smartpixel

Sicurezza informatica e protezione dei dati

Concetti generali e buone prassi per l’utilizzo sicuro di Internet e dell’ambiente di rete

L’importanza del fattore umano

Quando si parla di sicurezza informatica esistono solamente **due dati di fatto**:

- **la privacy non esiste**: qualunque dispositivo connesso a una rete lascia una traccia che può essere ricondotta all’identità dell’utilizzatore
- in rete **nulla è sicuro**: la sicurezza assoluta non esiste, è possibile solo un livello ragionevole di sicurezza → Kevin Mitnick (hacker protagonista delle più ardite incursioni nei sistemi del governo USA) sintetizzava il concetto nella frase "*Un computer sicuro è un computer spento*"

Il maggiore rischio per i nostri dati siamo noi stessi: spesso la prima breccia nella sicurezza di un sistema informatico non si ottiene con strumenti tecnici, ma sfruttando aspetti del comportamento umano codificati e standardizzati

Mai come ora è necessario porre l'attenzione alla sicurezza informatica e alla protezione dagli attacchi come elemento prioritario attraverso un approccio "**security-first thinking**": non si aspetta in maniera reattiva che un attacco si verifichi ma si agisce proattivamente creando le condizioni per evitare che questo accada

Minacce ai dati

Con il termine **sicurezza informatica** si intende l'attività di analisi delle minacce, vulnerabilità e del rischio associato ai dati informatici per proteggerli da possibili attacchi, problema sempre più diffuso per la crescente informatizzazione della società in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione delle attività di intrusione

- **dati**: entità informatiche espresse in bit che rappresentano fatti o eventi non ancora organizzati (ad es. numeri, lettere, immagini, video, suoni, ecc.)
- **informazioni**: dati elaborati, organizzati in modo da essere comprensibili per l'utente

I dati possono essere minacciati da:

- **persone**: dipendenti dell'azienda, fornitori di servizi (ad es. chi svolge la manutenzione HW/SW) e terzi (clienti, ospiti che accedono al Wi-Fi aziendale) avendo accesso ai dati possono perderli, danneggiarli o prenderne illegalmente possesso per rivenderli
- **eventi naturali**: incendi, inondazioni, terremoti
- **eventi artificiali**: vandalismo, guerre

Hacking e crimine informatico

L'**hacker** è un esperto di metodi, tecniche e operazioni di hacking (dall'inglese "*to hack*" intaccare), cioè dirette ad acquisire un'approfondita conoscenza dei sistemi HW/SW e della loro sicurezza per introdursi nel sistema, modificarlo o adattarlo alle proprie esigenze

All'inizio l'interesse era rivolto alla **conoscenza dei sistemi** e della loro sicurezza con azioni non dannose (gli hackers sono motivati dal gusto della sfida, da fini etici o politici indifferenti all'uso di mezzi illegali per raggiungerli), ma la diffusione dell'informatica ha portato sviluppi diversi:

- **cracker**: pratica la violazione dei sistemi informatici (cracking) per utilizzarne i dati a proprio vantaggio o anche solo per dimostrare la propria abilità informatica (black hat)
- **hacker etico**: si introduce per motivazioni etiche o accademiche in un sistema informatico per individuarne le vulnerabilità e informare la vittima dei suoi punti deboli (white hat)

Il **crimine informatico** è l'abuso della tecnologia informatica per la commissione di reati ed è regolato dalla legge 547/93 che punisce l'accesso abusivo a sistemi HW/SW per intercettare, modificare, danneggiare, impedire, interrompere o alterare comunicazioni informatiche

Tipologia di attacco informatico

Alcune **tecniche informatiche** permettono di intercettare informazioni personali o eseguire accessi non autorizzati alle reti altrui:

- **sniffing** (dall'inglese "*to sniff*", odorare): intercettazione passiva dei dati che transitano in una rete → può avere scopi legittimi (analisi e individuazione di problemi di comunicazione o tentativi di intrusione) o illeciti (intercettazione fraudolenta di password o altre informazioni sensibili) come nel caso delle tecniche "*man in the middle*" e "*man in the mail*"
- **spoofing** (dall'inglese "*spoof*", imbroglio): attacco che utilizza la falsificazione dell'identità (falsificazione indirizzo IP, MAC, phishing) per farsi riconoscere come fonte attendibile
- **exploit** (in inglese, sfruttare): tipologia di script, virus o worm che sfrutta una specifica vulnerabilità presente in un sistema informatico, per eseguire codice malevolo su di esso allo scopo di far ottenere all'attaccante l'acquisizione dei privilegi amministrativi
- **SQL injection**: tecnica di "*code injection*" che sfrutta le vulnerabilità di sicurezza del codice di una applicazione di gestione dati → vengono inserite delle stringhe di codice SQL malevole all'interno dei campi di input in modo che queste ultime vengano poi eseguite (ad esempio per fare inviare il contenuto del database all'attaccante)

Sicurezza e protezione dei dati

Le informazioni per essere sicure devono presentare determinate **qualità**:

- **confidenzialità**: non devono essere diffuse a persone non autorizzate
- **integrità**: il contenuto deve essere inalterato e protetto da modifiche accidentali dei dati
- **disponibilità**: sarebbe inutile garantire la sicurezza delle informazioni se poi, quando servono, per qualche motivo non sono recuperabili nei tempi necessari

A livello normativo, in esecuzione degli Accordi di Schengen e della direttiva 95/46/CE relativa alla tutela e libera circolazione dei dati personali venne emanata la **L. n. 675/1996** poi abrogata dal **D. Lgs n. 196/2003** "*Codice in materia di protezione dei dati personali*" che ha riordinato la materia (a causa della complessità normativa causata dalle numerose leggi emanate nel frattempo riguardanti singoli e specifici aspetti del trattamento dei dati)

Il 25 gennaio 2012 la Commissione Europea ha approvato la proposta di un regolamento sulla protezione dei dati personali in sostituzione della direttiva 95/46/CE: il 4 maggio 2016 viene emanato il regolamento UE 2016/679 (**GDPR**) entrato in vigore il 25 maggio 2018

General Data Protection Regulation

Il 25 maggio 2018 ha avuto piena attuazione il **Regolamento UE 2016/679**, General Data Protection Regulation (GDPR) che disciplina il trattamento dei dati personali dei cittadini dell'UE (dati anagrafici, genetici, di localizzazione, biometrici, giudiziari e relativi alla salute)

Il trattamento è lecito solo quando avviene in base al **libero e chiaro consenso** e i dati devono essere trattati in modo lecito, corretto e trasparente → il GDPR riconosce i seguenti diritti:

- **revocare** in ogni momento il consenso al trattamento dei dati personali
- **opporsi al trattamento** dei dati quando avviene su una base giuridica diversa dal consenso
- **accedere** ai propri dati, **verificare** la correttezza e richiedere l'**aggiornamento** o **rettificazione**
- ottenere la **limitazione** del trattamento, la **cancellazione** o **rimozione** dei dati personali
- ricevere i propri dati o **richiederne il trasferimento** senza ostacoli ad altro titolare
- **proporre reclamo** all'autorità di controllo della protezione dei dati personali competente o agire in sede giudiziale

Per maggiori informazioni consultare il sito www.garanteprivacy.it.

Tecniche di protezione dei dati

Ogni dispositivo è una **miniera di dati**: se non è adeguatamente protetto, può essere usato in modo non autorizzato (in caso di furto o smarrimento) o compromesso per farne un utilizzo fraudolento o illegale che farebbe ricadere la responsabilità sull'ignaro utente

La maniera migliore di proteggere i dati è di **applicare delle tecniche** attraverso le quali, anche se i dati finissero nelle mani dei malintenzionati (ad es. perché presenti all'interno di dispositivi mobili, più facili da rubare), non potrebbero essere comunque utilizzati:

- **sequenza**: password visuale in base a una griglia di nove punti (facile da indovinare)
- **PIN**: Personal Identification Number composto da 4 numeri, molto usato ma poco sicuro
- **password**: evoluzione del PIN, aumenta la sicurezza combinando lettere, numeri e simboli
- **tecniche biometriche**: basate sull'univocità delle caratteristiche fisiche degli utenti (ad es. il riconoscimento dell'impronta digitale o del volto) offrono la maggiore sicurezza
- **crittografia**: la password protegge l'accesso al dispositivo o all'applicazione, ma non ha effetto se i dati sono memorizzati su memoria removibile → in questi casi è preferibile cifrare i dati con un codice decifrabile solo da chi conosce il codice di cifratura

Tecniche di ingegneria sociale

L'**ingegneria sociale** (social engineering) è lo studio del comportamento individuale al fine di ottenere con l'astuzia o la frode informazioni riservate, aggirando così i sistemi di protezione HW/SW dei dati sempre più sofisticati e difficilmente penetrabili → l'ingegneria sociale utilizza diversi metodi:

- **pretexting**: chiamate telefoniche che, dietro la promessa di premi o altro genere di vantaggi, cercano di ottenere informazioni personali mascherandole con sondaggi anonimi
- **phishing**: tecnica basata sull'invio di comunicazioni ingannevoli (email, sms, chiamate telefoniche): il phisher si finge un servizio bancario che, minacciando la chiusura del conto o il blocco della carta di credito, chiede di inserire le proprie credenziali per poterle verificare
- **shoulder surfing** (le credenziali dell'utente sono spiate direttamente anche con telecamere) e **skimming** (con congegni per la manomissione dei distributori e terminali di pagamento)

Spesso la conseguenza è il **furto di identità**, cioè l'appropriazione indebita delle credenziali anagrafiche e/o di accesso a un dispositivo o servizio per usarlo a proprio vantaggio per compiere crimini informatici come frodi o furti

Furto di identità

Il **furto di identità** o l'uso improprio di una identità è un crimine che causa serie conseguenze sia emotive che finanziarie ed è di solito di un "*crimine d'opportunità*": l'utente può diventare vittima per il solo motivo che i propri dati personali non sono adeguatamente protetti

- fornire i propri dati solo a società con **buona reputazione**: diffidare di società sconosciute e verificare l'autenticità del sito web prima di inserire dati sensibili
- usare tutte le **opzioni di sicurezza** in particolare password robuste e siti web con connessione protetta con protocollo HTTPS
- controllare le proprie **policy di sicurezza**: controllare che ci sia la possibilità di verificare i propri dati personali sia online, sia contattando direttamente la società
- fare attenzione al **tipo di dati forniti**: i malintenzionati possono collezionare pezzi di informazioni da svariate fonti, quindi è fondamentale prestare attenzione alle informazioni pubblicate, specialmente sui forum e i social network
- usare e mantenere aggiornati i **programmi di protezione** (firewall e antivirus)
- controllare frequentemente il proprio **conto corrente** e segnalare in caso di discrepanze l'anomalia al proprio istituto di credito

Metodi malware

Il **malware** (deriva da "*Malicious*" e "*Software*") è un software capace di causare danni più o meno gravi al sistema informatico su cui viene eseguito, è usato principalmente per furto di dati, estorsione o per generare profitto e può introdursi nel sistema in diversi modi:

- **trojan horse**: software che oltre ad avere funzionalità lecite e desiderabili (utili per indurne l'utilizzo) contengono istruzioni dannose che vengono eseguite all'insaputa dell'utente
- **backdoor**: programmi eseguiti all'insaputa dell'utente che consentono un accesso non autorizzato al sistema informatico su cui sono in esecuzione
- **rootkit**: non dannosi, ma nascondono la presenza di particolari file o impostazioni di sistema e proprio per questo sono usati per mascherare spyware e trojan horse

Una forma di trojan è la **macro**, programmazione (ad es. in Visual Basic) di una procedura che può essere eseguita automaticamente o in base a una combinazione di tasti all'interno di un software di produttività → la macro automatizza lunghe procedure, ma (spesso quando la loro origine non è affidabile) può eseguire **codice malevolo**: disattivando la macro l'utente rinuncia alle sue funzionalità, ma è al sicuro dall'esecuzione di possibile codice malevolo

Tipi di malware

- **virus**: si tramette attraverso supporti non verificati, replica copie di se stesso all'interno di programmi o parti del disco fisso ogni volta che il file infetto viene aperto
- **worm**: si trasmette via Internet attraverso tecniche di ingegneria sociale, modifica il sistema operativo in modo da essere eseguito automaticamente e rallenta il sistema
- **adware**: attivano messaggi pubblicitari, possono causare rallentamenti e rischi per la privacy perché comunicano le abitudini di navigazione dell'utente ad un server remoto
- **spyware**: raccolgono informazioni (abitudini di navigazione ma anche password) sul sistema su cui operano per trasmetterle a destinatari interessati
- **keylogger**: registrano tutto ciò che viene digitato sulla tastiera (furto credenziali)
- **hijacker**: si appropriano dei browser causando l'apertura automatica di siti indesiderati
- **dialer**: modificano il numero telefonico della connessione predefinita con uno a tariffazione speciale per trarne illecito profitto all'insaputa dell'utente
- **botnet**: infezione controllata da remoto dal botmaster che è in grado di compromettere la rete e i dispositivi ad essa collegati per svolgere attività non autorizzate
- **ransomware**: cripta tutti i dati presenti su disco con una chiave di cifratura complessa → per ottenerla e decrittografare il dispositivo, bisogna pagare il cracker che lo ha infettato

Ransomware

Malware distribuito da siti compromessi, applicazioni ingannevoli e link malevoli via email/IM che **limita l'accesso** del dispositivo che infetta, richiedendo un riscatto ("*ransom*" in inglese) da pagare per rimuovere la limitazione (https://www.nomoreransom.org) → precauzioni:

- aggiornare sempre **sistema**, **applicazioni** e **software di sicurezza**
- evitare **App Store non ufficiali** e di concedere i **diritti di amministrazione** del dispositivo
- diffidare di **siti e email sospette** e verificare le **estensioni dei file** allegati
- per valutare il contenuto dei file utilizzare, invece di Office, **servizi online** di visualizzazione e anteprima DOC/XLS/PDF o **viewer** scaricabili gratuitamente (usare viewer meno noti di Adobe PDF Viewer che, essendo molto diffuso, è anche il più vulnerabile)
- **non attivare le macro** eventualmente presenti nei file, anche se nel documento compaiono indicazioni tipo "*attivare le macro per visualizzare correttamente il contenuto*"
- **fare backup** quotidiani dei dati importanti, possibilmente non su dischi collegati 24/7 al proprio PC e verificarne ogni tanto il funzionamento e il contenuto
- **utilizzare servizi cloud** come Dropbox, Google Drive o OneDrive che, seppur non pensati per la difesa dai ransomware, possono limitare i danni in caso di cifratura

Mining malware

Il **cryptojacking** o **cryptomining** è l'inserimento nei siti web (anche di ottima reputazione) di istruzioni che usano il dispositivo dell'utente a sua insaputa per eseguire i complessi calcoli matematici che generano le criptovalute e depositano il denaro virtuale nei conti dei truffatori

Lo **sfruttamento illecito del dispositivo** termina se l'utente smette di visitare il sito infetto o chiude il browser, ma non lascia sui dispositivi virus o altri elementi informatici pericolosi e non ruba dati personali: è comunque un furto di energia elettrica che arricchisce qualcuno alle spalle dell'utente e incoraggia i criminali a violare i siti per infettarli

In altri casi, il vettore di attacco sono siti web malevoli o adware ingannevoli inseriti in app infette (che reindirizzano a siti malevoli) che installano segretamente "**miner**", software che usano la capacità di calcolo dei dispositivi per creare criptovaluta all'insaputa dell'utente

In alcuni casi si tratta di vere e proprie **Botnet** (reti di dispositivi compromessi) in cui il malware sfrutta l'hardware del dispositivo per fare mining di criptovaluta, producendo guadagni per i malintenzionati che gestiscono il servizio (botmaster)

Mining malware

Oltre a incidere pesantemente sul **consumo di energia**, questa minaccia può invecchiare precocemente o **causare danni** permanenti ai dispositivi che nelle fase di mining mostrano un aumento elevatissimo del carico della CPU (raggiunge immediatamente il 100%) rilevabile da rallentamenti, surriscaldamento o un eccessivo utilizzo delle ventole

Per evitare che il computer si trasformi in uno zombie che ruba elettricità, dalle prestazioni ridotte a causa delle attività cyber criminali:

- **controllare l'utilizzo della CPU** attraverso "*Gestione Attività*" (CTRL+MAIUSC+ESC)
- **aggiornare il sistema operativo** con gli ultimi update di sicurezza
- usare un **software di sicurezza affidabile** (antivirus/antimalware) e mantenerlo aggiornato
- **non aprire allegati** a messaggi email o IM provenienti da mittenti sconosciuti e **non attivare le macro** eventualmente presenti all'interno dei file office
- non installare software/app da **fonti non attendibili**
- usare **estensioni adblocker** a difesa della navigazione via browser

Mobile banking malware

Il malware che colpisce il mobile banking è appositamente studiato per rubare i dati finanziari eventualmente memorizzati su un dispositivo: **si diffonde** attraverso siti malevoli, applicazioni ingannevoli e phishing email/IM ed è mirato al furto dei dati di autenticazione personale e alla effettuazione di prelievi non autorizzati → come difendersi:

- **scaricare l'applicazione mobile ufficiale** della propria banca
- assicurarsi ogni volta di **visitare il sito autentico** (HTTPS://) della banca di riferimento
- **evitare di connettersi automaticamente** al sito o applicazione di banking online
- **non condividere** né rivelare a terzi alcun dato relativo all'account, né il numero di carta di credito o la password, tramite messaggi di testo o email
- installare un'**applicazione di mobile security** in grado di segnalare eventuali attività sospette
- in caso di smarrimento del proprio dispositivo o cambiamento del numero di telefono, **contattare la banca** per eseguire l'aggiornamento dei propri dati personali
- usare sempre una **rete Wi-Fi protetta** o in alternativa una VPN per connettersi al sito o all'applicazione di mobile banking (NON usare le reti Wi-Fi pubbliche)
- **controllare frequentemente l'estratto conto** e contattare la banca in tutti i casi sospetti

3 regole di base

Nell'immaginario collettivo, Internet è popolata da cattivi ragazzi con felpa e cappuccio che attaccano il pc dell'ignaro utente, ma 99 volte su 100 la **più grande minaccia per i dati** è proprio l'utente che con la sua condotta inappropriata si predispone all'attacco → 3 regole di base:

- aggiornare il **sistema operativo** e il **software di sicurezza** all'ultima versione disponibile che spesso contiene le correzioni più recenti in ambito sicurezza
- **non comunicare credenziali o dati personali a siti web non affidabili** (phishing, siti clonati), ma verificare l'attendibilità della richiesta sempre tramite i siti web ufficiali, evitando di cliccare su link diretti (spesso abbreviati e quindi irriconoscibili) ricevuti via email o IM
- **non eseguire codice non verificato**: spesso si dice "*ho preso un virus*", ma è sempre l'utente che ha eseguito il codice malevolo (cliccando sull'allegato, installando qualche programma come l'aggiornamento Flash Player o perché usa contenuti ottenuti in modo illegale)

Basta poco per usare con serenità il web e approfittare dei benefici di Internet che, **ogni tanto, è un po' cattiva con chi non rispetta le regole di base** della sicurezza informatica

Software di sicurezza

Nessun sistema operativo è immune dai malware → per riconoscere, isolare e rimuovere le intrusioni, se non è già presente (come nel caso di Windows Defender), può essere necessario installare un **software di sicurezza** (antivirus/antimalware) che ha due funzioni principali:

- scansionare la **memoria RAM** per impedire l'esecuzione di codice virale
- controllare **file e cartelle** per individuare e rendere innocui eventuali file infetti

Il riconoscimento delle infezioni avviene sia grazie al confronto con l'archivio contenente le **definizioni dei malware** conosciuti che in base a metodi di **indagine euristica**, cioè basata sulla somiglianza di frammenti di codice virale con quello analizzato

Per essere efficace l'antivirus deve essere **aggiornato con frequenza** soprattutto l'archivio che contiene la definizione delle infezioni, perché nuovi malware vengono diffusi in continuazione: un limite dei programmi antivirus è che a volte generano dei **falsi positivi**, cioè indicano come infezioni programmi del tutto leciti

Software di sicurezza

La protezione da eventuali infezioni al sistema si attua attraverso diverse misure:

- prestare particolare **attenzione alle fonti**: non utilizzare alcun supporto o programma se non si è sicuri della sua provenienza
- installare un programma antivirus e/o antimalware da **aggiornare periodicamente** sia per la parte software, sia soprattutto le definizioni delle infezioni: in molti casi l'aggiornamento è automatico ma, se ciò non avviene, potrebbe essere un segnale di malfunzionamento, magari proprio perché un virus sta cercando di impedire al programma di individuarlo
- far **controllare** dall'antivirus e/o antimalware i supporti di memoria e gli allegati ricevuti con la posta elettronica prima del loro utilizzo
- eseguire con l'antivirus e/o antimalware **scansioni periodiche** del sistema
- disporre di un buon **sistema di backup e ripristino** di dati e programmi

Se l'antivirus individua file infetti o sospetti chiede all'utente se metterli in **quarantena**, cioè in una apposita cartella creata dall'antivirus, facilmente controllabile, dove i file infetti sono resi innocui perché non eseguibili

Download di file

Oltre a rappresentare una possibile fonte di diffusione di malware, il **download** di programmi o file (musica, film, ecc.) da Internet può avere serie conseguenze legali → il software è protetto dal diritto d'autore (copyright) perché assimilato alle opere letterarie e artistiche: sono punibili con pene pecuniarie e la reclusione la detenzione, riproduzione, distribuzione e vendita non autorizzata di software

Il software può essere distribuito attraverso diverse **licenze** o **contratti d'uso**:

- **freeware**: software fornito gratuitamente, messo a disposizione attraverso Internet
- **pubblico dominio**: software fornito senza copyright, l'utente può copiarlo e distribuirlo senza limiti, se non quello di citarne la fonte
- **demo/trial**: software distribuito in dimostrazione privo di alcune funzionalità
- **shareware**: software con copyright distribuito gratis in versione limitata con richiesta di registrazione a pagamento (di solito una piccola somma)
- **licenza d'uso**: software coperto da copyright, distribuito a pagamento il cui uso è regolato da contratti di licenza, che limitano la modifica, riproduzione o ridistribuzione del programma

Reti e connessioni

Una **rete informatica** funziona in base ad architetture hardware (client, server e apparati di connessione) e protocolli software (regole condivise con vengono trasmessi i dati) e permettono a più dispositivi di comunicare e condividere informazioni, dati e risorse:

- **LAN** (Local Area Network): connette sistemi informatici locali, limitati nello spazio, tramite cavi, connessioni dedicate e hardware specifico di interfaccia tra le unità e la rete
- **WAN** (Wide Area Network): reti geografiche (ad es. Internet) in grado di connettere sistemi e dispositivi (anche interaziendali) su una area molto estesa
- **MAN** (Metropolitan Area Network): rete con un'estensione limitata a un perimetro cittadino (è una forma di LAN e WAN come ad es. la rete civica di Milano)

Una **VPN** (Virtual Private Network) è una rete privata virtuale che però utilizza un protocollo di trasmissione pubblico e condiviso (ad es. la rete Internet): viene usata per collegare in modo sicuro più dispositivi attraverso un apposito software che si occupa di creare un tunnel sicuro attraverso la criptazione dei dati e l'autenticazione della comunicazione

Utilizzare la VPN

Una **VPN** è una **rete logica** (non ci sono connessioni fisiche) **e privata** (solo gli appartenenti alla rete possono scambiarsi dati) che **tutela l'anonimato**: il traffico è completamente anonimo (maschera l'indirizzo IP ponendo l'utente virtualmente in un altro paese) e i dati sono criptati e trasmessi al server, da cui poi il traffico sarà instradato al sito destinatario e viceversa

E' usata per connettersi da hotspot **Wi-Fi pubblici**, per aggirare le **restrizioni geografiche** ingannando la tariffazione Skype o alcuni siti web (Netflix limita l'accesso ad alcuni mercati) e per **scaricare in modo anonimo** (molto usate dai pirati informatici, per nascondere la propria identità) → per scegliere una VPN (tra le migliori NordVPN e IPVanish) è bene controllare:

- **politica dei logs**: di solito i server registrano dei file che tracciano chi si è connesso e con quale indirizzo IP → per tutelare l'anonimato alcuni servizi a pagamento hanno una politica molto rigida e non registrano le sessioni degli utenti sui server
- **numero e posizione dei server**: più sono i server, maggiore è la qualità dei servizio VPN
- **protocolli di sicurezza**: meglio i servizi che offrono una connessione IPSec, SSL o con doppia criptazione dei dati a 256bit

Reti cablate e wireless

Dal punto di vista hardware, un rete può essere:

- **cablata**: usa cavi di rame o fibra ottica, i cui vantaggi sono la velocità di trasmissione dei dati (non disperde il segnale) e la maggiore sicurezza (i dispositivi sono fisicamente connessi alla rete ed è impossibile collegarne uno senza l'autorizzazione dell'amministratore)
- **wireless** (Wi-Fi): hotspot che sfrutta onde radio (dispersione del segnale), meno costosa, più pratica (non servono i cavi e arriva anche dove non è possibile posare il cavo)

Le **minacce** che riguardano l'utilizzo di una rete sono:

- **virus** o **malware** spesso scaricato da Internet attraverso siti web o la posta elettronica
- **accessi non autorizzati**: soprattutto nelle reti Wi-Fi non adeguatamente protette da parte di intercettatori (eavesdropping), dirottatori di rete (network hijacking) e violatori di comunicazioni private (man in the middle)
- **violazione della privacy** nella misura in cui i dati personali non adeguatamente protetti possono essere esposti ad eventuali utilizzi fraudolenti

Sicurezza delle reti Wi-Fi

Una **rete Wi-Fi** può essere agganciata per intercettare i dati dei dispositivi connessi o anche solo in transito, soprattutto se non è protetta da una password efficace → per migliorare la sicurezza delle reti Wi-Fi sono stati elaborati diversi algoritmi di criptazione dei dati trasmessi:

- **WEP** (Wired Equivalent Privacy): nasce nel 1999 per garantire una sicurezza della privacy equivalente a quella delle reti cablate, ma si dimostra presto inadeguato per la brevità della chiave che la rende facilmente individuabile
- **WPA** (Wi-Fi Protected Access): nasce nel 2003/04 e convive con il successivo WPA2 che offre una maggiore sicurezza rispetto al precedente WPA, ma il cui sistema di crittografia è stato violato nel 2017 dall'attacco Key Reinstallation Attack (KRACKs)

La sicurezza può aumentare con il **filtro MAC address**: ogni scheda di rete ha un codice unico assegnato dal produttore che individua in modo univoco un dispositivo e consente di creare delle ACL (Access List) di dispositivi autorizzati all'uso della rete → il dispositivo con un MAC address diverso non verrà connesso, anche se conosce la password di rete (non è del tutto sicuro perché esistono dei software in grado di modificare il MAC address di un dispositivo)

Sicurezza delle reti Wi-Fi

Nel 2017 l'**attacco KRACKs** ha mostrato una serie di gravi falle nel WPA2 che permettono di intercettare dati sensibili e riguardano i dispositivi di ogni marca e modello dotati di Wi-Fi: l'attacco è del tipo **man in the middle** (l'aggressore si trova nel raggio rete Wi-Fi) e funziona solo con connessioni HTTP non cifrate (con HTTPS o una buona VPN l'attacco non è possibile)

Il sistema di crittografia WPA2 non protegge adeguatamente le comunicazioni e **la sicurezza è proporzionale alla complessità della chiave** che se non è sufficientemente robusta espone a:

- attacco **brute force**: cerca di indovinare la password provando in serie ogni combinazione alfanumerica di caratteri, simboli, lettere o numeri
- attacco **a dizionario**: simile al precedente, ma cerca di indovinare la password attraverso il confronto con un elenco di password di uso comune

Una tale situazione consiglia di **diffidare delle reti Wi-Fi pubbliche** per l'esecuzione di operazioni sensibili (non si conosce il livello di sicurezza dell'access point ed è più probabile che nell'area sia presente un malintenzionato) o, se proprio si deve, usare una VPN

Sicurezza delle reti Wi-Fi

Per tutelarsi è sempre meglio **modificare la chiave di rete predefinita** avendo cura di:

- utilizzare una **chiave alfanumerica complessa** (attacchi brute force)
- evitare password composte da **una sola parola in un'unica lingua** (attacchi a dizionario)
- **cambiare con regolarità** la password rispettando gli stessi criteri

La soluzione arriva nel 2018 con il **nuovo standard WPA3** che supera i limiti del WPA2 perché:

- usa la **cifratura individuale** di ogni singola comunicazione tra i dispositivi connessi
- **migliore protezione** dagli attacchi brute force che rende più difficile indovinare le password e impone un limite al numero di tentativi di accesso per ogni dispositivo
- **nuovo tipo di handshake** (processo con cui i dispositivi connessi in rete stabiliscono, prima di iniziare la comunicazione, velocità di trasmissione, protocolli di compressione e criptazione) che sarà meno vulnerabile da attacchi a dizionario
- gestione dei **dispositivi IoT senza schermo** tramite un altro device collegato alla rete locale
- **suite di sicurezza** per le reti Wi-Fi più sensibili (ad es. enti pubblici, settore industriale)

Controllo di accesso

L'**amministratore** gestisce le operazioni di accesso alla rete (assegna diversi livelli di privilegio e autorizza gli account), ne assicura l'efficienza (aggiornamenti di sicurezza) e controlla il traffico di rete → l'accesso alle risorse (file, cartelle, stampanti, accesso a Internet, ecc.) dipende dalla sua architettura e avviene in base all'account di rete (nome utente e password):

- **reti paritetiche**: tutti i dispositivi svolgono funzioni simili, l'autenticazione utente e le risorse condivise funzionano a livello locale, in base alle impostazioni dei singoli dispositivi
- **reti client/server**: il server si occupa dell'autenticazione utente su tutti i client e centralizza i permessi di accesso alle risorse di tutta la rete

Un **firewall** è un dispositivo o un software che controlla in base ad un organizzazione di regole programmate dall'amministratore, l'accesso e il traffico di rete per evitare intrusioni e accessi indesiderati → in genere il firewall è posto tra LAN e WAN (rete Internet), pertanto è inefficace se l'attacco proviene dall'interno (ad es. da parte di un utente o da un malware che ha già precedentemente infettato un qualsiasi dispositivo della rete)

Gestione delle password

La protezione di file e dispositivi da accessi indesiderati avviene impostando una **password** che permette l'accesso a chi la conosce, limitando il rischio di accesso non autorizzato:

- **robusta**: deve essere formata da una combinazione di almeno 8 caratteri alfanumerici, evitando di suggerire regolarità, in modo da renderla difficile da indovinare
- **unica**: servizi diversi richiedono password diverse, non utilizzare mai una stessa password per proteggere più servizi, file o dispositivi
- **protetta**: non va diffusa, non deve essere facilmente ricostruibile attraverso le tecniche di ingegneria sociale, va cambiata periodicamente con regolarità e conservata in modo da poterla ritrovare in caso di necessità

Per dare maggiore sicurezza all'accesso in rete si è diffusa l'**autenticazione a due fattori** con OTP (One Time Password): oltre alla password viene richiesto un codice di verifica aggiuntivo inviata via SMS o generata sul momento da un dispositivo in possesso dell'utente (app autenticatore per smartphone, dispositivo di sicurezza rilasciato dalle banche)

Sicurezza dei dispositivi mobili

I **dispositivi mobili** contengono informazioni personali (contatti, dati di navigazione e posizione, email, messaggi, password, documenti locali e sincronizzati con il cloud, dati delle applicazioni) che vanno protette anche in caso di smarrimento, furto o compromissione del dispositivo:

- bloccare sempre lo smartphone con una **password efficace**
- configurare opportunamente il **timeout** per il blocco automatico dello schermo
- abilitare la **crittografia dei dati** ed effettuare il **backup** periodico degli stessi
- **usare solo applicazioni sicure**: evitare di installare applicazioni da origini sconosciute o non autorizzate, ma solo dagli App Store ufficiali che ne controllano periodicamente la sicurezza
- controllare le **autorizzazioni** richieste dalle applicazioni evitando quelle ingiustificate che potrebbero accedere ai dati personali dell'utente
- registrare periodicamente la **geolocalizzazione** del dispositivo
- eseguire sempre gli **aggiornamenti** di sistema, perché introducono nuovi miglioramenti per schermare il dispositivo da vulnerabilità e malware, installare un **software di sicurezza**
- spegnere **Wi-Fi**, **bluetooth** e la tecnologia **NFC** quando non in uso
- **diffidare di qualsiasi link inatteso** ricevuto via email, SMS o IM

Come evitare le app ingannevoli o dannose

La scarsa informazione o la distrazione può indurre a installare **app false, ingannevoli o malevole** che possono spiare l'utente attivando a sua insaputa i servizi di localizzazione o la fotocamera, appropriarsi di password e dati personali, mostrare pubblicità invadenti, causare addebiti anomali o provocare danni al dispositivo → per imparare a riconoscerle:

- evitare le **fake app**: per raggirare l'utente, i malintenzionati spesso creano app clone (simili per nome, icona e funzionalità) di app popolari (come nel caso di WhatsApp che vanta numerosi casi di clonazione a scopo di truffa)
- verificare il **nome dello sviluppatore**: se non è riconoscibile come produttore di software autentico o quantomeno attendibile, probabilmente si tratta di una app ingannevole
- controllare le **recensioni** e il livello di **popolarità**: le app autentiche sono molto scaricate e perciò hanno numerose valutazioni da parte degli utilizzatori
- evitare app **torcia**, **booster/antivirus/pulizia**, per il **download di mp3** e gli **appstore alternativi**: possono essere dannose per le prestazioni del dispositivo e attivare contenuti malevoli
- in caso di ulteriore dubbio, **non cercare l'app tramite il nome nello store**, ma rintracciare il sito ufficiale del produttore dove sarà certamente indicato il link all'app autentica

Navigazione sicura del web

Internet non è sicura: è una rete pubblica che usa normalmente il protocollo HTTP, che trasmette i dati senza cifratura e perciò può essere intercettato e utilizzato dai malintenzionati

Il **protocollo sicuro HTTPS** (Hypertext Transfer Protocol Secure) trasmette i dati tramite HTTP all'interno di una connessione criptata dal TLS (Transport Layer Security) o dal suo predecessore SSL (Secure Socket Layer): HTTPS segnala al browser di usare il livello di cifratura aggiuntivo SSL/TLS per proteggere il traffico internet

HTTPS si basa su un **certificato digitale**, un documento elettronico rilasciato da un'autorità di certificazione che verifica l'identità del soggetto e garantisce la validità delle informazioni riportate nel certificato per le procedure di cifratura dei dati

Quando si usa il web per fare acquisti online o eseguire transazioni finanziarie (ad es. con il proprio home banking) è necessario verificare che il sito web utilizzi il **protocollo HTTPS** (segnalato nella barra degli indirizzi dalla presenza dell'icona di un lucchetto chiuso verde)

Navigazione sicura del web

Il riconoscimento del protocollo HTTPS aiuta a individuare i tentativi di **pharming**, tecnica simile al phishing, perché l'obiettivo è sempre indirizzare l'utente verso un server web clone attrezzato per carpire i dati personali della vittima, ma più sofisticata:

- quando l'utente digita nel browser l'indirizzo alfanumerico (ad es. www.google.it) di un sito web, questo è tradotto dal server DNS in un **indirizzo IP** numerico che serve per reperire nella rete internet il percorso per raggiungere il server web corrispondente a quel dominio
- il pharming **cambia questo riferimento** in modo che l'indirizzo alfanumerico punti a un diverso IP numerico, ridirezionando verso un altro sito clone (se richiede l'immissione di dati personali, questi potranno essere utilizzati a danno dell'ignara vittima)

L'utente può riconoscere la differenza solo se controlla attentamente (senza accettare frettolosamente) la **presenza del protocollo HTTPS**: se il sito usa una connessione sicura ed è autentico verrà mostrato il certificato digitale emesso da una autorità di certificazione conosciuta, che riporterà i dati esatti del sito (icona del lucchetto chiuso verde)

Impostazioni del browser

Le **buone prassi** per la navigazione in sicurezza del web:

- disabilitare il **salvataggio delle password** e il **completamento automatico** dei dati da parte del browser per evitare la diffusione a terzi dei propri dati personali
- utilizzare la **protezione anti-tracciamento** e la modalità di **navigazione anonima** che non conserva la cronologia dei siti visitati
- **eliminare la memoria dati** del browser che comprende la cronologia di navigazione e download, le ricerche effettuate, i dati per il completamento automatico dei moduli, i file temporanei di Internet, le password e i cookie
- fare **attenzione ai cookie** (file di testo contenente informazioni personali che i server web usano come gettone identificativo per riconoscere i browser durante le comunicazioni via HTTP): se leciti i cookie sono utili (ad es. per usare la email o un sito di e-commerce), ma possono essere usati come spyware per tracciare i comportamenti degli utenti
- usare software per il **controllo del contenuto** (impediscono l'accesso a certi siti, alcuni tipi di download e l'utilizzo di porte usate da certi programmi ad es. di file sharing) e di **controllo parentale** (filtrano i contenuti e consentono l'accesso al web solo in orari programmati)

Strumenti per proteggere la privacy

Browser, motori di ricerca e siti web **tracciano l'attività online** dell'utente per fornire (almeno) pubblicità personalizzata: come consiglia www.privacytools.io il browser più credibile sembra essere Mozilla **Firefox** che è prodotto una fondazione senza scopo di lucro (non una società commerciale) che non guadagna con i dati degli utenti

Uno degli strumenti per proteggere i dati dell'attività di navigazione, oltre alle impostazioni del browser, è l'utilizzo di un **motore di ricerca privato**, cioè che non salva i dati di navigazione o li conserva solo per poche ore e blocca automaticamente diversi elementi traccianti:

- **DuckDuckGo** (https://duckduckgo.com/): sede in Pennsylvania (USA), dichiara di non raccogliere o condividere informazioni personali
- **StartPage** (https://www.startpage.com/): sede a New York (USA), dichiara di non conservare né registrare gli indirizzi IP degli utenti
- **Qwant** (https://www.qwant.com): sede a Parigi, finanziato dall'UE è consigliato dal gruppo Anonymous, perché non profila gli utenti e garantisce anonimato con la dissociazione dell'IP
- **Firefox Focus** (solo app per mobile): browser privato che blocca gli elementi traccianti

Strumenti per proteggere la privacy

Le estensioni (add-on o plugin) sono **componenti aggiuntivi** che possono essere installati nel browser per estenderne le funzionalità e migliorare sicurezza, accessibilità, per bloccare la pubblicità o personalizzare l'interfaccia utente → estensioni **consigliate per la privacy**:

- **uBlock Origin**: completamente open source, occupa poca memoria e CPU, blocca la pubblicità in modo efficiente perché usa migliaia di filtri aggiuntivi rispetto ad altri blocker
- **HTTPS Everywhere**: abilita la crittografia alle comunicazioni con molti siti web popolari per proteggersi da attacchi del tipo "*man in the middle*"
- **Privacy Badge**: impara a riconoscere e blocca annunci ed elementi traccianti che seguono e rintracciano a sua insaputa l'utente durante la navigazione del web
- **Privacy Settings**: permette di modificare le impostazioni della privacy del browser applicando diversi profili di sicurezza a seconda delle esigenze dell'utente
- **Cookie AutoDelete**: rimuove automaticamente i cookie (e le informazioni usate) quando non sono più utilizzati dalle schede del browser aperte
- **Decentraleyes**: protegge la privacy intercettando le richieste delle grandi reti per la distribuzione di contenuti (CDN) e fornendo la risorsa richiesta localmente

Reti sociali

L'uso dei **social network** pone l'attenzione sulla riservatezza dei dati personali perché tutto ciò che va su Internet diventa di pubblico dominio e di fatto se ne perde il controllo

Siamo quasi ossessionati dalla privacy, ma più o meno inconsapevolmente conferiamo in modo spontaneo milioni di dati: se l'utente pratica il **senso di responsabilità**, evita di divulgare informazioni che permettano l'identificazione e la conseguente falsificazione dell'identità

Occorre controllare con regolarità le **impostazioni dell'account**, soprattutto le opzioni sulla privacy e l'individuazione della posizione per non lasciare completamente pubblico il proprio profilo e limitare l'esposizione ai potenziali rischi connessi all'uso dei social network:

- **cyberbullismo**: utilizzo di Internet per attaccare ripetutamente un individuo
- **adescamento**: tentativo di acquisire la confidenza di una persona, di solito un minore, per indirizzarla verso comportamenti inappropriati
- **false informazioni/identità** (profili fake) spesso usati per adescamento e cyberbullismo
- **phishing**: link o messaggi per ottenere informazioni attraverso tecniche di ingegneria sociale

Cambridge Analytica

E’ una società commerciale di analisi e ricerca dei dati in **psicometria**, scienza che misura gli atteggiamenti umani: è possibile da una serie ridotta di domande su argomenti che sembrano non direttamente correlati, comprendere attitudini, gusti e inclinazioni delle persone

Cambridge Analytica è stata accusata di aver **utilizzato in modo fraudolento** (violando le policy di Facebook) i dati di circa 50 milioni di utenti per profilarli attraverso una serie impressionante di attitudini e propensioni che possono essere forniti agli investitori

Nei casi della **Brexit** e delle **recenti elezioni USA**, sono state create in base a questi dati micro-segmentazioni molto precise su specifici bacini di elettori in modo da sottoporli a messaggi individualizzati mirati ad accrescere determinati sentimenti, percezioni ed emozioni al fine di manipolare il consenso in favore della vittoria elettorale

Indirizzando il giusto messaggio alla persona predisposta o coinvolta sul tema è più facile convincerla rafforzandone l'opinione e attivarla perché faccia proselitismo: da **information recipient** a **information seeker** e **opinion leader**, secondo un diffuso modello di propaganda

Cambridge Analytica

Su Facebook si trovano **finte app** come i test "*come sarai da vecchio*" o "*a quale celebrità di Hollywood assomigli*" che richiedono l'autenticazione utente: sembrano innocenti e banali ma astutamente nascondono l'insidia della raccolta dei dati personali, vero carburante per chi si occupa di influenzare le nostre decisioni, anche elettorali

Aleksandr Kogan psicologo dell'università di Cambridge ha creato un'app (test di personalità per fini accademici): per usarla era necessario l'accesso con il profilo Facebook → in questo modo l'app ha avuto accesso ai profili di circa 300.000 persone e tutti i contatti collegati anche se non avevano autorizzato l'app, permettendo l'elaborazione di un **profilo psicografico molto preciso** per ciascun utente (ampiezza totale 50 milioni di utenti)

Il **tutto è perfettamente legale** per Facebook a condizione che i dati non vengano condivisi con aziende terze cosa che invece Kogan ha fatto con Cambridge Analytica che ha usato i dati per indirizzare i voti in USA e in Gran Bretagna: Facebook sapeva tutto dal 2015 ma si limitò ad intimare alle parti di cancellare i dati, cosa che non accadde

Cambridge Analytica

E’ difficile chiedere ad altri di proteggere i nostri dati, se siamo noi i primi a non prestare la dovuta attenzione ad es. alle impostazioni di condivisione e della privacy → **cosa fare**?

- **cancellare definitivamente** il profilo Facebook e i dati associati
- **disabilitare le interazioni dell’account** Facebook con terze parti (Facebook login) con l’opzione "*impostazioni > app > disabilita piattaforma*"
- **decidere per ogni app** quali sono i dati che possono essere condivisi
- **controllare le app autorizzate** e rimuovere quelle "ficcanaso" o inutilizzate

Ma questa **NON è una soluzione**: il problema è il modello di business del social network che è progettato per usare specifici meccanismi di condivisione dei dati che rivende per fini di marketing al miglior offerente e permette a terze parti di raccoglierli allo stesso scopo

I social network sono strumenti straordinari per il marketing personalizzato che hanno come obiettivo la **profilazione**: i dati personali raccolti vengono utilizzati da società di marketing per creare profili commerciali e inviare pubblicità targettizzate in base ai nostri gusti

Tutelare la privacy online

- attivare la **protezione anti-tracciamento** nel proprio browser preferito
- usare un **motore di ricerca privato** che non memorizza le ricerche effettuate e pertanto non sarà mai in grado di salvare i dati o condividerli con terze parti a scopo commerciale
- non fornire il **numero di telefono** e compilare solo i **campi strettamente necessari**
- diffidare di **richieste di contatto** provenienti da persone non conosciute
- diffidare dei **giochi online** di provenienza dubbia o incerta perché spesso sono creati ad hoc per ottenere l'accesso alle informazioni e ai contenuti dell'utente
- alle **domande di sicurezza** per la reimpostazione della password, inventare risposte mai semplici o banali (ad es. il nome della madre, dell'animale preferito o della città di nascita) perché sono facilmente reperibili online
- fare attenzione alle **autorizzazioni concesse alle app** mobile: non dare accesso a rubrica, microfono, fotocamera o geolocalizzazione se non indispensabili al funzionamento dell'app
- **chiudere le app** (ad es. l'assistente vocale) una volta terminato l'utilizzo: potrebbero "ascoltare" i dati raccolti e trasmetterli
- **non scegliere un'unica azienda** per tutti i servizi online (email, cloud, mappe, social, ecc.): meglio differenziare per rendere più difficile la ricostruzione della propria identità

Cancellare l'account

C'è una differenza tra **disattivare** (rendere temporaneamente il profilo invisibile alla ricerca) e **cancellare** l'account (eliminazione definitiva): prima di procedere all'eliminazione definitiva dalla piattaforma è consigliabile scaricare il backup dei dati e rimuovere informazioni personali, contatti, foto, video e ogni altro contenuto precedentemente condiviso

Il sito **justdelete.me** (http://backgroundchecks.org/justdeleteme/) fornisce le istruzioni per cancellare l'account da moltissimi servizi web: di solito basta autenticarsi alla piattaforma e selezionare nell'area impostazioni l'opzione per la disattivazione/cancellazione, oppure usare i link diretti, come nei seguenti casi:

- **Facebook**: https://www.facebook.com/help/delete_account
- **Twitter**: https://twitter.com/settings/accounts/confirm_deactivation
- **LinkedIn**: https://www.linkedin.com/help/linkedin/answer/63?lang=it
- **Instagram**: https://instagram.com/accounts/remove/request/permanent/
- **Telegram**: https://my.telegram.org/auth?to=deactivate

VoIP e messagistica istantanea

La **messaggistica istantanea** (IM) è un mezzo di comunicazione che utilizza Internet per inviare e ricevere messaggi di testo (corredati da eventuali file allegati) ed effettuare chiamate (VoIP) audio e video tra due o più persone → come riconoscere i messaggi truffaldini?

- **vulnerabilità**: rendono possibile a terzi l'accesso al dispositivo e ai suoi dati (backdoor)
- **malware**: messaggi che incitano a cliccare su link malevoli che possono accedere ai dati dell'utente oppure rallentare o danneggiare il dispositivo
- **phishing**: messaggi che inducono con l'inganno l'utente a visitare un sito clone per fargli inserire dati personali o di autenticazione
- **spam** o **bufale**: messaggi indesiderati e notizie non veritiere che hanno il solo scopo di fare disinformazione (spesso innocui, diventano pericolosi se accompagnati da link)

Le armi migliori sono l'**indifferenza** (non aprire messaggi non riconoscibili e soprattutto non cliccare gli allegati), **non divulgare informazioni** riservate e file a persone sconosciute o poco attendibili, utilizzare **metodi di cifratura** delle comunicazioni e la **blacklist** per bloccare i mittenti

Hate speech

L’incitamento all’odio (hate speech) è l’**attacco** basato sull’identità di genere, razziale, religiosa, sessuale, su gravi disabilità e malattie: è correlato a **fake news** e **cyberbullismo**, espressioni di aggressività in rete che colpiscono i più giovani o inesperti e proprio per questo indifesi e fragili

In rete alcune **persone comunicano in modo diverso**, rivelano informazioni personali o intime, manifestano apertamente le proprie pulsioni dando sfogo a qualsiasi aspetto personale senza impegnarsi a farli convivere con equilibrio come si richiede ad una persona matura

In questo modo, l’**identità dell’individuo** viene sostituita in parte o completamente con diverse identità virtuali spesso anonime perché nascoste da pseudonimi (nickname) che liberano dalle inibizioni e autorizzano la perdita di contatto con il proprio senso di responsabilità

Gli **haters** sono utenti che, liberatisi dalla maschera della realtà, vivono una condizione di libero sfogo dei desideri più repressi, esprimendo critiche aspre e giudizi offensivi rivolti a completi estranei o insinuandosi senza pudore nelle più accese ed animate discussioni online che molto spesso riguardano temi caldi come politica o immigrazione

Hate speech

L’hater non vuole diventare come la persona che attacca, ma al contrario più questa ha successo, più l’hater vuole insultarla e denigrarla, perché **pone il suo pensiero come unica realtà possibile** e l’opinione delle persone a lui non affini sono errate o delle menzogne

L’hater provoca, irrita, deride, diffama, insulta con l’**intento di manipolare o disprezzare l’altro**: alcuni lo fanno per interessi economici, la maggior parte perché mossa da sentimenti negativi (invidia, gelosia) → il dialogo è inutile, attaccarli è improduttivo (alimenta il loro momento di gloria), meglio eliminarli se possibile oppure ignorarli, ma se non basta cosa fare?

Gli haters sono come abili giocatori di scacchi, pronti a ribattere colpo su colpo per portare l’utente sul proprio campo di gioco, provocandolo secondo uno schema prestabilito: l’**antidoto** è prevederne le mosse e cercare di imporre il proprio gioco per costringerli a desistere

E’ importante munirsi di una buona dose di **lucidità** e **concentrazione** per non cadere nelle provocazioni dell’hater e per non opporre argomentazioni facili da smontare: se non dovesse bastare ancora, possono essere denunciati al titolare del servizio o all’autorità giudiziaria

Fake news

Le **fake news** (notizie false) sono informazioni inventate, ingannevoli o distorte allo scopo di diffondere disinformazione attraverso i mezzi di comunicazione mainstream e media sociali

La loro caratteristica è la **polarizzazione**: più gli argomenti sono radicali o presentati in modo sensazionalistico o esagerato più si prestano al fiorire di bufale e notizie non verificate → **lo scopo è** catturare l'attenzione del lettore per orientarlo finanziariamente o politicamente

La diffusione capillare della disinformazione è favorito dalla tendenza al **confirmation bias** (pregiudizio di conferma) che induce le persone a cercare solamente informazioni che confermano quello che già pensano

Le fake news **sono come un virus** che si diffonde tramite l'esposizione alla disinformazione: la soluzione sta nell'agire come un programma antivirus, cioè saper identificare la fonte della notizia falsa per bloccarla in tempo (o quanto meno decidere di non condividerla) affinché non possa "*contagiare*" altri utenti

Fake news

Alcuni suggerimenti per riconoscere la **grammatica delle fake news**:

- diffidare dei **titoli accattivanti**, "*urlati*", esagerati o orientati al sensazionalismo
- **controllare l'URL**: molti siti imitano le fonti autentiche facendo piccole modifiche all'URL
- osservare la **formattazione** (errori ortografici), **foto** e **video** manipolati o fuori contesto, **date senza senso** o eventi con data modificata
- selezionare **fonti valide**, cioé riconosciute nel campo in cui operano (una fonte non è affidabile per tutto) e confrontare fonti attendibili ma contrastanti
- verificare l'**attendibilità delle fonti** e il loro numero (da quante fonti è riportata la notizia)
- **separare i fatti dalle opinioni** e utilizzare solo opinioni di esperti riconosciuti
- verificare la **presenza di prove**: ogni dato deve avere un riferimento preciso
- a volte è difficile distinguere le notizie false da **scherzi** e post umoristici o satirici creati per divertire (ad es. non diffondere come notizia affidabile i post provenienti da siti satirici)
- conservare un atteggiamento prudente verso l'informazione: non condividere compulsivamente tutto ciò che capita a tiro, ma soltanto ciò che si ritiene credibile attraverso una **lettura critica** del contenuto

Cyberbullismo

Il cyberbullismo non è semplicemente associato a fenomeni quali violenza, abuso e/o furto di identità, ma deve essere **perpetuato nel tempo**: è un attacco continuo, ripetuto, offensivo e sistematico attuato con gli strumenti della rete aggravato dalla **pervasività** e dall'**anonimato**

La vittima è esposta costantemente agli insulti, prese in giro, all'abuso dei suoi dati personali, alle molestie e ricatti e se il **persecutore è anonimo**, la vittima da un lato ha la sensazione di non sentirsi mai al sicuro, dall'altro può pensare che nessuno potrà aiutarlo

Il fenomeno richiede attenzione normativa – come è stato fatto con la **Legge 29 maggio 2017 n. 71** recante "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*" – ma soprattutto collaborazione tra famiglie e insegnanti e una capillare opera di sensibilizzazione all'educazione al digitale:

- **non criminalizzare Internet**, ma capire usi e dinamiche per trasmettere l'idea che c'è libertà solo se c'è responsabilità (condividere le regole di gestione della privacy, tagging e blocking aiuta a valutare l'opportunità di pubblicare i contenuti, come foto, video o altro, in rete)

Cyberbullismo

- essere consapevoli **tutto ciò che va online** può essere visto in forma permanente, pubblica e decontestualizzata (attenzione a pubblicare dati sensibili, specialmente i numeri di telefono)
- osservare ed **ascoltare in modo non superficiale** i propri figli/studenti, non limitarsi ad un banale "*Come è andata a scuola?*" o alle loro performance scolastiche
- **quanto avviene in rete è rilevante quanto ciò che accade a scuola**: chiedere "*com'è andata oggi su Facebook?*" è importante quanto "*com'è andata oggi a scuola?*"
- educare alla **collaborazione**, al valore della **cooperazione**, all'**educazione condivisa** attraverso il potere dell'esempio (non si può proibire l'uso dello smartphone se siamo i primi ad usarlo) significa diventare un sicuro punto di riferimento per i più giovani
- **farsi insegnare dai più giovani** il funzionamento delle piattaforme digitali permette di capire come funzionano, aiutando i ragazzi a discernerne l'utile dal pericoloso
- impostare **strumenti di ascolto alla rete** improntati all'apprendimento: approfittare dei tanti casi di cronaca per parlarne in aula/famiglia e capire se ci sono stati episodi analoghi in classe e quali potrebbero essere le reazioni
- non temere di **chiedere aiuto**, ma fare rete (con i compagni di scuola, gli insegnanti, eventuali figure di sostegno o psicologi, polizia, ecc.) per ridurre l'impatto dei pericoli della rete

Protezione dei minori

La maggior parte degli utenti del web adulti ed esperti ha ormai imparato ad usare il **giusto livello di precauzione** nell'interagire con chi non si conosce per evitare brutte sorprese (ad es. se si decide di incontrare qualcuno conosciuto online, dare il primo appuntamento in un luogo pubblico e affollato e non presentarsi da soli)

Non è la stessa cosa per i minori: la loro innata curiosità unità all'ingenuità della giovane età può metterli in una condizione di rischio nel momento in cui sono avvicinati online da soggetti malintenzionati → possibili precauzioni:

- **proteggere l'identità** dei minori evitando la divulgazione di specifici dati personali
- fare attenzione allo **sharenting**, cioè la tendenza di molti genitori a documentare ogni passo dei propri bambini con foto e video sui social network: i genitori dispongono di informazioni delicatissime che è necessario proteggere per non sottovalutare le conseguenze
- soprattutto nella fase iniziale di approccio al web, **accompagnare i minori nella navigazione** e insegnargli a raccontare le loro esperienze di navigazione

Non dare niente per scontato

I criminali informatici dispongono di software sempre più sofisticati e sono abilissimi ad attaccare singoli utenti e organizzazioni approfittando soprattutto dell'ingenuità umana:

- **non cliccare mai su links inattesi** o che non ci si aspetta di ricevere
- **ignorare i pop-up**: possono attivare malware che conducono i criminali direttamente nel pc
- **non memorizzare dati sui siti web**, soprattutto password e dati della carta di credito
- **usare più di un account email** per non concentrare i dati di identità in un solo account
- usare **password robuste**, **uniche** e **diverse** su ogni sito
- **non riutilizzare** su altri account la password della mail principale
- attivare la **verifica di accesso in due passaggi** attraverso SMS o app autenticatore
- **bloccare** con una password efficace i propri dispositivi fissi e mobili
- i Mac sono vulnerabili come gli altri, utilizzare un **buon software** antivirus/antimalware
- se disponibile, attivare e configurare una funzione **wipe my phone**: "*Find My iPhone*", "*Android Device Manager*" e "*BlackBerry Protect*" consentono di cancellare da remoto tutti i dati personali evitando che cadano nelle mani sbagliate
- acquistare online solo su **siti sicuri e affidabili** che usano la connessione HTTPS

Non dare niente per scontato

- fare attenzione sui **siti di acquisto ad asta**: controllare i feedback del venditore e tutelare il proprio conto online magari creandone uno appositamente dedicato ai pagamenti online
- il **rimborso per frode** non è scontato: le banche erogano il rimborso solo dopo che la vittima ha dimostrato di aver mantenuto segrete le proprie credenziali bancarie (se si è più volte protagonisti di frode dimostrare l'estraneità all'accaduto diventa difficile)
- rifiutare le **richieste di contatto** sui social media (specialmente Facebook e Linkedin) da parte di persone che non si conoscono
- **cautela nel condividere le informazioni**: sui social media uno dei rischi principali è il furto di identità, quindi se si pubblicano online informazioni strettamente personali qualcuno potrebbe usarle a nostro discapito
- **diffidare delle reti Wi-Fi pubbliche**: nella maggior parte dei casi non possono crittografare i dati che restano in parte visibili e qualsiasi malintenzionato dotato di un "*packet sniffer*" può intercettare i dati personali condivisi su una rete pubblica
- **usare un servizio DNS** (converte gli indirizzi web in indirizzi IP) per proteggere i dispositivi: di solito si usa il servizio DNS del provider di default, ma si può scegliere di iscriversi ad un altro servizio per essere reindirizzati ogni volta che si tenta di accedere ad un sito pericoloso

Posta elettronica

Normalmente la posta elettronica **non è sicura** perché invia i messaggi in chiaro, a meno che non si proceda alla cifratura del messaggio stesso: solo il legittimo destinatario, in possesso di una chiave di decodifica è in grado di leggerlo

Un altro aspetto critico della posta elettronica è che non è difficile inviare un messaggio spacciandosi per un'altra persona: la **firma digitale** è il risultato di una procedura di crittografia che rende manifesta e verifica l'autenticità (identità) del mittente e l'integrità di un documento

La firma digitale si basa su un **certificato digitale** rilasciato da un'autorità di certificazione legalmente riconosciuta: la sottoscrizione prevede la creazione di una coppia di chiavi (pubblica e privata) conservata all'interno di appositi dispositivi di firma (ad es. smart card o chiavetta USB) → assieme alla cifratura del messaggio, rende sicura la posta elettronica

Per fare un **confronto con la posta tradizionale**, un normale messaggio di posta elettronica può essere paragonato ad una cartolina postale, un messaggio cifrato ad una lettera in busta chiusa e un messaggio dotato di firma digitale ad una raccomandata

Truffe telematiche

I messaggi di posta elettronica sono il principale veicolo per la diffusione delle truffe telematiche, **reati che sottraggono in genere piccole cifre**, ma proprio per la loro diffusione capillare assicurano grossi proventi al truffatore:

- **finte vendite all'asta** con merci offerte e mai inviate ai clienti o con prezzi gonfiati
- **vendite di HW/SW** con merci mai inviate o diverse a quanto pubblicizzato
- **offerte di servizi gratis** che poi si rivelano a pagamento o non vengono forniti una volta pagati oppure ancora vengono forniti servizi diversi da quelli pubblicizzati
- **schemi di investimento** a piramide (multilevel business), opportunità di affari o franchising
- **opportunità di lavoro a distanza** con acquisto anticipato del materiale necessario
- **prestiti di denaro** (mai concessi) con richiesta anticipata di commissione
- **false promesse** di rimuovere informazioni negative per l'ottenimento di crediti (ad es. rimozione di nominativi da blacklist) o di concessione (con richiesta di commissione) di carte di credito a soggetti con precedenti negativi
- **numeri a pagamento** (tipo 899) da chiamare per scoprire un ammiratore segreto o una fantomatica vincita (di vacanze o oggetti)

Phishing

E’ una **truffa che sfrutta le tecniche dell’ingegneria sociale** con cui il malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale → tipi di phishing:

- **spear phishing**: attacco mirato verso un individuo o una compagnia, è la tecnica più diffusa su Internet, con una quota del 91% degli attacchi
- **clone phishing**: sfrutta una mail legittima che viene modificata negli allegati o nei link e rimandata ai riceventi con lo scopo di ingannarli, dichiarando di essere una versione aggiornata → si basa sulla fiducia generata da una mail precedentemente ricevuta
- **whaling**: attacco indirizzato verso figure di spicco di aziende o enti per ottenere le credenziali del manager o informazioni di rilevante valore economico o commerciale

"*Si possono investire milioni di dollari per i propri software, per l’hardware delle proprie macchine e per dispositivi di sicurezza all’avanguardia, ma se c’è anche solo un unico dipendente della nostra azienda che può essere manipolato con un attacco di ingegneria sociale, tutti i soldi investiti saranno stati inutili*" – Kevin Mitnick

Tre tipi di email da non aprire

La posta elettronica è il mezzo preferito per inoltrare messaggi di **phishing** che replicano nell'aspetto la comunicazione digitale di una società, ente o banca affidabile per ottenere con l'inganno i dati riservati dell'utente:

- **conferma dei dati personali**: nessuna società, banca o altro chiederà di confermare i dati compilando un modulo online o rispondendo all'email, perché non è un mezzo sicuro (di solito viene fatto personalmente o direttamente dal sito web ufficiale)
- **vincita premio in denaro**: se l'utente non è registrato al servizio, è impossibile vincere qualcosa, così come è improbabile ereditare una fortuna da uno sconosciuto parente
- **il dispositivo è stato colpito da un virus**: sfruttare la paura è una potente arma per spingere l'utente a fare qualcosa che in condizioni normali non avrebbe fatto → se il virus è in esecuzione, l'utente non riceve una notifica via email ma ne rileva l'esistenza attraverso allerte di sistema o da parte del software di sicurezza

Di solito il phishing si appoggia a siti web civetta riconoscibili dal nome di dominio: **solo HTTPS dimostra l'autenticità del dominio** (HTTP può essere dirottato con la tecnica del pharming)

Buone prassi

La posta elettronica può usare in modo esclusivo o combinato:

- **spam**: messaggi ripetuti non richiesti, di solito di carattere pubblicitario
- **malware**: messaggi con allegati o immagini infetti
- **phishing**: messaggi per ottenere con l'inganno i dati riservati dell'utente

NON dare seguito in nessun modo alla comunicazione, neanche per educazione o per dire che non si è interessati, perché ciò equivale a confermare indirettamente che l'indirizzo email è attivo, incoraggiando i malintenzionati ad utilizzarlo → la cosa migliore è:

- **non aprire i messaggi**, ma cestinarli direttamente, per evitare l'attivazione di file eseguibili legati alla visualizzazione delle immagini o all'apertura di eventuali allegati
- inserire nella **blacklist** i mittenti da bloccare ed eventualmente segnalarli alla Polizia delle Comunicazioni (https://www.commissariatodips.it/)
- **verificare** (con diverso mezzo di comunicazione) direttamente con la società, ente, banca in questione l'autenticità della comunicazione ricevuta

Molestie e truffe telefoniche

Sono in rapida crescita le **molestie** (contatti telefonici ripetuti e insistenti, tali da generare nella vittima uno stato di soggezione psicologica) e le **truffe telefoniche** soprattutto nei confronti di persone sole o anziane, incapaci di difendersi dagli interlocutori più spregiudicati

Il primo genere di truffa avviene da parte di computer che compongono numerazioni a caso oppure di operatori che utilizzano rubriche acquistate in modo fraudolento nel dark web:

- **ping calls (+216)**: il cellulare squilla per qualche istante, di solito non c'è neanche il tempo per rispondere e se l'utente richiama, magari incuriosito dall'aver ricevuto la chiamata, viene collegato con un numero che scala automaticamente (anche €1/sec.) il credito telefonico
- **call ID spoofing**: variante del ping calls che permette una schermatura del numero reale da cui arriva la chiamata e induce a pensare che si tratti di una telefonata lecita

In questi casi, la soluzione migliore è di **non rispondere** a chiamate da numeri non presenti in rubrica oppure contattare il nostro operatore telefonico e **chiedere il blocco delle chiamate** che svuotano il conto telefonico (per riavere il credito rubato, occorre procedere con una denuncia)

Raggiro con pretesti

Il **pretexting** (addurre pretesti) è il **phishing** che usa chiamate e sms attraverso le tecniche tipiche dell'ingegneria sociale: il malintenzionato si presenta in modo legittimo per indurre la vittima, con menzogne e raggiri elaborati, a fornire informazioni personali o riservate

Può presentarsi come dipendente di una banca, un ufficio pubblico, una compagnia telefonica o un'emittente televisiva e usare la **solita scusa** di una anomalia su proprio conto corrente o carta di credito che può essere risolto solo confermando le informazioni anagrafiche, le credenziali di accesso o altri dati simili

Lo **stile della telefonata** mira a condizionare la vittima con tecniche psicologiche diverse quali l'autorevolezza dell'interlocutore, colpa, panico, ignoranza, desiderio, avidità e buoni sentimenti (desiderio di aiutare il prossimo) che spiegano il tono conciliante, oppure ansioso, o rigido e distaccato o particolarmente accesso e aggressivo della comunicazione

In questi casi è meglio **riagganciare senza fornire alcuna informazione** o, al limite, contattare direttamente l'azienda presunta mittente della telefonata per eseguire le verifiche del caso

Contromisure e strumenti di difesa

L'**Autorità Garante** per la protezione dei dati personali stabilisce che, senza il proprio consenso, nessuno può prendere i nostri dati dagli elenchi telefonici per fare offerte commerciali per telefono o posta, ma come dimostrano le numerose telefonate ripetute anche in modo assillante questa disposizione non viene rispettata → **cosa fare?**

- la regola generale è **non rispondere** alle chiamate da numeri non presenti in rubrica
- vigilare e **valutare le telefonate** con una buona dose di diffidenza: bisogna partire dall'idea che ogni input proveniente dall'esterno che riguarda il nostro patrimonio o un mezzo di pagamento sia da considerare a rischio
- **verificare l'identità** del numero chiamante tramite motore di ricerca o siti che raccolgono le segnalazioni degli utenti (https://www.tellows.it, https://www.chistachiamando.it)
- inserire i numeri indesiderati nella **blacklist** dei contatti bloccati (smartphone)
- usare un **call blocker** (telefono fisso), sistema intelligente in grado di terminare tutte le chiamate indesiderate da numeri sconosciuti e da numeri in chiaro inseriti nella blacklist
- prendere nota del numero di telefono e segnalarlo all'Autorità Garante attraverso l'organismo regionale del CO.RE.COM (http://www.corecomfvg.it)

Registro delle opposizioni

Dal 2011 esiste il **registro pubblico delle opposizioni** (http://www.registrodelleopposizioni.it) a tutela della privacy del cittadino che decide di negare agli operatori di telemarketing l'utilizzo dei propri dati personali presenti negli elenchi telefonici:

- **attualmente**, con l'iscrizione al registro, il cittadino sceglie di non voler più ricevere telefonate per scopi commerciali o ricerche di mercato
- **con la nuova normativa in arrivo**, la tutela si estenderà ai cellulari e tutti gli altri dati presenti negli elenchi telefonici pubblici come gli indirizzi di casa o ufficio (se pubblicati negli elenchi telefonici) in modo da non vedersi più recapitare via posta messaggi pubblicitari

Gli operatori che continueranno a usare i dati iscritti nel registro rischiano una **sanzione da 10mila a 100mila euro** e - se l'inadempienza si ripete - la sospensione e successivamente la revoca dell'autorizzazione all'esercizio dell'attività

L'Autorità deve ancora individuare **due prefissi** per distinguere le telefonate degli enti che svolgono indagini statistiche da quelle dei call center (ricerche di mercato o scopi commerciali)

Gestione sicura dei dati

Per una maggiore sicurezza fisica si possono usare nei dispositivi predisposti i **cavi di sicurezza** (i più diffusi seguono lo standard Kensington Security Lock) che però non evitano del tutto il rischio della perdita dei dati in caso di furto, smarrimento o rottura del dispositivo

Diventa quindi fondamentale avere una copia di sicurezza dei dati (**backup**) per poterli ripristinare in originale in caso di necessità:

- il **backup serve solo se è aggiornato**: in base alla propria attività sul dispositivo stabilire con quale frequenza (giornaliera, settimanale, mensile, ecc.) fare la copia dei dati
- per non dimenticarsi, pianificare il **backup automatico** a scadenze regolari in un momento in cui il dispositivo è acceso ma non utilizzato (per evitare che la copia rallenti il lavoro)
- fare attenzione alla **collocazione del backup**: la copia di sicurezza va messa in un luogo il più sicuro possibile e diverso dalla sede originale dei dati (per questa ragione sempre più spesso la copia di backup viene effettuata online, su server remoti)

Distruzione sicura dei dati

Quando il dispositivo viene sostituito è necessario **eliminare i dati** dalle memorie di massa, ricordando che la semplice cancellazione di un file non garantisce la sua effettiva rimozione:

- i sistemi operativi moderni utilizzano il **cestino**, una cartella di sistema dove spostare i files cancellati che però restano residenti sul dispositivo e possono sempre essere ripristinati
- anche se il cestino viene svuotato, rimangono comunque **tracce dei files su disco**: non sono visibili con gli strumenti tradizionali, ma con programmi specifici possono essere ricostruiti quasi integralmente a seconda del tempo trascorso dalla loro cancellazione

Per cancellare definitivamente i dati occorre utilizzare altri metodi:

- **tritadocumenti** per i documenti cartacei
- **rendere inutilizzabili le memoria di massa** o smagnetizzarle con apparecchi (degausser) in grado di applicare intensi campi magnetici
- se la memoria di massa deve essere riutilizzata, eliminare i files in modo definitivo e sicuro con **appositi software** che sovrascrivono i files più volte in modo da renderli irrecuperabili