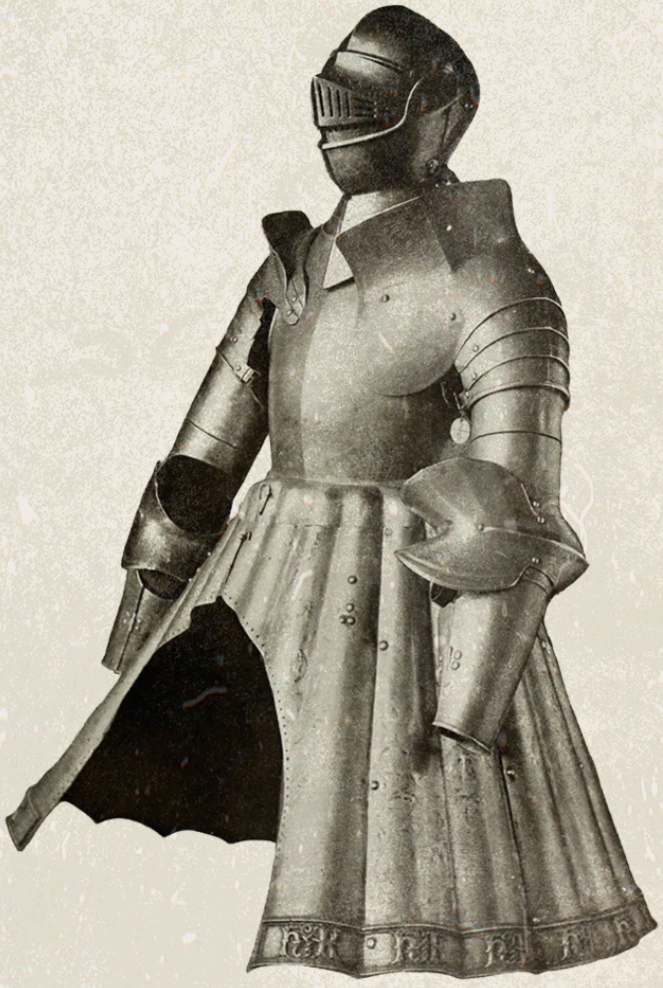
MANUALETTO DI SICUREZZA DIGITALE PER GIORNALISTI E ATTIVISTI



GUERRE DI RETE

Gli eBook di Guerre di Rete

MANUALETTO DI SICUREZZA DIGITALE PER GIORNALISTI E ATTIVISTI

Uno speciale per rafforzare le difese di due categorie a rischio

A cura di Carola Frediani, Sonia Montegiove, Patrizio Tufarolo

Con i contributi di Raffaele Angius, Carola Frediani, Sonia Montegiove, Rosita Rijtano, Matteo Spinelli, Taylor, CRP

Impaginazione a cura di Ufficio Furore - Federico Nejrotti

GUERRE DI RETE

INDICE

1. INTRODUZIONE DI CAROLA FREDIANI

Il nostro rapporto con le tecnologie è inevitabilmente contraddittorio. Mai come ora siamo circondati da strumenti abilitanti, che ci consentono di allargare le nostre capacità, ridurre sforzi e tempi di vecchie attività, dotarci di una somma di poteri da cui ormai siamo dipendenti, tanto da avere la sensazione di non poterne più fare a meno. Eppure questi stessi strumenti, in maniera spesso invisibile e inattesa, possono aprire dei varchi sulle nostre vite, il nostro lavoro, le nostre relazioni. E quando succede, proprio la loro potenza, insieme alla capacità di archiviazione, l'ubiquità, la granularità con cui estraggono informazioni che prima non sarebbero mai state raccolte, diventano un'arma a doppio taglio.

Questo vale per tutti, ma soprattutto per giornalisti e attivisti, che fanno dello scambio di informazioni (anche delicate, riservate, sensibili) una delle loro ragion d'essere. Il problema è che la macchina, intesa come l'assemblaggio caotico e strabordante di dispositivi, account, servizi digitali che ognuno di noi gestisce alla bell'e meglio mentre è intento a vivere, funziona splendidamente (o dà l'idea di funzionare in tal modo) senza disfunzioni, senza avvertimenti, senza preavvisi, fino al giorno in cui non funziona più. Fino al giorno in cui si riceve una strana notifica di Apple o Meta di essere stati oggetto di un attacco statale; fino a quando ritroviamo i nostri dati più privati online; o non riusciamo a entrare nel nostro account Instagram, che ha iniziato nel frattempo a delirare; o veniamo informati che qualcuno è entrato nella nostra casella di posta; o veniamo respinti alla frontiera senza nemmeno sapere perché; o la nostra fonte passa dei guai, e ci resta il sospetto che sia a causa delle comunicazioni avute con noi.

L’elenco potrebbe continuare e, a seconda dei Paesi e delle situazioni, appesantirsi. Perché mai come oggi giornalisti e attivisti possono essere un obiettivo: di criminali, di Stati, di poteri economici, di gruppi ideologizzati, di individui ossessionati, di società private di indagine.

È con questa consapevolezza che come Guerre di Rete abbiamo deciso di scrivere e pubblicare questo manualetto. Il diminutivo è d’obbligo per due motivi: non c’è manuale che possa coprire in modo esaustivo l’argomento o garantire sicurezza; e, in ogni caso, l’obiettivo del nostro ebook è quello di essere uno strumento propedeutico, per principianti o poco più, che vogliano gettare alcune fondamenta nella loro impalcatura digitale. Non sarà abbastanza, ma nemmeno vano.

Il nostro pubblico principale sono giornalisti e attivisti per le ragioni spiegate sopra, anche se ci sono delle differenze tra questi due profili, che non abbiamo approfondito in questo livello iniziale. Riteniamo comunque che buona parte di questo ebook - scritto e rivisto da giornalisti, esperti di sicurezza e attivisti - vada bene per entrambi i gruppi (e a dire il vero, non solo per loro).

Fatto questo chiarimento generale, due note di contenuto. Il manualetto ha un perimetro circoscritto. Intanto, si concentra solo sul digitale. Un’ovvietà, penseranno alcuni. Non proprio. Per giornalisti e attivisti la sicurezza digitale e quella fisica tendono a intrecciarsi e a influenzarsi spesso. Un'informazione su un dispositivo, in certi contesti, può farti arrestare; un post sui social può consentire circostanziate minacce fisiche; un'app o una configurazione particolare di sicurezza possono generare sospetti a un controllo. In alcuni casi i due piani entrano in conflitto: ci sono situazioni

in cui portare con sé un telefono o altri dispositivi può essere pericoloso, ma lasciarli incustoditi in un hotel potrebbe diventare un rischio digitale. Come avrete già capito da questi esempi, distillare indicazioni al riguardo in un manuale è assai problematico. La sovrapposizione di sicurezza fisica e digitale richiede un'analisi ad hoc e un piano specifico, che tengano conto della persona, del contesto, delle minacce, delle inconciliabilità, e di molti altri fattori.

Un altro limite del manualetto è che ci siamo concentrati sulle minacce cyber, non dando molto spazio alle fughe di dati che possono derivare da un uso sconsiderato di alcuni strumenti. Ad esempio, tutti quei tool di AI utilizzati per "sbobinare" interviste, trasformare audio in testo, fare ricerche su documenti di lavoro, riassumere riunioni e via dicendo. Prima di utilizzarli bisognerebbe sempre verificare quali sistemi di sicurezza adottino e come siano gestiti i dati: verifiche che a volte portano a sorprese spiacevoli. In generale, bisogna essere molto cauti se il materiale trattato contiene parti riservate e off the record.

Infine, un elemento generale di difficoltà sono proprio le minacce. Chi si occupa davvero di cybersicurezza è dotato di umiltà, e se non era umile ha imparato a esserlo col tempo. Perché la base di conoscenza acquisita, per quanto solida, è incredibilmente mutevole. Perché la complessità del piano umano, tecnico e organizzativo (di cui parleremo più sotto) è tale che l'errore, l'imprevisto, la falla sono sempre da mettere in conto. Le risorse stesse dedicate alla sicurezza devono essere aggiornate in continuazione.

E tuttavia, sottolineati tutti questi limiti, siamo convinti che sia possibile fare la differenza. Che informare su questi temi possa aiutare

concretamente persone che si occupano di questioni importanti per la società. Questo manualetto vuole fare la sua parte. Aiutarvi a iniziare un percorso. A rafforzare le vostre difese. A limitare le probabilità e gli impatti di eventuali minacce. A reagire e rispondere in modo più consapevole. A rendere la vita più dura agli attaccanti. Magari, qualche volta, a smascherarli più facilmente.

Il manualetto segue un percorso che va dal facile al difficile, da quello che va messo subito in sicurezza, e con poca fatica, a quello che richiede più lavoro. Si inizia inquadrando alcuni aspetti generali - i diversi piani della sicurezza, l'analisi delle minacce - e poi si va nel pratico. Siamo partiti dalla mail perché sappiamo che è ancora l'hub centrale delle nostre vite, e quindi un fortino da difendere. Passiamo poi ai social media che, nel bene e nel male, restano un luogo fondamentale per giornalisti e attivisti, sottovalutato dal punto di vista della sicurezza. Eppure una revisione attenta delle impostazioni di visibilità e di privacy dei nostri account potrebbe far emergere informazioni che non siamo consapevoli di "pubblicizzare". Poi parliamo di come si comunica con una fonte, o con qualcuno che necessiti di non essere esposto: il problema del primo contatto, quali app (e perché) possono essere utili, quali sistemi adottare per ricevere soffiate.

Sistemate la mail, i social, e le comunicazioni, è tempo di pensare ai dispositivi. Sono cifrati? Abbiamo backup? Come li gestiamo? È il caso di compartimentare?

Successivamente, ci addentriamo nell'aspetto della cybersicurezza più noto e forse temuto: phishing, malware, spyware. Senza fare miracoli, un utente

consapevole può però alzare di tanto l'asticella della sua protezione.
Infine, dopo una sezione su strumenti avanzati, più tecnica, concludiamo su come reagire a un attacco, e su dove trovare risorse utili.

E qui si conclude il nostro manualetto. Speriamo possa esservi utile. Noi abbiamo fatto la nostra parte. Ora è il vostro turno.

2. QUALCHE PRINCIPIO DI BASE DI RAFFAELE ANGIUS

La presunta complessità della cybersicurezza offre spesso un facile alibi per disinteressarsi in toto della materia, in una sorta di fatalismo cosmico che fa dire al potenziale bersaglio di un attacco "cosa mai avrei potuto fare". Eppure, in modo del tutto simile a una lingua, anche la sicurezza informatica inizia a svelarsi attraverso la conoscenza dei principi di base e delle sue parti, certamente accessibili a chiunque con un minimo di impegno. È dunque possibile mettersi nella condizione di proteggere se stesso e i propri asset informatici in modo efficace di fronte a un ragionevole numero di minacce. Ciò è tanto più importante quando si svolgono professioni o attività che ci espongono all'antagonismo di attori, privati, statali o altro, che possono avere un interesse conoscitivo su ciò che facciamo o che addirittura potrebbero voler interferire con le nostre attività.

Attivisti e giornalisti sono senz'altro al centro di questo scenario, come dimostrano centinaia di episodi che vedono queste due categorie nel mirino di molteplici poteri, di entità non definite, di intelligence e governi. Episodi avvenuti anche in Paesi teoricamente più democratici. Basti pensare all'uso di spyware, nel mondo, in Europa e nel nostro Paese. O anche all'uso di intercettazioni telefoniche a danno di cronisti per individuare le loro fonti. Senza entrare nel dettaglio dei singoli casi, occorre evidenziare ciò che tutti hanno in comune: l'impiego di strumenti digitali usati come armi. E da tali strumenti dobbiamo imparare a difenderci. A tale scopo può essere utile una scomposizione delle minacce e delle difese, fondata su tre pilastri: umano, tecnico, organizzativo.

Il pilastro umano, ovvero la sedia e la tastiera

Pebkac è un acronimo comunemente utilizzato negli ambienti hacker. Sta per *Problem exists between the keyboard and the chair* o, in italiano, *Il problema risiede tra la tastiera e la sedia*. È un modo comune di definire il punto di caduta di una gran parte dei problemi legati all'informatica, ovvero l'essere umano che è appunto seduto sulla sedia e davanti a una tastiera. Espandendo lo scopo di questa *boutade*, anche le minacce cyber si avvalgono sempre più spesso delle debolezze del bersaglio, dell'essere umano, in luogo delle vulnerabilità dei suoi dispositivi.

Questo è diventato ancora più vero nel tempo, con l'evoluzione delle misure tecnologiche volte a mitigare gli attacchi che un dispositivo digitale può subire. Indovinare una password attraverso l'osservazione del bersaglio oppure indurlo a cliccare su un link che porta, a sua insaputa, all'installazione di uno spyware sono metodi molto più pratici ed efficaci, nonché meno costosi. Basti pensare a un vecchio metodo di attacco utilizzato dalle autorità giudiziarie che, per installare uno spyware sul dispositivo di un bersaglio, ottengono che sia la compagnia telefonica in primis a creare dei disservizi sulla linea del malcapitato. Costui chiederà assistenza alla compagnia telefonica che, rassicurandolo, invierà un "messaggio autoconfigurante" il quale dovrebbe risolvere ogni problema di malfunzionamento. Ciò di cui non è cosciente il bersaglio è che l'intera esperienza è in realtà un attacco nemmeno troppo sofisticato e che quel messaggio autoconfigurante contiene in realtà il link per l'installazione di uno spyware che potrà prendere il controllo da remoto del dispositivo.

Questo è solo un esempio - tra decine che se ne possono fare - che dimostra come sia più facile indurre in errore il bersaglio, creando uno stato di disagio (il disservizio) e una promessa di soluzione (la rassicurazione che con un "messaggio autoconfigurante" tutto si sarebbe risolto).

In tal senso, la prima linea di difesa non è fatta di codici o algoritmi, ma di attenzione e consapevolezza. Le minacce informatiche più efficaci non sfruttano vulnerabilità tecnologiche, ma debolezze cognitive: la fiducia mal riposta, la fretta, la distrazione, l'illusione di essere al sicuro. È sufficiente un clic sbagliato, un file aperto senza pensarci, un link condiviso con leggerezza per esporre dati, contatti e identità.

La cybersicurezza, quindi, comincia da un cambiamento di mentalità. Significa imparare a leggere i segnali deboli del rischio digitale: riconoscere un'email sospetta, capire quando una richiesta è anomala, trattare le informazioni sensibili con la stessa cura che si riserva a un documento riservato in formato cartaceo. Significa anche sviluppare una forma di igiene digitale quotidiana: aggiornare i dispositivi, usare password uniche e solide, attivare la doppia autenticazione, custodire i dati come si custodisce una chiave di casa.

La dimensione umana della sicurezza è culturale: riguarda la fiducia, il giudizio e l'abitudine. In un mondo in cui la manipolazione digitale è alla portata di tutte le persone, la vera competenza non è soltanto tecnica, ma riguarda la consapevolezza: la capacità di agire con prudenza senza cedere alla paranoia, di verificare prima di condividere, di comprendere che la libertà online passa attraverso la responsabilità individuale.

Il pilastro tecnico, ovvero la difesa invisibile

Il secondo pilastro è tecnico, ed è quello che di solito si associa in modo immediato alla cybersicurezza. È l'insieme degli strumenti e dei controlli che proteggono i sistemi informatici: firewall, crittografia, antivirus, autenticazione a più fattori, backup, monitoraggio del traffico di rete. Ogni strumento tecnico è efficace solo se usato correttamente, aggiornato e inserito in un contesto coerente di regole e buone pratiche. Un software non utilizzato e un aggiornamento ignorato o un dispositivo non protetto possono diventare l'anello debole che vanifica ogni altra misura di difesa.

Basti pensare ai software "craccati", termine che indica i programmi informatici scaricati dalla rete illegalmente per aggirare il pagamento del software ufficiale. Se immaginiamo che per ogni software "craccato" c'è dietro un esperto informatico che ha preso il programma ufficiale, ne ha smontato il codice, ha asportato la parte volta a impedire gli usi illeciti e, infine lo ha riassemblato, suona quantomeno naive immaginare che già che c'era dentro non ci abbia nascosto qualche agente malevolo in grado di controllare da remoto il dispositivo di chiunque lo scarichi. Sembra un esempio teorico ma è dei più concreti: una testata di cui siamo a conoscenza ha perso temporaneamente il controllo delle proprie pagine web e degli account social (questi ultimi mai più recuperati) proprio per un attacco di questo tipo. Un software scaricato illegalmente che funzionava benissimo, salvo esfiltrare tutte le password di chi lo aveva installato.

La sicurezza tecnica funziona quando è dinamica, non statica. Le minacce evolvono costantemente: ciò che oggi protegge, domani può diventare

obsoleto. Le vulnerabilità emergono da componenti impensate, da fornitori terzi, da integrazioni invisibili.

Per questo la difesa tecnologica deve essere vista come un ecosistema in evoluzione, da mantenere, testare e rinnovare. La manutenzione della sicurezza non è un atto burocratico, ma un gesto di cura verso l'infrastruttura che sostiene la credibilità, la riservatezza e la continuità del lavoro.

Il pilastro organizzativo, ovvero strategia e organizzazione

Il terzo pilastro è organizzativo, ed è forse il più sottovalutato. È il livello in cui la sicurezza smette di essere un insieme di buone intenzioni e diventa struttura, metodo e responsabilità condivisa.

Ogni ambiente di lavoro che tratta informazioni - siano esse dati personali, materiali sensibili o semplici comunicazioni interne - ha bisogno di regole chiare: chi ha accesso a cosa, come vengono gestiti i backup, quali protocolli si attivano in caso di incidente, chi è responsabile di segnalare un'anomalia.

Questo piano è anche quello della governance: nel caso di una testata giornalistica è per esempio fondamentale definire ruoli, procedure e piani di emergenza, evitando che la sicurezza dipenda dall'improvvisazione o dal singolo individuo. Basti pensare agli accessi al cloud, dove più persone lavorano su uno stesso file o una cartella contenente i documenti a base di un'inchiesta. È sufficiente che venga compromesso il dispositivo di una sola

persona in una rete di collaboratori per mettere a rischio l'interezza dei dati e delle informazioni custodite.

La sicurezza organizzativa è una rete fatta di policy, formazione interna, audit periodici e comunicazione trasparente. Non esiste protezione tecnica che resista a lungo in un contesto dove mancano regole, coordinamento o responsabilità condivisa.

Una buona organizzazione non si limita a reagire, ma progetta la sicurezza sin dall'inizio: nel modo in cui archivia, comunica, sviluppa nuovi progetti o collabora con partner esterni. È la logica del "security by design".

I tre pilastri - umano, tecnico e organizzativo - non sono compartimenti separati, ma dimensioni complementari di una stessa cultura. La cybersicurezza, in ultima analisi, è un problema di fiducia: fiducia negli strumenti, nelle procedure, nelle persone con cui si lavora. Costruirla richiede tempo, disciplina e trasparenza. Ma soprattutto richiede la consapevolezza che la sicurezza non è mai un ostacolo alla libertà, bensì la condizione che la rende possibile.

Conosci le minacce specifiche per giornalisti e attivisti

Quando si parla di giornalismo, informazione, attivismo e minacce collegate al mondo tecnologico, può essere utile ricondurre il tutto a due soli oggetti d'indagine: da chi è costituita la minaccia e qual è l'oggetto di suo interesse. Partiamo da quest'ultimo e identifichiamo dunque l'*asset* da proteggere. Normalmente è un'informazione, un documento, un dato, ma

può trattarsi anche - spesso è questo il caso - dell'identità di una fonte o comunque di una persona con cui abbiamo contatti.

Le minacce fisiche non sono oggetto di questo manuale quindi non verranno esaminate le tecniche di controsorveglianza che garantiscono normalmente un certo livello di protezione da attori esterni che volessero seguirci per strada o spiare la nostra casa in appostamento. Dall'altra, cercando di stabilire un'impropria gerarchia delle minacce dal punto di vista digitale, viene naturale porre al primo gradino l'intercettazione telefonica. Seguono le tecnologie di sorveglianza digitale costituite da microspie e telecamere, per arrivare infine a spyware e metodi di acquisizione da remoto del contenuto dei nostri dispositivi. Ma non si devono trascurare nemmeno le minacce di natura comune, cybercriminale, che possono avere come esito ricadute economiche, reputazionali, e arrivare comunque alla perdita o distruzione di dati importanti. E in ultima analisi, anche perdere un dispositivo non protetto su un treno, ad esempio una chiavetta non cifrata, espone a rischi di varia natura, se nella chiavetta ci sono dati sensibili.

Come detto, una gerarchia delle minacce è una semplificazione necessaria per dare ordine ai pensieri, ma non necessariamente riflette la realtà dei fatti. Ogni tecnica è calibrata sull'asset che si vuole acquisire e pertanto un'intercettazione telefonica può risultare più pericolosa di uno spyware a seconda del contesto nel quale operiamo e in cui è incardinato il bene che vogliamo proteggere.

Vale tuttavia la pena evidenziare che una simile "scala delle minacce" riflette il costo delle stesse e offre un aggancio utile a introdurre il tema del rapporto tra costo e opportunità di un attacco digitale. Non tutti gli attaccanti operano con le stesse disponibilità economiche e, in un regime di scarsità, si tende a utilizzare lo strumento che offra il maggiore vantaggio economico rispetto all'asset che si vuole acquisire. Ne consegue che innalzando il livello di sicurezza dei nostri asset, dovrà aumentare anche il costo di qualunque attività volta a minacciarli.

Ed è esattamente quello che vogliamo che accada. Tanto più se si considera che nel conto economico di un attacco rientra anche il tempo richiesto per avere successo. Tanto più un attaccante dovrà investire risorse economiche e personali per avere una ragionevole probabilità di riuscita, tanto meno è probabile che l'attacco in sé abbia luogo. Certo, questo è vero soprattutto nel caso di attacchi di natura criminale (minacce esterne più orientate ad acquisire il controllo del nostro portafogli che non delle fonti con cui parliamo), mentre il ragionamento diventa ancora più puntuale se si parla di attività di intelligence o investigative.

Conosci te stesso (accenni di threat modeling)

Ogni difesa parte da una domanda semplice ma decisiva: chi sono e cosa devo proteggere? La risposta a questa domanda è il primo passo per il cosiddetto *threat model*, termine anglosassone che indica un processo di analisi volto a identificare le potenziali minacce dalle quali dobbiamo difenderci. Serve a capire dove risiedono i punti deboli, quali informazioni hanno valore e chi potrebbe essere interessato ad ottenerle. Ogni individuo o organizzazione custodisce asset diversi - documenti, fonti, contatti - e

ognuno di essi può diventare un bersaglio. La sicurezza non è mai assoluta, ma può essere proporzionata: il primo passo è mappare se stessi, il secondo è riconoscere le minacce.

Una prima serie di domande da porsi riguarda la propria superficie d'attacco: quali dati produco, dove li conservo, chi vi ha accesso, quali strumenti uso ogni giorno? Capire le proprie abitudini digitali equivale a disegnare una mappa della propria vulnerabilità. Come detto, non basta installare un software di sicurezza: bisogna sapere come e perché si può essere colpiti.

Poi viene la controparte, il "chi ci minaccia". I potenziali attaccanti non sono tutti uguali, né per motivazione né per risorse. Alcuni operano per interessi economici, altri per motivi politici o personali. Nel panorama delle minacce rientrano sicuramente nel *threat model* di giornalisti e attivisti anche gli attori statali. A seconda del tipo di lavoro fatto da attivisti e giornalisti - se ad esempio di natura internazionale - gli attori statali potenzialmente interessati a certe informazioni si moltiplicano.

Tra l'altro, alcuni Stati dispongono di tecnologie verosimilmente tra le più avanzate sul mercato. In questo caso pensiamo in particolare agli spyware con caratteristiche *zero-click*, ovvero capaci di installarsi sul dispositivo del bersaglio senza alcuna interazione da parte di quest'ultimo. Come vedremo, questo avviene in particolare grazie agli 0-day, vulnerabilità non note al produttore di un dispositivo e dunque particolarmente costose. Il punto fondamentale è capire quale può realmente essere il livello di minaccia al quale siamo esposti - a questo serve il *threat model* - in modo da stabilire un livello di protezione appropriato. Questo non è un dato fisso, bensì può

variare nel tempo e a seconda di quali attività si svolgono. Un'inchiesta più delicata per un giornalista oppure una trasferta in un Paese in cui potremmo essere maggiormente esposti sono elementi che concorrono a spostare l'asticella della minaccia e la flessibilità è cruciale.

In breve:

- ✓ Mappa i tuoi asset digitali, account, dispositivi;
- ✓ Analizza quali sono i dati più sensibili;
- ✓ Analizza chi potrebbe voler accedere a quei dati e perché.

3. INIZIA DALLA MAIL DI SONIA MONTEGIOVE

Era giugno 2025 quando veniva pubblicata la notizia dell'attacco ad alcuni giornalisti del Washington Post che si occupavano di politica estera e Cina, attraverso la compromissione di alcuni account email Microsoft. L'accesso non autorizzato ha permesso di accedere alle email inviate e ricevute, a documenti e bozze, con alto rischio non solo di esfiltrazione di dati, ma anche di impersonificazione per colpire altri colleghi o soggetti connessi. La casella di posta, considerata come uno dei più importanti e irrinunciabili strumenti di lavoro, può diventare un canale attraverso il quale far "entrare" abusivamente attaccanti con lo scopo di conoscere dati, conversazioni, processi aziendali fino ad arrivare a bloccare interi sistemi attraverso attacchi di tipo phishing. Questa tipologia di attacco, ormai nota alla maggior parte delle persone, risulta essere ogni anno in aumento e, complice l'intelligenza artificiale generativa, sempre più efficace, vista la possibilità di rendere le email più convincenti e difficili da rilevare come "sospette".

Perché la casella email è ancora tanto importante da proteggere? L'email, per un giornalista, non è semplicemente uno strumento di comunicazione, ma è anche un archivio strategico: nella casella di posta convivono bozze di articoli, scambi riservati con le fonti, documenti confidenziali, materiali non ancora pubblicati o coperti da embargo. Spesso la casella di posta è anche lo strumento attraverso cui è possibile conoscere i servizi fondamentali di redazione, ad esempio quale Content Management System viene utilizzato per la gestione del giornale online, i servizi in cloud di archiviazione interna, i tool di pubblicazione, le liste di distribuzione.

Proteggere l'email significa quindi proteggere l'intera filiera dell'informazione. Oltre a questo, l'account è anche la porta d'ingresso per molte altre piattaforme perché spesso funziona da account di recupero su cui mandare i messaggi di reset di password, dai social agli strumenti di collaborazione. Se un attaccante riesce a comprometterla, può sostituirsi all'utente, reimpostare le credenziali, bloccare l'accesso legittimo e prendere il controllo dell'identità digitale del giornalista. Persino gli alert di sicurezza, come le notifiche di accessi sospetti, transitano via email: un cyber criminale entrato abusivamente in un account può leggerli, cancellarli e continuare ad agire indisturbato.

Anche il social engineering ha un legame forte con l'email, in quanto colpisce spesso sfruttando la fiducia implicita nei messaggi di posta. Cybercriminali possono inviare comunicazioni da domini simili, quasi identici, a quelli di una istituzione con la quale siamo in contatto o di un'altra testata con la quale collaboriamo o da account già compromessi, facendo leva su urgenze redazionali o richieste apparentemente legittime di caporedattori o colleghi. L'apertura in fretta di un allegato, un login fatto "al volo" come da richiesta, un clic su un link che ci invita a scaricare qualcosa di potenzialmente interessante e utile per l'attività giornalistica e l'attacco è andato a buon fine.

Ha senso, pertanto, parlare di email anche in questo manuale perché un atteggiamento poco attento di una persona e la compromissione di un account di posta non mette a rischio solo il singolo giornalista, ma l'intera redazione.

Password, non parlarne non ti sento

Di password non si parla quasi più, se non, come nel caso del furto al Louvre, per ironizzare sull'ingenuità di chi le ha scelte così banali da renderle quasi imbarazzanti. In molti le ritengono quasi un retaggio del passato: le salviamo sui nostri browser in modo da non doverle digitare ogni volta, non ci ricordiamo più quelle di accesso a piattaforme per le quali abbiamo installato le app sul telefono, tendiamo a riutilizzare sempre le stesse per comodità. Eppure, le password rimangono uno dei pilastri fondamentali della sicurezza informatica: sono la prima linea di difesa contro accessi non autorizzati, furti di identità e attacchi mirati. Nonostante l'avvento dell'autenticazione a più fattori e di sistemi biometrici (di cui parleremo più avanti), la robustezza delle password è ancora essenziale.

Diverse sono le regole da seguire per cercare di scegliere password complesse. Il primo principio da tenere a mente è la lunghezza. Una password breve, anche se complessa, può essere più facilmente violata rispetto a una frase lunga e apparentemente semplice. Le cosiddette *passphrase*, sequenze di parole che creano una frase facilmente memorizzabile, offrono in linea di massima una resistenza superiore agli attacchi automatizzati. Ad esempio, una passphrase come "FlyingGreenCatPaintsBlue$1999" può sembrare articolata, ma in realtà è possibile memorizzarla ed è molto più difficile da intercettare rispetto a una parola complessa di pochi caratteri. Ogni carattere aggiunto, infatti, aumenta il numero di combinazioni necessarie a trovare la parola d'ingresso e violare l'account (anche se con l'arrivo dell'Intelligenza

Artificiale la questione è diventata un po' più complessa di come la raccontiamo). Diciamo che vale ancora la regola in base alla quale la lunghezza è un requisito importante, anche se assolutamente non esaustivo.

La seconda regola che non dobbiamo dimenticare è quella della non banalità. Abbiamo citato il caso del Louvre, ma sappiamo bene che ancora oggi una delle password più diffuse al mondo è una banale sequenza di numeri che va da 0 a 9. Nello scegliere una password dovremo sforzarci di non fare riferimento a dati personali facilmente reperibili online o a semplici combinazioni di parole. Tra i suggerimenti più simpatici ascoltati da un esperto di sicurezza informatica quello di scegliere una frase scritta nel dialetto della propria città. Questa, infatti, contiene parole che non sono nei vocabolari tradizionali e questo aspetto la rende più "sicura" rispetto alla possibilità che negli attacchi di forza bruta o a dizionario si vadano a provare combinazioni di parole. Inoltre, le frasi in dialetto potrebbero avere un'altra caratteristica interessante, ovvero quella di essere ricordate senza la necessità di essere scritte su bigliettini appoggiati sulla scrivania o su file denominati "password" e contenuti nel desktop del nostro portatile (pratiche da evitare sempre!).

Altro aspetto cruciale è quello dell'unicità: ogni servizio deve avere la sua password. Mai riutilizzare la stessa combinazione di lettere o parole per email, CMS della redazione, social network o altri servizi online. La logica è semplice: se un account viene compromesso, le altre credenziali non devono essere esposte. Qui entrano in gioco i password manager, strumenti sia a pagamento che gratuiti, che consentono di conservare tutte le password di accesso in un unico posto. I moderni password manager hanno

in realtà molte altre funzioni: generano password, permettono di loggarsi a servizi in maniera rapida e fluida, funzionano da app di autenticazione generando codici, e permettono di condividere password in modo sicuro con altri. Nel caso di gruppi strutturati e redazioni, può avere senso condividere una stessa cassetta di sicurezza digitale, che sincronizza le modifiche alle credenziali di accesso a più servizi per tutti i suoi membri.

In quanto alla frequenza con cui sceglierne di nuove, vale la pena sottolineare che le indicazioni del National Institute of Standards and Technology (NIST) americano sulle password hanno eliminato l'obbligo di cambiare frequentemente la password (ogni 90 giorni). Tale pratica, infatti, paradossalmente portava gli utenti a indebolirle. Dunque le linee guida consigliano di cambiare la password *solo* in caso di effettiva o sospetta compromissione.

Au-ten-ti-ca-zio-ne a due fattori: più facile a farsi che a dirsi

Oltre le password c'è di più. Siamo già abituati a sbloccare i telefoni inquadrando il nostro viso o passando con l'indice sul segnaposto dell'impronta. In alcuni casi usiamo la stessa modalità per autenticarci su alcuni servizi. Avere più modi per autenticarsi in un servizio online o per accedere a una piattaforma ci consente di difenderci qualora la password venga scoperta.

Quando si parla di più "fattori" ci si riferisce a diversi modi attraverso i quali possiamo confermare di essere noi a fare determinate operazioni. Il primo fattore di cui abbiamo già parlato è la password, ovvero qualcosa che

so. A questo posso aggiungere un secondo fattore di autenticazione, ovvero qualcosa che ho (per esempio uno smartphone dove mi arriva un codice tramite SMS o dove ho una app di autenticazione oppure ancora una chiavetta hardware). Il terzo fattore rappresenta qualcosa che sono, per esempio il mio volto o la mia impronta, ovvero il riconoscimento biometrico. Attivare più fattori di autenticazione è comprensibilmente qualcosa che mette maggiormente al sicuro gli "spazi virtuali".

Detto che è opportuno attivare un'autenticazione a più fattori praticamente per ogni piattaforma o servizio online che utilizziamo per il nostro lavoro, c'è da dire che anche questa modalità non è certo esente da rischi. Nel 2025 sono emerse campagne di phishing sofisticate che hanno bypassato proprio questo secondo livello di protezione. Uno di questi toolkit, chiamato Sneaky 2FA, si commercializza come "phishing-as-a-service": attraverso link ricevuti via email, le vittime vengono reindirizzate a pagine di login contraffatte di Microsoft 365, dove gli aggressori esfiltrano non solo le credenziali, ma anche i codici 2FA in tempo reale.

Tra i metodi 2FA più sicuri che possiamo scegliere ci sono le chiavi hardware che, come accennato in precedenza, richiedono un elemento fisico da conservare per poter effettuare un accesso. Invece le app di autenticazione rappresentano una migliore alternativa ai più vecchi SMS potenzialmente intercettabili, specialmente in attacchi mirati.

Un'altra modalità che si sta diffondendo è quella delle passkey basate sullo standard FIDO. Le passkey generano una coppia di chiavi: una privata, conservata in modo sicuro su un dispositivo dell'utente (ad esempio lo

smartphone, o una chiave di sicurezza fisica), e una pubblica, registrata presso il servizio a cui ci si autentica.

Al momento del login, il dispositivo firma una richiesta con la chiave privata, il cui utilizzo viene autorizzato dallo stesso criterio di sblocco del dispositivo (ad esempio, dati biometrici, PIN, sequenza).

In poche parole, le passkey incorporano il concetto di autenticazione a più fattori mediante la verifica dell'utente effettuata localmente sul dispositivo.

"Le passkey sono resistenti al phishing (...), non ci sono password da rubare e non ci sono dati di accesso che possono essere utilizzati per perpetuare gli attacchi", scrive la FIDO Alliance. Per usare una passkey sia il dispositivo che il servizio cui si accede devono supportare questa tecnologia. Qui l'elenco dei servizi che supportano passkey.

Certo, la sicurezza al 100% non esiste nemmeno nel caso di più fattori di autenticazione, in quanto le vulnerabilità software sono sempre dietro l'angolo. Ad esempio, Yubico a inizio 2025 ha confermato una vulnerabilità nel software di supporto per le chiavi hardware su sistemi macOS e Linux, ora risolta: in alcune configurazioni, un attaccante con accesso locale e la conoscenza della password avrebbe potuto bypassare l'autenticazione con chiave di sicurezza.

Chiaramente con l'evolversi delle metodologie di protezione si evolvono anche le modalità di attacco. Ma questo non deve scoraggiarci nel cercare soluzioni che, come nel caso dell'autenticazione a più fattori, abbassano il livello di rischio generale.

Programmi di protezione avanzata

Qualora sia necessario considerare un livello alto di attenzione e protezione, è possibile ricercare programmi di protezione avanzata specifici. Uno di quelli disponibili nel momento in cui scriviamo è il Programma di Protezione Avanzata di Google, un sistema di sicurezza studiato per proteggere gli account Google degli utenti ad alto rischio di attacchi mirati, come giornalisti, attivisti e figure con alta visibilità o dati sensibili.

Il programma richiede l'uso di chiavi fisiche di sicurezza o passkey, ovvero impedisce l'accesso alla casella di posta con i soli nome utente e password. La protezione non si limita al momento del login, visto che il programma restringe severamente l'accesso ai dati: solo le app Google e pochissime app di terze parti, accuratamente verificate, possono infatti interagire con il tuo account. Tutto il resto viene bloccato automaticamente. Anche i download e le installazioni sono sottoposti a controlli molto più rigorosi: le app possono essere installate solo da store verificati e ogni anomalia viene segnalata con tempestività.

A questo si aggiunge una scansione approfondita delle email in arrivo, pensata per identificare e bloccare tentativi di phishing e malware che potrebbero sfuggire ai filtri standard.

Anche Meta ha sviluppato strumenti dedicati. Su Facebook, ad esempio, esiste una modalità di protezione avanzata, pensata per chi subisce campagne di minacce o tentativi di intrusione negli account social. Attivarla significa avere controlli più rapidi sugli accessi da dispositivi

sospetti, una gestione più severa delle informazioni di recupero dell'account e una maggiore protezione della propria attività pubblica, come le liste di contatti o le interazioni con pagine sensibili. Sono impostazioni che non richiedono competenze tecniche particolari, ma solo un po' di tempo da dedicare a cercare come si attivano direttamente dal proprio profilo.

Accanto a questi programmi strutturati, esistono altri strumenti e soprattutto regole che dovremmo fare nostre per scegliere di volta in volta lo strumento migliore (che non sempre è l'email) per comunicare con qualcuno.

In breve:

- ✓ l'email è uno spazio importante da proteggere in modo adeguato;
- ✓ non fidarti di messaggi email che trasmettono un senso di urgenza oppure seguono modalità e procedure anomale;
- ✓ scegli password o passphrase lunghe, non ovvie e attiva l'autenticazione a più fattori per abbassare il livello di rischio;
- ✓ privilegia le app di autenticazione sugli SMS, le passkeys o le chiavette hardware sulle app;
- ✓ se non hai nemmeno ancora attivato la 2FA, intanto inizia a metterla con un SMS, e poi avanza di livello.

4. NELLA GIUNGLA DELLE IMPOSTAZIONI SOCIAL DI SONIA MONTEGIOVE

Quando parliamo di sicurezza informatica dei giornalisti e degli attivisti, a volte ci si concentra sulle minacce più note come malware, phishing, spyware, dimenticando che anche una condivisione non consapevole sui social network può esporre a rischi importanti. Non a caso, anche l'Ordine nazionale dei giornalisti, in una delle diverse revisioni del codice deontologico, ricorda che il decoro e la dignità professionale passano da qualsiasi strumento di comunicazione (social inclusi). Una condivisione sbagliata, un profilo pubblico, una platea con cui si condivide qualcosa che non è quella che si credeva, un troll che diventa stalker, una foto che rivela dettagli che non dovevano essere pubblici sono solo alcuni esempi di problemi che si possono incontrare nelle nostre giornate social.

Cercare tra le diverse impostazioni delle piattaforme social quella che può abbassare i livelli di rischio della condivisione non è banale. Muoversi in una "giungla" di consensi, filtri, bottoni può portare via tempo, ma rappresenta comunque un buon investimento.

Oltre alla sicurezza: gestisci privacy e contatti

Per molti giornalisti e attivisti - anche per ragioni di visibilità e di diffusione dei contenuti scritti - la tentazione di lasciare i profili social completamente aperti e accessibili è molto alta. Profili pubblici, impostazioni standard, massima raggiungibilità. Spesso lo si fa quasi in risposta al tipo di lavoro: costruisco informazione pubblica, dobbiamo poter essere visti, cercati e contattati da chiunque. Questo tipo di atteggiamente

porta con sé alcune vulnerabilità e per questo è opportuno mantenere il controllo sulle proprie condivisioni: decidere chi può vedere cosa, chi può scrivere, chi può interagire e quali informazioni si stanno consegnando ad altri.

Una prima possibilità da considerare è quella di separare i profili social personali da quelli professionali. Avere un profilo pubblico, aperto, pensato per il lavoro, permette di gestire la comunicazione con colleghi, fonti e lettori senza esporre aspetti della propria quotidianità e della vita personale. Parallelamente, un profilo privato, accessibile soltanto a persone conosciute delle quali ci si fida, con le impostazioni sulla privacy molto ristrette, diventa uno spazio per amici e relazioni autentiche. Anche se va ricordato che anche nelle modalità più private, dovremmo sempre considerare pubblico, o potenzialmente pubblico, tutto ciò che postiamo.
Questo perché se si vuole colpire un attivista o un giornalista si parte dal raccogliere informazioni sulla sua vita privata, sulle sue relazioni e sulle sue abitudini. Foto condivise, abitudini ricorrenti, luoghi frequentati, affetti. È la cosiddetta profilazione invisibile, un'analisi silenziosa che ricostruisce le nostre ritualità che potrebbero essere usate contro di noi per un attacco mirato.

Le impostazioni di privacy che possiamo scegliere dai setting delle diverse piattaforme social ci consentono di entrare nel dettaglio del chi può vedere cosa. Cercarle, capire come funzionano e attivarle è un buon investimento di tempo. Purtroppo, le piattaforme cambiano continuamente: funzioni che prima erano nascoste diventano predefinite, pulsanti a cui eravamo abituati vengono spostati, nuovi strumenti diventano disponibili a tutti. Per questo

è utile fare un controllo periodico (se non una volta al mese, magari ogni trimestre?) per vedere chi può leggere i post, chi può inviarci messaggi, se una persona può trovare il nostro numero di telefono o l'email facilmente, quali app sono collegate al profilo e quali dati queste app possono raccogliere. È una forma di "igiene digitale" essenziale quanto aggiornare un software installato sul nostro computer.

Come già accennato sopra, una regola semplice ed efficace rispetto alla condivisione potrebbe essere quella di chiedersi se è opportuno che quel messaggio, foto, video possa un giorno diventare pubblico, per sempre. Pubblico perché, anche condividendo qualcosa in una chat cifrata e privata o in un profilo blindato, potrebbe sempre esserci una persona pronta a portare fuori quel contenuto in pochi semplici gesti. Per sempre perché rimuovere un contenuto diventato pubblico può essere molto complicato. La domanda da farsi prima di pubblicare qualsiasi cosa è quindi: sarei a mio agio se questo contenuto lo vedessero tutte le persone per un tempo illimitato?

Se la risposta è no, è meglio non condividere.

L'amico del tuo amico non è tuo amico

Nella nostra vita "reale", nel momento in cui una persona di cui ci fidiamo ci presenta un amico, quella presentazione crea automaticamente un ponte di fiducia. Il contesto è chiaro, si capisce chi abbiamo davanti e perché siamo stati messi in contatto. L'amico del tuo amico diventa a volte anche amico tuo. Questa dinamica non funziona allo stesso modo sui social network, dove l'amico di un amico potrebbe essere una persona

completamente sconosciuta e che non ha alcun rapporto con la persona che conosciamo. Un contatto di un nostro contatto può essere qualsiasi cosa: un profilo falso creato ad hoc, un troll riciclato con un nome nuovo, un attivista che vuole orientare le nostre percezioni, una fonte manipolata da terzi o perfino qualcuno che mira a ottenere informazioni sensibili. Il legame "ho amici in comune" non è una garanzia: è solo un'illusione di vicinanza.

Per questo, prima di accettare una richiesta - anche se si vedono tre, quattro o venti amici condivisi - occorre fermarsi un momento e chiedersi:

- ✓ Chi è davvero questa persona?
- ✓ Perché vuole aggiungermi?
- ✓ Che cosa potrà vedere del mio profilo se accetto?
- ✓ Che informazioni sto aprendo?

Nei casi peggiori, quello che sembra un semplice "amico dell'amico" può trasformarsi in un osservatore silenzioso: qualcuno che fa monitoraggio di ciò che si pubblica, di chi commenta i tuoi post, di quando siamo online e perfino del luogo da dove ci connettiamo. Per questa ragione, ogni richiesta di collegamento va valutata bene, soprattutto se si sta gestendo un profilo personale dove vengono condivisi particolari delle nostre giornate che non è opportuno vedano tutte le persone.

Troll, molestie, minacce

Prima o poi succederà: arriverà il commento fuori luogo, la provocazione gratuita, la minaccia velata o esplicita. I social amplificano un po' tutto: il dibattito, il dissenso, ma soprattutto la violenza verbale di chi vuole colpire senza assumersi alcuna responsabilità. Imparare a riconoscere chi si ha "di fronte" è una forma di protezione.

Nelle interazioni quotidiane, è abbastanza frequente per esempio incontrare un *troll*, ovvero l'equivalente di un disturbatore da bar. Una persona che interviene solo per punzecchiare, provocare, cercare la rissa e che può far perdere tempo ed energia. Il troll contraddice a prescindere, provoca, istiga. Non sempre ha un obiettivo preciso: di sicuro cerca una reazione, qualsiasi reazione (meglio se scomposta, visto che questo gli consente di continuare nel suo flusso di conversazione carico di odio). In questo caso, la cosa migliore da fare è non rispondere (il celebre "*don't feed the troll*"). Ignorare spesso blocca ogni tentativo di alzare la curva dell'odio.

Diversa è la situazione in cui a commentare sia una comunità di persone organizzate. In questo caso, non si ha a che fare con una singola persona, ma con una piccola "macchina da guerra" che vuole spostare l'opinione pubblica e che è ben organizzata per essere presente in diverse conversazioni. Questo scenario si riconosce dal fatto che i commenti arrivano in modo ripetitivo, a volte da account appena creati, con stesse frasi incollate sotto post diversi. Per difendersi, in questo caso, è necessario segnalare alla piattaforma qualora si notino delle violazioni delle regole di comunità del social oppure limitare i commenti attivando una moderazione preventiva. In generale, è utile prevenire queste situazioni limitando nelle

impostazioni di privacy delle piattaforme chi può inviarci messaggi diretti, chi può postare sulla nostra bacheca, o anche chi può commentare sotto i post.

Nel flusso delle conversazioni social, può poi capitare di notare che le provocazioni si trasformano in vere e proprie minacce o intimidazioni. In questo caso, è preferibile documentare tutto attraverso degli screenshot o salvando intere pagine come prova, segnalare alla piattaforma, informare la redazione o l'organizzazione per la quale si lavora e valutare una denuncia alle autorità. Per capire quanto una minaccia possa essere seria, alcuni suggeriscono di usare la regola dei tre livelli:

1. Specificità: contiene dettagli reali sulla tua vita?
2. Ripetitività: è un episodio isolato o sta crescendo nel tempo?
3. Verosimiglianza: questa persona ha o sembra avere accesso a informazioni concrete su di te?

Se due di questi tre elementi sono presenti, è preferibile documentare prima e segnalare o denunciare poi.

In breve:

✓ Gestisci la tua visibilità e privacy nelle impostazioni, e separa i profili social di lavoro da quelli personali;

✓ Valuta con attenzione le richieste di contatto;

✓ Riconosci e difenditi in anticipo da troll e minacce.

5. PRONTO? HO INFORMAZIONI RISERVATE DI CAROLA FREDIANI

Nello scandalo americano Watergate, che portò alle dimissioni del presidente Nixon, il giornalista Bob Woodward incontrava la sua fonte - che dopo si scoprì essere Mark Felt, ex vicedirettore dell'Fbi, ma che all'epoca venne ribattezzata Gola profonda - in un parcheggio sotterraneo, dopo essersi "messaggiati" attraverso un sistema che includeva un vaso spostato sul balcone del giornalista (se lui voleva il contatto) o un cerchio a penna sulla pagina 20 del New York Times consegnato a Woodward (se Felt voleva il contatto). Oggi buona parte degli approcci tra fonti e giornalisti passano per diversi tipi di comunicazioni online o telefoniche. La facilità con cui si può arrivare a chiunque in pochi minuti rispetto al passato rischia di far dimenticare la probabilità che quelle interazioni siano facilmente tracciabili.

Il primo contatto

Giornalisticamente, da questo punto di vista, l'osso più duro è il primo contatto tra una fonte e un giornalista (o un attivista che raccolga segnalazioni di reati o malversazioni). Perché, una volta creato il canale di comunicazione, è più facile accordarsi per parlare in modo più protetto. Ma il primo contatto (via mail, telefono o messaggio sui social) è una traccia che resta anche a posteriori. Se la storia segnalata cresce di importanza, quella traccia potrebbe inchiodare la fonte.

In gergo questo scoglio viene chiamato il "problema del primo contatto", ovvero quando una fonte si rivolge a un canale che potrebbe compromettere immediatamente la sua riservatezza.

Come sempre accade nella sicurezza digitale, non ci sono soluzioni immediate e universali. Sicuramente può essere utile, per un giornalista investigativo, pubblicizzare il più possibile tutti i modi in cui si può essere contattati in modo relativamente sicuro a seconda del profilo del segnalatore. Come ha fatto la redazione del Washington Post che ha pubblicato una pagina per chi desideri contattarla, dove si può scegliere fra mail cifrate, Signal, Whatsapp, o piattaforme che facilitano comunicazioni anonime come Securedrop. Sta a chi segnala scegliere la più adatta, ma l'ideale sarebbe dare, nella stessa pagina che le raccoglie, anche qualche indicazione di come e quando usarle, proprio perché non tutti sono consapevoli dei rischi.

Anche Le Monde ha una pagina simile, che fornisce diverse opzioni. Tra queste, inviare una mail cifrata con PGP, per i più esperti. Oppure creare un account ProtonMail secondario (in pratica creato apposta), per i meno esperti. Meglio mantenersi comunque generici al primo contatto, consiglia il giornale francese, in modo da approfondire quando il canale è considerato più sicuro.

Il Guardian è particolarmente solerte nello spiegare pro e contro dei vari canali. Ad esempio, nel caso si scelga di mandare una mail, anche cifrata, il giornale offre le seguenti raccomandazioni: "Non utilizzare il tuo indirizzo email personale o di lavoro abituale. Crea un nuovo account email da usare esclusivamente per comunicare con il Guardian. Fallo da un computer che

non possa essere facilmente ricondotto a te. Quando crei un nuovo account email, assicurati che le informazioni fornite durante la registrazione non possano ricondurre l'account a te. Non utilizzare mai la stessa password per account diversi".

Molti ovviamente includono anche la buona vecchia lettera di carta anonima, un sistema relativamente sicuro (anche se oggi in molti casi tocca comunque entrare in un ufficio postale per spedirla, e ovviamente ciò ne diminuisce il potenziale di anonimato). Un sistema che non si presta bene se c'è la necessità di dialogare. Inoltre, può indurre un errato senso di sicurezza. Se n'è parlato molto nel caso di Reality Winner, la contractor dell'intelligence Usa e whistleblower arrestata per aver passato alla stampa (inviandolo per posta) un documento. Che conteneva dei "punti di tracciamento" invisibili che mostravano "esattamente quando e dove un documento, qualsiasi documento, viene stampato", scriveva l'esperto di sicurezza Rob Graham.

Questo genere di pagine di contatto - del Washington Post, di ProPublica e di altre testate - si sono moltiplicate dopo le rivelazioni di Edward Snowden nel 2013, quando i media capirono due cose: che la sorveglianza delle comunicazioni era più potente di quello che immaginavano; e che contattare in modo sicuro i loro giornalisti, molti dei quali non erano certo nativi digitali, era un'impresa.

Sono rimasti nella storia i molteplici tentativi di Snowden di convincere il giornalista Glenn Greenwald a usare la cifratura per comunicare assieme. Greenwald rischiò di perdere lo scoop del decennio per la sua noncuranza

digitale. Come racconta il tecnologo Micah Lee al riguardo: “Snowden aveva inviato una email a Glenn Greenwald, giornalista del Guardian e cronista degli eccessi della guerra al terrorismo, ma Greenwald non usava la crittografia e non aveva il tempo di aggiornarsi, così Snowden è andato avanti. Come è ormai noto, Snowden decise di contattare la Poitras [Laura Poitras, altra giornalista che sarebbe divenuta centrale nelle rivelazioni Snowden, ndr] perché lei usava la crittografia. Ma non aveva la sua chiave di crittografia, necessaria per inviare email criptate, e la chiave non era stata pubblicata sul web. Snowden, straordinariamente esperto di come viene monitorato il traffico Internet, non voleva inviarle un'email non criptata, anche solo per chiederle la chiave. Quindi doveva trovare qualcuno di cui riteneva di potersi fidare, che avesse la sua chiave e che usasse la posta elettronica criptata. Ero io”.

Le normali telefonate, e soprattutto gli SMS, sono da considerarsi del tutto insicuri. In particolare, gli SMS possono essere letti da una serie di terze parti: operatori telefonici, forze dell'ordine, intelligence (del tuo o di altri Paesi), criminali e spioni di varia natura. “Possiamo tranquillamente considerarli delle cartoline”, ha affermato Daniel Kahn Gillmor, tecnologo dell'American Civil Liberties Union. “Tutti lungo il percorso possono vederli”.

Anche per questo, nell’autenticazione a due fattori si dovrebbe smettere di usare gli SMS per ricevere i codici (alert: meglio tenersi gli SMS che non avere alcuna autenticazione a due fattori). A dirlo da anni sono una pletora di ricercatori di sicurezza. E la Cybersecurity and Infrastructure Security Agency (CISA), l’agenzia Usa per la cybersicurezza e la protezione delle

infrastrutture critiche, che dopo un clamoroso caso di cyberspionaggio di origine cinese a degli operatori telefonici americani, ha emanato una serie di indicazioni pratiche. Tra queste, usare le comunicazioni cifrate. E "non utilizzare gli SMS come secondo fattore di autenticazione. I messaggi SMS non sono crittografati: un malintenzionato che abbia accesso alla rete di un operatore di telecomunicazioni e intercetti questi messaggi può leggerli. [Inoltre. ndr] l'autenticazione a più fattori tramite SMS non è resistente al phishing e quindi non costituisce un'autenticazione forte per gli account di persone prese di mira". Anche se la CISA aggiunge, giustamente, che comunque alcuni servizi online potrebbero utilizzare gli SMS come impostazione predefinita durante le procedure di recupero dell'account; e quindi che potrebbe non essere possibile eliminare completamente i messaggi SMS dal servizio.

Si tratta comunque di un caso, e una finestra, molto specifici.

In breve:

- ✓ Telefonate, sms e email in chiaro non sono sistemi sicuri;
- ✓ Se sei una testata o un giornalista, dotati di strumenti di comunicazione sicura e annuncia tutte le modalità di contatto;
- ✓ Se sei una fonte, informati prima sui canali a disposizione, e scegli quelli che più si adattano alle tue capacità, e al tuo livello di rischio.

Non tutte le cifrature sono uguali di RAFFAELE ANGIUS

Il principio su cui si basa la protezione delle comunicazioni è la crittografia end-to-end, sistema che garantisce che il contenuto di un messaggio possa

essere letto solo da chi lo invia e da chi lo riceve. Tutti i soggetti intermedi – server, router, provider– non dispongono delle chiavi per decifrarlo. La crittografia end-to-end è, quindi, una barriera tecnologica che impedisce l'accesso anche al gestore del servizio stesso. Senza questa protezione, ogni messaggio potrebbe teoricamente essere intercettato, archiviato o analizzato.

Le due applicazioni di messaggistica più diffuse che adottano questa tecnologia sono WhatsApp e Signal. Entrambe utilizzano lo stesso protocollo di cifratura, chiamato Signal Protocol, ma differiscono per filosofia e struttura.

Signal è sviluppata da una fondazione indipendente e senza scopo di lucro, la Signal Foundation, che pubblica integralmente il proprio codice sorgente. Ciò significa che chiunque – ricercatori, esperti di sicurezza, utenti – può analizzare il codice, verificarne la solidità e segnalare eventuali vulnerabilità. La trasparenza è la base della fiducia: l'open source consente un controllo pubblico costante e impedisce che la sicurezza dipenda esclusivamente dalle dichiarazioni del gestore del servizio. Signal, inoltre, raccoglie pochissimi dati: non conserva elenchi di contatti, non registra la cronologia delle conversazioni e non tiene traccia dei metadati che descrivono le interazioni. Questo riduce drasticamente la quantità di informazioni che potrebbero essere esposte in caso di violazione o di richiesta delle autorità.

WhatsApp, pur impiegando lo stesso schema di cifratura, appartiene a un ecosistema chiuso e commerciale, controllato da Meta, azienda che basa la propria attività economica sulla profilazione degli utenti. Il codice non è

pubblicamente accessibile e, quindi, non è possibile sapere con certezza in che modo il protocollo venga implementato. Anche se la cifratura end-to-end protegge i messaggi, i metadati – cioè le informazioni su chi parla con chi, quando e quanto spesso – restano visibili ai server di WhatsApp e vengono utilizzati per finalità di analisi e integrazione con altri servizi del gruppo. La differenza, dunque, non sta solo nel grado di protezione del messaggio, ma anche nella governance del sistema: un'infrastruttura chiusa e a fini commerciali non può offrire le stesse garanzie di un progetto trasparente e indipendente.

Immaginiamo che uno Stato decida di chiedere al fornitore del nostro sistema di messaggistica il contenuto dei nostri messaggi. Né Whatsapp né Signal sarebbero in grado di rispondere positivamente a tale richiesta in quanto, come detto, il sistema di cifratura end-to-end impedisce allo stesso gestore del servizio di leggere i messaggi degli utenti. Tuttavia Whatsapp potrebbe sempre fornire i metadati, rivelando con chi abbiamo parlato o scambiato messaggi, per quanto tempo ed eventualmente di quale dimensione (questo rivelerebbe per esempio uno scambio di documenti o immagini). Ancora, per Whatsapp occorre stare attenti ad abilitare la cifratura del cloud, se lo si usa, in quanto i backup diversamente non sarebbero protetti.

Un caso a parte è quello di Telegram, spesso descritto in modo errato come una piattaforma "più sicura". Le chat ordinarie di Telegram non sono cifrate end-to-end: i messaggi vengono salvati sui server dell'azienda e possono essere letti dai suoi sistemi. Solo attivando manualmente le *chat segrete* si ottiene un livello di protezione simile alla cifratura end-to-end.

Tuttavia, Telegram utilizza un algoritmo crittografico proprietario, sviluppato internamente e non sottoposto a revisione pubblica da parte della comunità scientifica. Questo rappresenta un limite sostanziale: l'autosviluppo di sistemi crittografici, senza verifica esterna, espone a rischi imprevedibili, poiché la sicurezza non può mai essere garantita dalla segretezza del codice, ma solo dalla sua analisi aperta e continua. A ciò si aggiunge che il codice dei server di Telegram non è interamente open source, e quindi non è possibile sapere come vengano gestiti, archiviati o eventualmente condivisi i dati degli utenti, ma solo se il client è sicuro.

Oltre alle applicazioni più diffuse, esistono piattaforme che hanno scelto di costruire la propria identità intorno alla sicurezza e alla trasparenza. Due esempi significativi, entrambi europei, sono Threema e Wire, che rappresentano due approcci diversi ma complementari alla protezione delle comunicazioni digitali.

Threema, sviluppata in Svizzera, adotta la crittografia end-to-end per impostazione predefinita su messaggi, chiamate vocali, file e chat di gruppo. A differenza della maggior parte delle app di messaggistica, non richiede di associare un numero di telefono o un indirizzo e-mail: ogni utente riceve un identificativo casuale, il Threema ID, che consente di comunicare senza dover rivelare dati personali.

Il codice dei client è completamente open source e può essere analizzato pubblicamente, mentre il codice del server rimane proprietario. L'azienda consente tuttavia audit indipendenti periodici, e la gestione dei dati avviene su server situati in Svizzera, soggetti a una legislazione sulla privacy tra le più rigorose al mondo. Threema è un'app a pagamento, scelta che riflette

una precisa opzione etica: sostenersi con il contributo diretto degli utenti invece che con la raccolta di dati o pubblicità.

Wire, fondata nel 2014 da un gruppo di ex ingegneri di Skype e oggi con sede in Svizzera e Germania, offre una cifratura end-to-end attiva per impostazione predefinita in tutte le conversazioni. Il suo protocollo crittografico è open source ed è stato sottoposto a audit di sicurezza indipendenti, che ne hanno confermato la solidità. Anche il codice dei client e gran parte del codice server sono pubblici e verificabili su repository dedicati, pur con alcune componenti infrastrutturali non completamente documentate. Wire è progettata sia per l'uso individuale sia per quello professionale e organizzativo, integrando strumenti di amministrazione e collaborazione di gruppo. In questo contesto conserva alcuni metadati tecnici necessari al funzionamento multi-dispositivo e alla sincronizzazione, ma non archivia i contenuti delle conversazioni. L'azienda dichiara di minimizzare i dati raccolti e di non costruire grafi sociali completi degli utenti, anche se alcuni elementi del traffico di rete restano visibili ai server per motivi operativi.

In conclusione, occorre rilevare che il punto non è trovare un'app che risponda a ogni esigenza, ma dotarsi di un ecosistema che ci metta in grado di comunicare con i nostri interlocutori in modo sicuro e pratico. In tal senso, il livello di base è garantito da Whatsapp, le cui caratteristiche di sicurezza garantiscono un ecosistema sicuro per le conversazioni di tutti i giorni. Tuttavia, un minimo di flessibilità e di lettura del contesto può indurci a chiedere a un interlocutore di passare a strumenti più sicuri, come Signal, qualora la situazione lo richieda.

Comunicare con le fonti proteggendone le identità di RAFFAELE ANGIUS

La riservatezza, nel mondo digitale, non coincide sempre con l'anonimato. La crittografia end-to-end protegge il contenuto dei messaggi, ma non necessariamente nasconde chi comunica con chi, quando o da dove. Per ridurre ogni traccia, serve uno strumento capace di nascondere non solo le parole, ma anche i percorsi che le trasportano. È qui che entra in gioco Tor, acronimo di The Onion Router.

Tor è una rete di comunicazione che permette di navigare e scambiare dati in modo anonimo e decentralizzato. È stata sviluppata a partire dagli anni Novanta da un gruppo di ricercatori del Naval Research Laboratory statunitense, ed è poi passata alla gestione della fondazione Tor Project, un'organizzazione senza scopo di lucro con sede negli Stati Uniti.

Il suo principio di funzionamento si basa sulla tecnica dell'instradamento a cipolla: ogni connessione viene cifrata più volte e fatta passare attraverso una serie di nodi casuali nella rete Tor, ciascuno dei quali rimuove solo uno strato di cifratura senza conoscere l'origine né la destinazione finale del pacchetto. In questo modo, nessun nodo singolo ha una visione completa della comunicazione, e risalire all'identità o alla posizione dell'utente diventa estremamente difficile. Tuttavia, la cosa più importante da sapere è banalmente come lo si utilizza. Di fatto, l'interfaccia di Tor è costituita da una versione modificata del noto browser Mozilla Firefox: è sufficiente scaricare il client dal sito del Tor Project e aprirlo sul proprio pc per venire direttamente instradati sulla rete della cipolla (parliamo più in dettaglio di Tor a seguire).

Il whistleblowing

Tra i progetti che sfruttano questo principio di anonimizzazione c'è GlobaLeaks, un software open source sviluppato dal Centro Hermes per la Trasparenza e i Diritti Umani Digitali, un'organizzazione italiana impegnata nella tutela della privacy e nella promozione della trasparenza. GlobaLeaks fornisce una piattaforma per la segnalazione anonima e la condivisione sicura di documenti o informazioni sensibili, usata da numerose redazioni giornalistiche e organizzazioni civiche in tutto il mondo.

Tra queste figurano anche testate italiane come IrpiMedia e Wired, che hanno implementato sistemi basati su GlobaLeaks per ricevere materiale da fonti anonime. Una delle sue caratteristiche fondamentali è la possibilità di configurare l'accesso esclusivamente tramite Tor, impedendo qualunque connessione diretta da Internet "tradizionale". In questa modalità, chi invia i file o le informazioni resta anonimo anche nei confronti di chi gestisce la piattaforma: il sistema non registra indirizzi IP, non utilizza cookie di tracciamento e cancella automaticamente i metadati dai documenti caricati.

GlobaLeaks consente di creare canali di whistleblowing personalizzati, con percorsi differenziati per categorie di segnalazione, gestione dei messaggi cifrati e scambio di repliche tra la fonte e il destinatario in un ambiente completamente isolato e cifrato. Ogni segnalazione avviene attraverso un'interfaccia web sicura, dove la fonte riceve un codice univoco che consente di rientrare in seguito per verificare eventuali risposte.

Installare GlobaLeaks è un processo relativamente accessibile con poche nozioni di informatica. È infatti sufficiente avere un server sul quale far girare il software e, grazie alla documentazione particolarmente precisa, è possibile realizzare l'installazione in una manciata di minuti, a patto che si conoscano i rudimenti della gestione sicura di un server. Anche sul lato *client* la configurazione di GlobaLeaks è particolarmente intuitiva, permettendo di creare diversi percorsi o anche questionari da sottoporre al segnalante prima che possa effettivamente completare l'invio.

Dal punto di vista giornalistico, il percorso che l'utente deve seguire per inoltrare una segnalazione è particolarmente importante: senza rivelare la propria identità - a meno che non sia lo stesso segnalante a volerlo - può essere importante rispondere a domande che chiariscano se la persona può essere in pericolo per via delle informazioni in suo possesso o può essere utile chiarire se siano informazioni "esclusive" oppure già note pubblicamente. Ciascuna installazione offre dunque numerose possibilità di personalizzazione, sempre tenendo l'usabilità al centro del processo, in modo da non far scappare i segnalanti.

Accanto a GlobaLeaks, un altro strumento utilizzato da molte testate internazionali è SecureDrop, sviluppato originariamente da Aaron Swartz e poi mantenuto dalla Freedom of the Press Foundation. Anche in questo caso si tratta di un software open source che permette di ricevere documenti e messaggi in modo completamente anonimo e cifrato attraverso la rete Tor.

SecureDrop è concepito specificamente per le redazioni giornalistiche: ogni installazione funziona su server indipendenti. Le fonti possono caricare

materiali in forma cifrata, mentre i giornalisti li consultano su un sistema isolato, utilizzando chiavi di sicurezza dedicate. Nessun dato di connessione o identificativo viene conservato, e la comunicazione tra fonte e redazione avviene attraverso un'interfaccia onion raggiungibile solo via Tor.

In entrambi i casi, è centrale la diffusione di tali strumenti. Come per una email o un numero di telefono, è fondamentale che il potenziale segnalante trovi istruzioni chiare e semplici per accedere alla piattaforma in modo da inoltrare una segnalazione, così come farebbe usando un banale (ma evidentemente non sicuro) servizio di posta elettronica.

6. IL TUO COMPUTER E TELEFONO SONO TUTTO DI ROSITA RIJTANO

Quando il giornalista Mauro De Mauro venne rapito per poi non essere mai più ritrovato, a sparire fu anche l'ultimo materiale che aveva raccolto. Una "micidiale bonifica": così la Corte d'appello di Palermo definì il repulisti di tutto ciò che avrebbe potuto rivelare il destino toccato al cronista del quotidiano L'Ora, impegnato in un'indagine sulla morte dell'ex presidente dell'Eni, Enrico Mattei. Registrazioni, documenti, appunti che oggi De Mauro avrebbe conservato in uno smartphone o in un laptop. Strumenti che, in un colpo solo, hanno rimpiazzato agende, magnetofoni e macchine fotografiche, diventando le scatole nere delle nostre vite, non solo professionali. Li portiamo sempre, ovunque, usandoli per appuntamenti e interviste così come per le foto di famiglia. Mai prima nella storia era stato possibile trovare così tante informazioni sensibili e/o riservate su di noi, sui nostri cari e sul nostro lavoro in un unico posto.

Proprio per via della loro centralità, questi dispositivi sono diventati un bersaglio. Non solo nei Paesi retti da regimi autoritari, dove le perquisizioni ai danni di giornalisti, attivisti e oppositori politici sono prassi consolidata, ma anche in contesti considerati democratici. Lo sa bene chi di recente è volato negli Stati Uniti, dove il numero di smartphone e laptop controllati alle frontiere - senza la necessità di un mandato - quest'anno ha toccato un nuovo record: stando ai dati della polizia di frontiera e delle dogane USA, da aprile a giugno 2025 sono stati più di 15 mila i dispositivi finiti al vaglio degli agenti, con un +17% rispetto all'ultimo picco, raggiunto nello stesso periodo del 2022. Una pratica più volte

denunciata dal Committee to Protect Journalists perché "lesiva della libertà di stampa". E non mancano gli esempi nel continente europeo. Ma a volte non serve l'intervento di un'autorità o un attacco mirato per mettere a rischio un'inchiesta che magari dura da anni: basta che il dispositivo venga rubato o lasciato sul tavolino di un bar. È la loro esposizione costante - smarrimenti, furti, controlli - a rendere urgente una maggiore consapevolezza su come proteggerli, soprattutto considerando che al loro interno c'è tutta la nostra vita.

La regola aurea: cifrare il disco

Immaginiamo per un momento lo smartphone e il computer come una casa. Non una qualsiasi: la casa dove teniamo la nostra vita intera. Ogni stanza custodisce qualcosa di prezioso: un cassetto con le foto di famiglia, un armadio con le bozze mai pubblicate, un ripostiglio con le conversazioni private, cartelle piene di fatture e scambi di mail con fonti che hanno chiesto riservatezza. Ora, guardiamo la porta d'ingresso. Se è di legno sottile, basta una spallata per entrare e portare via tutto. Senza cifratura, i nostri dispositivi funzionano esattamente così. Se invece quella porta è d'acciaio, blindata, anche se qualcuno riesce a sollevare la casa e portarsela via, non potrà entrare. È questo, in sintesi, il potere della cifratura: rende il contenuto illeggibile a chi non possiede la chiave.

Tradotto: i dati vengono trasformati in un linguaggio incomprensibile, un codice che può essere "aperto" solo da chi ha la giusta chiave crittografica. La protezione può essere parziale o totale. C'è chi sceglie di cifrare singoli file o cartelle, come se ogni stanza avesse la propria serratura: è un livello di sicurezza alto ma più laborioso da gestire. Oppure si può preferire la strada

più semplice ed efficace nella maggior parte dei casi: blindare l'intera casa, cioè attivare la cifratura completa del disco (full-disk encryption). Una lezione che anche la Nasa ha imparato a caro prezzo. Era il 2012 quando un laptop aziendale che conteneva dati sensibili venne rubato dall'auto di un dipendente. "Sebbene il computer fosse protetto da password, il disco non era stato cifrato e le informazioni presenti sul laptop possono essere accessibili a persone non autorizzate", dichiarò all'epoca un dirigente dell'agenzia spaziale americana.

Bisogna fare attenzione alla robustezza della tecnologia che si sceglie per la cifratura, evitando servizi che non possiamo considerare affidabili al cento per cento. Su computer e laptop la procedura è ormai semplice, grazie a dei sistemi integrati. Windows integra BitLocker, macOS mette a disposizione FileVault, Linux offre LUKS: i primi due possono essere attivati tramite il pannello delle impostazioni, mentre LUKS deve essere configurato al momento dell'installazione del sistema operativo. Per recuperare i dati in caso di necessità, meglio dotarsi di una password di recupero, da trascrivere su un foglio di carta e salvare in un luogo sicuro, senza consentire lo sblocco tramite cloud o altri dispositivi, come uno smartwatch. Sugli smartphone siamo ancora più avanti: iPhone e Android più moderni sono cifrati di default.

Ma qui entra in gioco un dettaglio cruciale. Come spiega l'informatico forense Paolo Dal Checco, la cifratura da sola non basta: la chiave è l'anello debole. Se è troppo semplice, si scardina in pochi secondi. Con un attacco a forza bruta un computer può provare milioni di combinazioni ogni secondo. E, nonostante anni di sensibilizzazione, molti utenti continuano a scegliere

password deboli, esempio classico: 1,2,3,4,5. La differenza è netta: una sequenza di sei caratteri è da sconsigliare; una di almeno dodici - alfanumerica, con simboli e maiuscole/minuscole - alza la soglia al punto da rendere l'accesso proibitivo. Quello scarto "apparente" tra 6 e 12 caratteri è, in realtà, ciò che separa una casa sicura da una casa scassinata. È lì che si gioca la partita. Se puoi, scegli un codice alfanumerico lungo anziché il classico pin numerico (si tratta di un'opzione presente tra le impostazioni), evitando di credere che la biometria sia la panacea di tutti i mali: non solo perché le impronte, per esempio, possono essere replicate, ma anche perché è più facile costringerti a sbloccare il telefono con un dito che a rivelare una password memorizzata.

Infine, un dettaglio poco noto ma importante da considerare è lo stato AFU (After First Unlock), cioè la modalità in cui resta il telefono dopo il primo sblocco. In questa modalità, alcune chiavi crittografiche rimangono caricate in memoria e certi dati possono essere estratti. Se devi viaggiare in Paesi governati da regimi autoritari, la buona pratica è spegnere il telefono prima di separarsene. "Quando è possibile — prosegue Dal Checco — ci sono strumenti open source, come VeraCrypt, che permettono di creare un archivio cifrato di facciata, a cui affiancarne un altro dove custodire le informazioni davvero sensibili. Così puoi rivelare la password del primo senza svelare l'esistenza del secondo". È una tecnica avanzata, da usare con piena consapevolezza delle implicazioni legali del Paese in cui ti trovi. E qui entra un tema sensibile: cosa succede quando il computer viene sequestrato e sei costretto a rivelare le credenziali di accesso ai dati? La situazione cambia da Paese a Paese, da caso a caso. In alcuni ordinamenti,

il rifiuto può comportare delle sanzioni, se non persino il carcere. La difesa tecnologica, insomma, ha un limite umano.

Uno, due, cento backup (o almeno tre)

Immaginiamo di aver fatto tutto il possibile per proteggere il nostro dispositivo. Se però qualcuno lo ruba, rischiamo comunque di perdere le informazioni che contiene. A meno che non abbiamo già seguito la cosiddetta regola del tre. Si tratta di una buona pratica che prevede di avere due copie aggiuntive dei propri dati, oltre a quella presente sul device. Le copie vanno salvate su supporti diversi e custodite in luoghi distinti.

Un primo backup può essere fatto su un hard disk esterno cifrato, da conservare in un posto sicuro (esistono delle pen drive, con funzione di cifratura integrata). Un secondo backup, invece, conviene salvarlo sul cloud, accessibile via internet. Qui la cifratura diventa fondamentale per proteggere le informazioni da possibili attacchi informatici, e dagli occhi indiscreti del service provider. "Il cloud è un'estensione del proprio disco, dove i dati finiscono in chiaro anche se il proprio hard disk è cifrato", avverte l'esperto Paolo Dal Checco, raccomandando di cifrare sempre i file prima di caricarli online.

Molte applicazioni – come WhatsApp, Signal o Facebook Messenger – offrono un'opzione di cifratura nelle impostazioni per i backup. Per i file, uno strumento semplice e gratuito è CryptoMator, che permette di caricare documenti cifrati su Google Drive o Dropbox e continuare a lavorarci anche da remoto.

Un ulteriore livello di sicurezza si ottiene scegliendo un servizio cloud che adotti la cifratura end-to-end, cioè un sistema che cripta i dati sul dispositivo del mittente e li decifra solo su quello del destinatario, impedendo a terzi – compresi i fornitori – di accedere ai contenuti. Non tutti i servizi, però, funzionano allo stesso modo: Google Drive e Dropbox, ad esempio, cifrano i dati solo durante il transito. Questo vuol dire che Big G e Dropbox potrebbero avere accesso ai tuoi file, o consegnarli all'autorità giudiziaria in caso di necessità. Viceversa, Apple iCloud e ProtonMail garantiscono la protezione end-to-end. Nonostante ciò, la regola che gli esperti continuano a ripetere è semplice: è meglio non caricare affatto sul cloud i file davvero sensibili.

Dispositivi burner o da viaggio

Il 14 aprile 2025 il Financial Times ha rivelato che la Commissione europea aveva dotato i propri funzionari di smartphone e laptop da sfruttare una volta sola, per ridurre i rischi di spionaggio. L'occasione era una trasferta negli Stati Uniti per degli incontri organizzati dalla Banca Mondiale. Anche se la notizia è stata poi ridimensionata (l'uso di questi dispositivi sarebbe stato raccomandato, ma non imposto), ha riportato l'attenzione su un principio fondamentale: compartimentare, cioè usare dispositivi diversi per funzioni diverse.

Separare il più possibile la vita lavorativa da quella privata è una regola che vale anche per smartphone e computer. Si può scegliere, ad esempio, di utilizzare un telefono solo per determinati contesti – un viaggio internazionale o una manifestazione – e non impiegarlo per altro. In questo scenario, lo smartphone portato a una protesta non dovrebbe essere lo

stesso usato per chattare con gli amici o varcare una frontiera. Il numero andrebbe condiviso solo con chi ne ha davvero bisogno, evitando di collegare i diversi dispositivi alla stessa rete Wi-Fi o di usarli sempre dallo stesso luogo. Anche il trasporto va gestito con cautela: meglio non portare i due device insieme, a meno che uno non sia riposto in una Faraday bag. Queste borse schermate bloccano le emissioni elettromagnetiche, impedendo al device di trasmettere o ricevere segnali. In pratica, uno smartphone al suo interno non può comunicare né con le torri cellulari, né con le reti Wi-Fi, né fornire la propria posizione Gps. Il blocco della localizzazione è infatti uno degli usi più diffusi delle Faraday bag.

Michael Bazzell, tra i maggiori esperti di OSINT ed ex collaboratore dell'FBI, nel suo libro Extreme Privacy: What It Takes to Disappear in America (2019) racconta il proprio metodo: "Quando sono in viaggio, il mio telefono è sempre al mio fianco ed è il mio principale mezzo di comunicazione. Quando torno a casa, le cose cambiano. A circa cinque miglia da casa, metto il dispositivo in una borsa Faraday. Questo sacchetto impedisce a qualsiasi segnale di raggiungere o lasciare il telefono. Rimane lì fino alla mia successiva partenza. Poiché non è mai connesso a reti mentre si trova vicino a casa, non può rivelare la posizione della mia abitazione". Un discorso a parte lo meritano i cosiddetti burner phone, cioè telefoni poco smart, usa e getta, da sfruttare per comunicazioni temporanee, preservando la propria identità.

Ma pur senza arrivare a questi estremi, resta un principio facile da seguire: usare un dispositivo più pulito se si fa un viaggio in cui si rischia sorveglianza o sequestro dello stesso. Si può anche fare un backup del

proprio telefono e poi decidere per un reset. O si può solo optare per la cancellazione di specifiche app, foto e via dicendo. Tutto dipende sempre dal tipo di minaccia in cui possiamo incorrere. Minimizzare i dati equivale a minimizzare il danno.

L'ultimo viaggio del tuo vecchio device

Smaltire un vecchio dispositivo non è mai una questione banale. Dentro uno smartphone o un laptop non ci sono solo schede e circuiti: ci sono frammenti della nostra vita, dai messaggi alle foto, dalle credenziali di accesso agli appunti di lavoro. Per questo, prima di separarsene, bisogna seguire alcuni passaggi precisi. Il primo è semplice ma fondamentale: fare un backup. Copiare foto, video, documenti e qualsiasi altro ricordo digitale su un hard disk esterno o su un cloud sicuro evita rimpianti futuri. Una volta al sicuro, è il momento di "sganciare" il dispositivo da tutti i sistemi che lo riconoscono come nostro. Significa disattivare Dov'è su iPhone, togliere la geolocalizzazione su Android, scollegarlo da Amazon, dai password manager e perfino dall'antivirus: un modo per impedire che il nuovo proprietario possa ancora accedere a pezzi della nostra identità.

Poi arriva la parte più delicata: la cancellazione. Dal Checco avverte: "Non basta cancellare i file, occorre eliminare in modo sicuro tutti i dati residui." Un reset di fabbrica su smartphone e tablet è il minimo sindacale, ma sui computer serve qualcosa di più robusto. Su macOS c'è la funzione Inizializza disco dalla Recovery, che è sufficiente se in precedenza abbiamo attivato la cifratura. In caso contrario, sarà ancora possibile recuperare qualcosa: ecco perché il consiglio è sempre di cifrare il disco. Mentre su Windows si può ricorrere a software come BleachBit, CCleaner o Eraser.

C'è un dettaglio che spesso si dimentica: i vari account a cui è collegato il dispositivo, così come il cloud. Se dobbiamo disfarci del dispositivo perché è già stato compromesso, i cookie generati o rubati dagli attaccanti - e che vengono sfruttati da remoto - sopravvivono al reset del device da parte dell'utente. A meno che non vengano annullate le varie sessioni di accesso ai propri account accedendo ai singoli portali, con la verifica di eventuali ulteriori sessioni aperte e chiusura di ogni sessione non riconosciuta.

Per i più paranoici, e in caso di dubbi, la soluzione più drastica è anche la più sicura: rimuovere e distruggere fisicamente il disco, rigando le superfici o piantandoci un chiodo.

In breve:

- ✓ Cifra tutto il disco utilizzando un sistema di cifratura affidabile (come BitLocker, FileVault e LUKS);
- ✓ Chiave di sblocco lunga: almeno 12–14 caratteri, meglio una frase complessa;
- ✓ Su smartphone: preferisci codice alfanumerico al PIN standard; anche qui non stare sotto i 12 caratteri;
- ✓ All'occorrenza spegni il telefono prima di consegnarlo;
- ✓ Device diversi per funzioni diverse;
- ✓ Non smaltire un dispositivo senza aver fatto un'accurata procedura di cifratura/inizializzazione, o sovrascrittura (a seconda del dispositivo) o senza aver distrutto il disco.

7. PHISHING, MALWARE, SPYWARE: MANCA SOLO DARTH VADER DI ROSITA RIJTANO

All'inizio c'era il "principe nigeriano": una delle forme più note e primitive di phishing. Un'email in cui un sedicente dignitario chiedeva aiuto per trasferire somme di denaro da un conto all'altro, promettendo in cambio una percentuale. Col tempo, le truffe si sono evolute. Linguaggi, tecniche e strumenti si sono fatti sempre più sofisticati, fino ad arrivare all'intelligenza artificiale che può rendere ogni messaggio malevolo sempre più credibile.

Le email di phishing sono anche uno dei canali principali per diffondere malware: programmi pensati per infettare i computer, assumere il controllo dei sistemi e sottrarre informazioni sensibili. Tra le varianti più insidiose ci sono gli spyware, software spia capaci di infiltrarsi nei dispositivi e monitorare ogni attività. La cronaca dimostra che non si tratta di una minaccia confinata ai regimi autoritari. Queste "armi digitali" vengono impiegate anche dove i diritti sono tutelati. Governi, politici e aziende hanno usato - e usano - questi strumenti anche in Europa, contro giornalisti e attivisti. Uno degli ultimi casi scoperti ha per protagonisti proprio dei giornalisti italiani. Per difendersi, bisogna prima capire come funzionano questi attacchi. Conoscerli è il primo passo per costruire una consapevolezza reale e adottare strategie minime di autodifesa digitale.

Il sempreverde phishing

La prima grande campagna di phishing risale alla metà degli anni Novanta. Centinaia di utenti del provider statunitense AOL consegnarono le proprie password ai cybercriminali, convinti da email e messaggi che sembravano

provenire dallo staff della compagnia. Chiedevano di "verificare" il proprio account: un messaggio in apparenza credibile, ma che in realtà era opera dei cracker che avevano clonato l'interfaccia originale. Da allora il phishing è rimasto la minaccia informatica più diffusa. Fin dagli esordi, l'email è stata lo strumento preferito. Lo schema è sempre lo stesso: il mittente sembra appartenere a un'organizzazione affidabile - una banca, la posta, un servizio online - e il messaggio segnala un problema di sicurezza o di accesso. Per risolverlo, invita a cliccare su un link che rimanda a un sito contraffatto, costruito per imitare in ogni dettaglio quello autentico. L'utente inserisce le proprie credenziali, convinto di salvarsi da un rischio, e invece le sta consegnando ai truffatori.

Col tempo, lo schema si è adattato ai social network. Oggi il truffatore può creare copie di profili e pagine, convincendo le vittime a condividere informazioni personali o password. L'intelligenza artificiale ha moltiplicato la portata di queste tattiche: non solo consente di creare contenuti sempre più personalizzati, rendendo questi attacchi alla portata dei non informatici, ma permette anche di manipolare le voci e i volti. Non è più fantascienza ricevere un messaggio vocale su WhatsApp che sembra provenire dal proprio capo e che - con la sua stessa voce - chiede un bonifico urgente o un documento riservato. Ci sono anche i primi software malevoli scritti con l'intelligenza artificiale.

Tutti i settori sono nel mirino, ma quello dell'informazione è tra i più esposti. Secondo una ricerca di Proofpoint del luglio 2022, i media rappresentano un obiettivo strategico per due motivi principali: ottenere vantaggi di intelligence - scoprendo fonti, anticipando scoop - e manipolare

la percezione pubblica diffondendo disinformazione. Le analisi dell'azienda hanno rivelato che nel 2021, per esempio, i giornalisti statunitensi furono presi di mira da cinque campagne di phishing nei mesi che precedettero l'assalto al Campidoglio. Gli attaccanti, ritenuti vicini alla Repubblica Popolare Cinese, inviarono email in apparenza legate a temi di attualità. In realtà contenevano web beacon, strumenti invisibili capaci di raccogliere informazioni come le pagine visitate, la durata della navigazione e l'indirizzo IP del dispositivo.

Un'altra funzione del phishing è servire da porta d'ingresso per gli spyware. Questi programmi possono monitorare ogni attività del dispositivo: registrano le chiamate, leggono i messaggi, osservano foto e video, attivano la fotocamera e il microfono senza che l'utente se ne accorga. L'installazione può avvenire tramite un link o un allegato ricevuto via email, ma le versioni più sofisticate sfruttano le cosiddette vulnerabilità "zero-click" - falle nel software non ancora scoperte - che consentono l'infezione anche senza alcuna azione dell'utente. In certi casi, basta ricevere un messaggio su WhatsApp. Le aziende che producono spyware assicurano di venderli esclusivamente per indagini contro terrorismo e criminalità organizzata. Ma come vengano realmente usati resta un punto oscuro. Negli ultimi anni, gruppi di ricercatori e organizzazioni per i diritti digitali hanno trovato tracce di questi software nei dispositivi di attivisti, giornalisti e dissidenti in tutto il mondo.

Modalità paranoica

In genere, uno dei primi consigli contro il phishing è quello di controllare l'URL (l'indirizzo testuale) del link su cui siamo invitati a cliccare. Ma oggi

questo accorgimento serve sempre meno. Certo, fare attenzione è necessario, ma "ormai è molto difficile distinguere un link autentico da uno contraffatto", spiega Riccardo Sirigu, direttore della Business Unit Offensive Security del Gruppo Abissi, azienda specializzata in cybersecurity. La vera prevenzione, aggiunge, non passa tanto dalla tecnologia quanto dalla psicologia. "Queste minacce sfruttano vulnerabilità umane per farci ragionare di meno. È il cosiddetto bias cognitivo di urgenza: riceviamo un messaggio da Amazon, dal corriere o dalla banca che ci avverte che, se non agiamo subito, rischiamo di perdere qualcosa. È proprio lì che dobbiamo fermarci. Quando sentiamo crescere il panico o la fretta, è il momento di non agire".

Anche Kevin Mitnick, uno degli hacker più noti al mondo, che negli anni Ottanta fece impazzire l'FBI intrufolandosi nei sistemi aziendali più protetti, ha sempre sostenuto che il fattore umano fosse un anello debole della sicurezza. Nel suo libro L'arte dell'inganno scrive: "Le persone possono seguire le migliori tattiche consigliate dagli esperti, installare tutti i prodotti raccomandati, essere assolutamente rigorose nella configurazione dei sistemi e tempestive negli aggiornamenti. Ma sarebbero ancora vulnerabili". Mitnick spiega che l'ingegnere sociale non ha bisogno di attaccare le macchine: gli basta conoscere la mente umana. Sfrutta la psicologia per indurre la vittima a cedere alle sue richieste, facendo leva su emozioni come paura, eccitazione o senso di colpa. Per riuscirci, attiva meccanismi automatici che spingono a reagire d'impulso, senza analizzare tutte le informazioni disponibili.

Nel libro, Mitnick richiama le sei tendenze basilari della natura umana individuate dallo psicologo Robert B. Cialdini, spiegando come gli ingegneri sociali le sfruttino per manipolare le vittime. La prima: “Le persone tendono a cedere quando una richiesta proviene da chi appare autorevole”, scrive Mitnick. Racconta l’esperimento citato da Cialdini, in cui un individuo si finge medico e ordina agli infermieri di somministrare un farmaco non autorizzato: “Nonostante la richiesta violasse ogni procedura, nel 95 per cento dei casi gli infermieri stavano per eseguire l’ordine. L’apparenza di autorità è spesso sufficiente a ottenere obbedienza". Nella pratica, spiega Mitnick, un attaccante può spacciarsi per un dirigente, un membro dell’IT o un collaboratore di alto livello per ottenere informazioni sensibili.

Un’altra leva è la simpatia: “Siamo più propensi a obbedire a chi ci somiglia o ci sta simpatico. L’ingegnere sociale costruisce connessioni, imita i comportamenti, condivide interessi o origini per diventare qualcuno di cui fidarsi”. Così, durante una conversazione, può fingere passioni comuni o provenienze simili per abbassare le difese della vittima. Poi c’è la reciprocità: “Quando qualcuno ci aiuta o ci offre qualcosa, sentiamo il bisogno di ricambiare. È un impulso potente e può essere facilmente sfruttato". Mitnick cita il caso di un finto tecnico IT che “aiuta” un dipendente a rimuovere un virus e poi gli chiede di installare un servizio che richiede l’inserimento della password. “Il dipendente, per riconoscenza, acconsente, senza rendersi conto di essere caduto in una trappola".

Altro principio è quello della coerenza: “Una volta che ci impegniamo pubblicamente in un comportamento, vogliamo sembrare coerenti. Gli

attaccanti lo sanno e ci spingono a dimostrare la nostra affidabilità anche quando dovremmo fermarci". È il caso, spiega Mitnick, di chi convince un dipendente di una organizzazione a seguire scrupolosamente le politiche di sicurezza e poi le chiede la password "per verificare". C'è poi la prova sociale, o conformità: "Gli esseri umani guardano cosa fanno gli altri per capire cosa è giusto fare. Se qualcuno dice che i colleghi hanno già collaborato, tenderemo a fidarci e ad agire di conseguenza".

Infine, la scarsità: "La paura di perdere un'occasione è una delle leve più potenti. Se crediamo che qualcosa sia disponibile per poco tempo o in quantità limitata, decidiamo in fretta e male". Mitnick cita l'esempio di email che promettono premi alle prime registrazioni su un sito, inducendo l'utente a fornire dati e password spesso identiche a quelle aziendali: "La scarsità crea urgenza, e l'urgenza è il carburante del social engineering". Secondo Mitnick, per proteggersi serve prima di tutto capire come funziona questa manipolazione. È la base di qualsiasi programma di formazione efficace: riconoscere le proprie vulnerabilità per non cadere nelle trappole.

Limitare la superficie d'attacco

Sul versante tecnologico la prima regola è limitare la superficie d'attacco: l'insieme di punti - software, hardware e reti - attraverso cui un attaccante può tentare di entrare in un dispositivo e comprometterne dati e funzionalità. Meno superficie equivale a meno "porte" da difendere. "Ridurre la superficie d'attacco — spiega Sirigu — abbassa la probabilità che un singolo errore umano o una vulnerabilità software diventi una breccia sfruttabile". In concreto significa, prima di tutto, compartimentare e adottare più cautele sui device usati per lavoro. "Su questi dispositivi —

prosegue l'esperto — l'installazione di applicazioni va limitata il più possibile, così come i permessi concessi: vanno ridotti nel tempo e autorizzati solo se strettamente necessari. L'app di un giornale, per esempio, non ha bisogno di accedere alla fotocamera o alla posizione".

Per chi usa Apple, uno strumento importante è la Modalità isolamento, disponibile da iOS 16, iPadOS 16, watchOS 10 e macOS Ventura in poi. È pensata per ridurre la superficie attaccabile da spyware mercenari. Il rovescio della medaglia è un parziale calo di prestazioni e funzionalità:

- nei Messaggi viene bloccata la maggior parte degli allegati e non sono disponibili link e anteprime;
- nella navigazione web alcune tecnologie complesse vengono disattivate, i siti possono caricarsi più lentamente o non funzionare correttamente e font e immagini possono non apparire (tuttavia è possibile introdurre eccezioni per specifici siti o app)
- su FaceTime le chiamate in entrata sono accettate solo da contatti già chiamati nei 30 giorni precedenti e funzioni come SharePlay e Live Photos non sono disponibili;
- nei Servizi Apple gli inviti in arrivo, per esempio quelli dell'app Casa, vengono bloccati se non provengono da persone già autorizzate e anche Full Immersion e Game Center possono non comportarsi come previsto;
- in Foto vengono escluse le informazioni di geolocalizzazione, gli album condivisi vengono rimossi e i nuovi inviti bloccati, restando però visibili da altri dispositivi non in isolamento;

- ➢ per collegare iPhone o iPad a computer o accessori il dispositivo deve essere sbloccato e l'operazione approvata manualmente;
- ➢ il dispositivo non si connette automaticamente a reti Wi-Fi non sicure e disattiva il supporto 2G e 3G;
- ➢ non è possibile installare profili di configurazione né amministrare il dispositivo tramite un Mobile Device Management (MDM), cioè un software centralizzato di gestione dei dispositivi spesso usato in ambito aziendale; tuttavia i profili MDM installati prima che il dipendente attivi la modalità continuano a funzionare.
- ➢ un Apple Watch abbinato non squilla per chiamate e messaggi in arrivo.

Le limitazioni sono molte, ma per Sirigu rappresentano un buon compromesso, seppur non infallibile, contro gli attacchi zero-click che non richiedono alcun click dell'utente. Al momento Apple è l'unica a offrire uno strumento di questo tipo, per altri sistemi operativi proteggersi è più difficile (ma Android 16 nel 2025 ha comunque introdotto una modalità, Protezione Avanzata, che rafforza la sicurezza per soggetti a rischio). Restano comunque valide le regole di buon senso: compartimentare, evitare il download automatico dei file, controllare sempre le URL dei link e installare solo le app davvero necessarie.

Ridurre la superficie passa anche dall'igiene di base: dispositivi aggiornati all'ultima versione, password diverse e uniche per ogni servizio. Per gestire credenziali robuste serve un password manager affidabile, protetto con un sistema di autenticazione a due fattori.

Spyware, che fare

“Se mi avessero pedinato avrebbero scoperto meno di me”, dice Ciro Pellegrino, giornalista di Fanpage spiato per mesi con uno spyware: il 29 aprile 2025 ha ricevuto da un indirizzo Apple verificato l’avviso di compromissione del suo iPhone.

Qualche mese prima WhatsApp aveva inviato un messaggio simile a circa cento persone nel mondo, fra cui diversi italiani: un altro giornalista di Fanpage, il direttore Francesco Cancellato, e due attivisti di Mediterranea Saving Humans, Luca Casarini e Beppe Caccia. Le indagini del Citizen Lab, il laboratorio dell’Università di Toronto specializzato in spyware, hanno stabilito che sui dispositivi di Casarini, Caccia e Pellegrino era stato installato Graphite, prodotto dalla società israeliana Paragon Solutions e in dotazione ai servizi di intelligence italiani. In alcuni dei casi ricostruiti, l’installazione ha sfruttato una vulnerabilità che consentiva di aggiungere le vittime a un gruppo WhatsApp, a cui veniva inviato un PDF: era sufficiente riceverlo, senza nemmeno aprirlo, perché lo spyware si attivasse. Per Pellegrino, invece, sembra che l’intrusione sia avvenuta tramite iMessage.

Un rapporto del Copasir ha poi ricostruito che Caccia e Casarini sono stati effettivamente oggetto di sorveglianza da parte dei servizi. Viceversa, sul telefono di Cancellato non è mai stato chiarito cosa sia avvenuto e il governo ha sempre respinto ogni addebito. Sia sul caso di Cancellato sia su quello di Pellegrino - scoperto dopo l’inchiesta del Copasir - è in corso un’indagine della Procura di Roma.

Casi come questi dimostrano che è difficile tutelarsi, quando sei nel mirino dei servizi di intelligence di uno Stato. È sul piano politico che si gioca

l'ultima battaglia per la tutela dall'abuso degli spyware da parte dei governi contro attivisti e giornalisti. Strumenti che permettono un grado di sorveglianza mai così invasivo, al momento sfruttati senza una cornice regolatoria uniforme che stabilisca i confini giuridici e tecnologici dentro cui gli spyware possono essere impiegati.

Il tema non è solo italiano. In Europa, la questione è diventata centrale nel luglio 2021, quando il Pegasus Project - inchiesta di 17 testate coordinate da Forbidden Stories con il supporto tecnico di Amnesty International - ha condotto analisi forensi su decine di smartphone, individuando tracce di infezioni su dispositivi di avvocati, giornalisti, politici e giudici anche in Europa, dalla Polonia all'Ungheria fino a decine di attivisti indipendentisti catalani. Per la prima volta, è emerso con evidenza non solo che tra le vittime c'erano cittadini europei, ma anche che tra i responsabili c'erano Stati europei, non regimi extra-Ue. Lo scandalo ha toccato i vertici istituzionali, ma l'unico risultato concreto sul piano politico è stata la posizione del Parlamento europeo, che - pur con un voto non vincolante - ha chiesto un divieto temporaneo di vendita, acquisto e uso di spyware nell'Ue finché non saranno fissati standard comuni basati sul diritto internazionale, con moratoria revocabile solo a condizioni stringenti e previo accertamento indipendente degli abusi.

Ma, a oggi, tutti gli Stati membri continuano ad acquistare spyware e a metterli a disposizione dei servizi di intelligence o delle forze di polizia in assenza di una normativa condivisa. In Italia questi strumenti sono ormai centrali anche per le indagini. In teoria, l'uso dovrebbe rispettare la Carta dei diritti fondamentali, la direttiva ePrivacy e la direttiva Law

Enforcement, ma nei fatti la disciplina resta nazionale e spesso lacunosa. Come spiega l'avvocato Giovanni Battista Gallus, nel nostro Paese è regolata l'attivazione remota del microfono, ma restano scoperte geolocalizzazione, keylogging e registrazione video, con scarsa trasparenza e controlli deboli sui produttori.

La stessa possibilità di impiegare legalmente spyware come Pegasus per fini di interesse generale è controversa. In un documento pubblicato nel 2022, il Garante europeo per la protezione dei dati personali conclude che il sistematico impiego di Pegasus o di analoghe tecnologie altamente invasive non è compatibile con l'ordinamento giuridico europeo. Il livello di interferenza con il diritto alla privacy – si legge nel report – è così grave che l'individuo ne è di fatto privato. Una misura che non può essere considerata proporzionata e che riguarda non solo il diretto interessato ma tutti i suoi contatti. Inoltre – prosegue il Garante – priva le vittime di altre forme di protezione come la confidenzialità delle comunicazioni con un legale. Infine, il loro utilizzo può intaccare il diritto ad avere un giusto processo, uno dei pilastri dei sistemi legali dell'Unione.

La più efficace opzione per proteggere i nostri diritti fondamentali e le nostre libertà? "Bandire lo sviluppo e l'impiego di qualsiasi spyware con le capacità di Pegasus nell'Unione europea", conclude il garante, aggiungendo una lista non esaustiva di indicazioni per prevenire gli abusi: promuovere il controllo democratico più che la sorveglianza; implementare un framework legale europeo sulla protezione dei dati; far sì che la revisione dei giudici sia pre che post intercettazione tramite spyware sia effettiva e non una pura formalità; ridurre il rischio che i dati raccolti grazie a pratiche di

sorveglianza abusive raggiungano i database Ue, alimentando quindi un'intelligence europea basata su informazioni ottenute in modo illecito; smettere di sfruttare ragioni di sicurezza nazionale per legittimare la sorveglianza politicamente motivata; dare più poteri di controllo alla società civile; affrontare le minacce all'indipendenza dei giudici e alla libertà dei media.

In breve:

- ✓ Verifica le comunicazioni inattese, urgenti, ansiogene, o eccitanti prima di fare qualsiasi azione sulle stesse;
- ✓ Mantieni sempre tutti i software aggiornati, non appena esce l'update;
- ✓ Se sei a rischio di spyware, e hai un iPhone, attiva la modalità isolamento (in Impostazioni > Privacy e Sicurezza);
- ✓ Con Android 16, Google ha introdotto Protezione Avanzata, una modalità di sicurezza per tutelare gli utenti più esposti a minacce digitali complesse. Attivala nelle impostazioni di sistema.

8. STRUMENTI AVANZATI

In questa sezione ci inoltriamo su una parte più tecnica, che ovviamente non è sempre facilmente applicabile da parte di chi sta iniziando ora a mettere alcune basi di sicurezza digitale. Ma se invece siete già utenti provetti, qui potreste trovare informazioni utili.

Alcuni di questi strumenti, come GrapheneOS, hanno iniziato a diffondersi anche tra giornalisti e attivisti, sebbene alcune delle loro funzioni sembrino create per contesti di rischio altissimo, regimi dittatoriali o situazioni estreme. In ogni caso, pensiamo che siano soluzioni tecnicamente interessanti da conoscere.

VPN: come, dove e con quali limiti DI TAYLOR

Nel lavoro quotidiano davanti a uno schermo, spesso diamo per scontato che le nostre connessioni siano private. Ma ogni volta che ci colleghiamo a Internet lasciamo tracce: il nostro indirizzo IP, i siti visitati, la posizione approssimativa, a volte persino le abitudini di navigazione. In contesti dove la riservatezza è importante o dove una connessione non sicura può esporre dati sensibili, una delle prime tecnologie a cui si pensa è la VPN.

L'acronimo sta per Virtual Private Network, "rete privata virtuale". È un sistema che crea un collegamento cifrato tra il proprio dispositivo e un server remoto. Tutto il traffico Internet passa attraverso quel collegamento protetto, che impedisce a chiunque si trovi in mezzo, come il gestore di una rete Wi-Fi pubblica o il fornitore di connettività, di leggere le informazioni trasmesse. In sostanza, la VPN incapsula i dati in una sorta di tunnel digitale, rendendo il contenuto invisibile agli occhi esterni.

Il suo effetto più visibile è la modifica dell'indirizzo IP: quando ci si collega a un sito o a un servizio online, non è più il proprio indirizzo a comparire, ma quello del server VPN. È come se ci si spostasse virtualmente in un altro Paese, o comunque in un altro punto della rete. Questo consente di eludere restrizioni geografiche, di evitare la profilazione legata alla provenienza o semplicemente di proteggersi durante l'uso di reti insicure, come quelle di alberghi o aeroporti.

È però importante capire che una VPN non rende invisibili. Cambia soltanto chi può vedere il traffico. Invece del proprio provider, ora è il gestore del servizio VPN ad avere visibilità sui dati che attraversano la sua infrastruttura. La fiducia si sposta, non scompare. Per questo è essenziale scegliere con attenzione a chi affidarsi.

Molte VPN gratuite si finanziano raccogliendo informazioni sugli utenti o mostrando pubblicità mirate. È un controsenso: si cerca privacy e la si paga con i propri dati. I servizi a pagamento, al contrario, tendono a offrire maggiori garanzie, ma non basta la promessa commerciale. È utile verificare dove ha sede l'azienda, quale legislazione regola la gestione dei dati e se le politiche dichiarate di "no log", cioè di non conservazione delle attività degli utenti, sono state controllate da soggetti indipendenti. Alcune VPN rendono pubblico il proprio codice o si sottopongono ad audit di sicurezza che sono segnali di trasparenza preziosi.

Un'altra distinzione riguarda la gestione del servizio. È possibile anche installare un proprio server VPN, configurato su misura e controllato direttamente dall'utente. È una soluzione più sicura ma anche più complessa, che richiede tempo e competenze tecniche. Nella maggior parte

dei casi, un servizio commerciale serio e verificato rappresenta un buon compromesso tra protezione e praticità.

Va però ricordato che la normativa non è uniforme. In molti Paesi l'uso di una VPN è perfettamente legale, ma altrove può essere soggetto a restrizioni o, nei casi più rigidi, considerato illegittimo. Alcuni governi obbligano i fornitori locali a registrarsi e a condividere i dati con le autorità, altri bloccano direttamente i servizi non autorizzati. In questi contesti, l'impiego di una VPN può essere visto come un atto di disobbedienza tecnologica, con conseguenze legali anche gravi. È quindi fondamentale conoscere la legislazione del luogo in cui ci si trova prima di utilizzarla, soprattutto durante viaggi o soggiorni in Paesi con scarsa tutela della libertà di informazione.

Sul piano pratico, usarla è semplice: si installa un'applicazione, si sceglie un server e si attiva la connessione. Da quel momento, tutto il traffico passa per quel canale cifrato. È normale che la velocità della rete ne risenta leggermente, soprattutto se il server si trova lontano. Per un uso quotidiano è spesso sufficiente lasciarla attiva di default, disattivandola solo in caso di rallentamenti evidenti.

Più in generale, è utile pensare alla VPN come a uno strumento di consapevolezza digitale. Serve a ricordare che la rete non è uno spazio neutro, ma un insieme di intermediari che registrano, correlano e archiviano ciò che facciamo. Utilizzare una VPN significa riprendere un minimo di controllo su questo processo, scegliendo chi può vedere cosa. Non è una garanzia assoluta di sicurezza, ma un modo per ridurre la superficie d'attacco e spostare la bilancia un po' più dalla parte dell'utente.

Tuttavia, la vera protezione non viene solo da un'app o da un protocollo. Dipende soprattutto dall'atteggiamento con cui si affronta la tecnologia. Aggiornare regolarmente i dispositivi, usare canali di comunicazione cifrati, verificare le fonti dei software installati e mantenere un minimo di diffidenza verso link o allegati sconosciuti sono abitudini che fanno la differenza più di qualunque altra impostazione tecnica. Una VPN è uno strumento prezioso, ma rimane efficace solo se inserita in un modo di usare la rete che metta al centro la prudenza e la consapevolezza.

Pensarla come una maschera digitale è forse il paragone più corretto: permette di rendere meno riconoscibili i propri movimenti online, di confondere un po' le tracce, di lavorare con maggiore serenità in ambienti digitali sempre più osservati.

Tor Browser per più privacy, ma essere anonimi è un'altra storia DI MATTEO SPINELLI

Nell'estate del 2024 i media tedeschi hanno raccontato nei dettagli un'indagine della Bundeskriminalamt (la polizia federale) che ha dimostrato quanto sia sottile la linea tra privacy e anonimato. Gli investigatori cercavano l'amministratore di un sito criminale sul dark web. Per identificarlo hanno monitorato per mesi i nodi di ingresso e di uscita della rete Tor e confrontato gli orari del traffico con l'attività del sospettato. Incrociando questi dati sono riusciti a risalire alla sua identità. Il metodo, confermato dagli esperti del Chaos Computer Club, mostrava come l'uso di Tor offra più privacy ma non impedisca del tutto di essere tracciati quando le forze dell'ordine controllano parte dell'infrastruttura o si commettono errori.

Per capire perché bisogna partire dalla metafora da cui Tor prende il nome: The Onion Router. Immaginate di spedire una lettera sensibile affidandola prima a un'amica fidata (il nodo di ingresso), che la infila in una busta dentro un'altra busta e la passa a un conoscente (nodo intermedio), che a sua volta la passa a un terzo corriere (nodo di uscita). Solo il primo mittente conosce l'origine: ogni corriere legge solo l'indirizzo della busta esterna. Questo sistema di "cipolle" maschera l'indirizzo IP: il browser Tor, sviluppato da volontari e distribuito gratuitamente, instrada il traffico attraverso diversi router per rendere difficile l'identificazione dell'utente. Il risultato è una navigazione con un alto grado di privacy, tanto che giornalisti e attivisti lo usano per indagare su governi autoritari o aggirare la censura.

Tor consente anche di visitare siti .onion non indicizzati, ma la sicurezza si limita alle applicazioni configurate correttamente: se inserite il vostro nome o l'indirizzo email in un modulo web, quel sito saprà comunque chi siete. Anonimato e privacy non sono sinonimi: chiudere le tende vi protegge dagli sguardi, ma se salutate dalla finestra tutti sapranno che siete lì. Inoltre la connessione finale tra l'uscita di Tor e il sito non è cifrata, quindi un osservatore può intercettare i dati. Questo di per sé non costituisce una vulnerabilità, ma se il traffico è intercettato nel nodo d'uscita allora la vostra connessione è meno protetta.

Dobbiamo sempre tenere in considerazione che per quanto la rete che utilizziamo possa essere sicura, i nostri dati saranno sempre esposti se non la utilizziamo bene, oppure se i software con i quali ci colleghiamo hanno delle vulnerabilità. Nel 2013 l'FBI prese il controllo di Freedom Hosting, un fornitore di siti .onion, e inserì un malware che sfruttava una falla di Firefox per identificare i visitatori: chi non aveva aggiornato Tor Browser fu tracciato e i dati furono inviati a un server in Virginia. Lo stesso anno le rivelazioni di Edward Snowden mostrarono che la National Security Agency usava tecniche per identificare il traffico Tor e dirottare i browser verso server malevoli, sfruttando vulnerabilità di Firefox. Nel 2014 l'operazione Onymous, coordinata da Europol e FBI, portò al sequestro di centinaia di servizi nascosti e arresti. Secondo il progetto Tor a far crollare molti siti furono errori dei gestori o bug nelle applicazioni, anche se non è escluso un attacco alla rete.

Questo è accaduto perché il software Tor è una versione di Mozilla Firefox ESR (Extended Support Release), la quale è stata modificata per

implementare il sistema onion routing. Pertanto qualunque vulnerabilità software avesse Firefox, la stessa veniva portata su Tor.

Questi esempi mostrano come l'anonimato e la sicurezza digitale debbano prima di tutto passare attraverso una consapevolezza di chi la attraversa. Solo con la conoscenza degli strumenti con cui navighiamo possiamo difenderci da eventuali aggressioni alla nostra privacy, che esse siano da governi, da gruppi criminali o da singoli.

Quindi come possiamo utilizzare al meglio gli strumenti a nostra disposizione? Il progetto Tor elenca alcune regole. Non installate plugin o estensioni non affidabili che potrebbero aggirare Tor e rivelare il vostro IP. Non usate programmi peer-to-peer come BitTorrent: spesso ignorano le impostazioni proxy e inviano l'indirizzo reale al server. Non aprite documenti scaricati via Tor mentre siete ancora connessi: i file possono contenere risorse che si caricano fuori dalla rete e svelano la posizione. Preferite sempre siti HTTPS e abilitate la modalità "Solo HTTPS" nel browser. Aggiornate sempre Tor all'ultima versione e non modificate le impostazioni di default; se dovete creare un account usate dati fittizi e un indirizzo email separato. La lentezza invoglia a cambiare browser: evitatelo, perché anche pochi secondi fuori dalla rete possono rivelare la vostra identità.

Strumenti complementari possono aiutare. Tails, il sistema operativo amnesico usato da Edward Snowden e Laura Poitras, si avvia da chiavetta e indirizza tutto il traffico attraverso Tor, inoltre non salva dati localmente e integra strumenti di cifratura. Questo riduce il rischio di lasciare tracce sul computer e protegge le fonti. Alcuni consigliano di combinare Tor con una

VPN: la VPN nasconde alla rete Tor la vostra posizione e viceversa, ma affidatevi solo a fornitori trasparenti.

In sintesi, Tor Browser è uno strumento di autodifesa potente: maschera l'indirizzo IP e rende più difficile collegare l'attività online a una persona. Tuttavia non è una bacchetta magica. L'anonimato richiede disciplina, aggiornamenti costanti e buon senso: servono attenzione a ciò che si condivide, a come si effettuano i "primi contatti" con le fonti e a quali applicazioni si usano. La cipolla è una buona metafora: se viene tolto qualche strato la nostra privacy può rimanere protetta, ma per sparire davvero bisogna evitare di lasciare bucce in giro.

GrapheneOS di CRP

GrapheneOS (GOS) è un sistema operativo basato su Android ed utilizzabile sugli smartphone della linea Pixel di Google. A differenza delle stock ROM di altri brand di telefonia (come Samsung o Nokia), GrapheneOS introduce significativi miglioramenti in termini di privacy e sicurezza, attraverso numerosissime funzionalità attentamente progettate dalla sua comunità di ricerca per operare efficacemente contro avversari reali. I primi vagiti del progetto risalgono al 2015 (al tempo si chiamava Copperhead OS) e fin da allora la sua traiettoria di sviluppo si è contraddistinta per il tentativo di fornire ai suoi utenti una sicurezza robusta e semplice, efficace anche contro avversari sofisticati e capace di mitigare minacce avanzate. Quali sono le caratteristiche di design di GOS che lo rendono uno strumento ideale per giornalisti che maneggiano informazioni sensibili e attivisti che si muovono in contesti ad alto rischio?

Le fondamenta dell'approccio filosofico di GrapheneOS poggiano su due pietre angolari, due principi largamente adottati dalla maggior parte delle comunità di sicurezza online: trasparenza del codice sorgente e riduzione della superficie d'attacco. Il cuore pulsante di questo sistema operativo – la *baseline* del suo codice, per dirla con un gergo più tecnico – è AOSP, acronimo di *Android Open Source Project*: una versione completamente open source del sistema operativo del robottino, il cui codice sorgente è privo di porzioni chiuse o proprietarie (e quindi non ispezionabili dalla vasta comunità di ricercatori di sicurezza, sempre alla ricerca di bug e vulnerabilità). Inoltre, GrapheneOS può contare su un team di sviluppo estremamente attivo, impegnato a migliorare costantemente il codice

AOSP – per renderlo più sicuro e solido – e a rimuovere dalla baseline una serie di funzionalità che potrebbero essere usate da un attaccante per compromettere la privacy e la sicurezza del dispositivo.

Sotto il cofano di GrapheneOS c'è però molto più. La documentazione del progetto racconta di una miriade di funzioni, pazientemente sviluppate e testate in un arco temporale lungo dieci anni, che testimoniano come questo sistema operativo sia stato progettato per essere resistente ad una grande varietà di vettori d'attacco. Per esempio, scorrendo la pagina "Features" del sito ufficiale di GOS, salta immediatamente all'occhio una lunga lista di funzioni incorporate nella ROM, progettate per mitigare l'efficacia degli *exploits* – ovvero quelle tecniche di attacco che sfruttano eventuali falle presente nel sistema operativo, o nel software installato sul dispositivo, per prenderne il controllo con finalità malevole.

GOS inoltre implementa misure di difesa particolarmente sofisticate contro gli attacchi che utilizzano come vettore la porta USB-C del telefono (quella utilizzata per collegarlo a un alimentatore o a un altro computer). È ormai prassi, per forze di polizia di tutto il mondo, accompagnare il sequestro di un telefono con l'uso di strumenti di analisi forense progettati appositamente per sbloccarlo, estrarne i dati ed analizzarli, anche quando è protetto da password e cifratura. Il più famoso tra questi prodotti è l'*UFED*, acronimo di *Universal Forensic Extraction Device*, della compagnia israeliana Cellebrite. UFED è una scatoletta con uno schermo a cristalli liquidi che, connettendosi alla porta USB di uno smartphone, permette di ricavarne le chiavi di cifratura del disco, le password custodite al suo interno o i dati delle singole applicazioni. Con GOS, strada sbarrata però. Infatti, quando il

dispositivo è bloccato, ogni nuova connessione USB viene disabilitata sia a livello software che hardware, rendendo così inservibili dispositivi come l'UFED. Un limite riconosciuto dalla stessa Cellebrite che nella documentazione fornita ai clienti – e trapelata su alcuni media online – ammette che il suo prodotto non è in grado di violare uno smartphone GrapheneOS, a meno che questo non venga regolarmente aggiornato. Un problema tutto sommato marginale, considerando che GOS integra di default un sistema di aggiornamento in background che installa patch di sicurezza e migliorie nel codice, senza richiedere alcun intervento da parte dell'utente.

Accanto a queste proprietà di sicurezza se ne trovano molte altre, altrettanto significative. Tra queste è possibile annoverare la *Duress Password*, ovvero un PIN secondario che una volta digitato al posto della normale password cancella in maniera automatica e permanente i dati presenti sul telefono. Oppure l'*Auto Reboot*: come dice il nome stesso, una funzione che riavvia automaticamente il telefono dopo un certo periodo di inattività (da impostare a piacimento) e riduce il tempo a disposizione di un attaccante per provare a violare un dispositivo quando un utente è ancora loggato nel sistema. Infine, merita una menzione speciale anche il sistema *Auditor* – anche questa un'innovazione sviluppata dai creatori di GOS – che verifica periodicamente l'autenticità e l'integrità del firmware e del software installati sul dispositivo.

GOS presta però una particolare attenzione anche alla protezione della privacy degli utenti, senza per questo sacrificare o compromettere l'usabilità dello smartphone. Grazie ad un sofisticato sistema di *sandboxing*,

applicazioni come il Play Store di Google o i Google Play Services – il sistema di notifiche sviluppato da Mountain View, indispensabile per il funzionamento di molte app comuni (tra cui quelle bancarie) ma notoriamente poco rispettoso della privacy – vengono infatti isolate in appositi recinti che impediscono loro di accedere in modo improprio ai dati di altre applicazioni o a quelli dell'utente.

Un altro pezzo forte di GOS è senz'altro il livello di usabilità raggiunto negli anni. Fino a qualche tempo fa, la procedura per sostituire la stock ROM di Google con GOS richiedeva una certa familiarità con l'uso del terminale e una buona conoscenza dei passi da seguire per completare l'installazione con successo. Anche un piccolo errore nel procedimento avrebbe potuto rendere il telefono completamente inservibile, al punto tale da non poterlo più nemmeno accendere (una condizione definita come *bricking* del dispositivo). Per ovviare a questo problema e permettere anche ai meno tecnici di avvantaggiarsi delle proprietà di sicurezza di GOS, il suo team di sviluppo ha introdotto una modalità di installazione nota come *WebUSB.* Con questo metodo installare GOS diventa facile come bere un bicchier d'acqua: basta collegare lo smartphone al proprio computer, collegarsi al sito ufficiale del progetto e seguire le indicazioni che appaiono sul monitor.

Unica nota dolente. Come scritto in apertura, GOS gira solo sui telefoni della linea Pixel di Google, tutt'altro che economici. Si tratta però di una scelta anche questa dettata da motivazioni di sicurezza. I Pixel offrono specifiche hardware avanzate che li rendono unici nel panorama Android. Un esempio è il chip di Titan M2 in cui vengono conservate le chiavi

crittografiche più sensibili (come quelle per la cifratura dei dati e di autenticazione), isolandole dal resto del sistema e proteggendole anche in caso di compromissione del dispositivo. Inoltre, un altro fattore fondamentale è il supporto software che Google fornisce ai suoi dispositivi. I telefoni Pixel ricevono patch di sicurezza Android ogni mese direttamente da Google, e tutti i firmware necessari per il loro funzionamento (inclusi quelli del modem radio o del chip Titan M) sono di pubblico dominio.

9. “MAMMA MI HANNO “HACKERATO” E ALTRE EMERGENZE DI ROSITA RIJTANO

Quando i giornalisti di Fanpage hanno scoperto che il loro iPhone era stato compromesso da uno spyware, i primi consigli ricevuti dal Citizen Lab di Toronto sono stati due: mantenere la calma e non spegnere il cellulare, interrompendo però ogni connessione con il mondo esterno. L’istinto porterebbe a “staccare tutto”, come nel celebre video di “Hackerino”, in cui due hacker strappano la spina del computer dopo un presunto tentativo di intrusione andato male, gridando “Ci stanno tracciando! Stacca, stacca!”. In realtà, è proprio ciò che non si deve fare.

Tracce forensi preziose per capire chi ha attaccato il dispositivo e in che modo possono trovarsi nella memoria Ram, la memoria volatile. Quando il telefono viene spento o riavviato, quella memoria si azzera: significa perdere per sempre informazioni che potrebbero rivelarsi fondamentali per le indagini. Inoltre, gli spyware più avanzati sono in grado di accorgersi dello spegnimento o del riavvio del device e di cancellare ogni traccia della loro presenza. Allo stesso tempo, lasciare il dispositivo ancora connesso alla rete mobile, al wi-fi o con il bluetooth attivo permette all’attaccante di continuare a controllarlo da remoto. Gli spyware, infatti, sfruttano i canali di comunicazione attivi per inviare comandi, estrarre documenti, password, messaggi e registrazioni audio, installare altri malware, o eliminare le prove delle proprie azioni. Fino a che il dispositivo resta online, l’intruso può ancora vedere cosa succede, rubare dati e password, aumentare il proprio controllo o persino bloccare l’accesso degli account collegati al proprietario legittimo.

La prima azione corretta - secondo le indicazioni di Citizen Lab - è quindi isolare completamente il device dalle connessioni (rimuovendo la scheda sim, disabilitando wi-fi e bluetooth), senza però spegnerlo. È importante anche non compiere ulteriori operazioni che possano alterare le prove o allargare il raggio di azione degli attaccanti: niente accessi ad altri account "per verificare se funzionano" (le password potrebbero essere rubate) e nessuna attività che possa aggiornare app o attivare servizi. In questo modo si interrompe l'accesso in tempo reale, si preservano le prove digitali, si impedisce un'ulteriore diffusione del malware o la perdita di dati e si evita di insospettire l'intruso.

Da quel momento in poi, tutte le comunicazioni e le verifiche devono avvenire soltanto da un dispositivo considerato sicuro. In sostanza, ogni cellulare o computer compromesso va trattato come una scena del crimine digitale: preservare le tracce è essenziale per capire cosa sia successo e, se possibile, risalire a chi c'è dall'altra parte. Importante è anche documentare tutto ciò che succede sul telefono, quando e se possibile, come fare screenshot di alert, messaggi e pop up. Solo dopo l'analisi di esperti si potrà decidere come e quando spegnerlo, bonificarlo e distruggerlo (o consegnarlo alle autorità per le indagini). È altrettanto importante valutare i rischi a cui potrebbero essere state esposte le nostre fonti. Un dispositivo compromesso può infatti aver consentito all'attaccante di accedere a conversazioni sensibili, contatti, documenti riservati e informazioni che mettono potenzialmente in pericolo le persone con cui lavoriamo. Queste persone devono essere informate tempestivamente dell'accaduto, così da poter adottare a loro volta misure di protezione adeguate. Avvisare le fonti non è solo una buona pratica di sicurezza: è un dovere etico e professionale.

Significa garantire che nessuno sia lasciato all'oscuro di un possibile rischio e che tutti possano prendere decisioni consapevoli riguardo alla propria sicurezza fisica e digitale.

Il passaggio successivo consiste nel mettere in sicurezza tutto ciò che potrebbe essere stato compromesso, a partire dai nostri account digitali. Occorre cambiare tutte le password utilizzando esclusivamente un dispositivo considerato sicuro, cioè non collegato in alcun modo al telefono o al computer infettati. La priorità va data agli account email e ai servizi cloud, che spesso rappresentano la "chiave maestra" per accedere a tutto il resto. Seguono le app di messaggistica collegate al numero di telefono, e i servizi finanziari o legati ai pagamenti digitali. È poi necessario forzare il logout da tutte le sessioni aperte, per evitare che l'attaccante continui a operare in background anche dopo il cambio delle password.

Se pensate che sia faticoso gestire tutto da soli, avete ragione: non fatelo, è l'ultimo - ma fondamentale - consiglio. Cercate il prima possibile il supporto di esperti del settore. Ci sono diverse organizzazioni specializzate nel supportare giornalisti e attivisti che subiscono attacchi digitali. Ecco un elenco (non esaustivo):

- Citizen Lab, laboratorio dell'Università di Toronto che ha condotto molte inchieste internazionali sull'uso di spyware contro giornalisti e attivisti da parte dei governi (compreso il caso Paragon in Italia), e fornisce assistenza e supporto alle vittime. Questi i contatti: inquiries@citizenlab.ca; (416) 946 8903; https://citizenlab.ca.

- Una realtà italiana è Osservatorio nessuno, un'associazione no profit che difende i diritti digitali. Supporta attivisti, giornalisti e organizzazioni della società civile fornendo assistenza tecnica e strumenti per proteggere la loro privacy e sicurezza online. Tutti i contatti si trovano a questo link: https://osservatorionessuno.org/it/contatti/.

- L'Electronic Frontier Foundation (EFF) è un'organizzazione internazionale no profit di avvocati e legali rivolta alla tutela dei diritti digitali e della libertà di espressione. Sul proprio sito mette a disposizione non solo una serie di guide pratiche per l'autodifesa digitale, ma anche una serie di strumenti open source a supporto sviluppati dal team hi-tech (https://www.eff.org/pages/tools). Questi i contatti: https://www.eff.org/about/contact.

- Un'altra organizzazione internazionale no profit è Access Now. Un punto di forza è la Digital Security Helpline attiva h24, che offre assistenza tecnica diretta in tempo reale e consulenza a giornalisti e attivisti (https://www.accessnow.org/help-it/#contact-us). Tutti i contatti qui https://www.accessnow.org/contact-us/.

- La no profit Tactical Tech ha sede a Berlino ed è impegnata a investigare gli impatti sociali, politici e ambientali della tecnologia. Offre risorse (https://tacticaltech.org/resources/), consulenza e possibilità di partnerariato per attivisti e giornalisti che vogliono fare inchieste su temi hi-tech. Il sito è https://tacticaltech.org/.

➢ Infine, la Freedom of the Press Foundation (FPF), un'organizzazione internazionale no profit che difende la libertà di stampa. Sviluppa strumenti di comunicazione sicura usati da molte redazioni investigative nel mondo e forma giornalisti a proteggere se stessi e le fonti dalle minacce digitali. Qui i contatti e le risorse: https://freedom.press/contact/.

In breve:

✓ Non spegnere il dispositivo, ma isolalo rimuovendo la sim, disabilitando wi-fi e bluetooth;

✓ Passa a un dispositivo sicuro;

✓ Contatta le fonti più a rischio;

✓ Cambia le password di tutti i tuoi account e forza i log out dalle sessioni aperte;

✓ Rivolgiti a degli esperti.

AUTORI & CURATORI

Raffaele Angius. Lavora per la testata investigativa IrpiMedia dove si occupa prevalentemente di tecnologie di sorveglianza, tutela delle fonti e reati informatici, collaborando stabilmente anche con Wired Italia. È professore a contratto di Privacy e Protezione dei dati all'Università di Perugia.

Carola Frediani. Ha lavorato per anni come giornalista occupandosi di sorveglianza, cybercrimine e cybersicurezza. Oggi è nel team di cybersecurity di una Ong internazionale per i diritti umani. Scrive la newsletter Guerre di Rete e ha cofondato il sito Guerredirete.it.

Sonia Montegiove. Giornalista, informatica, formatrice. Fa parte della redazione di Guerre di Rete.

Federico Nejrotti. Autore e co-fondatore di Ufficio Furore, studio di progettazione che crea cultura radicale. Appassionato da sempre di internet governance, è stato responsabile delle comunicazioni di cheFare, agenzia per la trasformazione culturale, e capo-redattore dell'edizione italiana di Motherboard, il magazine di scienza e tecnologia di VICE.

Rosita Rijtano. Giornalista, appassionata di tecnologia, diritti, e criminalità organizzata. È Bertha Investigative Journalist Fellow 2026 per Wired Italia. Collabora con testate nazionali e internazionali, come Occrp, Guerre di Rete e L'Espresso. Il suo ultimo libro – Insubordinati, inchiesta sui rider (Edizioni Gruppo Abele) – ha vinto il premio Oxfam Raccontare la disuguaglianza.

Patrizio Tufarolo. Professionista della sicurezza informatica. Si occupa di analisi e gestione del rischio IT presso un ente europeo[1]. Attivo nella comunità di Cyber Saiyan e contributore del progetto divulgativo Guerre di Rete, partecipa alla diffusione di una cultura della sicurezza accessibile e consapevole.

Taylor, **CRP** e **Matteo Spinelli** sono tre attivisti, esperti di cybersicurezza.

[1] Il contributo alla presente pubblicazione è stato fornito a titolo personale