



*Guida* GALATTICA  
di AUTODIFESA DIGITALE

FEDERICO MAGGI

Quest'opera, ancora incompleta, è una traduzione arricchita dell'opera Surveillance Self Defense dell'Electronic Frontier Foundation (EFF) [12], con qualche adattamento per la lingua italiana e qualche esempio per chiarire ove necessario.



Quest'opera è distribuita con Licenza “CC BY-SA 3.0” .

Foto di copertina: Alexander Andrews: <https://unsplash.com/photos/fsH1KjbdjE8>.

# *Indice*

---

<b>Prefazione</b>	<b>vi</b>
<b>1 Pianificazione della sicurezza</b>	<b>1</b>
1.1 Esempio concreto (non digitale) . . . . .	2
1.2 Da dove cominciare per costruirsi il proprio piano di sicurezza digitale? . . . . .	4
1.3 Domanda 1: Cosa voglio proteggere? . . . . .	5
1.4 Domanda 2: Da chi voglio proteggere i miei asset? . . . . .	5
1.5 Domanda 3: Cosa accade se qualcosa va storto? . . . . .	6
1.6 Domanda 4: Quanto è effettivamente necessario proteggere? . . . . .	8
1.7 Quanto sono disposto a spendere? . . . . .	9
1.8 Per concludere: siamo solo all'inizio . . . . .	9

<b>2 Comunicare in modo sicuro</b>	<b>11</b>
2.1 Come funziona la cifratura “end to end”? . . . . .	12
2.2 Garanzie di una cifratura “end to end” . . . . .	12
2.3 Attenzione ai dettagli . . . . .	13
2.4 Creazione e scambio delle chiavi . . . . .	14
2.5 Un solo segreto, da custodire con cura . . . . .	15
2.6 Chi mi dice che sei proprio tu? . . . . .	16
2.7 Telefonate e SMS . . . . .	18
2.8 Quanto possiamo fidarci di un sistema di comunicazione? . . . . .	19
2.9 Cosa non fa la cifratura “end to end” . . . . .	20
2.10 C’è altro oltre la cifratura “end to end” . . . . .	22
2.11 Per concludere: calma e consapevolezza prima di tutto . . . . .	23
<b>3 Uso consapevole dei social media</b>	<b>24</b>
3.1 Suggerimenti per creare un profilo online . . . . .	25
3.2 Una sfogliata alla privacy policy . . . . .	27
3.3 Modificare le impostazioni di sicurezza e privacy . . . . .	28
3.4 Compartimentare informazioni e account . . . . .	30
3.5 Gruppi di discussione, con consapevolezza . . . . .	31
3.6 Per concludere: Sicurezza e privacy sono sport di squadra . . . . .	32

<b>4</b>	<b>Password e altri segreti</b>	<b>33</b>
4.1	Password, passphrase e segreti . . . . .	33
4.2	Creare password robuste “automagicamente”	36
4.3	password da memorizzare . . . . .	39
4.4	Una nota sulle “domande di sicurezza” . . . .	39
4.5	Sincronizzare le password su più dispositivi .	40
4.6	Autenticazione a più fattori . . . . .	41
4.7	Fattori: ciò che si sa, ciò che si ha, ciò che si è	43
4.8	Dai token fisici a quelli virtuali . . . . .	44
4.9	Per concludere: è complicato . . . . .	45
<b>5</b>	<b>Stare al Passo</b>	<b>47</b>
<b>L'autore</b>		<b>49</b>
<b>Bibliografia</b>		<b>51</b>

# *Prefazione*

---

Questa guida promuove un uso consapevole e sicuro della tecnologia. Per tutti. O meglio, per chi si accorge che qualcosa sta "sfuggendo di mano," o va troppo veloce, e vuole capirci di più. Vuole riprendersi il controllo della sfera tecnologica della propria vita.

Con questa guida voglio arrivare a scalpare gli scettici, quelli che non vogliono fare "il passo" per partito preso, perché "ho sempre fatto così, non cambio mica". Sono tecnologia ed innovazione in sé a non far spostare gli scettici, neanche di un millimetro? Oppure è il fatto di non essere pienamente consapevoli dei benefici e della possibilità di farne un uso sicuro? Vorrei gettare luce in questa zona.

Voglio far titubare quelli che hanno i gadget all'ultimo grido, quelli che "hai visto questa nuova app? Devi provar-

la!”. Quelli che non si fermerebbero davanti a niente, “tanto a chi interessano i miei dati, anche se me li rubano?” Vorrei mostrare loro i rischi di sicurezza cui vanno incontro, sia in quanto utilizzatori, sia in quanto cittadini digitali [9].

Ho insegnato per tanti anni sicurezza informatica a centinaia di studenti di ingegneria del Politecnico di Milano. Ora vorrei allargare un po’ lo spettro, con un taglio più divulgativo, ma senza semplificare troppo.

L’idea di scrivere una guida come questa è nata il giorno in cui decisi di fare un breve seminario divulgativo per raccontare ai miei compaesani alcuni aspetti del lavoro. Ho parlato di video orribili autogenerati, pubblicati su YouTube solo per generare profitto, deepfake, dati rubati, bullismo e adescamento online, sicurezza e privacy. Al termine del seminario, qualcuno dal pubblico mi chiede *“e quindi, cosa possiamo fare?”* Purtroppo non avevo una risposta breve. Non c’è una risposta breve, perché consapevolezza e sicurezza informatica sono un processo, un percorso. Sono un processo nelle aziende e nelle organizzazioni, ma anche per l’individuo. Io ho deciso di puntare sugli individui, notoriamente i più difficili da raggiungere. Questa guida è il mio primo passo concreto in questa direzione.

La prima versione di questa guida è fortemente basata sulla Surveillance Self-Defense [12], un’ottima risorsa alla portata di tutti pubblicata dall’Electronic Frontier Founda-

taion<sup>1</sup>. Dopo un po' di ricerche sono venuto a conoscenza di varie iniziative di traduzione<sup>2</sup>, ma non esattamente in linea con quello che avevo in mente. Pertanto ho deciso di iniziare a tradurre e adattare all'italiano una selezione dei suoi contenuti. In questa prima versione ho arricchito solo con alcuni esempi, per velocizzare i tempi, ma in futuro aggiungerò altri contenuti e probabilmente stravolgerò completamente la struttura e la guida originale da cui sono partito.

---

<sup>1</sup><https://eff.org>

<sup>2</sup><https://selfence.altervista.org/elementi-di-autodifesa-digitale/>,  
<https://numerique.noblogs.org/>

## CAPITOLO 1

# *Pianificazione della sicurezza*

---

Cercare di proteggere tutti i nostri dati e dispositivi da chiunque e in ogni momento è controproducente e frustrante. La sicurezza (informatica) è un processo attraverso il quale, con una pianificazione ragionata, si prepara una strategia di difesa adatto alle nostre esigenze specifiche.

La sicurezza informatica non ha a che fare (soltanto) con gli strumenti che utilizziamo o con i programmi che scarichiamo o installiamo. Tutt'altro! Il primo passo consiste nel capire, precisamente, da quali minacce informatiche vogliamo proteggere i nostri dati e dispositivi. Solo in secondo luogo ci focalizzeremo sul come.

In gergo tecnico, per minaccia s'intende un potenzia-

## *Guida Galattica di Autodifesa Digitale*

le evento (accidentale o intenzionale) che potrebbe rendere inefficaci o inutili le misure di sicurezza che proteggono ciò che per noi ha un valore. Ad esempio, eventi atmosferici come alluvioni o temporali sono minacce accidentali, perché potrebbero distruggere i computer o dischi su cui abbiamo memorizzati i nostri dati preziosi. Al contrario, l'esistenza di soggetti interessati a rubare le nostre password è una minaccia intenzionale.

Per contrastare una minaccia è necessario capire cosa intendiamo proteggere e da chi. Quest'attività è si definisce in gergo “threat modeling” [10]—che tradotto alla lettera significa “modellazione delle minacce,” (suona male, lo so). Più semplicemente vuol dire essere in grado di comprendere “come sono fatte” le minacce (i loro mezzi, risorse, interessi, etc.).

Questo capitolo spiega i concetti basilari per costruire un “piano di difesa” per i nostri dati e capire quali soluzioni sono più adatte.

### **1.1 Esempio concreto (non digitale)**

Ma com’è fatto un piano di sicurezza? Facciamo un esempio concreto. Immaginiamo di dover mettere al sicuro la nostra casa e gli oggetti di valore in essa custoditi. Iniziamo col domandarci:

## *Guida Galattica di Autodifesa Digitale*

- **Cosa c'è in casa mia che vale la pena proteggere?** Gioielli, dispositivi elettronici, documenti fiscali e d'identità, passaporti, fotografie, etc., sono i primi valori e beni a cui solitamente si pensa. Questi si definiscono "asset." Da chi voglio proteggerli? Ladri, co-inquilini e ospiti sono solo alcuni esempi di potenziali avversari.
- **Se qualcosa andasse storto, vi sarebbero gravi conseguenze?** Gli asset che abbiamo in casa e che desideriamo proteggere sono unici e impossibili da rimpiazzare? In caso contrario, avremmo tempo e denaro sufficienti per sostituirli? Siamo assicurati contro i furti?
- **Quanto è necessario proteggerli? Ci sono spesso furti nel quartiere?** Co-inquilini e ospiti sono affidabili? Che capacità avrebbero tali avversari? Ad esempio, nel caso di furti, si tratta di ladroncini improvvisati o di professionisti ben attrezzati? Quanto spesso ospito persone sconosciute?
- **Quanto intendiamo esporci per evitare tali conseguenze?** Siamo disposti a comprare e installare una cassaforte? Possiamo permetterci una serratura di alta qualità? Avremmo tempo e risorse per aprire una

## *Guida Galattica di Autodifesa Digitale*

cassetta di sicurezza in banca per tenere i nostri valori?

Riflettendo su queste domande riusciremo a capire le minacce specifiche (ovvero, che interessano il nostro caso specifico), gli asset, le capacità degli avversari e la “probabilità” (volutamente tra virgolette, perché non in accezione statistica) che una minaccia si concretizzi in un evento.

### **1.2 Da dove cominciare per costruirsi il proprio piano di sicurezza digitale?**

Fare una pianificazione della sicurezza significa essere in grado di rispondere a queste cinque domande. Riprendiamo gli esempi appena visti, calandoli nella nostra sfera digitale:

1. Cosa voglio proteggere?
2. Da chi?
3. Cosa accade se qualcosa va storto?
4. Quanto è effettivamente necessario proteggere?
5. Quanto sono disposto a spendere per evitare le conseguenze di una minaccia?

## *Guida Galattica di Autodifesa Digitale*

Vediamo da vicino ognuna di queste domande.

### **1.3 Domanda 1: Cosa voglio proteggere?**

Gli asset sono ciò che per noi ha valore e che intendiamo proteggere. Nel contesto della sicurezza digitale, gli asset sono tipicamente “ciò che è un dato o un’informazione”. Per esempio, email, contatti, messaggi, posizione geografica e, più in generale, “i nostri file”. I nostri dispositivi, come ad esempio il nostro smartphone, sono quasi sicuramente un asset.

**Cosa fare?** Stendiamo una lista dei nostri asset. Dati memorizzati, dove, chi vi ha accesso, cosa previene che chi non dovrebbe accedervi non vi acceda?

### **1.4 Domanda 2: Da chi voglio proteggere i miei asset?**

Per rispondere a questa domanda è importante identificare chi potrebbe avere interesse verso di me e i miei dati. Una persona o entità che costituisce una minaccia per i nostri asset è un avversario. Ad esempio: il nostro datore di lavoro, un (ex) partner, la concorrenza, il governo, o un criminale informatico in una rete pubblica.

## *Guida Galattica di Autodifesa Digitale*

**Cosa fare?** Compiliamo una lista dei nostri avversari, o di coloro che potrebbero tentare di impossessarsi dei nostri dati. La nostra lista potrebbe includere individui, organizzazioni, agenzie governative o aziende.

**Attenzione!** A seconda di chi sono i nostri avversari, in alcune circostanze, potrebbe essere necessario distruggere questa lista una volta finita la nostra pianificazione della sicurezza. Volendo fare un passo in più: la maggior parte dei dati e delle informazioni creati durante la pianificazione della sicurezza costituiscono essi stessi degli asset e, in quanto tali, vanno protetti.

### **1.5 Domanda 3: Cosa accade se qualcosa va storto?**

Ci sono molte strade che i nostri avversari potrebbero seguire per avere accesso ai nostri dati. Per esempio, potrebbe leggere le nostre comunicazioni private direttamente, mentre transitano in una rete; oppure potrebbe cancellarle o alterarle.

I moventi di ogni avversario sono i più disparati e le loro tattiche possono variare significativamente. Ad esempio, se l'avversario è un'agenzia governativa che vuole arginare la diffusione di un video con scene di violenze perpetrate

## *Guida Galattica di Autodifesa Digitale*

da una polizia, allora potrebbe accontentarsi banalmente di cancellare le copie (dei file) di tale video, oppure di limitare il funzionamento corretto dei siti che lo offrono in streaming. Un esempio opposto è quello di un nostro avversario politico, che come movente potrebbe avere l'accesso a documenti segreti, allo scopo di pubblicarli senza il nostro consenso, per screditarcici.

In questo senso, fare una pianificazione della sicurezza significa capire quanto gravi possono essere le conseguenze nel caso in cui un nostro avversario riuscisse ad accedere a uno dei nostri asset. Per determinare l'entità del danno dobbiamo considerare le capacità di ognuno dei nostri avversari. Per esempio, gli operatori telefonici hanno accesso (in varia misura, a seconda dei casi e della legge specifici) ai tabulati telefonici. Se decidiamo di considerare il nostro operatore telefonico come nostro avversario, allora dobbiamo essere consapevoli che, tra le sue capacità, c'è anche quella di accedere a tali dati. Altro esempio: un criminale collegato ad una rete Wi-Fi pubblica ha la capacità di intercettare, quantomeno, le nostre comunicazioni non opportunamente cifrate, mentre un'agenzia governativa può avere risorse, mezzi, e quindi capacità, più elevate.

**Cosa fare?** Prendiamo nota di cosa ogni avversario potrebbe arrivare a fare con i nostri asset (dati privati, ad esempio).

## **1.6 Domanda 4: Quanto è effettivamente necessario proteggere?**

Il livello di rischio è la probabilità che uno asset sia concretamente affetto da una specifica minaccia. O, in altre parole, che una minaccia si concretizzi verso uno specifico asset.

Il livello di rischio va di pari passo con le capacità di cui sopra. Ad esempio: anche se gli operatori telefonici hanno accesso ad una grande quantità di nostri dati sensibili, il rischio che si mettano a pubblicarli online—a scapito della nostra reputazione—è molto basso.

È importante distinguere tra cosa potrebbe succedere e la probabilità che effettivamente tale evento avvenga. Per esempio, esiste la minaccia di crollo per qualiasi edificio, ma il rischio di tale evento è più elevato nelle aree sismiche.

Quantificare il rischio è un processo personale e soggettivo. Alcuni decidono di ignorare certe minacce indipendentemente dall'effettiva probabilità di accadimento, semplicemente perché giudicano troppo dispendioso anche solo considerare la mera esistenza di tali minacce—a qualsiasi probabilità. In altri casi, alcune persone ignorano alti rischi perché non li vedono la minacci come un problema.

**Cosa fare?** Scriviamo una lista di minacce che intendiamo prendere sul serio, e altre che invece consideriamo troppo rare o di basso impatto da destare preoccupazione.

## **1.7 Domanda 5: Quanto sono disposto a spendere per evitare le conseguenze di una minaccia?**

Non esiste una scelta perfetta per la sicurezza (informatica e non). Non tutti hanno le stesse priorità, preoccupazioni o accesso a risorse. Una valutazione del rischio ci aiuterà a pianificare la giusta strategia per ogni specifico caso, bilanciando comodità, costo e sicurezza.

Per esempio, un avvocato che rappresenta il proprio cliente in un caso di sicurezza nazionale sarà disposto a investire cospicue risorse per proteggere le comunicazioni riguardanti il processo; un genitore che invia email con “foto di gattini simpatici” ai propri figli non sarà disposta ad investire un granché per proteggere tali comunicazioni.

**Cosa fare?** Mettiamo giù una lista di opzioni che abbiamo a disposizione per mitigare le minacce specifiche che ci riguardano. Nel farlo, dobbiamo considerare le nostre risorse finanziarie, tecniche o sociali.

## **1.8 Per concludere: siamo solo all'inizio**

Ricordiamoci che una pianificazione della sicurezza cambia nel tempo, perché nel tempo cambiano le nostre situazioni.

## *Guida Galattica di Autodifesa Digitale*

Pertanto è bene revisionare con regolarità le nostre scelte. Concretamente, una volta terminata una pianificazione in base alla situazione corrente, mettiamoci un promemoria sul calendario per ripetere la stessa attività, eventualmente riconsiderando le nostre valutazioni.

Partiremo da una delle esigenze essenziali: comunicare con gli altri. Nel prossimo capitolo vedremo come comunicare in modo sicuro.

## CAPITOLO 2

# *Comunicare in modo sicuro*

---

La comunicazione non è mai stata così facile grazie alle reti di telecomunicazioni ed Internet. Di pari passo, non è mai stato così facile intercettare le comunicazioni dei loro utenti.

Senza le opportune accortezze per salvaguardare la nostra privacy—e quella di chi comunica con noi—qualsiasi telefonata, messaggio, video chiamata, chat o altra attività sulle social network, sono in qualche modo intercettabili. Volendo riprendere la terminologia introdotta nel Capitolo 1, esiste una minaccia costituita da un avversario (ad esempio, un oppositore politico, un governo, un criminale) interessato a leggere le nostre comunicazioni—che in questo esempio sono gli asset che vogliamo proteggere.

Spesso, il modo più sicuro per comunicare in modo strettamente riservato sarebbe di persona, senza computer

o telefoni. Non essendo questo sempre possibile, la seconda migliore alternativa è l'utilizzo di sistemi di comunicazione digitale basati su cifratura "end to end," ovvero da un capo della comunicazione all'altro.

## **2.1 Come funziona la cifratura "end to end"?**

La cifratura, o crittografia, "end to end" garantisce che l'informazione (che vogliamo proteggere) sia "codificata" dal mittente iniziale (il primo capo, o "end") in modo tale che sia "decodificabile" solo e soltanto dal destinatario finale (il secondo capo, o "end"). Questo significa che nessuno, al di fuori di mittente e destinatario, può capire il contenuto di una comunicazione cifrata. Attenzione: non stiamo dicendo che un aggressore in una rete Wi-Fi pubblica, il vostro provider Internet, etc., non possano leggere il contenuto delle nostre comunicazioni. Semplicemente non potranno comprenderne il contenuto—in quanto, appunto, cifrate.

## **2.2 Garanzie di una cifratura "end to end"**

Se un sistema di cifratura "end to end" è progettato e realizzato correttamente, nessuno—nemmeno chi l'ha costrui-

to—può accedere al contenuto delle informazioni (cifrate) che vi transitano. Ad esempio, nemmeno Facebook (che gestisce WhatsApp) può sapere i contenuti in chiaro dei messaggi (testuali, vocali, multimediali, etc.) che ci scambiamo. Stesso discorso per Telegram o Signal: è matematicamente dimostrabile che, se usate correttamente, nessuno—al di fuori di chi ha accesso ai due dispositivi che si “parlano”, ovviamente—può decifrare il contenuto. Il fatto che noi—in quanto utenti—vediamo i nostri messaggi in chiaro, non significa che questi non siano cifrati: semplicemente, non ci accorgiamo di quest’operazione, che il software (le app) svolge automaticamente per noi.

## **2.3 Attenzione ai dettagli**

La cifratura “end to end” può essere applicata a qualsiasi tipo di comunicazione: testo, immagini, video, audio, etc. Non confondiamola con il “lucchetto” che appare sul nostro programma di navigazione quando navighiamo su un sito il cui indirizzo inizia con <https://>: tale cifratura, “di trasporto”, si limita a crittografare la comunicazione tra noi e il server, non tra noi e i destinatari. Ad esempio, immaginiamo che qualcuno abbia creato un ipotetico sito, chiamiamolo Chat Sicura (<https://chatsicura.it>) per comunicare con altre persone. Anche se “c’è il lucchetto” e c’è [//](https://), l’uni-

ca garanzia che abbiamo è che nessuno tra noi e il server chatsicura.it potrà leggere le nostre comunicazioni. Se non è utilizzata cifratura “end to end”, i gestori di Chat Sicura saranno in grado invece di leggere il contenuto, proprio perché i dati sono cifrati sul nostro dispositivo e decifrati sui server di Chat Sicura.

## **2.4 Creazione e scambio delle chiavi**

Premetto che quando usiamo WhatsApp, Telegram, Signal, o altri strumenti basati su cifratura “end to end”, non vediamo nulla di tutto questo, che avviene automaticamente.

La cifratura “end to end” funziona in questo modo. Quando due persone (chiamiamole Alice e Bob) vogliono comunicare, ognuno dovrà generare delle chiavi uniche—normalmente due per ogni soggetto, una per cifrare e una per decifrare. Queste chiavi sono poi utilizzate dal sistema (dall’app) per codificare i dati in modo tale che, attraverso una serie di trasformazioni matematiche, soltanto chi è in possesso della corrispondente chiave per decifrare, sarà in grado di effettuare l’operazione inversa, e quindi leggere il testo in chiaro. Quindi se Alice usa la chiave di Bob per cifrare un messaggio, soltanto Bob potrà decifrarlo, perché solo lui è in possesso per la chiave per decifrare. Quindi, tornando all’esempio di WhatsApp, Telegram o Signal, i dati che pas-

## *Guida Galattica di Autodifesa Digitale*

sano sui rispettivi server saranno cifrati con le chiavi dei destinatari (ad esempio, quella di Bob), pertanto nessuno, nemmeno i gestori dei rispettivi servizi, potranno decifrarli, perché le chiavi restano sui dispositivi di chi le ha generate.

Alcuni servizi di comunicazione, come ad esempio Google Hangouts, per citarne uno, pubblicizzano l'uso di "crittografia", ma utilizzano chiavi generate e controllate da Google, non dagli utenti finali che comunicano. Questa non è crittografia "end to end". Per essere veramente sicura, solo i due capi della conversazione devono essere in possesso dei segreti (le chiavi) necessari per cifrare e decifrare le informazioni che transitano. È un po' come se l'installatore del vostro antifurto vi impostasse il codice segreto: dovreste essere voi a impostarlo, in sua assenza.

### **2.5 Un solo segreto, da custodire con cura**

Chiaramente, un sistema basato su cifratura "end to end" implica che gli utenti conservino correttamente le chiavi. Se una chiave (o il dispositivo, lo smartphone che la memorizza) viene persa, ovviamente chi ne entra in possesso potrà leggere le comunicazioni del legittimo proprietario—o scrivere messaggi per conto suo. Notate che "perdere" qui non significa necessariamente "perdere fisicamente". Per fare un esempio concreto, se qualcuno vuole origliare in casa

## *Guida Galattica di Autodifesa Digitale*

vostra non è necessario che sia presente in casa vostra; gli basta installare una microspia e sparire. Allo stesso modo, se qualcuno riesce a prendere il controllo del nostro smartphone, anche solo per pochi minuti, potrebbe essere in grado di installare un software per leggere le vostre chat, in barba alla cifratura “end to end”—proprio perché si troverebbe nella posizione di poter accedere non soltanto alle chiavi, ma anche ai messaggi che, giustamente, dovranno essere decifrati.

Se un’app di comunicazione basata su cifratura “end to end” è progettata bene, avrà degli opportuni meccanismi di isolamento dei dati, per conservare con cura le chiavi, in modo che non sia così semplice rubarle. Qui il ruolo del sistema operativo sottostante (macOS, Windows, Android, iOS) è pure fondamentale. Se app e sistema operativo sono di qualità, saranno necessari almeno privilegi di amministratore per riuscire a rubare le chiavi, e comunque non dovrebbe essere affatto un’operazione facile

## **2.6 Chi mi dice che sei proprio tu?**

L’altra domanda che sicuramente vi sarete posti è: quando vengono generate le chiavi? Risposta breve: al primo avvio. E poi: come facciamo ad esser sicuri che “Alice sia proprio Alice” e “Bob sia proprio Bob”? È sufficiente fidar-

## *Guida Galattica di Autodifesa Digitale*

si del numero di telefono (nel caso di WhatsApp, Signal o Telegram)? Riposta breve: no.

Le chiavi vengono generate “al primo avvio” dell’applicazione in questione e da quel momento sono “legate” all’identità associata a quel dispositivo. In soldoni, significa semplicemente che, da quel momento in poi, tale dispositivo contiene tali chiavi. Se cambiate dispositivo, le chiavi si perdono e ne vanno rigenerate di nuove. No, non si possono “portare dietro”, perché se così fosse significa che c’è un modo semplice per leggerle e copiarle, pertanto significherebbe che non sono conservate in modo sicuro.

E come faccio a sapere che il mio amico Mario con cui sto chattando...sia proprio lui? Se un sistema “end to end” è fatto bene, ci deve dare la possibilità di verificare le chiavi reciprocamente con i nostri destinatari. Questo avviene e deve avvenire necessariamente di persona. O, quantomeno, attraverso un altro canale di comunicazione precedentemente instaurato, di cui già ci fidiamo, e che sappiamo per certo essere associato al nostro amico Mario. In altre parole: non possiamo utilizzare WhatsApp per verificare se stiamo chattando con “il vero Mario” via WhatsApp. Sarebbe come chiedere all’oste se il vino è buono. Funziona che ci dobbiamo trovare di persona, guardarci in faccia (se non ci conosciamo, usare i documenti di identità) e, utilizzando l’opportuna funzione messa a disposizione dal sistema,

## *Guida Galattica di Autodifesa Digitale*

verificare le chiavi. Ad esempio, Signal permette di farlo con un QR code da inquadrare con la telecamera dello smartphone.

Se un sistema di messaggistica non ci dà la possibilità di verificare autonomamente le chiavi, allora significa che, usandolo, ci stiamo automaticamente fidando di un sistema non del tutto trasparente.

### **2.7 Telefonate e SMS**

Quando facciamo una telefonata o inviamo un SMS, l'audio della telefonata e il testo del messaggio non sono cifrate per nulla—men che meno sono cifrate “end to end”. Entrambi sono infatti intercettabili, ad esempio da un'agenzia governativa o da chi ha potere sulle compagnie telefoniche.

Se nella nostra pianificazione della sicurezza (affrontata nel Capitolo 1) abbiamo concluso che tra i nostri avversari potrebbe esserci un'agenzia governativa, allora dovremmo evitare di utilizzare telefonate ed SMS tradizionali e passare ad alternative sicure, con il bonus di avere anche video-chiamate, come le già citate WhatsApp e Signal (a cui aggiungo Wire). Tutte permettono, oltre alla comunicazione scritta, di effettuare chiamate audio-video cifrate “end to end”, al contrario di altri servizi che invece non offrono

questa garanzia, come Google Hangouts, Kakao Talk, Line, Snapchat, WeChat, QQ, Yahoo Messenger.

Alcuni servizi come Facebook Messenger e Telegram offrono cifratura “end to end” solo se abilitata manualmente dall’utente. Altri, come iMessage di Apple, offre cifratura “end to end” solo se entrambi i capi della conversazione usano lo stesso tipo di dispositivi (nel caso di iMessage, entrambi gli utenti devono utilizzare un iPhone).

## **2.8 Quanto possiamo fidarci di un sistema di comunicazione?**

I sistemi di comunicazione, anche se basati su cifratura “end to end”, sono prodotti da qualcuno. Ci permettono sicuramente di difenderci da avversari come enti governativi, criminali informatici, e il servizio di comunicazione stesso, ma non coprono un caso. Nessuno impedisce a questi soggetti di nascondere delle modifiche nelle app stesse, delle cosiddette “porte sul retro” (backdoor), o semplicemente dei “difetti” che di fatto semplificano la vita di un criminale che “ascolta sul filo” e vuole decifrare le nostre comunicazioni.

Diversi gruppi indipendenti, come ad esempio l’EFF, passano parecchio tempo a verificare che i gestori famosi (tra cui ad esempio WhatsApp, che è gestita da Facebook, o

## *Guida Galattica di Autodifesa Digitale*

Signal) facciano ciò che promettono in termini di cifratura. Sempre meglio di un sistema non trasparente, o peggio che non usa cifratura “end to end”. Tuttavia, non c’è soluzione semplice per eliminare anche questo piccolo pezzetto di “fiducia” residua, che dobbiamo necessariamente porre in chi realizza e gestisce gli strumenti che decidiamo di utilizzare per comunicare.

A dirla proprio tutta, esistono delle soluzioni “aperte”, che non si basano su alcun gestore o produttore centralizzato, e che permettono a chiunque di poter verificare non soltanto le chiavi, ma anche il prodotto, il software stesso, per controllare che faccia esattamente ciò che promette. Cosa che invece non è semplice fare ad esempio con WhatsApp, in quanto tra tutti il più chiuso. Tali sistemi aperti e decentralizzati, tuttavia, sono decisamente poco vicini all’utente, sono complicati da configurare e utilizzare, e sono generalmente basati su sistemi di cifratura un po’ datati.

### **2.9 Cosa non fa la cifratura “end to end”**

La cifratura “end to end” protegge i contenuti, non il meno—ma rilevante—fatto che stiate comunicando. Più in generale, non protegge i cosiddetti metadati, ovvero i “dati che descrivono altri dati”—in questo caso “dati che descrivono il fatto che stiate comunicando con qualcuno”, dati di

## *Guida Galattica di Autodifesa Digitale*

contorno. Tra i metadati vi sono, ad esempio, data e ora di inizio e fine di una telefonata, numero di telefono (o indirizzo email) di mittente e destinatario, e spesso anche la posizione geografica. Tipologia e quantità di metadati variano a seconda del sistema che si impiega. Ad esempio, WhatsApp colleziona molti più metadati rispetto a Telegram. Signal ne colleziona il minimo indispensabile al funzionamento e infatti è considerato il più sicuro e riservato dei tre.

Perché i metadati possono essere un problema? Perché indirettamente dicono molto su una conversazione, anche quando il contenuto stesso della conversazione è cifrato. Ad esempio:

- Non si sa di cosa abbia parlato Mario al telefono alle 2:24 di notte per 18 minuti, ma si sa che il numero chiamato (che è un metadato) è di un servizio di telefonate “per adulti”.
- Si sa che avete chiamato una linea di prevenzione suicidi mentre vi trovavate sul ponte di Brooklyn, ma non si sa di cosa abbiate parlato.
- Si sa che qualcuno ha chiamato, in quest’ordine, un centro per fare test HIV, il suo medico, e poi l’assicura-

zione sanitaria privata, ma non si conosce il contenuto delle telefonate.

Eccetera, eccetera, eccetera. Chiaro il punto? I metadati, se opportunamente analizzati, possono rivelare molto sul contenuto di una conversazione, anche se il contenuto è perfettamente cifrato.

## **2.10 C'è altro oltre la cifratura "end to end"**

La cifratura "end to end" è importante, ma è solo una delle tante caratteristiche di un sistema di comunicazione sicuro. Come detto, è perfetta per chi vuole evitare di essere spiato da agenzie governative o aziende con molto potere. Tuttavia, per la maggior parte degli individui, nessuno di questi costituisce una minaccia. Pertanto, comunicare in modo cifrato non è la soluzione prioritaria.

Per esempio, immaginate che tra gli avversari da cui vogliamo proteggerci ci sia il nostro datore di lavoro, un nostro co-inquilino, o chi, in generale, può facilmente avere accesso fisico ai nostri dispositivi—anche per qualche istante. Con avversari dotati di tali capacità, la cifratura "end to end" end non aiuta, perché i messaggi vengono decifrati e memorizzati sui dispositivi. Contro tali avversari è molto

## *Guida Galattica di Autodifesa Digitale*

più utile avere messaggi “effimeri”, ovvero messaggi che si autodistruggono dopo qualche tempo.

Altri soggetti potrebbero invece esser più preoccupati dal fatto di dover fornire a qualcuno il proprio numero di telefono, ma non dal contenuto delle telefonate e dei messaggi scambiati. Per tali soggetti, avere la possibilità di usare un numero “alias”, non legato alla propria persona fisica, è più importante di una cifratura “end to end”.

Altri fattori importanti da considerare per comunicare in modo sicuro vanno oltre le caratteristiche di sicurezza e riservatezza. Un’app molto sicura è inutile se nessuno dei vostri amici la usa, perché magari è difficile da installare o configurare, oppure è costosa, lenta, o la qualità del servizio è bassa.

### **2.11 Per concludere: calma e consapevolezza prima di tutto**

Ancora una volta è necessario sedersi con calma e riflettere, per capire chiaramente quali caratteristiche sono importanti, nel nostro specifico caso, per comunicare in modo sicuro. Compreso questo sarà più facile orientarsi nel vasto e intricato panorama delle offerte, commerciali e non.

## CAPITOLO 3

# *Uso consapevole dei social media*

---

I social media (o “i social”, come va di moda) sono tra i siti web più polari. Facebook ha quasi due miliardi e mezzo di utenti, e Instagram e Twitter ne contano centinaia di milioni.

Concepiti originariamente per condividere pensieri, fotografie e informazioni personali, i social network sono oggi l’equivalente delle piazze, dove si discute, ci si organizza, si prendono decisioni e si creano correnti di pensiero. Tutte queste attività possono essere svolte consapevolmente e nel rispetto della privacy degli utenti, ma non è spesso questo il primario interesse di chi opera e gestisce i social media. Vedremo a breve il perché.

## *Guida Galattica di Autodifesa Digitale*

Quando si decide di utilizzare un social media è bene considerare queste domande: mi serve davvero? Posso interagire in un social network mantenendo un adeguato livello di privacy? Posso tenere segreta la mia identità? I miei contatti e le associazioni di cui faccio parte? Che informazioni voglio tenere private e da chi voglio nasconderle?

A seconda delle circostanze, ciascuno di noi potrebbe volersi proteggere o dal gestore del social network stesso (che quindi, seguendo quanto visto nel Capitolo 1, è nostro avversario), o da altri utenti della stessa—o entrambe le cose.

### **3.1 Suggerimenti per creare un profilo online**

Vogliamo utilizzare il nostro vero nome? Alcuni siti richiedono che si usi il nome vero (la cosiddetta “real name policy,” secondo la quale, se ognuno utilizza sempre e solo il proprio nome vero, questo aiuterebbe a creare una diffusa fiducia nel prossimo, e quindi a comunicare in maniera più sicura), anche se nel corso degli anni questo vincolo è stato rilassato. Se non ce la sentiamo di usare il nostro vero nome, non usiamolo!

Quando ci registriamo, non esageriamo con i dettagli:

## *Guida Galattica di Autodifesa Digitale*

inseriamo lo stretto indispensabile. Se vogliamo proteggere la nostra vera identità, meglio utilizzare un indirizzo email “ad hoc”, non usato altrove, ed evitiamo di utilizzare il nostro numero di telefono personale. Questi due dati (email e numero di telefono) ci identificano “univocamente” e possono essere impiegati per correlare account tra social network distinti—anche se sotto nomi diversi.

Scegliamo la foto del profilo con attenzione. Non solo ogni fotografia contiene dei metadati (invisibili se non si sa come cercarli, come ad esempio le coordinate geografiche e la data e l’ora dello scatto), ma anche l’immagine in sé potrebbe rivelare informazioni su di noi. La foto è stata scattata nelle vicinanze della nostra abitazione, posto di lavoro, o altro luogo riservato? Ci sono cartelli stradali o indirizzi visibili?

Scegliere una password robusta, univoca, e abilitare l’autenticazione a due fattori (2FA). Queste raccomandazioni non valgono soltanto per l’uso dei social media, quindi ne parlerò in seguito in una parte dedicata.

Molte piattaforme di social media—come d’altronde molti siti—offrono le cosiddette domande segrete per reimpostare una password, nel caso questa vada persa: “Qual è il nome del tuo gatto?”, “Dove vivevi da giovane?”, etc. Alcune delle risposte a queste domande possono essere facilmente ottenute rovistando tra la nostra attività online, sui

social media stessi. Inoltre, se si tratta effettivamente di segreti, potreste non volerli rivelare a chi gestisce la piattaforma. Quindi è bene scegliere delle risposte deliberatamente false. E se dimentichiamo le risposte false? Ne parleremo in futuro, sempre nella parte dedicata alla gestione delle password, e dei segreti in generale.

## **3.2 Una sfogliata alla privacy policy**

Leggere integralmente una privacy policy è un’impresa per pochi. Tuttavia, vale la pena dare almeno un’occhiata alla sezione che riguarda i nostri dati, come vengono impiegati, se e con quali finalità vengono condivisi e con quali terze parti, e come il gestore risponde alle richieste delle forze dell’ordine—cosa richiede, in caso di reato, per accedere ai dati riservati di un sospettato?

L’azienda che gestisce un social network è orientata al profitto. Quindi, cinicamente, il “prodotto” siamo noi. O meglio: i dati che produciamo e consumiamo attraverso i social sono ciò che viene monetizzato—attraverso pubblicità e altri accordi commerciali con terze parti. Per questo motivo, i gestori delle piattaforme social raccolgono spesso una grande quantità di dati da ciascuno degli utenti, andando anche oltre quanto noi consapevolmente condividiamo. Dove ci troviamo, quali sono i nostri interessi, a quali pub-

blicità reagiamo e come, quali altri siti visitiamo, anche e soprattutto al di fuori dai social network stessi. Se vogliamo evitare che il gestore della piattaforma conosca e possa utilizzare queste informazioni è meglio utilizzare browser (ad esempio Firefox o Brave, oppure con opportune estensioni) che bloccano il “tracking” (e quindi la propagazione) di queste informazioni che implicitamente produciamo semplicemente perché “siamo online”.

### **3.3 Modificare le impostazioni di sicurezza e privacy**

Per esempio, vogliamo che tutti i nostri post siano visibili a tutti (anche a chi non ha un account social), oppure solo a una ristretta cerchia di utenti? Vogliamo che il nostro profilo sia rintracciabile attraverso il nostro indirizzo email o numero di telefono? Vogliamo che la nostra posizione sia condivisa automaticamente? Con chi?

Anche se ogni social network ha le sue specifiche impostazioni, possiamo dividere le impostazioni in due macro gruppi:

- Le impostazioni di **sicurezza** ci permettono di bloccare o “zittire” alcuni account, di essere notificati di attività sospetta (ad esempio se qualcuno tenta di “for-

## *Guida Galattica di Autodifesa Digitale*

zare” il nostro account). Qui è anche possibile reimpostare la propria password, (dis)attivare l'autenticazione a due fattori (2FA), aggiungere un indirizzo email o numero di telefono “di emergenza”, a cui inviare le informazioni per il reset delle credenziali. Inutile sottolineare la criticità di questi dettagli.

- Le impostazioni di **privacy** riguardano invece “chi può vedere cosa”. Qui possiamo specificare quali categorie di utenti (tutti, amici di amici, amici, etc.) possono vedere quale contenuto (posizione, foto, contatti, tag), e se è possibile trovare il nostro nome nel motore di ricerca del social network.

Alcuni siti offrono dei “check up” di sicurezza e privacy. Facebook e Google sono probabilmente i migliori esempi. Si tratta di procedure guidate che spiegano passo passo, in linguaggio semplice, come impostare le opzioni di sicurezza e privacy. Sono uno strumento eccellente per la maggior parte degli utenti e un ottimo punto di partenza per i più esperti.

Infine, ricordiamoci che queste impostazioni sono soggette a modifiche. A volte diventano più restrittive, permettono un controllo più granulare; a volte il contrario. Normalmente si viene informati via email quando vengono ap-

portate modifiche sostanziali. È bene prendere seriamente questi aggiornamenti.

### **3.4 Compartimentare informazioni e account**

Per alcuni è molto importante avere diverse identità virtuali—per motivi legittimi. Pensiamo ad esempio ai social network, account pseudonimi, in varie community online, siti di incontri, siti di networking professionale.

Numeri di telefono e fotografie sono due categorie dati che richiedono molta attenzione. Le foto, in particolare, possono permettere di “collegare” due account che intendevamo tenere separati—ad esempio, due profili sotto nomi diversi con medesima foto.

Se dobbiamo rimanere anonimi o tenere separate le identità associate a due profili distinti dobbiamo utilizzare foto univoche, non reperite online. Utilizzando Google Immagini è infatti possibile usare una foto per cercarne un’altra identica o simile. Questa funzionalità permette a noi di controllare se una foto che abbiamo deciso di usare è facilmente reperibile online, e ad un nostro avversario di risalire al sito di origine di tale foto. Un simile discorso vale per altre informazioni quali numero di telefono, soprannome e

indirizzo email.

### **3.5 Gruppi di discussione, con consapevolezza**

I gruppi di discussione nascono come i funghi, perché è diventato estremamente semplice e veloce crearli. Dal go-liardico gruppo WhatsApp o Telegram per organizzare il sabato sera, alla miriade di gruppi Facebook (su invito e pubblici) in cui si discutono temi di rilievo.

È bene sapere che, a seconda della piattaforma che state utilizzando, l'amministratore del gruppo ha normalmente accesso a più informazioni di un normale membro, e che anche un normale membro può vedere chi altro fa parte del gruppo. Il livello di accesso alle informazioni può variare da gruppo a gruppo ma anche a seconda dalla piattaforma: ad esempio in un gruppo Telegram nemmeno l'amministratore può sapere il numero di telefono degli altri membri (salvo quelli che abbiamo già in rubrica, ovviamente), mentre in un gruppo WhatsApp “tutti vedono tutto”.

Man mano che i gruppi crescono è difficile tenere traccia di chi ne fa parte, e più un gruppo è frequentato più è probabile che qualcosa possa sfuggire di mano all'amministratore—che, ad esempio, potrebbe approvare l'ingresso

di un membro senza controllarne a fondo le credenziali, dando quindi accesso a degli sconosciuti.

### **3.6 Per concludere: Sicurezza e privacy sono sport di squadra**

Non limitiamoci ad usare consapevolmente gli strumenti che i social media ci offrono. Facciamo un passo in più e parliamone con i nostri amici, specie se notiamo che stanno inconsapevolmente rivelando informazioni sensibili. Anche senza avere un account, e anche se rimuoviamo i tag sulle foto e sui post dei nostri amici, una foto di gruppo in cui compare la nostra faccia è sufficiente per sapere che quel giorno eravamo in quel luogo con tali persone.

Sicurezza e privacy sono, come abbiamo detto nel Capitolo 1, un processo: questo vale per le grandi realtà aziendali, ma anche per noi stessi; non limitiamoci a salvaguardare la nostra sicurezza, ma informiamo chi ci sta attorno.

## CAPITOLO 4

# *Password e altri segreti*

---

In questo terzo capitolo impariamo a capire il valore dei nostri segreti e come ragionare per metterli in sicurezza.

### **4.1 Password, passphrase e segreti**

Nella guida originale dell'EFF, da cui la presente è derivata, questa sezione è posticipata. Credo invece che sia fondamentale chiarire subito alcuni punti. Il concetto di “password” (parola chiave), è noto, ma non è mai ribadito abbastanza quanto sia importante la sua robustezza. Una password è tanto più robusta quanto più è difficile da ottenere per un avversario. L'avversario ha tre modi per farlo:

- rubarla (ad esempio da un sito che la memorizza, e che poi viene compromesso),

## *Guida Galattica di Autodifesa Digitale*

- indovinarla (basandosi su altre informazioni, ad esempio su di noi),
- trovarla per enumerazione esaustiva.

Contro il furto, la robustezza di una password non può farci niente: se c'è un leak di dati, è andata e bisogna cambiarla immediatamente. La robustezza ha a che fare con gli ultimi due punti. Una password non deve essere in alcun modo relazionata o riconducibile a noi come individui (virtuali o esseri umani), al nostro circolo sociale, alla nostra famiglia, etc. Inoltre, deve essere sufficientemente lunga e complessa affinché sia sconveniente (in termini di tempo) per l'avversario mettersi a provarle tutte: talmente sconveniente che l'avversario non possa attendere così a lungo.

Questi requisiti fanno sostanzialmente a pugni con il fattore umano, che determina l'accettabilità di una soluzione tecnica (e quindi, a lungo termine, la sua scomparsa o meno). Se una password è lunga, complessa e non riconducibile a noi, come facciamo a ricordarcela? Non ce la ricordiamo: semplicemente saremmo forzati a scriverla da qualche parte. Purtroppo, anche con le soluzioni basate su password manager—che vedremo tra poco—c'è un residuo di segreti che dobbiamo necessariamente memorizzare.

## *Guida Galattica di Autodifesa Digitale*

Quindi come si fa? Le password complesse sono difficili da pronunciare, tantomeno mnemoniche. Un approccio per ottenere una buona robustezza è puntare sulla lunghezza. Stiamo parlando delle passphrase (tradotto, frasi chiave): frasi composte da parole (facili da ricordare in quanto tali), almeno 4. Attenzione però, non deve trattarsi di una frase né di senso compiuto né famosa. La passphrase perfetta è composta da “parole a caso”. Se proprio ci manca la fantasia, esistono dei generatori che pescano parole a caso da un dizionario.

È più facile ricordare una passphrase? Sicuramente è più mnemonica di una password parimenti robusta. Per esempio, la passphrase “umani rompere deleterio fioraio” (che, dopo averla scritta un paio di volte, ce la ricordiamo) si becca in milioni di miliardi di secoli con un computer in grado di fare decine di migliaia di tentativi al secondo. Al contrario, la password “A3assl3C814753sds” che sembra robusta, richiederebbe meno di 2 miliardi di secondi, ma è sostanzialmente impossibile da memorizzare. Se poi cerchiamo delle password complesse ma “umane”, tipo “P1r4tesOfTh3Web”, che comunque sembra robusta, richiederebbe solo 2 giorni di tentativi. Se volete divertirvi a fare calcoli analoghi potete usare <https://www.useapassphrase.com> o strumenti simili.

## 4.2 Creare password robuste “automagicamente”

Riutilizzare la stessa password su più account distinti è una pessima idea. Se qualcuno dovesse rubarla—o indovinarla—avrebbe accesso a tutti gli account per cui è utilizzata. È quindi fondamentale utilizzare password univoche e robuste. Fortunatamente ci sono oggi app e programmi facili da utilizzare per generare e gestire password, e segreti, più in generale. Questi “password manager” (in italiano, “gestori delle password”) sono in grado di generare e memorizzare password in modo sicuro, così da poterne usare una per ogni account, senza necessità di memorizzarle tutte.

Un gestore di password fa tutto questo per noi:

- Genera password robuste e complesse, difficili da indovinare per chiunque.
- Memorizza in modo cifrato una grande quantità di password e altri segreti (risposte alle domande di sicurezza, numeri di carte di credito, scansioni di documenti).
- La cifratura, e quindi tutto l’archivio di segreti, è protetto con una singola password—detta master password.

## *Guida Galattica di Autodifesa Digitale*

I più acuti avranno notato che stiamo proteggendo un certo numero di asset (le nostre credenziali) ricorrendo a un sistema (il password manager) la cui sicurezza dipende da un solo asset: la master password. Abbiamo ridotto il numero di asset da molti a uno.

Di conseguenza:

- il password manager diventa un “single point of failure”
- i password manager diventano oggetto di interesse per gli avversari, ovvero aumentano le minacce
- essendo essi stessi dei software hanno naturalmente dei difetti, che li rendono vulnerabili ad attacchi specifici

Ovviamente, stiamo assumendo che il dispositivo (computer, smartphone, server) che ospita il password manager sia fidato e non compromesso ad esempio da un software malevolo (malware). Stesso discorso vale per il password manager stesso: in base alle nostre aspettative dovremo scegliere di quale software fidarci. Generalmente, come per tutti i software, la scelta spazia tra: un software libero, open source, di cui conosciamo il codice sorgente, abbastanza diffuso; oppure, una soluzione chiusa, proprietaria, fornita da

## *Guida Galattica di Autodifesa Digitale*

un’azienda con una reputazione da mantenere, con un ampia base di utenti, cospicuo giro d'affari e, quindi, risorse per frequenti screening di sicurezza—di cui raramente sapremo i risultati. Non è questa la sede, ma entrambi gli approcci hanno pregi e difetti.

Se pensiamo di essere a rischio di un attacco informatico sofisticato (ad esempio, da parte di agenzie governative, stati nemici, etc.), allora potremmo considerare un’alternativa più semplice. Per esempio, possiamo creare delle passphrase e annotarle su un taccuino che teniamo sempre con noi o in un posto sicuro. È una soluzione un po’ contro tendenza, che ci fa riflettere proprio sull’importanza di una corretta analisi del rischio. Se davvero siamo minacciati da un avversario potente e se nel nostro password manager c’è un’informazione (asset) importante, allora è ragionevole pensare che quest’avversario avrà mezzi tali da arrivare e compromettere il nostro computer, per rubare la parola chiave per sbloccare il nostro gestore delle nostre password. Pertanto ha senso considerare alternative per togliere l’asset dalla portata di un attacco informatico. Inoltre, anche se in modo non sofisticato, è sempre meglio avere password uniche annotate da qualche parte, piuttosto che riutilizzare le stesse 2-3 password e tenercelle in testa. Avendole annotate, in caso di problemi, sapremo esattamente quali sono le nostre password e quali cambiare, se necessario.

### 4.3 password da memorizzare

Sono poche le password che non è necessario—e talvolta non è consigliabile—mettere in un password manager:

le password di sblocco di un dispositivo le password di cifratura di un disco, perché questa viene chiesta all'avvio di un computer (vedremo in futuro cosa significa) la master password del nostro password manager

Ove possibile, queste dovrebbero essere sostituite con delle passphrase. A volte non è possibile usare delle passphrase, a causa delle politiche di complessità delle password, che spesso remano nella direzione opposta. Pertanto è necessario utilizzare un password manager.

### 4.4 Una nota sulle “domande di sicurezza”

Ne abbiamo già parlato nel Capitolo 3 di questa guida: facciamo attenzione alle “domande di sicurezza” usate da alcuni siti per confermare la nostra identità e permetterci di re-impostare una password persa.

Prima di tutto ricordiamoci che le risposte sostituiscono la nostra password persa, quindi chi le conosce è quasi come se conoscesse la nostra password, perché potrà reimpostarne una. Sottolineiamo “quasi” perché a volte que-

## *Guida Galattica di Autodifesa Digitale*

ste domande vengono poste all’utente solo dopo aver inserito altre informazioni segrete, come ad esempio il numero di cellulare—in altre parole, fungono da conferma, da secondo fattore.

Altro aspetto fondamentale da ricordare è che, se corrispondenti alla realtà, alcune risposte alle domande possono essere indovinate o reperite online. Pensiamo ad esempio alla nostra data di nascita, al nome del nostro animale domestico (in quanti diffondono foto e nomi dei propri animali domestici?), etc. Il modo sicuro di impostare le risposte è di generarle in modo casuale e memorizzarle in un password manager. E chiaramente, non vanno riutilizzate le stesse risposte—esattamente come non si fa per le password.

Cerchiamo di fare mente locale e fare una lista dei siti dove abbiamo inserito domande di sicurezza e mettiamoci al lavoro.

### **4.5 Sincronizzare le password su più dispositivi**

Molti password manager ci permettono di accedere alle password e gestirle da più dispositivi, più o meno automaticamente. Ogni password manager implementa a suo modo la

sincronizzazione dei dati: alcuni usano un semplice file (ad esempio memorizzato su servizi come Dropbox o simili), altri si basano su un’infrastruttura cloud proprietaria.

L’ineggabile vantaggio di permettervi di accedere alle nostre password da più dispositivi ha il prezzo di un rischio più elevato. Un avversario che vuole accedere alle informazioni di un password manager completamente “offline” dovrà riuscire prima ad accedere al nostro dispositivo. Al contrario, se il file è “sempre online” (perché deve esserlo, inevitabilmente), allora l’avversario proverà ad attaccare il servizio cloud dove è memorizzato—che, in molti casi, può essere più semplice che accedere al nostro dispositivo.

Ancora una volta si tratta di valutare il rischio e capire se è il caso di investire risorse nel proteggersi dall’uno o dall’altro caso, o da nessuno dei due. Indipendentemente dalla nostra valutazione, è generalmente una buona idea tenere una copia di backup del database del password manager, perché in caso di perdita potremmo non poter più accedere alle nostre password e ai nostri segreti.

## 4.6 Autenticazione a più fattori

Scegliere password robuste e distinte per ogni sito diminuisce drasticamente il successo di un avversario che vuole accedere ai nostri account. Tuttavia, in una buona pianifi-

## *Guida Galattica di Autodifesa Digitale*

cazione della sicurezza dobbiamo considerare l’ipotesi che, prima o dopo, qualche credenziale possa andar persa, trafugata, rubata. Le password sono tipicamente il primo fattore di autenticazione. È oggi molto comune avere un secondo fattore di autenticazione, che serve a confermare che siamo veramente noi ad essere in possesso di quel segreto (primo fattore), e non chi ce l’ha rubato.

Come si fa? Le password sono “qualcosa che l’utente sa”. Il secondo fattore deve essere qualcosa di diverso: “qualcosa che l’utente possiede” (un dispositivo fisico, difficile da rubare), o “qualcosa che l’utente è” (le impronte digitali). La logica dell’autenticazione a più fattori consiste nel fatto che è molto più difficile rubare tutti i fattori contemporaneamente. Sarà anche facile clonare le impronte digitali, ma se queste sono usate solo come un secondo fattore (e non in sostituzione delle password), sarà difficile che un avversario riesca a rubarci sia una password che le impronte digitali. Stesso discorso vale per quei dispositivi che generano numeri apparentemente casuali, recentemente sostituiti sempre di più dai cellulari, con ovvi vantaggi di usabilità a scapito di un lieve aumento del rischio di sicurezza.

## 4.7 Fattori: ciò che si sa, ciò che si ha, ciò che si è

Un'autenticazione a due fattori (o fasi) ben fatta richiede sempre che l'utente si identifichi (a volte di persona) presso l'entità che rilascia il secondo fattore. Ad esempio, bisognava andare fisicamente in banca per dimostrare la nostra identità fisica affinché ci fornissero un token (che altro non è che un dispositivo che contiene una chiave crittografica unicamente associata al nostro account), che ogni 30-60 sparava fuori un numero diverso ogni volta, detto anche one-time password (OTP). Impropriamente aggiungerei. Perché un OTP è una password che, solo quando usata, non vale più. Mentre i codici generati da un token non sono più validi dopo 30-60, a prescindere che vengano usati. È diverso, ma l'effetto finale è lo stesso.

Questo approccio piuttosto macchinoso—però piuttosto sicuro—non avrebbe mai preso piede su larga scala. I vari siti con milioni o miliardi di utenti non avrebbero mai potuto identifierli tutti di persona, consegnando ad ognuno un dispositivo fisico. Si iniziò a usare gli SMS, quindi la logica diventò: “tu possiedi il tuo cellulare, quindi solo tu puoi ricevere un SMS con un codice”. L'ovvio vantaggio è che diventa immediatamente alla portata di chiunque, su scala globale. Il prezzo da pagare? Nel Capitolo 2 di

questa guida, quando abbiamo parlato di come comunicare in modo sicuro, abbiamo visto che, tra tutti i mezzi di comunicazione, gli SMS sono facilmente intercettabili.

Tuttavia questo cambiamento permise a “tutti” i gestori di siti e piattaforme di comunicazione di implementare l’autenticazione a due fattori, permettendo a tutti gli utenti di beneficiare di un più alto livello di protezione: anche nel malaugurato caso in cui un avversario riesce a rubare username e password, per usarle deve riuscire a rubare anche il rispettivo cellulare—o in grado di intercettarlo al momento giusto.

## 4.8 Dai token fisici a quelli virtuali

Il passo successivo è ancora in corso e consiste nell’usare delle app su dispositivo mobile, che altro non sono che l’equivalente virtuale dei vecchi dispositivi che le banche ci fornivano dietro identificazione di persona. Poi ci hanno aggiunto la conferma con un’impronta digitale con un PIN, o entrambi, che di fatto fungono da terzo fattore. In questo modo, anche se ci rubano il cellulare, dovranno anche (1) rubarci le impronte digitali, (2) riuscire a clonarle talmente bene da non far scattare il limite di tentativi sbagliati, oltre il quale dovranno anche averci rubato anche il codice

## *Guida Galattica di Autodifesa Digitale*

di sblocco del cellulare, e (3) sperare che noi nel frattempo non lo blocchiamo da remoto.

Ragioniamo ancora nei termini della nostra pianificazione di sicurezza vista nel Capitolo 1. Da cosa vogliamo difenderci? Da qualcuno che intercetta i nostri SMS per rubarci i token di autenticazione? Da qualcuno che entra in casa nostra per rubarci il cellulare? Da qualcuno che riesce ad infettare il nostro cellulare con un app malevola che “ruba” i codici di autenticazione generati dall’app?

E se perdiamo o non abbiamo accesso al generatore di token? Qui ritornano le vere OTP, quelle da stampare e nascondere nel portafogli per le emergenze. Sono davvero ad uso singolo, perché una volta che ne usiamo una, il gestore del servizio ne prenderà nota e la “distruggerà”. Ci stiamo proteggendo da qualcuno che ci ruba il portafogli? No! Ci stiamo proteggendo da qualcuno che cerca di intercettarle mentre le usiamo, per provare poi ad entrare nel nostro account. Se le usiamo noi per primi è fatta: nessun’altro potrà mai più utilizzarle.

### **4.9 Per concludere: è complicato**

Proteggere un dato, un sistema attraverso una password è semplice: nonostante l’evoluzione tecnologica, c’è ancora un certo grado di complessità dal lato di chi le password

## *Guida Galattica di Autodifesa Digitale*

le deve creare, memorizzare, utilizzare tutti i giorni. I gestori di password sono però un'occasione. Prima di tutto per "fare bene," ma anche per "fare mente locale": quanti indirizzi email ho? Quanti account? Su quanti siti? Quante password mi invento ogni volta? Sembrano domande semplici, ma ve le siete mai poste veramente?

## CAPITOLO 5

# *Stare al Passo*

---

Quest'opera è incompleta: la sto pubblicando mentre la scrivo. Se volete rimanere aggiornati, potete seguirne lo sviluppo su <https://www.ggad.it>, oppure potete seguire le brevi notizie e suggerimenti che pubblico su <https://contec.maggi.cc> o via Telegram, iscrivendovi al canale <https://t.me/contec>. Nel frattempo, vi lascio in buona compagnia.

Infatti non sono certo l'unica persona che scrive su queste tematiche: anzi, spendo la maggior parte del mio tempo in attività di ricerca. Scrivere è una cosa secondaria e non mi sento per niente portato: ho appena cominciato e non so neanche se continuerò.

Sono stati scritti tantissimi libri sulle tematiche di sicurezza informatica e impatto della tecnologia sulla società. A

## *Guida Galattica di Autodifesa Digitale*

parte i fondamentali [1, 2, 3] (forse più adatti ad un pubblico tecnico o accademico), di seguito nella bibliografia trovatem> una mia personalissima selezione delle opere di autori italiani che vi propongo.

Per il resto, in particolare nel panorama Italiano, mi schiero contro i tanti libri che con tono "sensazionalistico" promettono di svelare tutti i segreti "degli hacker" per sconfiggerli. Non c'è nessun segreto: c'è solo tantissima esperienza e lavoro, difficilmente condensabili in un libro. Vi sconsiglio pertanto la lettura di tali libri.

Dulcis in fundo, vi consiglio di seguire Guerre di Rete (<https://guerredirete.substack.com>), dall'omonimo saggio [7] di Carola Frediani: una newsletter settimanale che condensa i fatti più rilevanti a livello internazionale e unisce sapientemente i puntini mettendo ordine tra i mille fatti che si registrano ogni giorno.

## *L'autore*

---

Federico Maggi opera da oltre dieci anni nel campo della sicurezza informatica, dapprima come consulente in Italia, poi come ricercatore e docente presso la Facoltà di Ingegneria del Politecnico di Milano, e ora come ricercatore per una nota multinazionale.

Federico ha effettuato analisi di sicurezza su una vasta gamma di sistemi come applicazioni web, protocolli di rete, dispositivi embedded, protocolli di comunicazione radio, robot industriali, automobili e dispositivi mobili.

Federico ha contribuito alla ricerca e allo sviluppo di diverse tecnologie di difesa, in particolare per la rilevazione automatica di intrusioni informatiche e frodi, usando tecniche di machine learning e intelligenza artificiale, che oggi sono estremamente diffuse.

## *Guida Galattica di Autodifesa Digitale*

Nella sua esperienza di insegnamento, Federico ha educato migliaia di studenti di ingegneria su come analizzare i sistemi informatici con occhio critico per trovarne falle di sicurezza e per progettarli in maniera sicura. Ha inoltre curato i lavori di tesi di decine di studenti.

Il lavoro di ricerca di Federico è noto a livello internazionale tramite i numerosi convegni o seminari a cui è invitato o dove presenta i suoi risultati alla comunità scientifica e industriale.

Altre informazioni circa l'attività di ricerca dell'autore sono disponibili sul suo sito: <https://maggi.cc>.

# *Bibliografia*

---

- [1] Ross J. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. WI, 2008. ISBN: 978-81-265-1667-4.
- [2] Matt Bishop. *Introduction To Computer Security*. 01 edizione. Boston: Addison-Wesley Professional, 31 dic. 2004. 745 pagine. ISBN: 978-0-321-24744-5.
- [3] Matthew Bishop. *Computer Security: Art and Science*. 01 edizione. Boston: Addison-Wesley Professional, 10 dic. 2002. 1084 pagine. ISBN: 978-0-201-44099-7.
- [4] Stefano Chiccarelli e Andrea Monti. *Spaghetti hacker*. Trento: Monti & Ambrosini, set. 2011. 320 pagine. ISBN: 978-88-89479-14-8.

*Guida Galattica di Autodifesa Digitale*

- [5] Nunzia Ciardi e Rosita Rjitano. *Con lo smartphone usa la testa*. Milano: Sperling & Kupfer, 5 giu. 2018. 170 pagine. ISBN: 978-88-200-6484-6.
- [6] Carola Frediani. *Deep web. La rete oltre Google. Personaggi, storie, luoghi dell'internet profonda*. Viterbo: Stampa Alternativa, 28 apr. 2016. 192 pagine. ISBN: 978-88-6222-519-9.
- [7] Carola Frediani. *Guerre di rete*. Laterza, 2 mar. 2017. 179 pagine. ISBN: 978-88-581-2736-0.
- [8] Carola Frediani e P. Iabichino. *#Cybercrime. Attacchi globali, conseguenze locali*. Milano: Hoepli, 30 mag. 2019. 160 pagine. ISBN: 978-88-203-8920-8.
- [9] Alfonso Fuggetta. *Cittadini ai tempi di Internet. Per una cittadinanza consapevole nell'era digitale*. 1 edizione. Franco Angeli, 13 nov. 2018. 184 pagine. ISBN: 978-88-917-7981-6.
- [10] Dieter Gollmann. *Computer Security, Third Edition*. 3 edizione. Chichester, West Sussex: Wiley, 15 feb. 2011. 456 pagine. ISBN: 978-0-470-74115-3.
- [11] Stefano Quintarelli. *Capitalismo immateriale: Le tecnologie digitali e il nuovo conflitto sociale*. Bollati Boringhieri, 21 feb. 2019. 221 pagine.

*Guida Galattica di Autodifesa Digitale*

- [12] *Surveillance Self-Defense*. URL: <https://ssd.eff.org/en>.
- [13] Giovanni Ziccardi. *Hacker. Il richiamo della libertà*. Venezia: Marsilio, 16 feb. 2011. 286 pagine. ISBN: 978-88-317-0925-5.
- [14] Giovanni Ziccardi. *Il giornalista hacker: Piccola guida per un uso sicuro e consapevole della tecnologia*. Marsilio, 24 apr. 2012. 71 pagine.
- [15] Giovanni Ziccardi. *Il libro digitale dei morti. Memoria, lutto, eternità e oblio nell'era dei social network. Con ebook*. Turin: UTET, 4 apr. 2017. ISBN: 978-88-511-4452-4.
- [16] Giovanni Ziccardi. *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*. Milano: Cortina Raffaello, 11 feb. 2015. 252 pagine. ISBN: 978-88-6030-722-4.
- [17] Giovanni Ziccardi. *L'odio online. Violenza verbale e osSESSIONI in rete*. Milano: Cortina Raffaello, 24 mar. 2016. 256 pagine. ISBN: 978-88-6030-806-1.
- [18] Giovanni Ziccardi. *L'ultimo hacker*. Venezia: Marsilio, 25 gen. 2012. 367 pagine. ISBN: 978-88-317-1127-2.
- [19] Giovanni Ziccardi. *La rete ombra*. Marsilio, 11 ott. 2018. 424 pagine. ISBN: 978-88-317-2988-8.

*Guida Galattica di Autodifesa Digitale*

- [20] Giovanni Ziccardi. *Tecnologie per il potere. Come usare i social network in politica*. Milano: Cortina Raffaello, 21 feb. 2019. 254 pagine. ISBN: 978-88-328-5071-0.