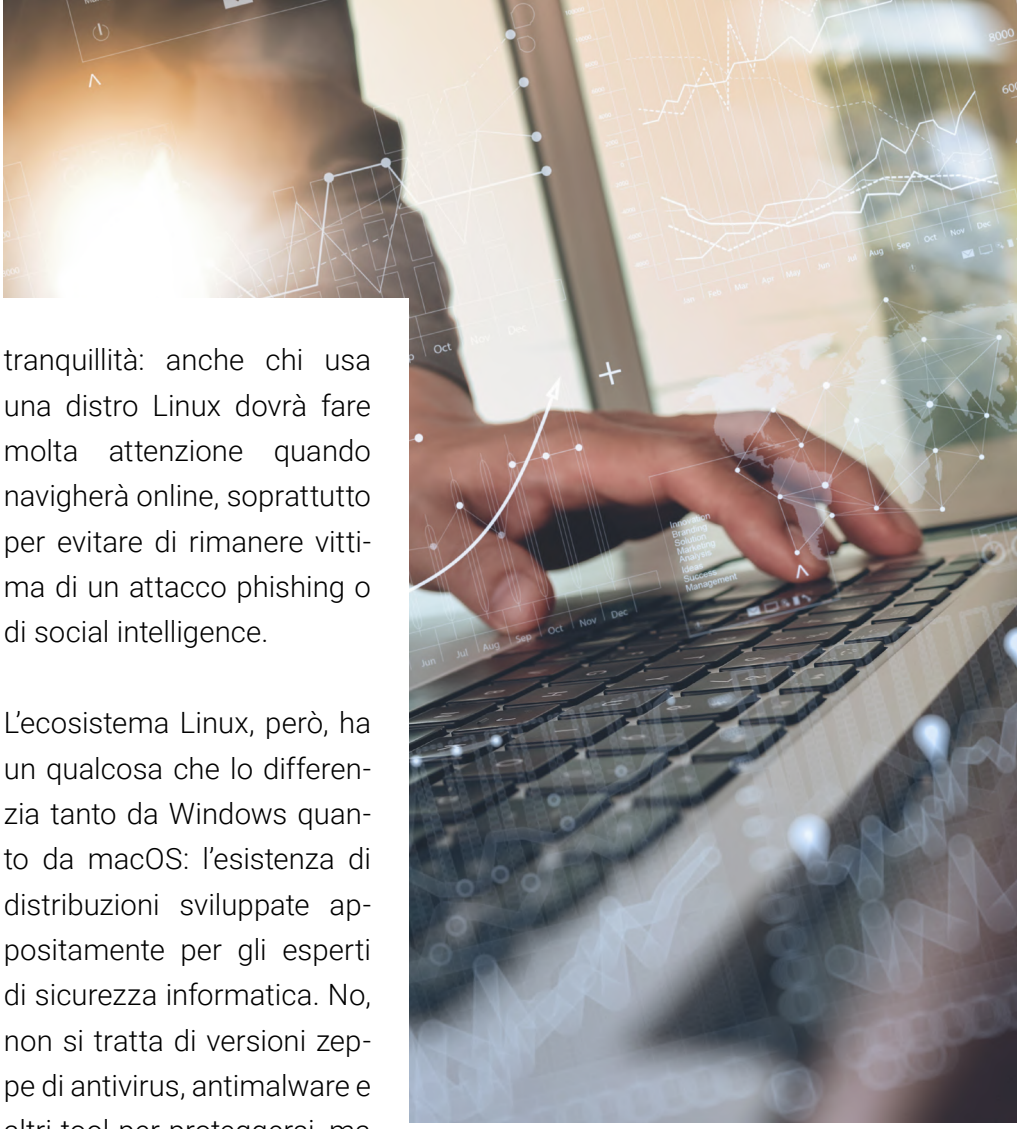
Negli ultimi due decenni, però, **la diffusione dei Mac è cresciuta in maniera vertiginosa** – specialmente in ambito lavorativo – e, parallelamente, sono aumentate anche le minacce rivolte agli utenti della mela morsicata. Come rilevato nel report "Threats to macOS users" rilasciato

da Kaspersky nel settembre 2019, dal 2012 al 2018 si è assistito a una veloce escalation, che ha fatto crescere il numero di minacce nei confronti di utenti macOS: se nel 2012 si registravano poco più di 500 malware per sistemi della mela morsicata, nel 2018 sono più di 85 mila. Cresce anche il numero di tentativi di attacco, che ha fine 2018 ha superato la soglia dei 4 milioni. Ovviamente, si tratta di numeri incomparabili rispetto a quelli che si registrano per Windows ma segnalano, comunque, una tendenza ineluttabile.

Con il passare degli anni, dunque, le differenze tra Windows e macOS (quanto meno sul fronte della sicurezza informatica) si sono andate assottigliando e sono destinate a farsi sempre più labili. Così, se fino a qualche anno fa era possibile utilizzare un Mac senza antivirus o altri strumenti di difesa informatica, tra qualche tempo sarà obbligatorio installarne uno (e già adesso è consigliabile farlo), così come si dovrà fare maggiore attenzione ad altre minacce provenienti dal web.

2.6 Le distro Linux per la sicurezza informatica

Il discorso fatto inizialmente per macOS vale anche per Linux. Essendo un sistema operativo (o, per meglio dire, un ecosistema di sistemi operativi) impiegato da un piccola nicchia – seppure in forte crescita – **le minacce informatiche rivolte agli utenti del pinguino sono ancora esigue**. Questo non vuol dire, però, che si possa navigare in tutta



tranquillità: anche chi usa una distro Linux dovrà fare molta attenzione quando navigherà online, soprattutto per evitare di rimanere vittima di un attacco phishing o di social intelligence.

L'ecosistema Linux, però, ha un qualcosa che lo differenzia tanto da Windows quanto da macOS: l'esistenza di distribuzioni sviluppate appositamente per gli esperti di sicurezza informatica. No, non si tratta di versioni zeppe di antivirus, antimalware e altri tool per proteggersi, ma l'esatto opposto. Stiamo parlando di sistemi operativi "costruiti attorno" a una raccolta di tool pensati per testare la sicurezza delle reti e dei sistemi informatici. Ci riferiamo a prodotti come **Kali Linux e BackTrack** che, con il loro carico di programmi di informatica forense, *penetration test* e altro consentono agli esperti di ricavare informazioni da reti di computer considerate a loro modo inespugnabili.

3. Smartphone sotto attacco: nuovo fronte per la sicurezza informatica

Gli analisti di settore sono tutti concordi. Indipendentemente da quale software house o società di analisi abbia effettuato la ricerca, la conclusione cui sono giunti è la stessa: **gli smartphone sono costantemente sotto attacco** e, nei prossimi anni, la situazione è destinata a peggiorare. Il quadro dipinto ha tinte piuttosto fosche, sia per il presente sia per il futuro.

I dati più aggiornati parlano di minacce informatiche in continuo aumento e in continua evoluzione. Nel suo "*Mobile malware evolution 2019*", **Kaspersky** rileva l'emergere di due trend: la **crescita degli stalkerware** e la presenza di trojan horse mascherati da "app legittime" direttamente negli store di applicazioni. Conclusioni simili sono state raggiunte da **McAfee**: come si legge nel suo "McAfee Mobile Threat Report", la software house oggi di proprietà di Intel mette in evidenza la crescente complessità dei malware per smartphone e la crescita delle cosiddette "fake app", le applicazioni malevole "travestite" da software legittimo. Per gli israeliani di **Check Point**, tanto per citare un altro report annuale,

nella prima metà del 2019 si è assistito a una crescita del 50% degli attacchi rivolti a smartphone e altri dispositivi mobili. Nel report "Cyber Attack Trends: 2019 Mid-Year Report", in particolare, viene messa in evidenza l'aumento esponenziale di malware legati al mondo finanziario e, in particolare, dell'home banking.

Insomma, uno scenario tutt'altro che roseo e che, mostrano i dati, è destinato a peggiorare nel corso dei prossimi anni. E non solo da un punto di vista quantitativo: **il pericolo maggiore è legata a un'evoluzione qualitativa dei malware per smartphone**, che potrebbe renderli ancora più dannosi e distruttivi di quanto non lo siano oggi. Un'evoluzione, per alcuni versi, in atto già ora: sempre più app malevole, infatti, sono ingegnerizzate per infiltrarsi silenziosamente nella memoria del dispositivo e **rubare quante più informazioni possibili**. E, data la quantità enorme di dati personali e riservati che troviamo archiviata su un dispositivo mobile (sia esso uno smartphone, un tablet o addirittura uno smartwatch) è di fatto impossibile restare impassibili di fronte a questo scenario.

3.1 Sicurezza degli smartphone, cosa bisogna sapere

Per comprendere quanto sia diventato importante proteggere il nostro smartphone da possibili attacchi hacker sarà sufficiente passare in rapida rassegna tutte le app installate al suo interno. Mediamente, **ogni utente installa sul dispositivo tra le 60 e le 70 app** di tutti i tipi:

si va dai videogame alle app per modificare foto, passando per le caselle di posta elettronica, social network, messaggistica istantanea, home banking e browser. Insomma, una vera e propria miniera d'oro per tutti quei cracker che vanno alla ricerca di dati e informazioni personali di ogni genere.

Non deve sorprendere, dunque, che negli ultimi mesi e negli ultimi anni **siano cresciuti in maniera esponenziale gli attacchi condotti con malware progettati e realizzati per spiare gli utenti**. Come dimostrano le ricerche citate in apertura, gli esperti del settore hanno rilevato un forte aumento di stalkerware, trojan horse, spyware e altri software malevoli di questo genere. Lo smartphone, dunque, è diventato sempre più uno strumento che permette ai cybercriminali di spiare ogni singolo aspetto della nostra quotidianità, da quelli più personali (come foto o messaggi inviati su WhatsApp, Telegram o Instagram) a quelli più professionali (documenti e messaggi di posta di lavoro, tanto per citarne due).

E, forse ancor più di quanto accade con i computer, **il comportamento dell'utente è fondamentale** per garantire la sicurezza di smartphone e altri dispositivi mobili. Il caso di Jeff Bezos, in questo caso, è esemplare.

Il fondatore di Amazon, di certo non l'ultimo arrivato nel campo della sicurezza informatica, è stato vittima di un attacco hacker (pare orchestrato da uno stato sovrano). Bezos, forse un po' distrattamente, avrebbe pigiato su di un link ricevuto su WhatsApp da un contatto poco affidabile. Questo avrebbe permesso ai cybercriminali di accedere a tutte le informazioni archiviate sull'iPhone del papà di Amazon e rubare informazioni riservate. Senza la "distrazione" (se così vogliamo definirla) di Bezos, i cracker non avrebbero avuto alcuna possibilità di entrare in possesso dei dati che cercavano.

Quanto accaduto al malcapitato Bezos, però, può esserci di grande aiuto per capire cosa fare per proteggere al meglio il nostro smartphone e le informazioni contenute al suo interno. Ovviamente, si potranno utilizzare app e software di protezione come antivirus e antimalware ma **non saranno assolutamente sufficienti**. L'utente deve essere consapevole del fatto che per utilizzare lo smartphone in tutta sicurezza sarà necessario avere un livello di attenzione molto elevato, in qualunque istante e in qualunque situazione. Anche il messaggio apparentemente più innocuo, infatti, può tradursi in una iattura: senza che ce ne accorgiamo, potremmo finire su un portale web che installerà automaticamente un programma malevolo sul dispositivo, grazie al quale un cracker potrà spiare letteralmente ogni cosa che facciamo.

A differenza di un PC, infatti, **lo smartphone è sempre con noi, ovunque ci troviamo**. Se un criminale informatico dovesse riuscire a installare un malware spia nel telefonino potrebbe avere accesso al GPS e "pedinarci" passo dopo passo, monitorando così ogni nostro spostamento; potrebbe accendere microfono e fotocamere e ascoltare cosa diciamo o addirittura spiarci nell'intimità; potrebbe poi accedere a tutte

le altre app installate sul dispositivo e leggere i messaggi che scambiamo o scorrere le foto della galleria. Certo, i toni utilizzati in questo paragrafo **potrebbero sembrare allarmistici**, ma non è affatto così: l'esempio del furto subito da Jeff Bezos è solo uno dei tanti che si potrebbero fare e che, sfortunatamente, accadono praticamente con cadenza quotidiana.

Come accennato, poi, le minacce per dispositivi mobili potrebbero ben presto conoscere un ulteriore salto di qualità, rendendo la vita degli utenti ancora più complicata e complessa. Per questo motivo è più che consigliabile approfittare di ogni singolo istante per farsi trovare pronti nel momento in cui questo "salto evolutivo" avverrà.

3.2 Malware per smartphone: i più diffusi

Anche se in rapida trasformazione, il panorama dei malware per smartphone è molto meno evoluto rispetto a quello dei PC. Come abbiamo visto, **esistono decine di famiglie di malware per computer**, ognuna con le sue caratteristiche e peculiarità. Sul fronte dei dispositivi mobili, invece, le maggiori famiglie si possono contare sulle dita di una mano; anzi, a voler essere precisi le più diffuse sono solamente tre. Almeno per ora. Imparando a capire **come si diffondono** e **quale è il loro comportamento** una volta che hanno infettato un dispositivo sarà possibile anche capire come difendersi da loro.

TROJAN

Pur non essendo la famiglia più numerosa, è senza dubbio quella che pone più pericoli per gli utenti finali. Come accade nei PC, i trojan sono utilizzati da cracker e cybercriminali per introdursi all'interno dei dispositivi mobili. La famiglia dei trojan, a sua volta, si divide in "sotto-famiglie": ci sono i **trojan propriamente detti**, che permettono ai cybercriminali di crearsi "un'apertura" nei sistemi di difesa degli smartphone e di trafugare dati ogni volta che ne vogliono; ci sono poi i cosiddetti **banking trojan** o trojan bancari e, come dice il nome stesso, puntano a impossessarsi dei dati di accesso al conto corrente online.

SPYWARE

Altra grande famiglia di malware per smartphone è quella degli spyware, ossia dei software malevoli che possono essere utilizzati per spiare le attività del possessore del dispositivo. Anche in questo caso, la famiglia si divide in molteplici "sotto-famiglie": ci sono, ad esempio, **gli stalkerware**, che vengono usati per accedere liberamente ai messaggi, lista chiamate e galleria fotografica dello smartphone; ci sono poi gli spyware che consentono di "intercettare" ogni tipologia di comunicazione effettuata dal device mobile (chiamate, messaggi e così via); non vanno dimenticati poi le app spia che permettono di accedere alle fotocamere dello smartphone e scattare foto o realizzare video a distanza; infine, le app spia per pedinarci, che sfruttano chip GPS per tracciare spostamenti e movimenti.

ADWARE

Sono probabilmente la famiglia di malware per smartphone più numerosa ma, per alcuni versi, anche la meno pericolosa. Gli adware vengono creati per motivi economici e non per rubare dati o spiare i possessori degli smartphone. Letteralmente, **sono "malware pubblicitari"**, pensati per mostrare inserzioni pubblicitarie mentre navighiamo online (e non solo) e consentire ai cybercriminali di guadagnare dalle visualizzazioni. A volte, gli adware sono in grado di mostrare pubblicità senza che l'utente se ne accorga: vengono riprodotte in background mentre abbiamo altre app aperte, evitando così di "rovinare" l'esperienza d'uso del dispositivo. Potrebbe però accadere che le troppe pubblicità mostrate sovraccarichino il dispositivo, facendolo surriscaldare e diminuendo sensibilmente la durata della batteria.

3.3. Come difendere lo smartphone dai cybercriminali

Le minacce ai nostri dispositivi mobili, dunque, diventano sempre più numerose e sempre più complesse. **Cosa bisogna fare, dunque, per difendere le informazioni che sono archiviate al loro interno?** Come abbiamo già accennato in precedenza, la sicurezza dei dispositivi mobili è legata a due fattori: da un lato ad app e altri sistemi di sicurezza software che possono essere installati sulla memoria del dispositivo; dall'altro l'elemento umano, fondamentale per evitare che applicazioni di dubbia natura riescano a far breccia tra le difese del dispositivo.

Partiamo, però, dal primo dei due fattori: quello "in codice". Ossia, le applicazioni per la sicurezza informatica che gli utenti possono scaricare e installare sui loro dispositivi. Le più note sono, ovviamente,

gli antivirus, ma non sono le sole. Anche su piattaforma mobile, infatti, si assiste a una proliferazione di prodotti che promettono di aumentare i livelli di sicurezza del telefonino e di altri dispositivi mobili. Anche su piattaforma mobile, ad esempio, troviamo degli **antimalware** che permettono di proteggere lo smartphone da minacce "di nicchia" e non ampiamente diffuse.

Ma non sono questi gli unici strumenti di difesa a disposizione degli utenti. Nel corso degli anni sono state realizzate e sviluppate soluzioni che consentono di proteggere i dati conservati all'interno della memoria. Ad esempio, utilizzare **un'app di messaggistica che fa uso di protocolli crittografici** consente di proteggere le proprie conversazioni da attacchi *man in the middle*, mentre un'**app VPN** ha gli stessi effetti sulla normale navigazione online. Gli utenti più "avanzati" potrebbero trovare utili app che **monitorano il consumo dei dati**: studiando l'andamento dei flussi in ingresso e in uscita dal dispositivo, o rilevando picchi anomali, è possibile scoprire se ci siano app che stanno "sifonando" danni verso l'esterno (ossia, inviano dati verso un server remoto creato per contenere informazioni trafugate da migliaia di dispositivi) o app che, al contrario, stanno caricando dati sul nostro dispositivo (comportamento tipico degli adware).

Fanno poi parte di questo elenco anche applicazioni che, a una prima occhiata, potrebbero anche non sembrare direttamente collegate al settore. Possono tornare molto utili, ad esempio, i **password manager e le app per la verifica a due passaggi**, che offrono un livello di sicurezza supplementare per l'accesso ai propri account di posta elettronica e social. Alcuni utenti, infine, potrebbero trovare utili per proteggere i loro dati personali le cosiddette **locker app**, applicazioni che bloccano l'ac-

cesso ad alcune app (a scelta dell'utente) e le rendono accessibili solo dopo aver inserito un codice di sblocco.

Oltre alle app, come detto in precedenza, è fondamentale che l'utente adotti un comportamento consapevole, evitando di compiere azioni che possano compromettere sistemi e soluzioni di sicurezza informatica. Un esempio? Le **app a pagamento "craccate"** e scaricate da fonti poco raccomandabili. Solitamente, applicazioni di questo genere vengono create da cracker e altri cybercriminali e servono come "testa di ponte" per penetrare all'interno del dispositivo. Oltre all'app che si vuole scaricare gratuitamente, infatti, sono solitamente presenti malware di ogni genere, solitamente trojan horse.

Altrettanto importante è la **gestione dei permessi delle app**. Si tratta delle autorizzazioni che le applicazioni chiedono prima di essere installate sul telefono per accedere alle componenti e alle funzionalità del dispositivo. Per poter funzionare al meglio, ad esempio, Instagram chiederà le autorizzazioni per poter utilizzare la fotocamera e accedere alla Galleria fotografica del dispositivo. Si tratta di permessi pienamente legittimi, necessari per sfruttare al meglio le funzionalità di Instagram. Ma non è sempre così: alcuni sviluppatori "furbetti" approfittano

del fatto che nessun utente (o quasi) presta attenzione alle domande che gli vengono poste prima dell'installazione e ottiene così permessi per le funzioni più disparate, dalla fotocamera al GPS. Si è scoperto, ad esempio, che le app torcia che andavano così di moda fino a non più di 5 anni fa tracciavano gli spostamenti degli utenti e rivendevano questi dati per motivi commerciali.

Più in generale, non dovranno essere messi in atto tutti quei comportamenti online che potrebbero in qualche modo rivelarsi deleteri per il dispositivo. Anche in questo caso, gli esempi sono molteplici: dall'evitare di pigiare su link poco sicuri al **download di file dalle app di messaggistica** (una leggerezza che è costata cara a Jeff Bezos, come abbiamo accennato), passando per le visite a portali poco raccomandabili.

In questo scenario, un ruolo di primaria importanza viene recitato anche da Apple e Google. I due giganti della Silicon Valley, infatti, **implementano nativamente dei sistemi di sicurezza all'interno dei rispettivi sistemi operativi** (iOS e Android, ovviamente) e degli store dai quali gli utenti scaricano le loro applicazioni. Entrambi i sistemi operativi integrano sistemi di crittografia legati al codice di sblocco o ai sistemi biometrici: in questo modo i dati saranno accessibili solo dopo aver sbloccato il dispositivo e nessuno che ne venisse in possesso

(ad esempio, rubandolo o trovandolo per strada) sarebbe in grado di recuperare le informazioni in memoria con programmi *ad hoc*.

Inoltre, sia **Apple sia Google analizzano il codice sorgente delle applicazioni** (con algoritmi di intelligenza artificiale e "revisori" in carne e ossa) prima di pubblicarle sull'App Store e sul Google Play Store. Google, inoltre, integra il sistema "Play Protect", una sorta di antivirus che scansiona l'app prima che venga installata sul dispositivo.

3.4 Antivirus Android, quali sono e la loro efficacia

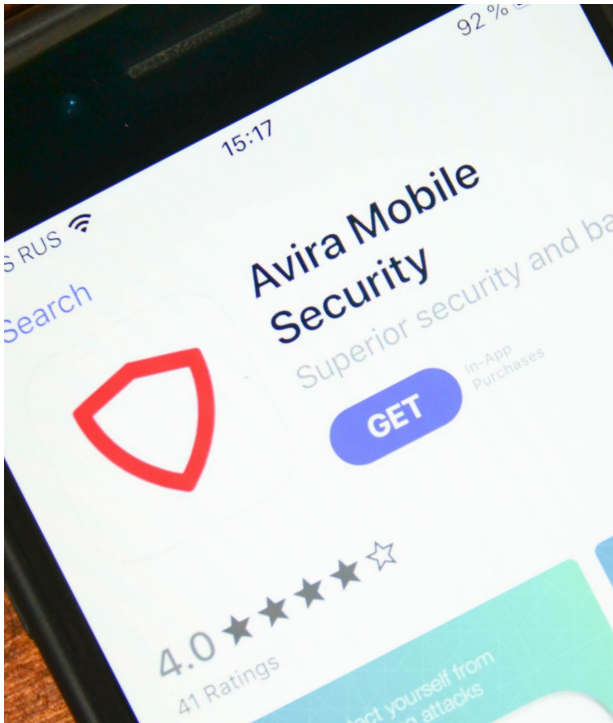
Tra i vari prodotti di sicurezza pensati per i dispositivi mobili, gli **antivirus Android** sono una delle soluzioni che va per la maggiore. Non tutti, però, sono d'accordo sulla loro completa efficacia. Secondo una ricerca condotta da un gruppo di ricercatori dell'università statunitense Georgia Tech, infatti, **non tutti gli antivirus Android fanno quello che promettono** (ossia, trovare ed eliminare virus e altri malware dal proprio dispositivo).

Gli studiosi statunitensi hanno testato **58 differenti applicazioni antivirus** utilizzando alcuni tool per realizzare malware "adattivi", in grado dunque di bypassare i controlli dei sistemi di sicurezza installati sul dispositivo. Di tutte le app testate, solamente due sono state in gradi di rilevare la presenza dello strumento di *hacking*, mostrando come

la strada che gli antivirus Android devono percorrere verso la piena maturità è ancora lunga.

Scegliere il miglior antivirus Android, però, non è un'impresa semplice. Come dimostrano alcune ricerche, le app contro i virus sono anche **le più contraffatte dai cracker**. Potrebbe capitare, quindi, di scaricare un'applicazione che apparentemente è un antivirus, ma in realtà si tratta di un malware che permette al suo creatore di accedere ai documenti presenti nella nostra memoria e trafugarli; di tracciare i nostri movimenti con il GPS; spiarci attraverso fotocamera e microfono e molto altro ancora.

Insomma, se non si fa attenzione a ciò che si sta scaricando, si rischia non solo di non proteggere smartphone e dati, ma addirittura di spianare la strada a un cyberattacco in piena regola. Per questo motivo, nel caso in cui vogliate installare un'app antivirus sul vostro smartphone Android, è consigliabile affidarsi alle maggiori case sviluppatrici del settore che, magari, hanno realizzato prodotti di sicurezza informatica anche per computer.



Come abbiamo già visto nel caso degli antivirus per PC, anche per gli antivirus Android è possibile affidarsi

a società terze specializzate nell'esecuzione di test sul funzionamento e sulle capacità di rilevamento delle minacce. I **tedeschi di AV-Test**, ad esempio, conducono delle prove su base trimestrale per verificare se e quanto le app siano efficaci nel rilevare le minacce. Ne viene fuori una classifica, pubblicata sul loro portale web[4], che permette così di scoprire quali sono le piattaforme di sicurezza più complete e sicure da installare sul proprio dispositivo mobile.

Tra queste spiccano, tanto per fare un esempio, nomi conosciuti come quelli di **Avira Antivirus, Bitdefender, Norton 360 e Trend Micro Mobile Security**, ma anche software house specializzate in prodotti per la protezione dei dispositivi mobili come OnAV di Securi.

3.5. Sicurezza iPhone: iOS è (davvero) a prova di virus?

Se vi è capitato di sentire o di leggere che **iOS e gli iPhone sono a prova di malware e virus**, sappiate che sii tratta di un'affermazione non completamente vera, anche se verosimile. Come accade per macOS, il numero di minacce informatiche "ingegnerizzate" per il sistema operativo mobile dell'iPhone sono pochissime, ma stanno crescendo nell'ultimo periodo. Questa peculiarità sembra renderlo del tutto immune, ma non è affatto così.

4. https://www.av-test.org/en/antivirus/mobile-devices/

Comunque, chi possiede un iPhone può ritenersi “mediamente” più sicuro rispetto a un utente Android per un motivo ben preciso: i box di sabbia. O, per dirla all’inglese, per le **sandbox**. Non si tratta, ovviamente, delle sabbiere nelle quali sono soliti giocare i bambini nel giardino di casa o nei giardini pubblici, ma dei meccanismi che consentono

di eseguire qualunque applicazione e qualunque programma (e, quindi, aprire qualunque tipo di file) in assoluta sicurezza. I sandbox isolano le app in esecuzione all’interno di un “recinto protetto” che non ha collegamenti con l’esterno. In questo modo, anche se l’app fosse infetta non potrà uscire dalla sua sandbox e non potrà compromettere altre app o altre componenti del sistema operativo.

Sin dalla prima versione, realizzata ormai oltre 10 anni fa, iOS esegue nativamente tutte le applicazioni all’interno di una sandbox. Ciò rende più complesso il transito di dati da un’applicazione all’altra, ma al tempo

stesso **mette al sicuro l'esperienza d'uso dell'utente** e fa sì che i malware abbiano vita difficile su iOS. Questo, però, non vuol dire che le app malevole per iOS non esistono. Anzi: come si legge nel "2020 State of Malware Report" di Malwarebytes, **"i malware per iPhone esistono, ma non c'è modo di fare una scansione"**.

Quello che pochi sanno, infatti, è che **non esiste un vero e proprio antivirus per iPhone**. Il fatto che le app girino all'interno delle sandbox rende difficile la stessa scansione alla ricerca di eventuali minacce o file malevoli. Le "app di sicurezza" per iPhone che è possibile scaricare dall'App Store altro non sono che suite per la sicurezza online, all'interno delle quali si possono trovare moduli anti-phishing, ad blocker, VPN e parental control.

3.6 Truffe telefoniche, come riconoscerle e come difendersi

La sicurezza dei dispositivi mobili non passa solamente dalla protezione da cyberminacce come malware o tentativi di "accesso forzoso" compiuti da cracker. La minaccia può essere per alcuni versi più subdola e, per questo, più difficile da identificare e riconoscere. Capita sempre più spesso, infatti, che i possessori di smartphone siano vittime di truffe telefoniche di ogni genere, che puntano a rubare soldi (sia dal conto telefonico, sia dal conto corrente) o dati utili a impadronirsi dell'identità dell'intestatario della SIM.

Per riuscirci, i cybertruffatori utilizzano tecniche che variano a seconda dell'obiettivo da raggiungere. In alcuni casi possono essere più aggressivi e diretti; in altri utilizzano degli schemi che puntano prima di tutto ad acquistare la fiducia dell'utente, per poi colpirlo "nell'intimità". A grandi linee, comunque, le varie tipologie di truffe telefoniche possono rientrare all'interno di tre macrocategorie. Vediamo quali sono.

SIM SWAP

Tra le varie truffe telefoniche è una delle ultime ad aver fatto la propria comparsa sul palcoscenico mondiale. E, data anche la sua "giovane età", è considerata essere una delle più pericolose, soprattutto per i rischi che comporta sul fronte della protezione dell'identità personale e dei profili web. *SIM Swap* sta, letteralmente, per "scambio di SIM" e come lascia intendere il nome **comporta il "furto" del proprio numero di telefono**. Diffuso soprattutto negli Stati Uniti, viene utilizzato per accedere ai profili personali protetti da verifica in due passaggi. Questa tecnica prevede che il criminale conosca la reale identità della vittima, ovviamente il numero di telefono e altri dati personali. Una volta che ha raccolto queste informazioni, il truffatore si presenta in un negozio oppure chiama il servizio clienti del provider dei servizi di telefonia e usa le informazioni personali raccolte per convincere il commesso/l'operatore a disabilitare la SIM legittima e "spostare" il numero di telefono del truffato su una nuova SIM in suo possesso (fare un *SIM swapping*, dunque). Nel caso trovi un consulente "credulone" (e che non chiede un documento per verificare la reale identità della persona che si trova di fronte), il criminale otterrà una nuova SIM con il numero di telefono della vittima prescelta. A questo punto potrà utilizzarlo per accedere alla casella di posta elettronica, profilo social o, ancora peggio, al conto corrente bancario facendosi inviare i codici di accesso ai profili via SMS.

SMISHING

Si tratta dell'equivalente telefonico del phishing. Solo che, al posto dei messaggi di posta elettronica, vengono utilizzati gli SMS. Nonostante cambi il "mezzo di trasmissione", le modalità di attacco e gli obiettivi dei cybertruffatori sono gli stessi: furto di credenziali, di informazioni personali o di denaro. Nel messaggio-truffa, i criminali vestono solitamente i panni di un istituto di credito (la banca o le Poste) che ci avvisa di un pericolo riguardante il nostro conto corrente – e i nostri soldi, ovviamente. Si viene così invitati a contattare un centro assistenza, con tanto di numero in bella evidenza. All'altro capo della cornetta, però, non risponderà la nostra banca, ma un truffatore che ci sottrarrà dati utili per entrare nel nostro conto online o per impossessarsi della nostra identità.

VISHING

Crasi delle parole inglesi "Voice" e "Phshing", il vishing viene detta anche truffa del consenso rubato. Il cybertruffatore, in questo caso, crea un sistema di chiamate automatizzato che consente di contattare un numero elevato di persone in pochissimo tempo.

Il vishing può essere declinato in vario modo: dalle chiamate dei call center che riescono a "estorcere" il nostro consenso per un cambio di operatore o fornitore di servizio alle truffe ben più articolate, grazie alle quali impossessarsi dei dati personali dell'utente.

WANGIRI

Detta anche "truffa dello squilletto", si palesa tramite chiamate brevissime o singoli squilli provenienti da numeri di telefono esteri, solitamente del Nord Africa o dell'Est Europa (non mancano, però, casi anche di truffe dello squillo condotte tramite numeri britannici).

La speranza dei truffatori, in casi come questi, è che l'utente provi a richiamare il numero: al primo squillo verranno addebitate cifre elevatissime (anche diversi euro per pochi secondi di chiamata) o attivati abbonamenti settimanali indesiderati e difficilissimi da disdire.

4. Sicurezza informatica, il pericolo viene dal web

Il ruolo che il web – e la Rete in generale – gioca sul fronte della sicurezza informatica è tutt'altro che secondario. Sin dagli albori delle minacce e delle infezioni malware, infatti, **le reti di computer sono state fondamentali per la loro diffusione**. Quello che viene identificato come il primo malware della storia altro non era che un semplicissimo worm creato con l'obiettivo di "misurare l'estensione" di Arpanet, la progenitrice del moderno Internet. Oggi, se possibile, questo ruolo, questa importanza è addirittura aumentata: tutte le tipologie di infezioni e di minacce passano necessariamente dalla Rete. Gli attacchi condotti con altri mezzi (come USB o supporti di memoria infetti) sono infinitesimali rispetto a quelli che sfruttano una connessione di rete, di qualunque natura essa sia.

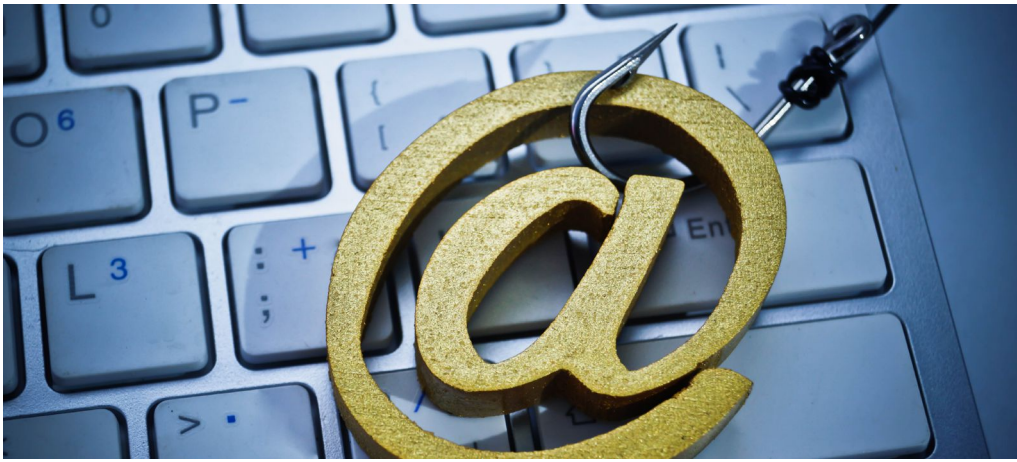
A questo si aggiunge una sorta di "neutralità della Rete" (non nel senso in cui viene normalmente intesa questa locuzione) nei confronti dei dispositivi che utilizziamo quotidianamente. Navigando online (o stando semplicemente connessi) **corriamo il rischio di essere attaccati**

e infettati sempre e comunque, indipendentemente dal fatto che utilizziamo un computer, uno smartphone, uno smartwatch o un qualunque dispositivo dell'Internet of Things (dagli elettrodomestici intelligenti ai sensori utilizzati nelle fabbriche). Per questi motivi, e innumerevoli altri, è necessario prestare particolare attenzione quando si naviga su Internet: basta un click su un link o il download di un'app per compromettere il nostro dispositivo e trovarsi, nel giro di pochi secondi, in un mare di guai.

Conoscere tutti i pericoli che si possono correre utilizzando un computer o uno smartphone connesso alla Rete, dunque, è di fondamentale importanza per **evitare di commettere errori che faciliterebbero la vita a cracker, truffatori e cybercriminali vari**. Come detto in precedenza, infatti, l'utente in carne e ossa è il vero anello debole della catena della sicurezza informatica, la "variabile impazzita" che fa sì che un tentativo di attacco si trasformi in un incredibile successo o in un misero fallimento. Se, ad esempio, l'utente evitasse di cliccare sul link presente nel messaggio di posta elettronica o non scaricasse il video che un suo amico gli ha inviato su WhatsApp o qualunque altra applicazione di messaggistica istantanea, il criminale informatico che sta tentando di attaccarlo avrebbe ben poche possibilità di riuscire nel suo intento.

Insomma, il ruolo che gli utenti hanno nell'ambito della sicurezza informatica è quanto mai attivo: sta a loro prendersi cura dei loro dispositivi e dei loro profili web. Altrimenti sarà qualcun altro a farlo al loro posto (e la cosa non sarà affatto piacevole, ovviamente).

4.1 Sicurezza online, attenzione doppia



Anche se le tecniche di attacco online create da cybercriminali vari possano sembrare differenti, di fatto qualunque tipo di minaccia web condivide la stessa origine. A grandi linee, infatti, possiamo ricondurre tutte le possibili mosse dei criminali informatici a due grandi categorie: **phishing** e ***social engineering***. Andando ad analizzare in profondità le varie tipologie di attacco, infatti, si potrà scoprire che alla loro base si troverà una di queste due tecniche.

Ad esempio, una **campagna di diffusione malware** potrà prendere il via da una serie di e-mail phishing, mentre una **truffa** potrebbe iniziare con un approccio di tipo "social engineering", che permetterà agli attaccanti di scoprire le abitudini e i comportamenti della vittima. I due appena citati non sono altro che due dei tanti casi di questo genere che potrebbero

essere presi in analisi: attacchi phishing o di social engineering avvengono tutti i giorni, con un ritmo sempre crescente. Grazie anche a strumenti di automazione legati al machine learning e all'intelligenza artificiale, infatti, i cybercriminali sono in grado di avviare delle campagne malware senza che ci sia bisogno di un loro continuo controllo. Anzi, nei sistemi più avanzati gli attacchi phishing e malware sono in grado di "auto-evolvere" per adattarsi alle strategie di difesa messe in atto dalla vittima designata.

Sarà dunque fondamentale sapere **che cos'è una campagna phishing o cosa è l'ingegneria sociale** e come funzionano queste due minacce così da poterle riconoscere al primo colpo ed evitare di restare "impigliato" nella rete dei malfattori digitali.

4.2 Cos'è e come riconoscere un attacco phishing

Il phishing (neologismo inglese derivante dalla parola *fishing*, "pescare" in italiano) è una tecnica informatica che, in caso di successo, consente ai criminali informatici di **entrare in possesso di informazioni riservate della vittima** (o delle vittime, in caso di attacco su vasta scala). Per riuscire in questo scopo i criminali informatici utilizzano tecniche piuttosto collaudate: il più delle volte inviano agli utenti messaggi verosimili riguardanti gli argomenti più disparati: dalla banca che ci avvisa che il nostro conto corrente online è sotto attacco ed è il caso di cambiare

la password, oppure un avviso di giacenza di un pacco da ritirare per il quale sono necessarie le generalità della persona. In parole povere, **un attacco phishing si concretizza nell'invio di messaggi verosimili con lo scopo di carpire informazioni da uno o più utenti**. La comunicazione può avvenire con un qualunque mezzo che consenta di mettere in contatto due o più persone: se fino a qualche anno fa la posta elettronica era lo strumento preferito, oggi non mancano casi di phishing che viaggiano attraverso gli SMS (detto ***smishing***), sulle piattaforme di messaggistica istantanea (su WhatsApp se ne contano a centinaia al giorno, ormai) o sulle reti social, spesso e volentieri sotto forma di inserzioni pubblicitarie. Ma, esattamente, **come funziona un attacco phishing?** Apparentemente, lo schema alla base è molto semplice: il cybercriminale "attiva" una campagna spam, inviando decine di migliaia di messaggi in contemporanea sfruttando server infetti o direttamente sotto il suo controllo. All'interno della comunicazione si fa riferimento a un evento che è accaduto (o che deve accadere) che potrebbe riguardare una vasta platea di utenti. Come abbiamo già detto, si potrebbe ricevere un messaggio riguardante un tentativo di furto di password, con la richiesta di aggiornare la chiave d'accesso alla propria e-mail, al conto bancario o al profilo social; oppure di un pacco in attesa di essere ritirato (o una fortunata vincita a qualche strana lotteria) per il quale è necessario fornire nome, cognome, data di nascita e magari anche il codice fiscale. In ogni messaggio phishing "che si rispetti" è sempre presente **un link che rimanda apparentemente al sito della propria banca o del corriere**.

Guardando bene, però, il sito presenta qualche imprecisione e, soprattutto, la URL somiglia a quella "ufficiale", ma si differenzia per piccoli dettagli. Se non si dovesse far caso a questi dettagli e si dovessero inserire le informazioni all'interno del form, si sarà "abboccato" all'esca lanciata dal cyber truffatore e gli avremo regalato i nostri dati e le informazioni personali.

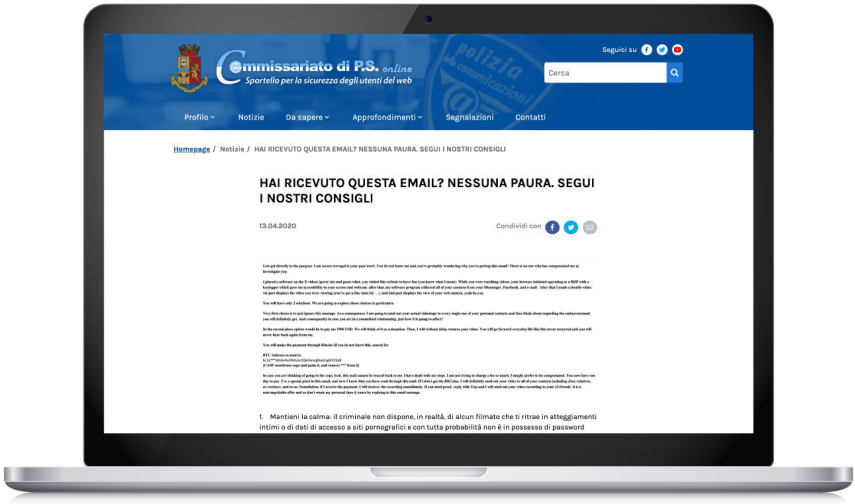
Come difendersi dal phishing? Molto semplicemente, facendo attenzione alla URL del sito sul quale si "atterra" dopo aver cliccato sul link. Pur essendo molto simile, non sarà mai identica a quella della propria banca, del proprio fornitore di posta elettronica o del corriere. Ad esempio, invece di bnl.it il messaggio di posta potrebbe arrivare da bnl.it, dove la "l" minuscola è sostituita dalla "I" maiuscola; oppure, anziché poste.it il messaggio viene inviato da pos.te.it o da poste.info (nel primo caso, il messaggio viene inviato dal server "te.it", mentre nel secondo cambia l'estensione del dominio).

Tratto dal profilo Facebook *Commissariato di PS Online.*

La difesa dal phishing, però, dovrebbe partire prima di "atterrare" sul sito creato dal truffatore digitale. Già dal messaggio è possibile intuire che ci sia qualcosa di strano: prima di tutto, **nessuna banca invierà mai un messaggio per avvisare il cliente di cambiare password** o chiavi d'accesso al proprio conto corrente online. Poi, l'italiano di questi messaggi è quanto meno rivedibile: solitamente, infatti, si tratta di messaggi "standard" in inglese tradotti in italiano con traduttori online o software di questo genere. Ciò fa sì che non sempre le traduzioni siano corrette e ci saranno sempre uno o più errori grammaticali o sintattici che dovrebbero fungere da "campanello d'allarme".

4.3. Cos'è e come riconoscere il social engineering

Anche se molti li confondono, phishing e social engineering non sono affatto la stessa cosa. Certo, hanno molti punti in comune e, in alcuni casi, **il social engineering è "propedeutico" al phishing**, soprattutto in caso di attacchi mirati verso un numero limitato di vittime. Però è sempre bene non confonderli. Detto anche **ingegneria sociale**, il social engineering è una tecnica (o, per meglio dire, una serie di tecniche) che fa forza su leve psicologiche e comportamentali per ottenere da una vittima specifica dati sensibili e personali. L'obiettivo finale, dunque, è lo stesso del phishing, anche se le strade che vengono percorse per ottenere quei dati sono più variegate e, soprattutto, "l'operazione" richiederà molto più tempo di altre tecniche di attacco.



Tratto dal sito web *www.commissariatodips.it*

A differenza delle altre tipologie, però, **l'ingegneria sociale non sfrutta alcuna falla o vulnerabilità software**. Piuttosto, sfrutta delle "vulnerabilità" psicologiche degli utenti, andando a giocare sulle loro abitudini online per ottenere informazioni personali e sensibili. Un attacco di questo genere prevede, prima di tutto, lo studio del comportamento che la vittima ha online, raccogliendo quante più informazioni disponibili pubblicamente. Terminata questa fase di "studio", il cybercriminale passa a quella di attacco: sfruttando i social o le piattaforme di messaggistica avvicina l'utente, provando a entrare in confidenza con lui o lei. L'obiettivo, a questo punto, è conquistare la sua fiducia, in modo che possa vederlo come un amico e una persona di cui fidarsi. Se tutto va come da programma (del cybertruffatore, ovviamente) si arriva alla terza fase, quella nella quale la vittima si fida completamente dell'altra persona conosciuta online, tanto da confidargli dati e informazioni che potrebbero tornargli utili, ad esempio, per impossessarsi della sua identità (non solo online, ma anche nella vita privata) o compiere azioni criminali fingendo di essere

Tratto dal profilo Facebook *Commissariato di PS Online.*

l'altra persona (come mettere in vendita oggetti rubati, contraffatti o inesistenti). Ad esempio, potrebbe arrivarci **l'email di un nostro carissimo amico** che, nel corso di un viaggio all'estero, si è trovato improvvisamente senza denaro e avrebbe proprio bisogno del nostro aiuto per tornare a casa. Per questo sarebbero necessarie alcune centinaia di euro, da accreditare su una carta prepagata ricaricabile, in modo che possa acquistare un biglietto aereo.

A differenza del phishing, **riconoscere un attacco di ingegneria sociale è molto più complesso**. Se ci si trova di fronte a un cybertruffatore esperto, infatti, sarà difficile capire sin dall'inizio quale sia il suo piano. L'unico modo per evitare di cadere nella trappola del social engineering è non dare mai propri dati o informazioni di qualunque genere a persone conosciute esclusivamente online. In questo modo saranno al sicuro, all'interno della propria testa.

E se proprio ci sono ancora dei **dubbi sulla reale identità di chi vi ha contattato**, potrete sempre fare la "prova contraria": nell'esempio di prima, provare a contattare il vostro amico via telefono o app di messaggistica istantanea, per verificare dove si trovi e magari organizzare una videochiamata, così da esser definitivamente certo che a fare la richiesta non sia stato lui (o, al contrario, che si trova effettivamente in difficoltà). Nel caso il messaggio ricevuto non fosse di un amico, non è detto che dobbiamo lasciar cadere l'email come "lettera morta". Ci sono infatti

alcuni simpatici programmi online ideati per rispondere ai messaggi di posta elettronica che individuiamo come “phishing” o “social engineering”. In questo modo, il truffatore perderà tempo a rispondere agli algoritmi di intelligenza artificiale, credendo invece di dialogare con una persona in carne e ossa.

4.4 Cos’è e a cosa serve la crittografia nel web

Nonostante la loro origine preceda di qualche migliaio di anni la comparsa dell’informatica (il primo “codice crittografico” viene fatto risalire addirittura agli antichi egizi), gli **algoritmi di crittografia** sono oggi tra i migliori alleati di chi si occupa di sicurezza informatica. Non è di certo un caso che tutti gli applicativi più “sensibili” (come la navigazione online o le piattaforme di messaggistica istantanea) siano “schermati” da algoritmi di questo genere.

Precisiamo immediatamente che **la crittografia non interessa gli utenti finali da un punto di vista tecnico-pratico**, ma più dal punto di vista

degli "effetti" che essa avrà sulla protezione dei nostri dati e delle informazioni che inviamo e riceviamo mentre siamo online. L'utilizzo della crittografia, infatti, non richiede alcuna "azione pratica" da parte dell'utente, ma sarà attiva di default in tutte le applicazioni o programmi che supportano un tipo di algoritmo crittografico anziché un altro. Questo vuol dire che non sarà necessario possedere conoscenze informatiche avanzate (come conoscere linguaggi di programmazione o il funzionamento di una rete di computer), ma sarà comunque necessario capire **come funziona la crittografia** per comprendere quali siano i vantaggi che garantisce quando siamo online.

4.4.1

Che cos'è la crittografia e a che cosa serve

La crittografia, sia in ambito informatico sia non informatico, è quel processo che permette di **"codificare" informazioni sensibili o riservate** in modo che possano essere lette o modificate da chi possiede la chiave di decodifica. Probabilmente, il caso di crittografia più conosciuto dal "grande pubblico" è quello di Enigma, la macchina crittografica creata nella Germania nazista per cifrare le informazioni che lo stato maggiore dell'esercito inviava alle varie unità dislocate in Europa. Secondo molti storici, la vera svolta nel secondo conflitto mondiale si ebbe quando il laboratorio di ricerca guidato da **Alan Turing**, matematico considerato tra i fondatori dell'informatica moderna, riuscì a trovare la chiave per decodificare i messaggi dell'esercito nazista.

Al di là di questa digressione storica, il principio alla base della crittografia informatica è lo stesso utilizzato dai nazisti per proteggere le loro comunicazioni: sfruttare un set di istruzioni per codificare delle informazioni che, viaggiando attraversi canali di comunicazione "in chiaro", rischiano di essere intercettate. **La crittografia, dunque, ha uno scopo "difensivo" e serve a proteggere informazioni sensibili**: così, anche se qualcuno dovesse riuscire a "inserirsi" nel canale di comunicazione e se ne impossessasse (in ambito comunicativo viene definito *"attacco man in the middle"*), non sarebbe comunque in grado di decodificarle e utilizzarle.

4.4.2 Come funziona la crittografia

Indipendentemente che si parli di crittografia legata al mondo informatico o di crittografia in senso generale, il **funzionamento alla sua base è a grandi linee il medesimo**. In tutte le operazioni di crittografia il messaggio originale viene modificato in base ad alcune regole definite dall'algoritmo, dette chiavi di codifica e decodifica. Solamente l'utente che possiede la chiave adeguata potrà decodificare il messaggio cifrato e accedere così alle informazioni "originali".

A seconda della tipologia di chiave usata, ci si trova di fronte a due tipologie di processi crittografici differenti: **a chiave simmetrica e a chiave asimmetrica**. Ecco come funzionano.

• **CRITTOGRAFIA A CHIAVE SIMMETRICA** - Si tratta della tipologia di crittografia più semplice e veloce da applicare, ma per alcuni versi anche la meno sicura. La chiave che viene impiegata nel processo di codifica è la stessa che deve essere utilizzata anche in fase di decodifica (per questo detta simmetrica) ed è inizialmente posseduta solamente da chi "inizializza" il processo crittografico. Affinché il destinatario del messaggio sia in grado di leggerlo, però, deve ricevere la chiave da chi lo ha generato. In questo modo se un cybercriminale dovesse riuscire a intercettare il messaggio codificato e la chiave crittografica sarebbe in grado di accedere liberamente a tutte le informazioni. Sul piano della sicurezza e della protezione, insomma, lascia molto a desiderare.

• **CRITTOGRAFIA A CHIAVE ASIMMETRICA** - Questo sistema, più lento ma più sicuro rispetto al primo, utilizza una coppia di chiavi differenti tra loro (una pubblica e una privata) per codificare e decodificare il messaggio. La chiave privata viene generata dall'applicativo o dal software che utilizza questa tipologia di algoritmo ed è per questo disponibile solo sul dispositivo che ne fa uso; la chiave pubblica, come indica il nome, è invece condivisa da tutti gli utenti che partecipano alla comunicazione. In questo modo, la chiave pubblica viene utilizzata per codificare il messaggio, mentre quella privata serve per decodificarlo. Una tipologia "particolare" di crittografia a chiave asimmetrica è quella *end-to-end* utilizzata dalle piattaforme di messaggistica istantanea.

4.5 Sicurezza WhatsApp: i pericoli delle chat

La crittografia end-to-end, che WhatsApp integra ormai da alcuni anni, da sola **non può bastare per proteggerci da tutti i pericoli che corrono sulla piattaforma di messaggistica istantanea** di proprietà di Facebook. Con i suoi oltre 2 miliardi di utenti, infatti, WhatsApp rappresenta un'occasione ghiottissima per tutti i cybercriminali alla ricerca di uno strumento per avvicinare una possibile vittima. O, quanto meno, per ricavare informazioni personali che possono tornare utili, ad esempio, in un attacco di social engineering. Per questo motivo, **quando si utilizza WhatsApp si dovrebbe fare sempre molta attenzione ai messaggi e ai file che si ricevono**. Il caso Bezos, ancora una volta, è esemplare: per rubare tutti i dati personali che il fondatore di Amazon aveva

sul suo iPhone è stato sufficiente scaricare un normalissimo filmato di una manciata di secondi. E, capirete benissimo, che se c'è cascato l'uomo più ricco del mondo, può cascarci chiunque.

Ma **quali sono i pericoli che si corrono su WhatsApp** (e, più in generale, sulle piattaforme di messaggistica istantanea)? I più vari. In rapida sequenza, i cybercriminali potrebbero usare l'app per scambiare messaggi per:

- Infettare lo smartphone con malware di ogni tipo (dagli spyware ai trojan horse, passando per ransomware);
- Spiare le chat degli altri utenti (nonostante la crittografia end-to-end, infatti, ci sono alcune app che permettono di leggere le chat WhatsApp);
- Attacchi phishing;
- Operazioni di social engineering;
- Stalking;
- Ricatti a sfondo sessuale;
- Truffare e rubare denaro agli altri iscritti;
- Far girare bufale e fake news sugli argomenti più disparati.

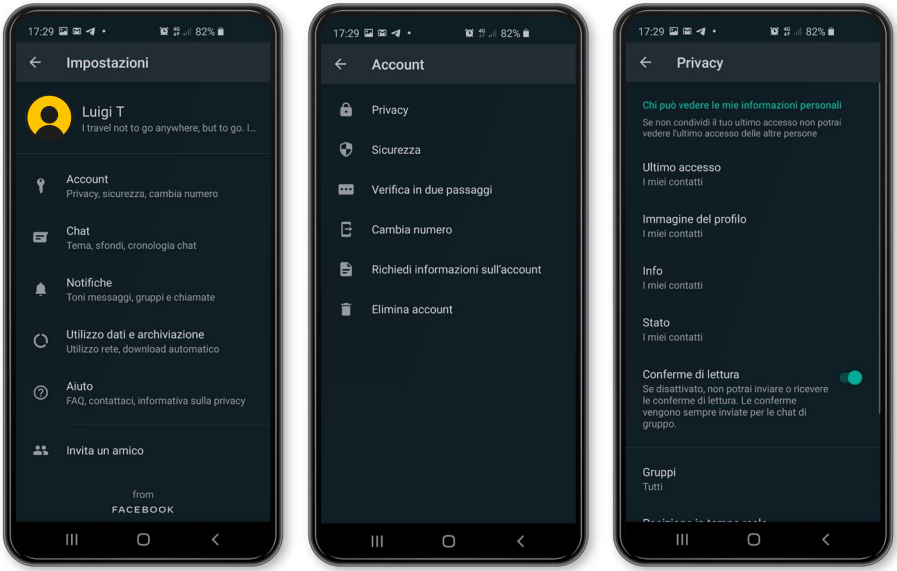
Insomma, parafrasando il titolo di un vecchio film, **nulla di nuovo sul fronte della sicurezza informatica**. Questo, però, non vuol dire che queste minacce non siano efficaci. Anzi: è vero l'esatto contrario. Le cronache dei quotidiani (non solo quelli a tema informatico, ma anche quelli "generalisti") sono piene di attacchi (o tentativi) condotti tramite la piattaforma di chat più famosa e utilizzata al mondo. Tanto che, per limitare la portata "malevola" dei messaggi, gli sviluppatori di WhatsApp sono stati costretti, ad aprile 2020, a ridurre il numero di persone

cui è possibile inoltrare contemporaneamente un messaggio etichettato come "frequente" e ricevuto in una conversazione (dai precedenti 5 contatti è stato portato a 1 solo contatto).

Fortunatamente, però, la piattaforma di Facebook mette a disposizione diversi **strumenti che consentono di proteggere il proprio account e le informazioni personali** che sono contenute al suo interno. Si tratta di operazioni piuttosto semplici e veloci, che sono però estremamente efficaci per tenere alla larga scocciatori e curiosoni.

4.5.1 Attivare l'autenticazione a due fattori

Attivando la verifica in due passaggi su WhatsApp, sarà praticamente impossibile che qualcuno riesca a "rubarci" il profilo. Questa funzione, infatti, consente all'utente di creare un codice numerico di sei cifre che dovrà essere utilizzato ogni volta che si avvierà la procedura di autenticazione su un nuovo dispositivo. Se si cambia smartphone e si sta spostando WhatsApp (con le sue chat) su un nuovo dispositivo, sarà sufficiente inserire il codice creato. Se qualcun altro, invece, vorrà provare a impossessarsene, rimarrà fortemente deluso: senza codice, infatti, non sarà possibile accedere al profilo desiderato. Per farlo bisogna accedere alle **Impostazioni**, premere su **Account** e poi su **Verifica in due passaggi**. Si aprirà una nuova schermata in cui inserire il codice per l'autenticazione a due fattori.



4.5.2 Controllare le impostazioni della privacy

Per evitare che informazioni private – come la foto profilo, ad esempio – possano finire nella disponibilità di qualche malintenzionato, è bene sempre controllare le impostazioni della privacy del proprio profilo. In questo modo, ad esempio, sarà possibile indicare chi può vedere l'orario e la data di ultimo accesso; chi l'immagine del profilo; chi le info personali e chi lo Stato. Per modificare le preferenze basterà accedere alle **Impostazioni** dell'app, scegliere **Account** e poi **Privacy**.

4.5.3. Privacy dei gruppi

Spesso e volentieri, i pericoli maggiori (quanto meno sul fronte delle catene di Sant'Antonio e sulle fake news) arrivano proprio dai gruppi di WhatsApp. Fortunatamente, l'app consente di impostare la privacy dei gruppi e decidere così chi può aggiungerci e chi no alle conversazioni collettive. Si dovrà aprire le **Impostazioni** dell'app, scegliere **Account** e poi **Privacy**. Scorrere la schermata sino a trovare la voce **Gruppi** e pigiarci su. Qui ci saranno tre opzioni: Tutti; I miei contatti; I miei contatti eccetto...: sarà sufficiente scegliere quella che si ritiene più idonea alle proprie necessità e il gioco è fatto.

4.5.4. Attivare lo sblocco con impronta digitale

Lo sblocco con impronta digitale è una delle ultime funzioni di sicurezza che WhatsApp ha inserito all'interno della sua piattaforma. Attivandola, sarà possibile accedere all'applicazione solamente dopo aver effettuato la scansione dell'impronta digitale che solitamente utilizziamo per sbloccare il telefono. Su iPhone, inoltre, è disponibile anche lo sblocco di WhatsApp con la scansione del viso (il FaceID, per intendersi). Per attivare la funzione di sicurezza sarà necessario aprire le **Impostazioni** di WhatsApp, pigiare su **Account**, poi su **Privacy** e scorrere l'elenco delle opzioni. L'ultima sarà **Blocco con impronta digitale**: per attivarla si dovrà pigiare sulla voce di menu e spostare il cursore da destra verso sinistra. Una volta attivato si potrà anche impostare il "timer" per attivare blocco automatico dell'app, in modo che nessuno possa leggere le chat anche se lasciamo il telefonino in giro incustodito.

4.6 Come gestire la privacy sui social network

WhatsApp, ovviamente, non è l'unica piattaforma che un cybertruffatore potrebbe sfruttare per spiarci o carpire informazioni sul nostro conto. Tutte le reti social, per la loro stessa natura, si prestano infatti a **essere utilizzate come mezzo o strumento per raccogliere dati su abitudini o per "approcciare" un gran numero di persone**. Proprio per questi motivi, dunque, sarà necessario porre particolare attenzione a come si gestisce il proprio profilo su Facebook, Twitter o Instagram e, in particolare, a quelle che sono le impostazioni per la privacy e la protezione dei dati personali.

Anche se le varie piattaforme social non hanno molte caratteristiche che le accomunino (Facebook è un po' "l'emblema" dell'intero settore; Twitter è più identificabile come un sito di microblogging; Instagram è prettamente un social per immagini), hanno però **policy di privacy**

molto simili tra loro. Questo vuol dire che l'utente potrà mettere in atto le stesse "pratiche" su tutti i profili, risparmiando tempo e avendo la certezza che i propri dati saranno al sicuro.

Prima di tutto, si deve **verificare il livello di privacy "generale" del proprio profilo**. Il consiglio, indipendentemente dalla piattaforma che si utilizza, è quello di renderlo privato. In questo modo sarà possibile farsi "seguire" solo da contatti che si conoscono e si limiterà di molto la visibilità di post, immagini e video che si condivideranno sulla piattaforma.

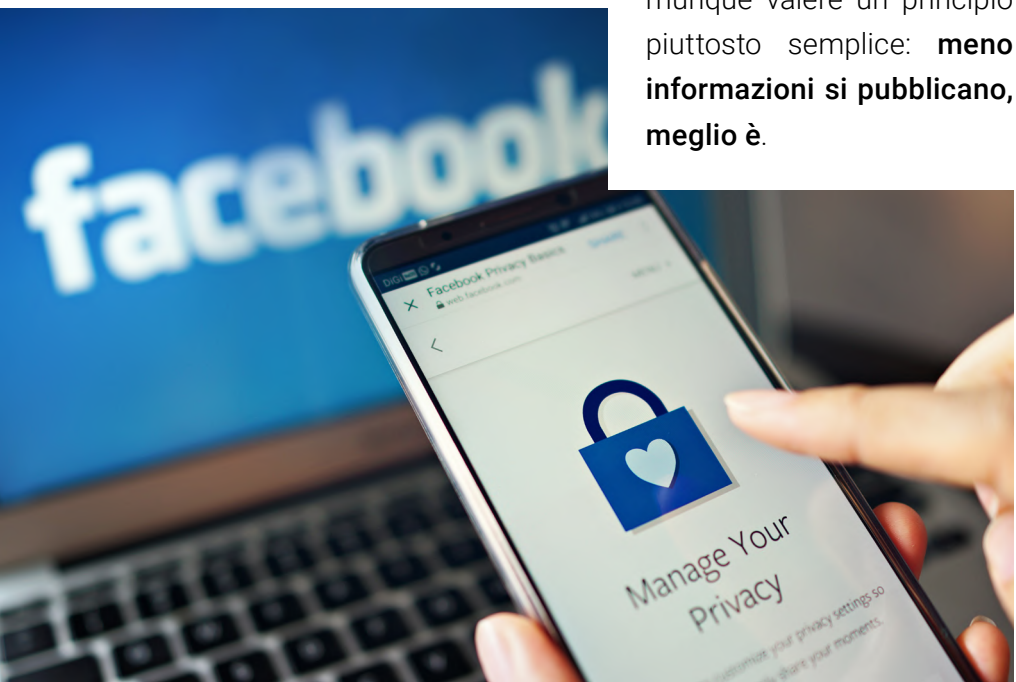
Se non si vogliono adottare soluzioni così "draconiane", allora si sarà costretti a prendere una decisione in tal senso ogni qualvolta che si pubblica un contenuto. Prima di cliccare sul tasto "Pubblica" o "Invia", infatti, si dovrà valutare per bene l'impatto che questo potrà avere, **le informazioni personali che potrebbero essere contenute al suo interno** (ad esempio, la località in cui ci troviamo in quel preciso istante), se si rivelano dati e dettagli che, invece, dovrebbero rimanere privati. Insomma, prima di postare qualcosa di nuovo sul proprio profilo pubblico ci si dovrà pensare su almeno due volte. Da valutare, in questo caso, la possibilità di pubblicare dei contenuti solo per una "parte" dei nostri amici o follower (come le liste Facebook o gli "Amici più stretti" di Instagram). Questo consentirà di **ridurre l'esposizione di determinati contenuti** e si avrà la certezza che solo una ristretta cerchia possa visualizzarli.

Altro punto da valutare attentamente riguarda **le informazioni che si inseriscono all'interno del profilo stesso**. Le varie piattaforme potrebbero chiederci dove viviamo e dove lavoriamo, qual è la data di nascita e altri dettagli strettamente personali (come il numero di telefono, ad esempio). Nel caso queste informazioni fossero di pubblico dominio,

un cybercriminale potrebbe sfruttarle per creare un profilo "clone", oppure per architettare delle truffe ai danni di altri utenti (dai dati personali, ad esempio, è possibile risalire piuttosto facilmente al codice fiscale di una persona).

Altrettanto importante sarà agire sulle **impostazioni di tracciamento**. Anche se non ce ne rendiamo conto, tramite l'app installata sullo smartphone i social network possono accedere alla nostra posizione grazie al GPS del dispositivo. Ciò vuol dire che potranno sempre sapere dove sappiamo e, nel caso facessimo poca attenzione, potremmo anche rendere pubblici i nostri spostamenti. Un dettaglio tutt'altro che trascurabile: qualcuno potrebbe approfittare di queste informazioni per fare una "visita indesiderata" al nostro appartamento mentre noi siamo fuori per un viaggio di piacere o di lavoro.

Al di là di tutti i casi particolari di cui si può discutere sui social deve comunque valere un principio piuttosto semplice: **meno informazioni si pubblicano, meglio è**.

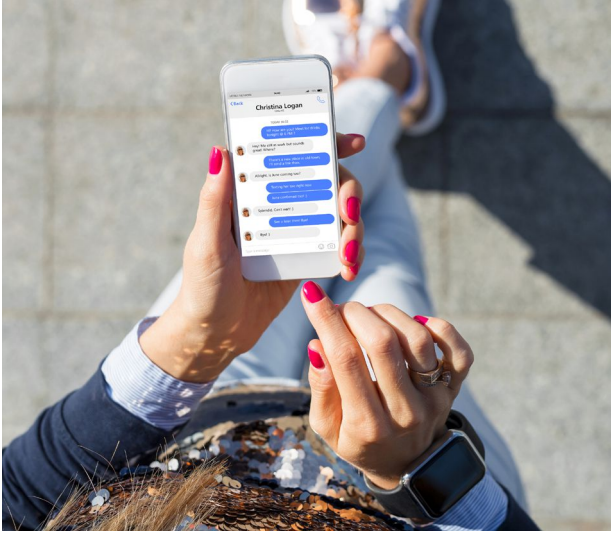


47 Come proteggere gli account online

La privacy, però, è solo uno degli aspetti che bisogna "curare" del proprio profilo. Capita sempre più spesso, infatti, che i criminali informatici non si "accontentino" solamente di alcune informazioni, ma puntano al "colpo grosso". Ossia, a **rubare profili e account personali**, per poterli poi utilizzare per i loro scopi malevoli. Con un indirizzo di posta elettronica,

ad esempio, possono inviare messaggi spam e phishing ai contatti salvati in rubrica, in modo da essere più credibili e far cadere nella trappola un numero maggiore di utenti. I profili social, invece, sono l'ideale per campagne di ingegneria sociale "mirate": ciò consente di risparmiare moltissimo tempo nell'individuazione e nello studio delle vittime.

Ovviamente, i cracker non tenteranno di rubare gli account singolarmente. L'operazione richiederebbe sin troppo tempo e porterebbe a ben



pochi risultati. Piuttosto, preferiscono cercare falle e vulnerabilità nei server dei gestori di posta elettronica o delle piattaforme social e di messaggistica per **riuscire a rubare in un colpo solo milioni e milioni di credenziali di accesso ai vari servizi**. In gergo tecnico, quando questi furti hanno successo si parla di ***data breach*** e, in più di qualche occasione, gli utenti vengono a conoscenza dell'avvenuto furto solamente quando è troppo tardi (poche ore dopo, qualche giorno dopo o, nei casi peggiori, anche dopo settimane).

Scorrendo l'elenco dei **peggiori *data breach* della storia**[5] si scopre che nessuno è al riparo da questa eventualità. Yahoo, tanto per fare un nome, è stata ripetutamente vittima di attacchi ai database, che hanno consentito agli hacker di impossessarsi di oltre 3 miliardi di credenziali di account di posta elettronica. Un altro "cliente celebre" è **Facebook**: un cracker, girovagando online, è riuscito a impossessarsi dei dati di accesso di diverse decine di milioni di iscritti alla piattaforma, ricavati all'interno di un database contenente informazioni di 540 milioni di utenti. Insomma, è necessario adottare misure e precauzioni che, anche in caso di furto di credenziali "di alto livello", metta al riparo sia le informazioni contenute all'interno dell'account, sia l'account stesso.

5. https://www.purdueglobal.edu/blog/information-technology/worst-data-breaches-infographic/

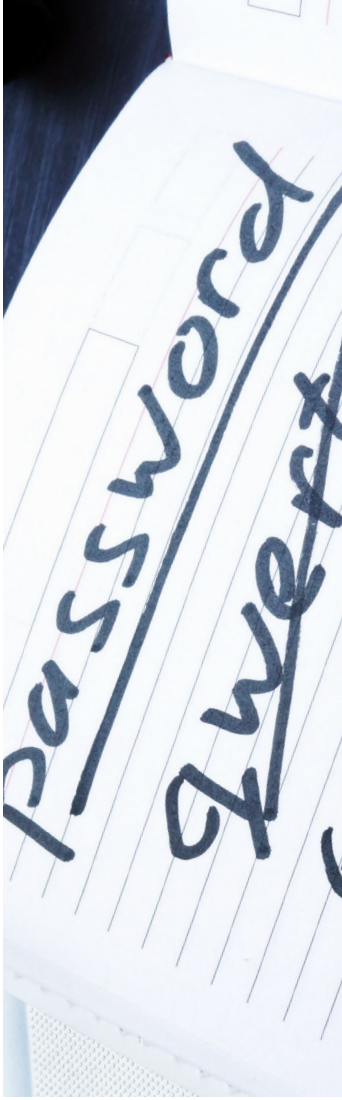
4.7.1 Come verificare se la propria e-mail è stata rubata

Prima di passare ai consigli per proteggere gli account online, però, vogliamo aiutarvi a capire se uno dei vostri indirizzi di posta elettronica o account social sia stato violato. Per farlo sarà sufficiente collegarsi al sito web **https://haveibeenpwned.com** e inserire l'indirizzo e-mail nel campo al centro della schermata. Nel giro di qualche secondo, il portale creato dall'esperto di sicurezza informatica Troy Hunt vi dirà se l'e-mail è presente in uno dei tanti database che sono stati trafugati e disponibili per il download online.

4.7.2 Creare una password sicura

Il primo passo da compiere per proteggere al meglio i propri profili online passa dalla creazione di una password che sia quanto più possibile difficile da "indovinare". Questo, ovviamente, non mette al riparo da eventuali "furti massivi" operati ai danni del fornitore del servizio, ma eviterà che qualche cracker in erba sia in grado di indovinare la nostra chiave d'accesso tirando a indovinare.

Sono diverse le tecniche che si possono utilizzare per creare una password sicura. La prima è quella di **realizzare una chiave d'accesso di almeno 10 caratteri, composta da caratteri alfanumerici e segni di punteggiatura**, in modo da aumentarne la complessità. Una tecnica che sta acquistando sempre maggiore forza negli ultimi tempi è quella di sostituire le password con **passphrase**: anziché creare una stringa casuale, si creano stringhe composte da 2 o 3 parole di senso compiuto. Questo permetterà di creare chiavi di accesso più lunghe, ancora più complesse da indovinare rispetto a quelle casuali ma, allo stesso tempo, più facili da ricordare.



4.7.3

Attivare l'autenticazione a due passaggi

Per proteggere gli account da possibili data breach, invece, è più che consigliabile attivare l'autenticazione a due passaggi ogni volta che sia possibile. Questa tecnica prevede che per entrare all'interno dei propri profili web sia **necessario inserire anche un secondo codice oltre alla password**. Il codice viene generato casualmente da un'app installata su uno smartphone sincronizzato con la casella di posta elettronica o il profilo social oppure dai server del servizio e ricevuto via SMS.

4.7.4 Usare i password manager

Buona norma vorrebbe che **per ogni account creato si dovrebbe utilizzare una password differente**. In questo modo, anche se una chiave d'accesso dovesse venire scoperta, gli altri profili sarebbero comunque al sicuro. Un'operazione piuttosto complessa, visto che si sarebbe costretti a ricordare a memoria decine e decine di credenziali differenti per altrettanti profili. Una soluzione è offerta dai password manager, programmi ideati per archiviare in maniera sicura le credenziali di tutti i profili e "tirarle fuori" nel momento del bisogno. Ossia, quando si sta tentando di effettuare il login a uno dei propri account. In questo modo si verrà "liberati" dal carico mnemonico richiesto da tale operazione e potremmo finalmente decidere di cambiare password in tutta sicurezza.

4.8 Acquisti online, come farli in sicurezza

Impossibile parlare di sicurezza informatica online senza dedicare un paragrafo agli acquisti online. Questa operazione, per quanto possa sembrare semplice, nasconde una lunga serie di pericoli che **mettono a rischio tanto i dati quanto le nostre finanze personali**. Basta un errore, anche il più banale, per diventare l'ennesima vittima di un cybertruffatore

o essere in qualche modo complice (involontario) di una truffa online. Quando si fanno acquisti online, dunque, sarà necessario mettere in atto alcune iniziative che consentano di proteggere sia le nostre informazioni, sia i soldi presenti sul conto corrente o la carta di credito.

4.8.1. Come riconoscere un e-commerce affidabile

Sull'affidabilità e sicurezza di portali di commercio elettronico come Amazon, Yoox, Zalando ed ePrice (per non citare quelli legati alle catene della grande distribuzione) nessuno può nutrire dei dubbi. Anche se in alcuni casi il comportamento di venditori terzi potrebbe scalfire la fiducia dell'acquirente, nel 99,9% dei casi la transazione andrà a buon fine, con piena soddisfazione di chi compra e di chi vende.

Potrebbe anche accadere, però, di trovare un prodotto a un prezzo più basso su un sito di e-commerce "minore" o di nicchia, poco conosciuto

e poco visitato. Cosa fare in casi come questi? **Come riconoscere un sito affidabile e distinguerlo da uno poco affidabile sul quale potremmo essere truffati?** Semplice: grazie al web. In Rete, infatti, sono disponibile diverse piattaforme che raccolgono recensioni non solo sui singoli prodotti, ma anche su siti e piattaforme di varia natura. Il più conosciuto e utilizzato in questo ambito è, senza dubbio, **TrustPilot**: basterà inserire il nome nel campo di ricerca e attendere qualche istante per visualizzare le valutazioni lasciate da utenti che prima di noi hanno fatto acquisti sul sito. E nel caso in cui non dovesse esserci alcuna recensione… beh, la risposta già la conoscete: girate al largo.

Un altro metodo per verificare l'affidabilità di un sito passa dalla **sezione "contatti" del portale**. Cercatela, verificate quali siano le informazioni inserite al suo interno e, se è disponibile un numero di telefono, provate a chiamarlo. In alternativa, inviate un messaggio all'indirizzo di posta elettronica e valutate attentamente la risposta che riceverete: potrebbe magari trattarsi di un messaggio creato da un bot in maniera "artificiale".

4.8.2 Pagare online, come evitare di farsi rubare i soldi

Altra cosa cui fare attenzione quando si fanno acquisti online è, ovviamente, il processo di pagamento. Se qualcosa non dovesse andare per il verso giusto, infatti, non si rischierebbe solo di perdere il denaro della transazione, ma si potrebbe anche mettere a rischio lo stesso metodo

di pagamento. Detto in parole più semplici, **si potrebbe anche rischiare che qualcuno cloni la carta di credito** e la utilizzi per fare acquisti sconsiderati online o nella vita reale.

Evitare che ciò accada, però, è più semplice di quanto si possa immaginare. Prima di tutto, un buon modo per non perdere denaro è quello di **utilizzare una carta prepagata ricaricabile al posto di una carta di credito**. Così, anche se qualcuno dovesse riuscire a clonarla, i cybertruffatori non potrebbero spendere più denaro di quello che ci abbiamo caricato su. Questa soluzione, per quanto sicura, potrebbe non essere adeguata nel caso in cui si facciano acquisti online piuttosto frequentemente.

Altri accorgimenti sono invece di natura "tecnica" e "tecnologica". Prima di tutto, si deve verificare che il portale di e-commerce **utilizzi il protocollo di crittografia HTTPS**, in modo che le informazioni riguardanti la transazione vengano codificate prima di essere spedite ai server che gestiscono l'intero processo di pagamento. Altrettanto importante è affidarsi a sistemi di pagamento affidabili e riconosciuti come PayPal, Nexi o simili: in questo caso si potrà star certi che la transazione viaggerà attraverso server sicuri e non si metteranno a rischio le proprie finanze.

4.8.3. Cosa fare in caso di truffa online

Siete **vittima di una truffa online e non sapete cosa fare?** Molto dipende da quello che vi è accaduto. Se un cybertruffatore è riuscito a entrare in possesso dei dati della vostra carta di credito o del vostro conto corrente dovrete, prima di tutto, chiamare il numero verde della banca e **bloccare i metodi di pagamento**. Ciò vi permetterà di fermare "l'emorragia" di denaro immediatamente e limitare i danni subiti. Successivamente dovrete recarvi presso un Commissariato di Polizia o Stazione dei Carabinieri e sporgere denuncia. Come ultimo passaggio non vi resta che recarvi presso la filiale della banca e fare richiesta per il rimborso della cifra sottratta.

Se, invece, **vi è stata rubata la casella di posta elettronica o un profilo social** dovrete provare a recuperarlo non appena lo scoprirete. Magari siete ancora in tempo e il cybercriminale non è ancora riuscito a fare "danni". Se l'operazione non dovesse dare i risultati sperati, provate a mettervi in contatto con l'assistenza del fornitore del servizio e verificare se sia possibile rientrare in possesso del "maltolto". Anche in questo caso, inoltre, sarà necessaria una denuncia alle autorità: se il ladro dovesse aver commesso un reato con la vostra "identità digitale", sareste scagionati da qualunque accusa.

5. Sicurezza informatica, cosa aspettarsi

Anche nel mondo della cybersecurity, come in moltissimi altri settori, la regola aurea è sempre la stessa: ***follow the money***. Per comprendere quello che sarà il futuro della sicurezza informatica e come si svilupperà in futuro si deve seguire il flusso di denaro generato dalle varie campagne di attacchi hacker di "alto livello". Secondo l'ultimo "Global Risk Report" del World Economic Forum[6], il cybercrime è già nella top 5 dei maggiori rischi a livello globale e, nel 2020, i danni provocati da attacchi cibernetici raggiungeranno l'incredibile cifra di **6 mila miliardi di dollari**. Se la community dei cracker e dei black-hat hacker fosse una nazione, avrebbe il terzo PIL globale, giusto alle spalle di Stati Uniti e Cina, ma davanti al Giappone.

E, stando alle previsioni dello stesso Forum economico mondiale, la situazione non è di certo destinata a migliorare. Anzi: secondo gli esperti

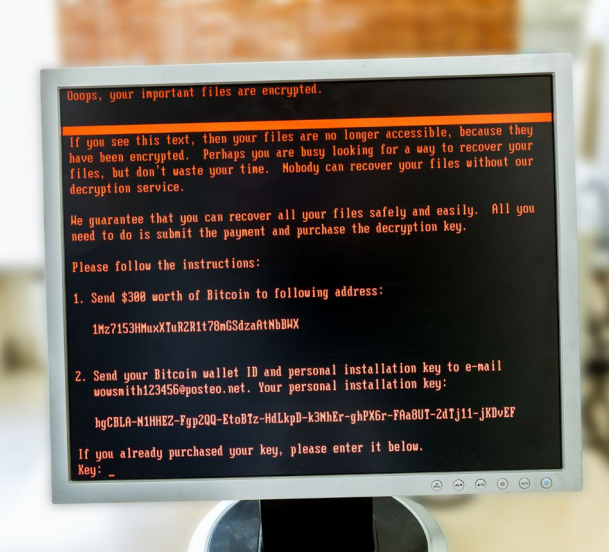
6. https://reports.weforum.org/global-risks-report-2020/wild-wide-web/

interpellati dal WEF **si corre il rischio sempre più serio che gli effetti di un attacco informatico abbiano pesanti ricadute anche nel mondo "fisico"**. Nel corso degli anni, si legge nel report, si è venuto a creare una sorta di mondo "ciber-fisico", nel quale ciò che accade nel mondo virtuale ha un impatto significativo anche nel mondo reale.

Per questo motivo è necessario porre un'attenzione sempre più elevata nei confronti della sicurezza informatica e delle sue minacce. Un attacco informatico, ad esempio potrebbe mettere fuori uso la rete elettrica in una città, provincia o regione (cosa accaduta in Ucraina, ad esempio) oppure bloccare il funzionamento di un servizio pubblico (come accaduto nel Regno Unito a causa di un attacco ransomware). Insomma, come abbiamo già detto in apertura di questo e-book, tentare di far finta di nulla è del tutto inutile: **se non ci interessiamo della sicurezza informatica sarà lei (in qualche modo) a interessarsi di noi**.

5.1 L'evoluzione della sicurezza informatica

Rispetto a quelle prime righe di codice che, sul finire degli Anni '70, "emulavano" il comportamento dei worms, il mondo delle minacce informatiche ha fatto enormi passi in avanti. Spaventosi, sotto molteplici punti di vista. Oggi **i cyberattacchi possono prendere le forme più disparate**: dalle "semplici" infezioni virali, che possono compromettere il funzionamento di un singolo dispositivo, ad attacchi distruttivi di grande magnitudo, capaci di provocare danni a infrastrutture e servizi



sensibili. Di questa seconda categoria fanno parte, ad esempio, gli attacchi **ransomware**, che hanno dimostrato il loro poteri distruttivo a cavallo tra il 2017 e il 2018, e gli attacchi **DDoS**, che tornano a manifestarsi a cadenza quasi regolare.

A peggiorare ulteriormente la situazione troviamo la **diffusione sempre più ampia delle cosiddette *Malware as a service***, piattaforme che consentono di "assemblare" malware pezzo dopo pezzo anche a chi è totalmente digiuno di programmazione e tecniche di sicurezza informatica. Piattaforme di questo genere possono essere acquistate nel dark web per poche centinaia di euro e possono essere attivate in qualunque momento e in qualunque parte del mondo. Ben presto, dunque, potremmo ritrovarci sommersi da cracker in erba che sperano di racimolare qualche soldo attaccando computer e altri dispositivi informatici di ignari utenti.

Per non parlare, poi, dei **dispositivi IoT**, indicati da più parti come una delle peggiori minacce per la sicurezza informatica nel medio-lungo periodo. Di nuovi modelli di dispositivi smart ne compaiono ormai a migliaia ogni anno, tanto che il loro numero aumenta in maniera esponenziale. **Si stima che entro il 2030 ci saranno 50 miliardi di dispositivi IoT connessi a Internet** che potrebbero essere utilizzati per "ingrassare" le fila di qualche botnet. Come dimostrano alcuni attacchi avvenuti negli anni passati, nella Rete ci sono letteralmente centinaia di migliaia

di device interconnessi che possono essere hackerati nel giro di pochi secondi, anche dal cybercriminale meno esperto. Un vero e proprio esercito di "mercenari involontari" pronto a rivoltarsi contro i loro stessi creatori o possessori.

Con il passare degli anni, dunque, i cybercriminali hanno via via ampliato le tecniche e gli strumenti a loro disposizione per condurre attacchi informatici. Oggi, **dopo 40 anni circa di evoluzione**, possono contare su di un vero e proprio arsenale utile a colpire obiettivi di qualunque genere – dal PC o smartphone del singolo utente al server di una multinazionale – e perseguire gli scopi più vari. E, proprio come accade con l'evoluzione biologica, l'opera di "raffinazione" di queste armi non è affatto terminata. Anzi: sul palcoscenico della sicurezza informatica stanno per affacciarsi nuovi protagonisti con un potenziale distruttivo superiore a quello di qualunque altro strumento visto sino a oggi.

5.2 Sicurezza informatica e intelligenza artificiale, rapporto complesso

La vera protagonista del settore per gli anni a venire sarà l'**intelligenza artificiale**. Già da qualche tempo a questa parte algoritmi di intelligenza artificiale e machine learning vengono utilizzati da un lato e dall'altro della "barricata". Ossia, sono utilizzati sia per **migliorare le misure di sicurezza dei sistemi informatici** (specialmente di quelli deputati alla difesa "aziendale"), sia per scovare nuovi bug e vulnerabilità e trovare

un modo per sfruttarle in attacchi sempre più devastanti. E nei prossimi anni assisteremo a un vero e proprio boom del settore: secondo le previsioni di Marketsandmarkets, **il mercato dell'intelligenza artificiale applicata alla sicurezza informatica è destinato a raggiungere il valore di 38,2 miliardi di dollari**, con tassi di crescita del 23% annui.

Ma **a cosa serve l'intelligenza artificiale nell'universo della sicurezza informatica?** I possibili utilizzi sono molteplici. Ad esempio, sarà possibile sfruttare algoritmi per migliorare le performance dei motori di analisi euristica (quelli degli antivirus, per intendersi) e scoprire nuove famiglie e nuove tipologie di malware molto più in fretta di quanto accada ora. O, ancora, si potranno impiegare algoritmi di machine learning ("apprendimento automatico" in italiano) per analizzare il comportamento online – o all'interno di una rete aziendale – degli utenti e scoprire per tempo se un account sia stato compromesso e rubato ed è utilizzato per trafugare dati sensibili. Da non sottovalutare, poi, il ruolo che intelligenza artificiale e machine learning possono giocare nel campo della prevenzione delle truffe online e del furto di identità.

Il **grande vantaggio degli algoritmi di intelligenza artificiale** sta nella loro capacità di analizzare una grande mole di dati in pochi istanti e reagire quasi istantaneamente a comportamenti che deviano dagli "standard". Il lavoro che un team di esperti di sicurezza potrebbe compiere in alcuni giorni, o addirittura settimane, può essere portato a termine da una famiglia di algoritmi nel giro di una manciata di secondi. Questo consente, ovviamente, di risparmiare moltissimo tempo, dando la possibilità di bloccare per tempo possibili minacce e tentativi di attacco. Tanto per fare un esempio, algoritmi di intelligenza artificiale vengono

utilizzati per studiare l'andamento dei flussi di traffico verso un sito o un server e individuare se è in corso un attacco DDoS. Se così dovesse essere, i controlli automatizzati faranno letteralmente scattare il campanello d'allarme, permettendo a operatori in carne e ossa di intervenire e "disinnescare" l'attacco.

Come accennato, però, l'intelligenza artificiale si sta "facendo spazio" anche dall'altro lato della barricata. L'enorme capacità di analisi e calcolo,

infatti, **viene utilizzata anche da cracker e gruppi di cybercriminali interessati a scoprire nuove falle e nuove strategie di attacco**. E se dal "lato opposto" gli algoritmi di AI e machine learning vengono utilizzati principalmente per prevenire attacchi studiando il comportamento di malware già conosciuti (o le abitudini di uno o più utenti), dal lato dei cybercriminali la potenza dell'intelligenza artificiale viene utilizzata per "ingegnerizzare" tecniche di attacco già esistenti e renderle ancora più efficaci.

Come sottolineato in un report dell'Europol[7], l'intelligenza artificiale è uno dei fattori che, nel prossimo futuro, potrebbero rendere l'intero mondo dell'elettronica e dell'informatica meno sicuro. L'accesso a tool potenziati dall'intelligenza artificiale **potrebbe permettere anche a cybercriminali con limitate conoscenze tecniche di compiere attacchi di alto livello**. Potrebbe accadere, ad esempio, che un black-hat hacker utilizzi algoritmi di machine learning per condurre attacchi phishing, malware o di social engineering con il minimo sforzo ma grandissima efficacia. Qualche esempio? Il machine learning, ad esempio, potrebbe aiutare

7. https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf

a diffondere con maggior successo nuovi malware, "creandone" di nuovi che siano capaci di aggirare le misure di sicurezza di una rete privata, di un server o un singolo utente. Oppure essere utilizzata per attacchi di tipo "deepfake", che consentono di realizzare filmati contraffatti e impossibili da riconoscere a occhio nudo. O, ancora, utilizzare algoritmo di apprendimento automatico applicati al linguaggio, in modo da realizzare messaggi sempre più "naturali" e convincenti.

Ma, cosa forse anche più preoccupante, l'intelligenza artificiale può essere la **migliore alleata nel furto di credenziali e identità online**. Algoritmi di intelligenza artificiale e di machine learning "ben addestrati" possono generare milioni di possibili chiavi d'accesso nel giro di poche decine di secondi. Questo vuol dire che mettere a segno i cosiddetti "attacchi a dizionario" è più semplice di quanto lo sia mai stato in passato. Anche la più complessa delle password o delle passphrase – creata seguendo i migliori consigli del settore – potrà indovinata nel giro di qualche minuto, o qualche ora al massimo.

5.3 Sicurezza informatica: cosa aspettarsi

Per concludere questo ultimo capitolo riprendiamo il concetto che abbiamo utilizzato per introdurlo: ***follow the money***. Anche se ci sono ancora oggi moltissimi *ethical hacker*, la gran parte dei cracker e delle organizzazioni cybercriminali si muovono con un unico obiettivo: **quello di fare soldi**. E, senza ombra di dubbio, la più grande fonte di guadagno

per i cybercriminali sta nei dati (degli utenti, delle aziende e delle organizzazioni organizzative) che riescono a rubare e nella loro capacità di "monetizzarli". Il *follow the money*, dunque, può tradursi anche in ***follow the data (breach)***: seguendo l'andamento dei maggiori furti di dati – principalmente credenziali di accesso a servizi di posta

elettronica, istituti bancari e social network, ma non solo – sarà possibile scoprire, o quanto meno provare a ipotizzare, quali saranno le principali minacce informatiche dal quale guardarsi nei prossimi anni. È così possibile assumere, ad esempio, che **i "virus" puri siano destinati a scomparire**. L'interesse a infettare un sistema informatico semplicemente per distruggere qualche file o costringere l'utente a reinstallare il sistema operativo andrà probabilmente scemando, lasciando spazio a minacce ben più pericolose. Dunque, le famiglie malware che dovrebbero conoscere un maggior incremento sono quelle collegate

al furto dati, al furto dell'identità online e che consentono di "monetizzare" più in fretta.

Occuperanno un posto in un'ipotetica "prima fila" i **trojan horse**, gli **spyware** e tutti quei malware che consentono ai criminali informatici di introdursi in un sistema informatico e "sifonare" le informazioni che cercavano. Per un cracker sarà fondamentale utilizzare degli strumenti che gli consentano di trovare falle nei software o nei sistemi operativi e sfruttarle a proprio favore per introdursi all'interno di un server, di un PC o uno smartphone. In questo contesto, come abbiamo visto, l'intelligenza artificiale giocherà sicuramente un ruolo di primaria importanza: gli algoritmi di machine learning potranno aiutare a trovare nuove strategie per evitare antivirus, antimalware e altri sistemi di sicurezza oppure per far "evolvere" in maniera automatica (ossia, senza intervento manuale del creatore) il malware stesso.

Altra famiglia di malware che potrebbe "tornare in auge" è quella dei **ransomware**. E non solo per chiedere riscatti a utenti poco esperti. È stato notato, infatti, che in caso di attacchi rivolti alle aziende o personaggi esposti (politici, industriali o altro), che l'infezione ransomware non è fatta a scopo estorsivo, ma con il chiaro intento di rendere i file archiviati nel disco non più consultabili o utilizzabili. Per questo motivo si ritiene che, nel futuro prossimo, i ransomware potrebbero essere impiegati in attacchi che in qualche modo "esulano" dal loro scopo originario: non monetizzare immediatamente l'infezione, ma provocare un danno a medio-lungo termine nei confronti della persona attaccata.

E dove non arriveranno i malware, arriverà l'uomo. Nei casi più delicati, infatti, il fattore umano sarà ancora fondamentale per la buona riuscita

dell'attacco. In particolare, i cracker dovranno agire direttamente in quelli che potremmo definire che "attacchi mirati", rivolti contro un bersaglio preciso e identificato. In occasioni come queste, i cybercriminali dovranno utilizzare raffinate tecniche di social engineering combinati con precisi attacchi phishing, che consentano di conquistare la fiducia dell'obiettivo e successivamente attaccarlo, senza che però se ne renda conto. Il **caso di Jeff Bezos**, di cui abbiamo già parlato nelle pagine precedenti, può aiutarci a capire come funzionano e come funzioneranno questa tipologia di attacchi: la persona da colpire viene prima studiata, poi approcciata (utilizzando magari un falso profilo, impersonando una persona che si conosce) e solamente alla fine, magari dopo mesi e mesi, parte l'attacco vero e proprio.

Comunque, al di là della tecnica che gli hacker vorranno utilizzare (dagli spyware al phishing, passando per gli attacchi distruttivi con ransomware), in futuro **dovremmo porre sempre maggiore attenzione a come proteggiamo i nostri dati, con chi li condividiamo** (non solo persone, ma anche società) e come li conserviamo. I cybercriminali, qualunque sia il loro reale obiettivo, tenteranno con sempre maggior forza di impossessarsene e ottenerne il profitto più alto possibile.

GLOSSARIO

ADWARE
A differenza di moltissime altre famiglie di malware, quella degli adware è probabilmente tra le meno pericolose. Si tratta di programmi malevoli che infettano il PC o lo smartphone per mostrare video pubblicitari e banner. Lo scopo, in questo caso, non è quello di rubare dati o distruggerli, ma semplicemente di guadagnare sulla visualizzazione di pubblicità da parte degli utenti.

ANTIMALWARE
Come gli antivirus, anche gli antimalware si pongono l'obiettivo di proteggere computer e smartphone da infezioni di software malevolo di ogni genere. Lo "scudo" offerto dagli antimalware è più mirato e si concentra su famiglie malware magari meno conosciute ma, proprio per questo, più difficili da scovare.

ANTIVIRUS
Con il nome di antivirus vengono indicati tutti quei software pensati e sviluppati per proteggere PC e smartphone da tentativi di infezione e intrusione. Inizialmente questi programmi agivano esclusivamente (o quasi) contro virus; oggi, invece, offrono una protezione molto più ampia, rilevando, bloccando ed eliminando (o mettendo in quarantena) in tempo reale le potenziali minacce. Per riuscire in questa "impresa", gli antivirus utilizzano varie tecniche: le più efficaci sono quella euristica e quella "signature based".

ATTACCO DDOS
Acronimo di "Distributed Denial of Service" ("Interruzione distribuita del servizio" in italiano), l'attacco DDoS è tra i più temuti dei big della Rete. Si tratta di una minaccia di "alto livello", ma che fa sentire i suoi effetti anche agli utenti finali. Gli attacchi di questo genere sono solitamente rivolti a CDN (acronimo di Content delivery network, rete di distribuzione dei contenuti) o datacenter e mirano a comprometterne il funzionamento. I cybercriminali "inondano" di traffico dati questi nodi di rete, sino a quando non riescono più a sopportarne il flusso e smettono di funzionare. In gergo tecnico si dice che il nodo è saturo e tutti i contenuti "presenti" a quell'indirizzo non sono più raggiungibili. Solitamente, questa tipologia di attacco viene utilizzata per "mettere offline" siti e portali web, anche di grandi dimensioni.

ATTACCO MAN IN THE MIDDLE
Si tratta di una delle tecniche di cyberspionaggio più utilizzate. Come dice il nome, l'attacco consiste nel "mettersi nel mezzo" di una comunicazione tra due utenti (o due nodi della rete), così da intercettarne tutte le comunicazioni e il traffico.

BLACK-HAT HACKER
Detto anche cracker, è un esperto informatico che sfrutta le proprie conoscenze nel campo della programmazione e sicurezza personale per ricavarne un vantaggio personale. Ad esempio, può sfruttare una vulnerabilità presente in un software per spiare utenti o controllare da remoto i loro dispositivi. O, ancora, può vendere queste informazioni al miglior offerente, ricavandone somme ingenti.

BOTNET
Letteralmente "rete di bot", si tratta di un insieme di dispositivi informatici infetti e controllati a distanza da un hacker. Le botnet sono solitamente composte da centinaia di migliaia – se non milioni – di device di ogni genere, definiti in gergo "device zombie". Una volta infetti sono "assoggettati" al volere del cybercriminale che controlla il malware e ne eseguono tutti i comandi. Sono così utilizzati per creare un flusso dati "artificiale" utile per saturare la banda dati di un nodo e realizzare un perfetto attacco DDoS.

BUG BOUNTY PROGRAM
Promossi da software house e organizzazioni varie, i programmi "Bug bounty" sono rivolti a white-hat hacker ed esperti di programmazione informatica. Tramite questi programmi, infatti, le case sviluppatrici ricompensano (bounty, in inglese, vuol dire "premio") chi trova falle nel codice sorgente di software e applicazioni e non li sfrutta a proprio vantaggio. In questo modo, le software house possono risolvere il problema prima che diventi di dominio pubblico, evitando che possa causare la diffusione di malware o compromettere il funzionamento dei programmi.

BUG
Letteralmente "baco", "piccolo insetto", indica un errore di programmazione in un software (vedi anche vulnerabilità) che consente a un cybercriminale di introdursi in un sistema informatico. Il nome risale agli albori dell'informatica, quando il primo errore in un software venne causato da uno scarafaggio (un bug, per l'appunto), che era finito tra le schede perforate del programma.

CLOUD COMPUTING
Con il termine cloud computing si intendono tutte quelle tecnologie che consentono di usufruire di risorse hardware e software attraverso Internet. Con il cloud computing aziende e fornitori di servizi possono mettere a disposizione l'accesso a server, potenza di calcolo, database, spazio d'archiviazione, software e altri servizi. Solitamente il cloud

computing viene suddiviso in PaaS (acronimo di Platform as a Service), SaaS (acronimo di Software as a Service) e IaaS (acronimo di Infrastructure as a Service). Negli ultimi anni, però, il cloud viene utilizzato anche per diffondere e vendere malware, tramite piattaforme MaaS (ossia Malware as a Service).

CLOUD STORAGE
Un servizio cloud storage mette a disposizione degli utenti spazio di archiviazione online di svariate decine di gigabyte, accessibile da qualunque dispositivo dotato di connessione a Internet. In questo modo un utente potrà archiviare file online senza occupare spazio sul disco rigido del PC o nella memoria dello smartphone, ma avendoli comunque a disposizione: basterà fare il login al proprio account per accedere allo spazio online e scaricare tutto ciò di cui ha bisogno.

CRITTOGRAFIA
Tra le tecniche di sicurezza informatica più utilizzate (e utili per l'utente finale), la crittografia consiste nel convertire, tramite l'utilizzo di particolari algoritmi, una serie di dati da un formato leggibile a un formato codificato. Pur esistendo diversi metodi crittografici per "rendere illeggibili" dei file archiviati sul PC o inviati via Internet, quelli più utilizzati sono due: cifratura a chiave simmetrica (nella quale la "chiave di lettura" del messaggio è inviata in allegato con il messaggio stesso) e cifratura a chiave asimmetrica (nella quale vengono utilizzate due "chiavi di lettura", una pubblica e una privata, in modo che solo il destinatario possa effettivamente decifrare il messaggio).

CRYPTOJACKER
Famiglia malware nata in seguito al "boom" delle criptovalute, non produce danni diretti al sistema informatico. Almeno in apparenza: i cryptojacker, infatti, sfruttano la potenza di calcolo del PC per creare criptovalute ("minare", in gergo tecnico), che verranno però accreditate sul conto del cybercriminale, e non dell'utente. Come detto, però, l'innocuità è solo apparente: un cryptojacker, infatti, mette sotto stress tutte le componenti del PC, abbreviandone l'aspettativa di vita.

CYBER TERRORISMO
Equivalente cibernetico e digitale del terrorismo "armato". Si tratta quindi di operazioni, a sfondo politico e/o ideologico, che prevedono l'utilizzo di attacchi informatici per manomettere il funzionamento di sistemi informatici di infrastrutture critiche o per entrare in possesso di informazioni di rilievo.

CYBERBULLISMO
Potremmo definirlo come la versione digitale del bullismo e sta a indicare tutte quelle offese, minacce, insulti e attacchi condotti per via telematica. Rivolto principalmente verso giovani e adolescenti, il cyberbullismo si manifesta principalmente sulle piattaforme

di messaggistica istantanea e social network, dove un soggetto viene preso di mira e deriso (oppure offeso) da un gruppo di persone.

CYBERCRIME
Traducibile in "Crimine informatico" in italiano, indica tutte quelle attività compiute da cracker o black-hat hacker tese a compromettere le difese di sistemi informatici. I crimini informatici permettono al pirata informatico di prendere il controllo sia dell'hardware sia del software del sistema colpito.

CYBERCRIMINALE
Vedi hacker.

CYBERWARFARE
Detta anche "Guerra cibernetica", indica l'utilizzo di dispositivi informatici e tecniche hacking per attaccare una nazione, causando danni comparabili a quelli di un conflitto armato. Una tipica azione di cyberwarfare è quella dell'attacco ai sistemi di controllo di centrali elettriche o telefoniche, così da mettere fuori uso il sistema energetico o comunicativo di una nazione nemica.

DARK WEB
Secondo alcune stime, la parte di Internet "visibile" agli occhi dei motori di ricerca - e, quindi, a quelli degli utenti - è appena il 4% della "dimensione totale" della Rete. La parte restante è formata da server e siti web che non vengono indicizzati e ricercati e da una nicchia di contenuti illegali. Questa ultima parte, che a grandi linee occupa la stessa dimensione del web "visibile" viene definito come Dark Web, ossia "Web Oscuro". Per accedere a questa parte della Rete è necessario utilizzare un software TOR (acronimo di The Onion Project), un programma che anonimizza la connessione e permette di navigare in assoluta sicurezza. Cosa si trova nel Dark Web? Un po' di tutto, basta che sia illegale. Fino a qualche anno fa nel Dark Web era disponibile una sorta di e-commerce chiamato The Silk Road ("La via della seta" in italiano) sul quale era possibile acquistare stupefacenti, armi e addirittura organi umani. Alcuni "shop" specializzati, invece, permettono di acquistare prodotti legati alla sicurezza informatica: kit di sviluppo malware (i cosiddetti Malware as a Service) o database di credenziali e password trafugati da siti web attaccati nei mesi e anni precedenti.

DEEP WEB
Anche se spesso vengono confusi, Dark web e Deep web sono due parte differenti della Rete. La prima, come visto poco sopra, è la parte "oscura" di Internet; la seconda è quella "sommersa", non indicizzata dai motori di ricerca ma comunque raggiungibile tramite un normale browser (a patto di conoscerne l'indirizzo esatto). Qui si possono trovare tutti i contenuti accessibili, ad esempio, dopo un login: l'estratto conto della banca, i risultati

delle analisi del sangue, interi database e molto altro ancora. Ovviamente, anche nel deep web è possibile trovare materiale illegale, ma la sua percentuale è di gran lunga inferiore a quella del materiale legale.

DEEPFAKE
Tecnica di videoediting, sfrutta l'intelligenza artificiale per far assumere a una persona presente in un video le sembianze di un'altra, scambiandone i volti. I risultati ottenuti sono solitamente molto buoni, tanto che è impossibile riconoscere un video deepfake a occhio nudo. Pur non essendo direttamente correlata a minacce di sicurezza informatica, questa tecnica è considerata uno dei maggiori pericoli per la privacy e la protezione delle informazioni personali: sono sufficienti una manciata di foto di un volto per "assumere l'identità" di chiunque.

FALLA
Vedi vulnerabilità.

FIREWALL
Letteralmente "Muro di fuoco", si tratta di un programma di sicurezza che analizza il flusso di pacchetti dati in entrata e in uscita dal PC per verificare che non ci sia nulla di anomalo. In caso di pericolo (un cracker che prova a introdursi nel nostro sistema informatico o uno spyware che prova a "sifonare" dei dati dalla nostra memoria), il firewall interviene e interrompe la connessione, così da preservare l'integrità del sistema. Inoltre, l'utente può impostare regole predefinite che bloccano il traffico in entrata o uscita a prescindere, senza che ci sia bisogno di un evento malevolo.

FLEECEWARE
I fleeceware sono app legittime che ogni utente può scaricare sul proprio smartphone dall'App Store e dal Play Store, ma che nascondono una sorpresa. Dopo pochi giorni (o, in alcuni casi, poche ore) di utilizzo, viene attivato automaticamente un abbonamento da svariate decine di euro, senza che l'utente se ne accorga. Un metodo legale, o quasi, per spennare ("to fleece", in inglese) persone inconsapevoli di cosa sta per accadergli.

HACKER
Esperto informatico con conoscenze che spaziano dalla programmazione alla crittografia, passando per la sicurezza informatica. Un hacker utilizza così le sue abilità e la sua preparazione per scovare vulnerabilità e falle all'interno del codice sorgente di app, software e protocolli, in modo da accrescerne la sicurezza. Da non confondere con la figura del cracker (o black-hat hacker), il cui scopo è esattamente opposto.

INTERNET OF THINGS
Spesso abbreviato in IoT, l'Internet delle Cose indica un sistema di "oggetti intelligenti"

che comunicano tra loro sfruttando una connessione dati che può essere cablata o senza fili. Grazie al continuo scambio di dati e ai sensori di cui sono dotati, gli oggetti possono acquisire informazioni sull'ambiente che li circonda e "adattarsi" di conseguenza. Potenzialmente, ogni oggetto della nostra quotidianità può diventare un dispositivo IoT: dalle lampadine al termostato, dal frigo ai robot per la cucina, passando per TV, robot industriali e molti altri ancora.

MALWARE
Crasi dei termini inglesi "Malicious Software" (software malevolo in inglese), malware è un termine generico utilizzato per indicare qualunque tipologia di programmi o stringhe di codice che possono mettere a rischio dati e informazioni presenti nella memoria del dispositivo attaccato. Sono esempi di malware i worm, i virus, gli stalkerware, gli spyware, i ransomware, gli adware e qualunque altra famiglia di programma creata per attaccare device elettronici.

PASSPHRASE
È l'evoluzione della password: una chiave d'accesso composta da più parole di senso compiuto che, da un lato, rende più complesso il lavoro di chi prova a rubare password con metodi automatizzati (tramite i cosiddetti "attacchi dizionario", ad esempio) e, dall'altro lato, fa sì che le chiavi d'accesso siano facilmente ricordabili.

PASSWORD MANAGER
Buona norma vorrebbe che utilizzassimo una password differente per ogni account che abbiamo. I password manager nascono proprio per facilitarci in questo compito: dove non arriva la memoria, arrivano programmi ad hoc che archiviano le credenziali in un database sicuro e crittografato. Le credenziali così salvate verranno poi riproposte non appena si tenterà di effettuare l'accesso a uno dei propri account.

PASSWORD
Letteralmente "parola d'accesso", è la chiave d'accesso che impostiamo e utilizziamo per accedere ai profili web (posta elettronica, social network, banca online e altro).

PATCH
In italiano sta per "toppa", un termine che descrive alla perfezione il suo ruolo nel mondo informatica. Le patch sono infatti delle piccole porzioni di codice o piccoli programmi rilasciati per correggere una precisa vulnerabilità di sicurezza (o comunque un numero limitato di bug).

PENETRATION TEST
Serie di strumenti e programmi che consentono di valutare la sicurezza di una rete, di PC o di un sito web provandone a superare (o penetrare, in gergo tecnico) i sistemi di difesa.

PHISHING
Il phishing è una delle tecniche di attacco informatico maggiormente utilizzate. Si tratta di un tentativo fraudolento di ottenere dati e informazioni personali di un utente come le sue credenziali di posta elettronica o social, i dati della carta di credito e altri. Solitamente, un attacco phishing viene condotto tramite messaggi di posta elettronica, ma sempre più spesso vengono utilizzati i servizi di messaggistica istantanea e i social network, che consentono di raggiungere un numero di persone più ampio in minor tempo (e senza "filtri" a difenderli) Il phishing, così come lo abbiamo descritto, rientra nel più ampio settore dell'ingegneria sociale, che sfrutta informazioni private degli utenti per poterli truffare o rubare loro informazioni personali.

RANSOMWARE
Tra le famiglie malware più pericolose, è anche una delle ultime ad aver fatto la sua comparsa. I ransomware, o software del riscatto, sfruttano una combinazione di ingegneria sociale e phishing per infettare un computer e infiltrarsi in una rete informatica. Una volta che il virus è all'interno del PC o dello smartphone, l'utente può ben poco: il ransomware crittografa immediatamente tutti i dati presenti nella memoria e riavvia il dispositivo. Alla riaccensione, l'utente visualizza un messaggio di riscatto ("ransom" in inglese) da pagare solitamente in bitcoin.

ROOTKIT
Tra le famiglie malware più pericolose, i rootkit consentono a un cracker di ottenere i permessi di root del sistema operativo. Ciò consente al cybercriminale di controllare ogni singolo aspetto del PC, sia a livello software sia a livello hardware. I permessi di root, infatti, sono i cosiddetti "permessi da amministratore", che conferiscono potere assoluto sulla gestione del sistema operativo.

SCANSIONE "SIGNATURE BASED"
Detta anche "analisi delle firme", è alla base del funzionamento della gran parte dei software antivirus. Ogni programma di sicurezza ha un database di "firme", una porzione di software di tutti i malware noti da confrontare con file e programmi presenti nella memoria del PC o dello smartphone. In caso di corrispondenza tra la firma e il software analizzato, quest'ultimo verrà "immunizzato", mettendolo in quarantena o eliminandolo dalla memoria.

SCANSIONE EURISTICA
Detta anche "analisi euristica", si contrappone a quella basata sulle firme perché, anziché limitarsi allo studio e al confronto del codice del software malevolo, ne studia anche il comportamento. Gli antivirus ad analisi euristica valutano così come si comporta un determinato software e, in caso ci siano delle analogie con il comportamento di malware noti, lo mette in quarantena, così da renderlo innocuo. In questo modo è possibile

individuare virus e malware non ancora conosciuti o per i quali non sono ancora disponibili delle "firme".

SEXTORTION
Neologismo inglese nato dall'unione di "Sex" ed "Extortion", è una truffa a sfondo sessuale condotta sul web. Le vittime di sextortion ricevono email o messaggi sui social network da sconosciuti che sarebbero entrati in possesso di loro immagini compromettenti (foto nude o in atteggiamenti sessuali) e sarebbero pronte a diffonderle pubblicamente. Per evitare che ciò accada, alle vittime viene chiesto il pagamento di una somma a mo' di "riscatto": una truffa bella e buona, dato che nella stragrande maggioranza dei casi le immagini compromettenti non esistono.

SICUREZZA INFORMATICA
Con il termine "sicurezza informatica" si intendono tutte quelle tecniche e quelle strategie volte a difendere server, datacenter, computer, smartphone, dispositivi IoT e qualunque device elettronico da attacchi di natura informatica. Gli attacchi sono solitamente diretti ad accedere, modificare o distruggere informazioni presenti all'interno dei dispositivi, a estorcere denaro o "prendere possesso" da remoto degli stessi dispositivi.

SMISHING
Lo smishing è un tentativo di truffa telematica condotto via SMS (il suo equivalente "informatico" è il phishing, per intendersi). In quello che potremmo definire "caso tipo", l'utente riceve un messaggio dalla propria banca per un tentativo di accesso anomalo al conto corrente online e per questo è necessario modificare la password del profilo. In realtà, il sito su cui si viene indirizzati è un "falso realizzato ad arte", che permette ai cybertruffatori di accedere indisturbati al conto corrente online.

SPAM
Invio massivo di messaggi di posta elettronica non richiesti, solitamente di carattere pubblicitario o promozionale. Anche se si tratta di una pratica in netto calo rispetto al passato, si calcola che tra il 55% e il 60% delle email inviate ogni giorno siano di spam e, dunque, inutili. Di per sé lo spam non è pericoloso, ma potrebbe anche trattarsi di una tattica per "nascondere" mail di phishing e trarre così in inganno un utente.

SPYWARE
Il nome è piuttosto evocativo: spyware nasce infatti dall'unione dei termini inglesi spy (spiare) e ware (per software). Si tratta di un malware che infetta PC, smartphone e sistemi informatici con l'obiettivo di spiare l'utente, trafugare informazioni presenti nella memoria del dispositivo e inviarle a server remoti gestiti dagli stessi hacker – oppure organizzazioni criminali – che hanno creato il malware.

STALKERWARE
Tra gli ultimi arrivati sul panorama della sicurezza informatica mobile, gli stalkerware sono app che consentono a un utente di spiare e controllare ogni singolo aspetto di uno "smartphone obiettivo". Si tratta di una tipologia particolare di spyware che, una volta installata su un dispositivo mobile, permette di accederne a tutte le risorse: fotocamera, galleria fotografica, rubrica, app per SMS, social network e piattaforme di messaggistica istantanea.

TROJAN HORSE
Come Ulisse entrò a Troia sfruttando un cavallo di legno, gli hacker sono soliti crearsi delle "aperture" nei sistemi di difesa di PC, smartphone e altri sistemi informatici utilizzando i trojan horse (letteralmente "cavallo di Troia"). Si tratta di software che, una volta all'interno del dispositivo, crea un accesso remoto che un cybercriminale può utilizzare sia per trafugare dati, sia per accedere al device e prenderne possesso a distanza.

VIRUS
I virus sono una delle famiglie malware più importanti e conosciuti. Si tratta di programmi che infettano un PC o un sistema informatico per tentare di distruggerne i dati, corromperne i file di sistema o alternarne le prestazioni. A differenza di altri malware, i virus sono in grado di autoreplicarsi e diffondersi in altri computer o smartphone sfruttando la connessione a Internet o altri sistemi di comunicazione.

VPN
Acronimo di Virtual Private Network, la VPN è una rete informatica virtuale protetta da crittografia. Molto utilizzata a livello aziendale, ma sempre più apprezzata anche da utenti "normali", la VPN viene creata attraverso una tecnica detta di "tunneling", ossia uno "scudo crittografico" che forma una connessione a "prova di cracker" tra due punti di una rete. Tutti i dati che passano sotto questo "scudo" sono crittografati e, per questo, indecifrabili e inutilizzabili in caso di attacco man-in-the-middle.

VULNERABILITÀ
Difetto di progettazione, codifica o configurazione di un software (ma anche di protocolli informatici) che consente a un hacker o cybercriminale di compromettere l'integrità del sistema. Sfruttando una vulnerabilità del sistema operativo (o di un software installato su PC), ad esempio, è possibile accedere alle informazioni archiviate nella memoria del dispositivo oppure ottenere i privilegi di amministratore e spiare tutte le attività dell'utente.

WHITE-HAT HACKER
Detto anche hacktivist, è la "nemesi" del Black-hat hacker. Si tratta di un hacker "etico", specializzato in penetration test e altre metodologie di prove il cui scopo è di verificare il livello di sicurezza e affidabilità di reti informatiche. Il solo scopo di un White-hat hacker

è quello di portare alla luce falle e vulnerabilità insite nei sistemi di network informatici, in modo che i gestori della rete possano correre ai ripari.

WORM
Letteralmente "verme", è una famiglia di malware che sfrutta le macchine infettate per replicarsi e diffondersi su altri PC (nella stragrande maggioranza, il worm si "auto-invia" sfruttando la posta elettronica). Il worm, solitamente, non viaggia mai solo: funge infatti da "apripista" per altri malware, come keylogger, backdoor o spyware.

ZERO DAY
Attacco informatico che sfrutta vulnerabilità non ancora rese pubbliche per le quali non è ancora disponibile una patch o un aggiornamento. Si tratta di una delle minacce più gravi, dal momento che non esistono soluzioni disponibili.