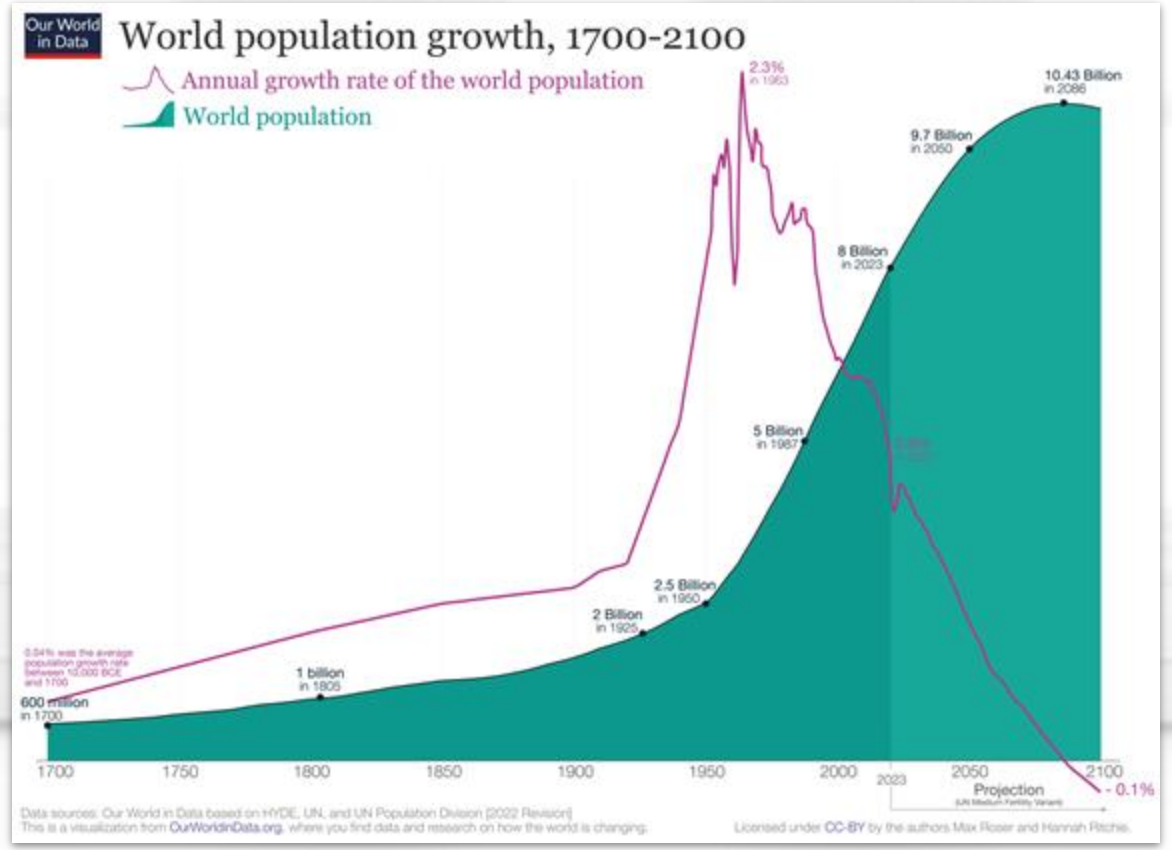
Cyber security e Autodifesa Digitale

Furto di dati, tempo e pensieri

dott. Andrea Tironi

Il contesto in cui viviamo, il mondo digitale di oggi

Trend Demografico



Trend Tecnologico

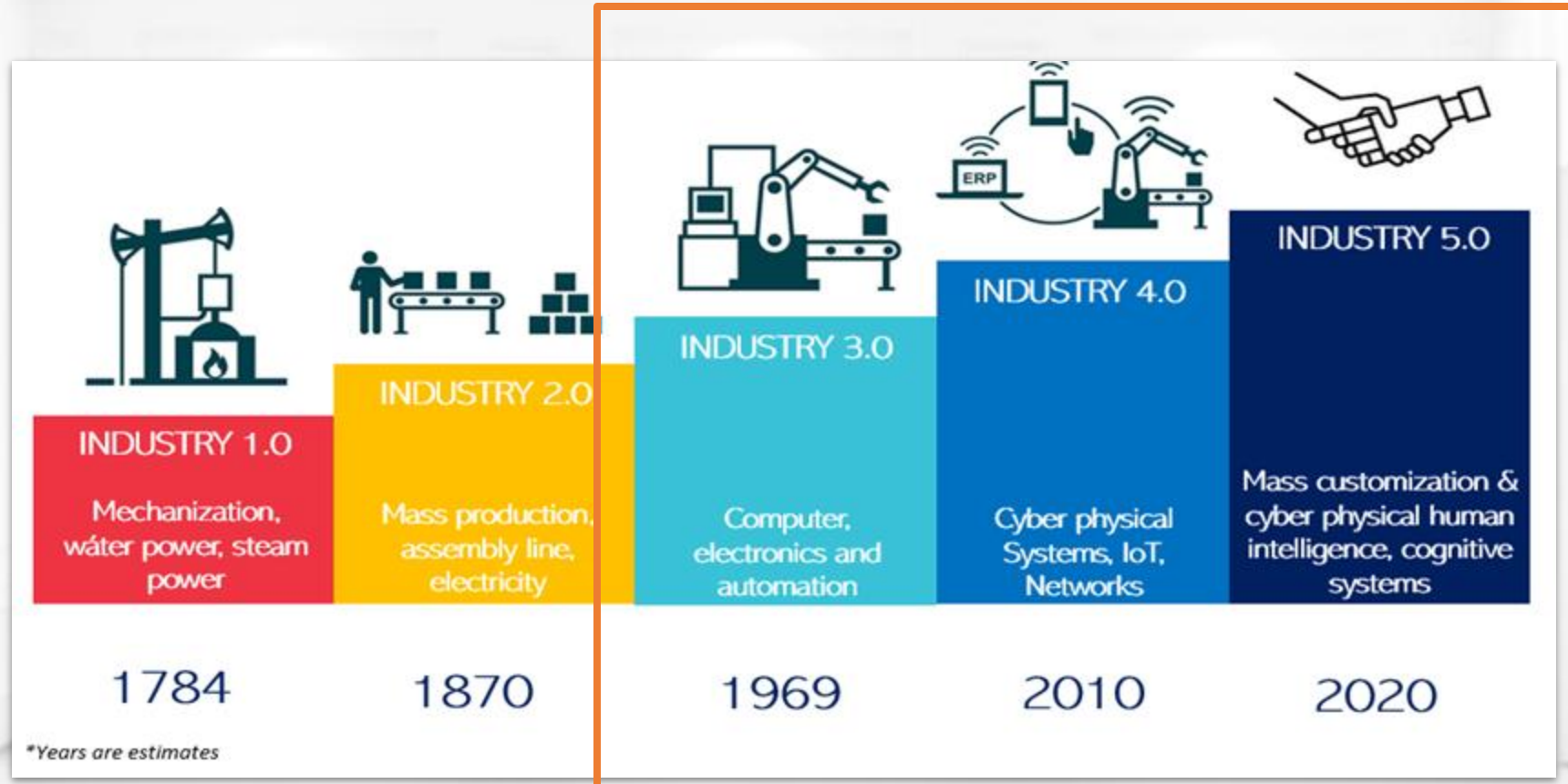


Immagine da Linkedin

Trend Digitale

Informatizzazione
Anni ‘60-oggi

Internet
Anni 90-oggi

Social Media Era
e Smartphone Era
2005-Oggi

Ai Era

2022 - ?

Technology Change

Prima rivoluzione con **Copernico** che ha fatto cadere la centralità dell'uomo rispetto all'universo.

La **seconda** con **Darwin** che con la sua teoria dell'evoluzione ha mostrato l'origine animale dell'uomo e quindi ha messo in discussione l'antropocentrismo.

La **terza** con **Freud** che con la scoperta dell'inconscio ha messo in discussione il dominio della mente e della ragione.

La **quarta** rivoluzione appartiene al nostro presente, l'era in cui l'**intelligenza artificiale e la realtà virtuale** segnano il primato del digitale sull'analogico mettendo in forte discussione il controllo dell'umano sul mondo in cui vive.

Generation Turnover

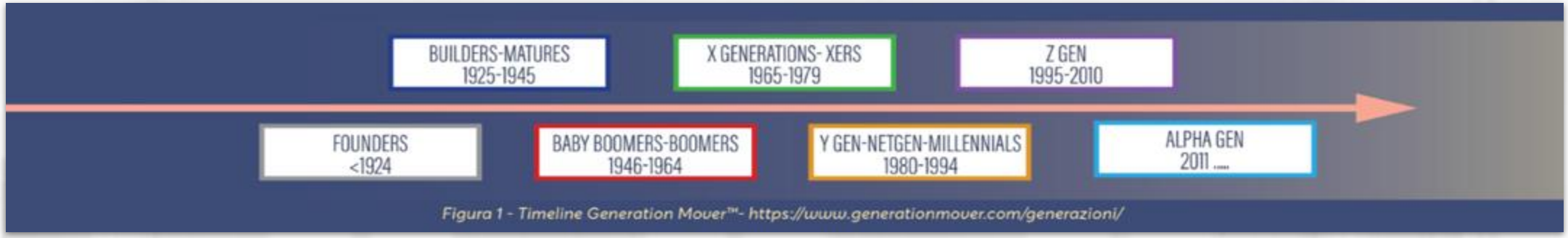


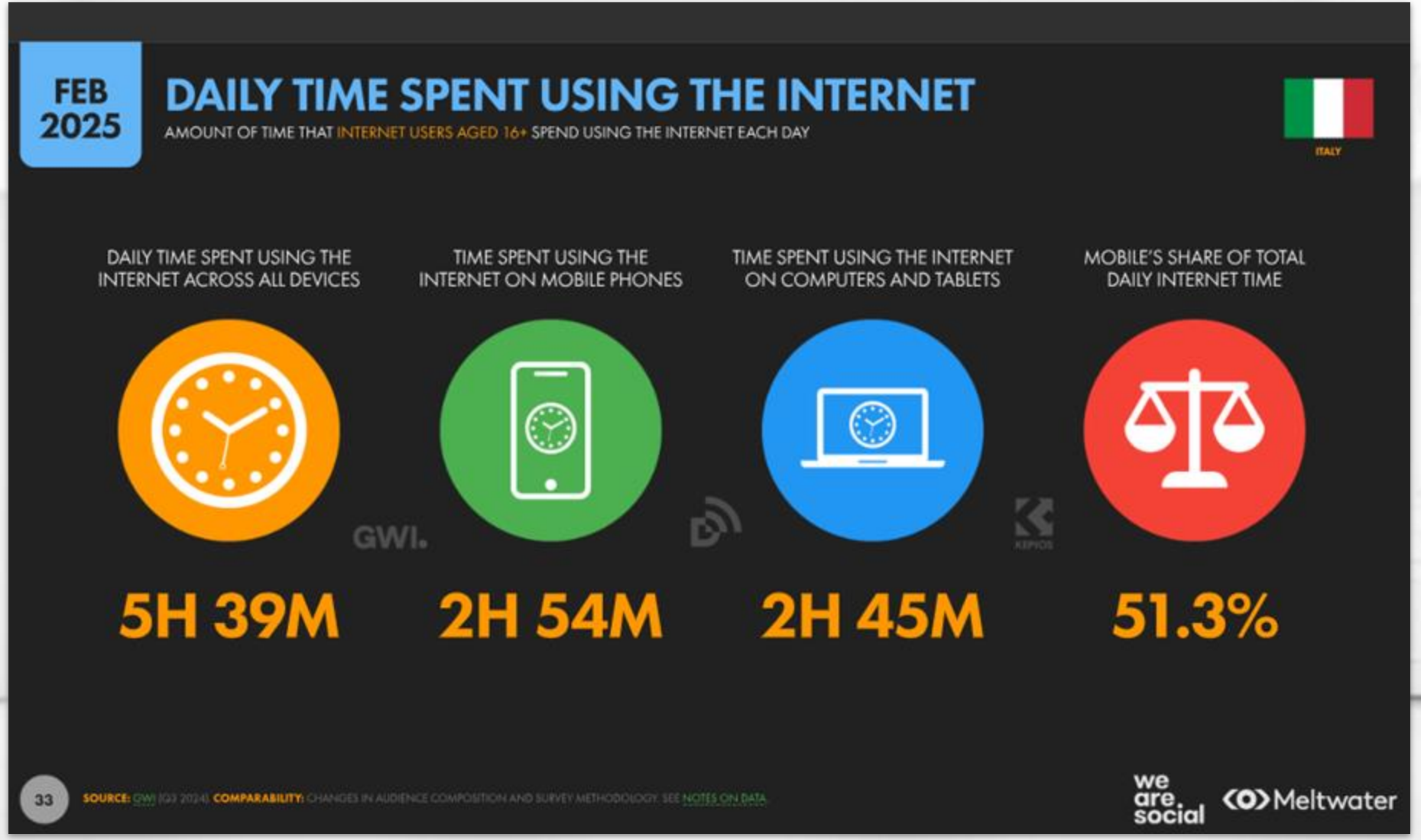
Immagine e dati da Italian Institute for the Future, Studio su Italia 2032

7 generazioni sulla terra (volendo anche 8)
5 generazioni nel mondo del lavoro

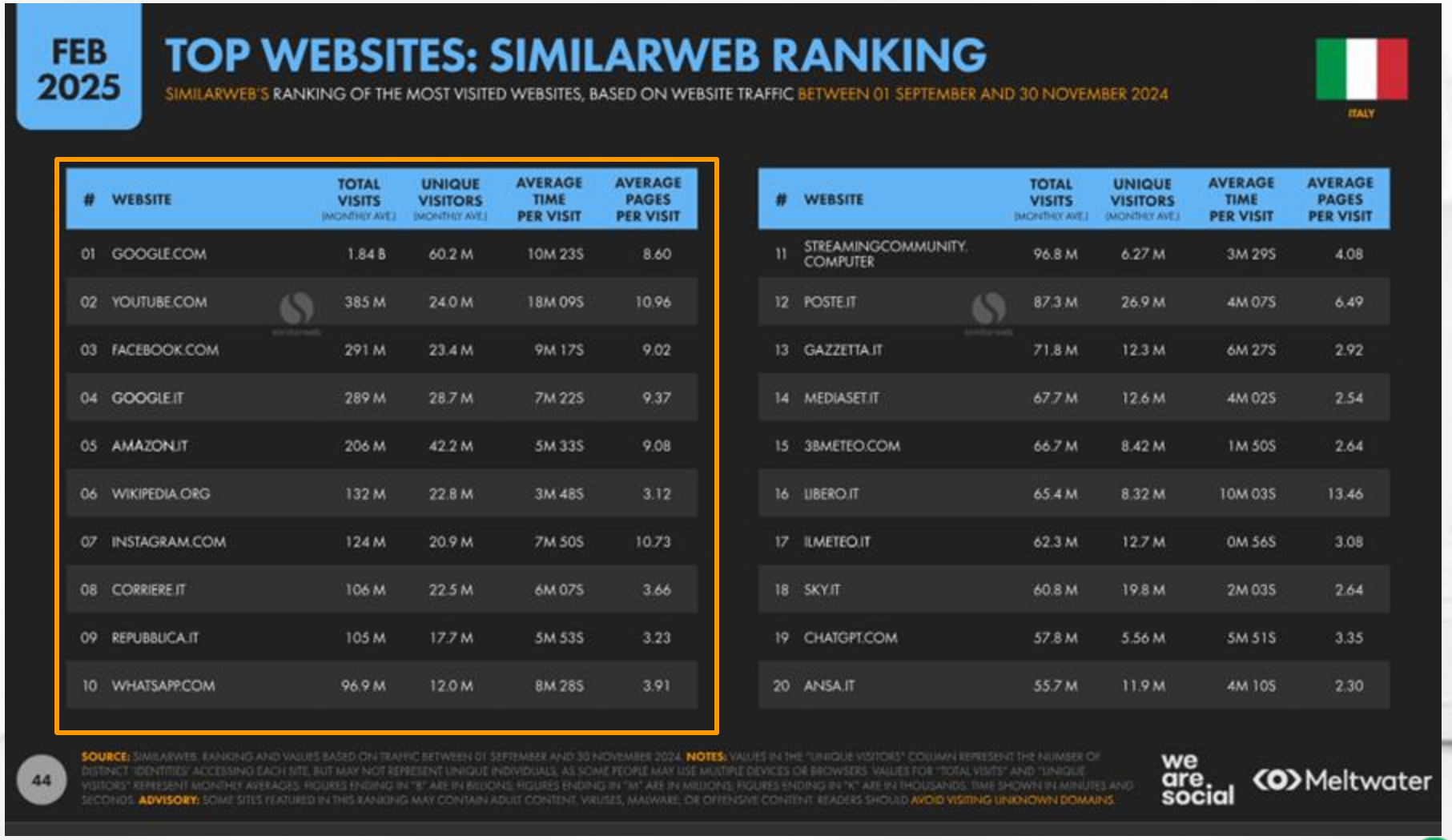
La diversità diventa marcata, si riduce il turnover e aumenta il tempo di permanenza delle generazioni nate prima.

Inoltre i nativi digitali e nativi ai non è detto che siano consapevoli e capaci di utilizzare le tecnologie al meglio, o che riesca a vivere con serenità nel mondo virtuale.

Genz tempo su internet



GenZ - Cosa utilizzano



FEB 2025

TOP WEBSITES: SIMILARWEB RANKING

SIMILARWEB'S RANKING OF THE MOST VISITED WEBSITES, BASED ON WEBSITE TRAFFIC BETWEEN 01 SEPTEMBER AND 30 NOVEMBER 2024

ITALY

#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
01	GOOGLE.COM	1.84 B	60.2 M	10M 23S	8.60
02	YOUTUBE.COM	385 M	24.0 M	18M 09S	10.96
03	FACEBOOK.COM	291 M	23.4 M	9M 17S	9.02
04	GOOGLE.IT	289 M	28.7 M	7M 22S	9.37
05	AMAZON.IT	206 M	42.2 M	5M 33S	9.08
06	WIKIPEDIA.ORG	132 M	22.8 M	3M 48S	3.12
07	INSTAGRAM.COM	124 M	20.9 M	7M 50S	10.73
08	CORRIERE.IT	106 M	22.5 M	6M 07S	3.66
09	REPUBBLICA.IT	105 M	17.7 M	5M 53S	3.23
10	WHATSAPP.COM	96.9 M	12.0 M	8M 28S	3.91

#	WEBSITE	TOTAL VISITS (MONTHLY AVE.)	UNIQUE VISITORS (MONTHLY AVE.)	AVERAGE TIME PER VISIT	AVERAGE PAGES PER VISIT
11	STREAMINGCOMMUNITY.COMPUTER	96.8 M	6.27 M	3M 29S	4.08
12	POSTE.IT	87.3 M	26.9 M	4M 07S	6.49
13	GAZZETTA.IT	71.8 M	12.3 M	6M 27S	2.92
14	MEDIASET.IT	67.7 M	12.6 M	4M 02S	2.54
15	3BMETEO.COM	66.7 M	8.42 M	1M 50S	2.64
16	LIBERO.IT	65.4 M	8.32 M	10M 03S	13.46
17	ILMETEO.IT	62.3 M	12.7 M	0M 56S	3.08
18	SKY.IT	60.8 M	19.8 M	2M 03S	2.64
19	CHATGPT.COM	57.8 M	5.56 M	5M 51S	3.35
20	ANSA.IT	55.7 M	11.9 M	4M 10S	2.30

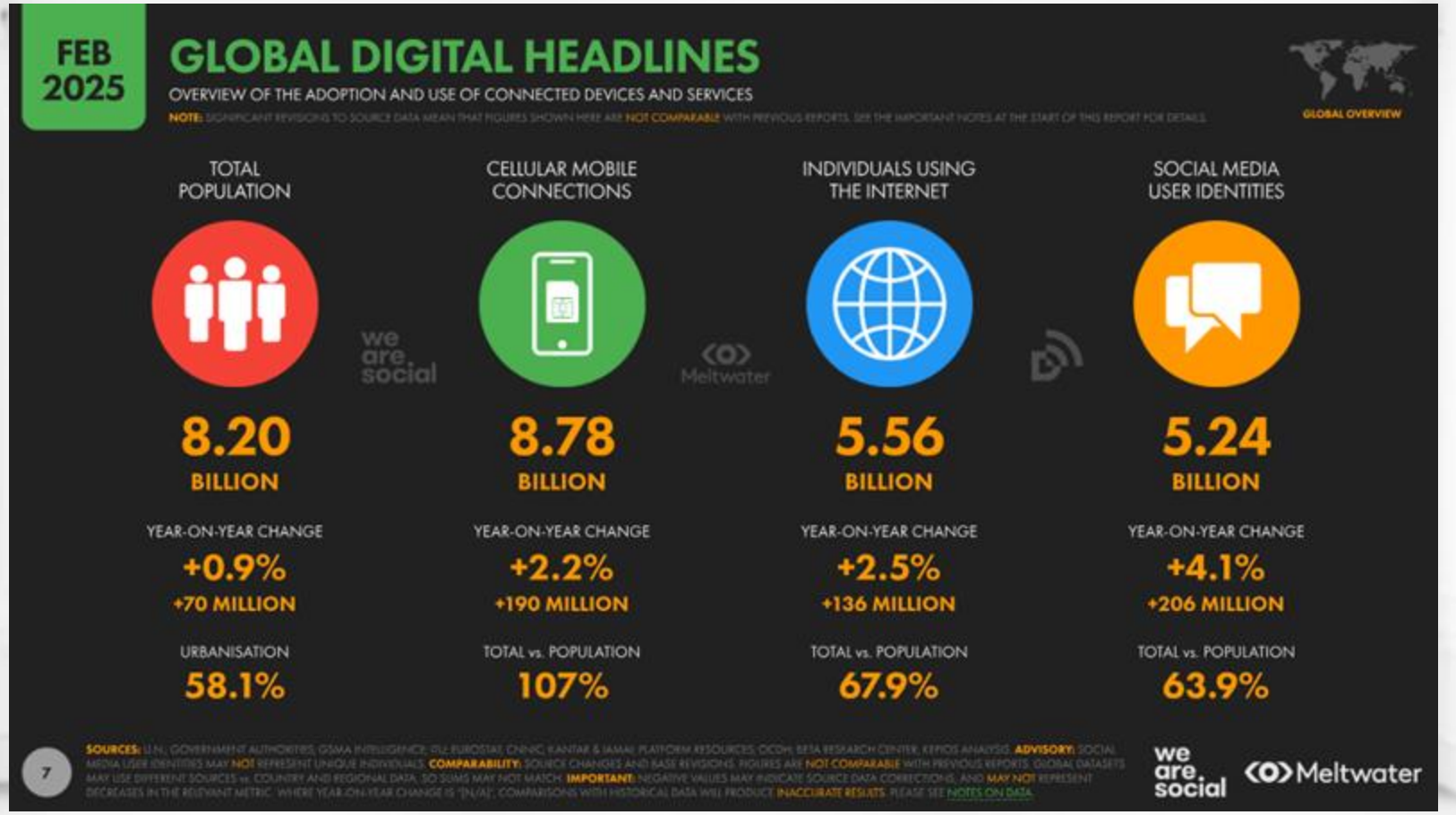
44

SOURCE: SIMILARWEB. RANKING AND VALUES BASED ON TRAFFIC BETWEEN 01 SEPTEMBER AND 30 NOVEMBER 2024. NOTES: VALUES IN THE "UNIQUE VISITORS" COLUMN REPRESENT THE NUMBER OF DISTINCT "IDENTITIES" ACCESSING EACH SITE, BUT MAY NOT REPRESENT UNIQUE INDIVIDUALS, AS SOME PEOPLE MAY USE MULTIPLE DEVICES OR BROWSERS. VALUES FOR "TOTAL VISITS" AND "UNIQUE VISITORS" REPRESENT MONTHLY AVERAGES. FIGURES ENDING IN "B" ARE IN BILLIONS; FIGURES ENDING IN "M" ARE IN MILLIONS; FIGURES ENDING IN "K" ARE IN THOUSANDS. TIME SHOWN IN MINUTES AND SECONDS. ADVISORY: SOME SITES FEATURED IN THIS RANKING MAY CONTAIN ADULT CONTENT, VIRUSES, MALWARE, OR OFFENSIVE CONTENT. READERS SHOULD AVOID VISITING UNKNOWN DOMAINS.

we are social · Meltwater

formazione PA

Cosa utilizziamo



formazione PA

formazione PA

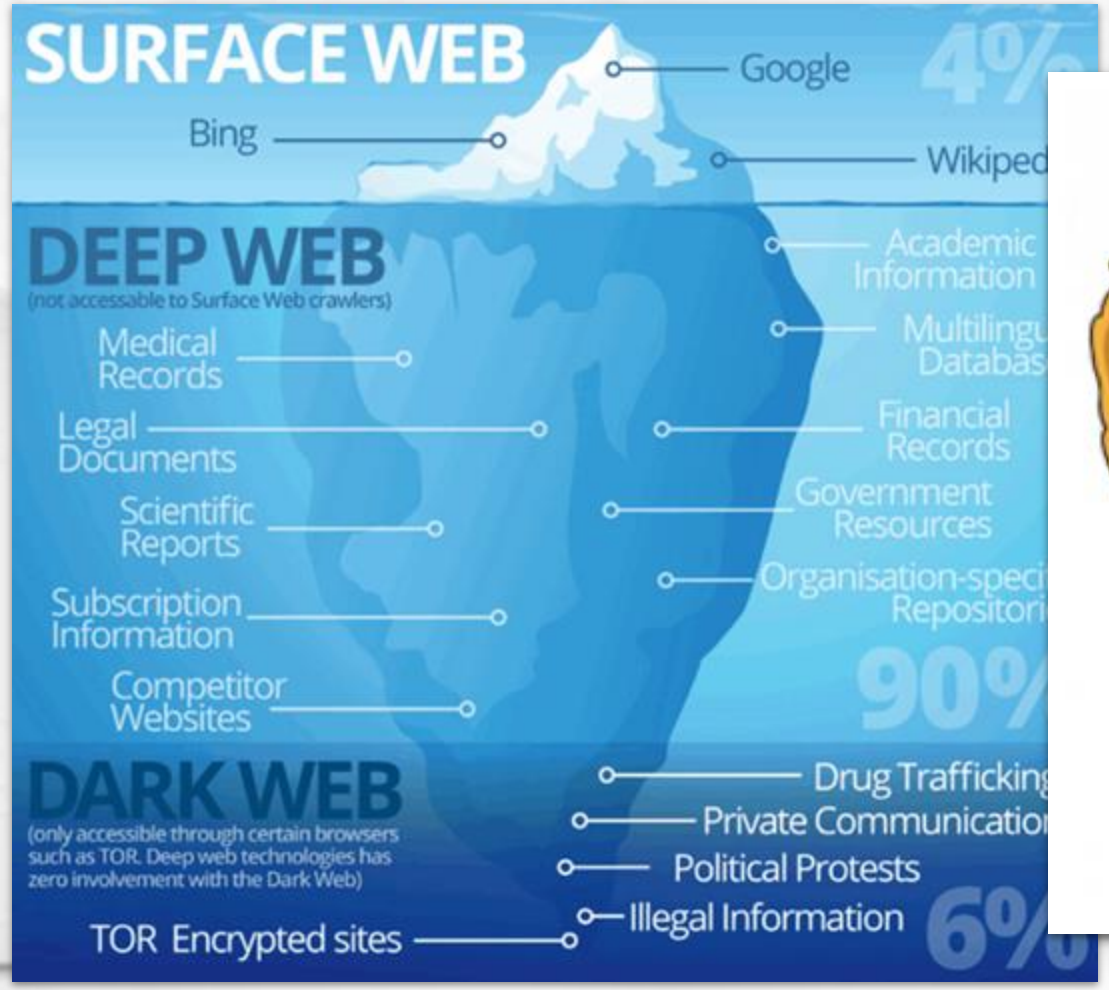
SEI LE 5 PERSONE
CON CUI PASSI PIÙ TEMPO

SEI I 5 ALGORITMI
CON CUI PASSI PIÙ TEMPO

Il contesto in cui viviamo

Il mondo digitale

Contestualizziamo



1 minuto di internet

Storia

Iperstoria

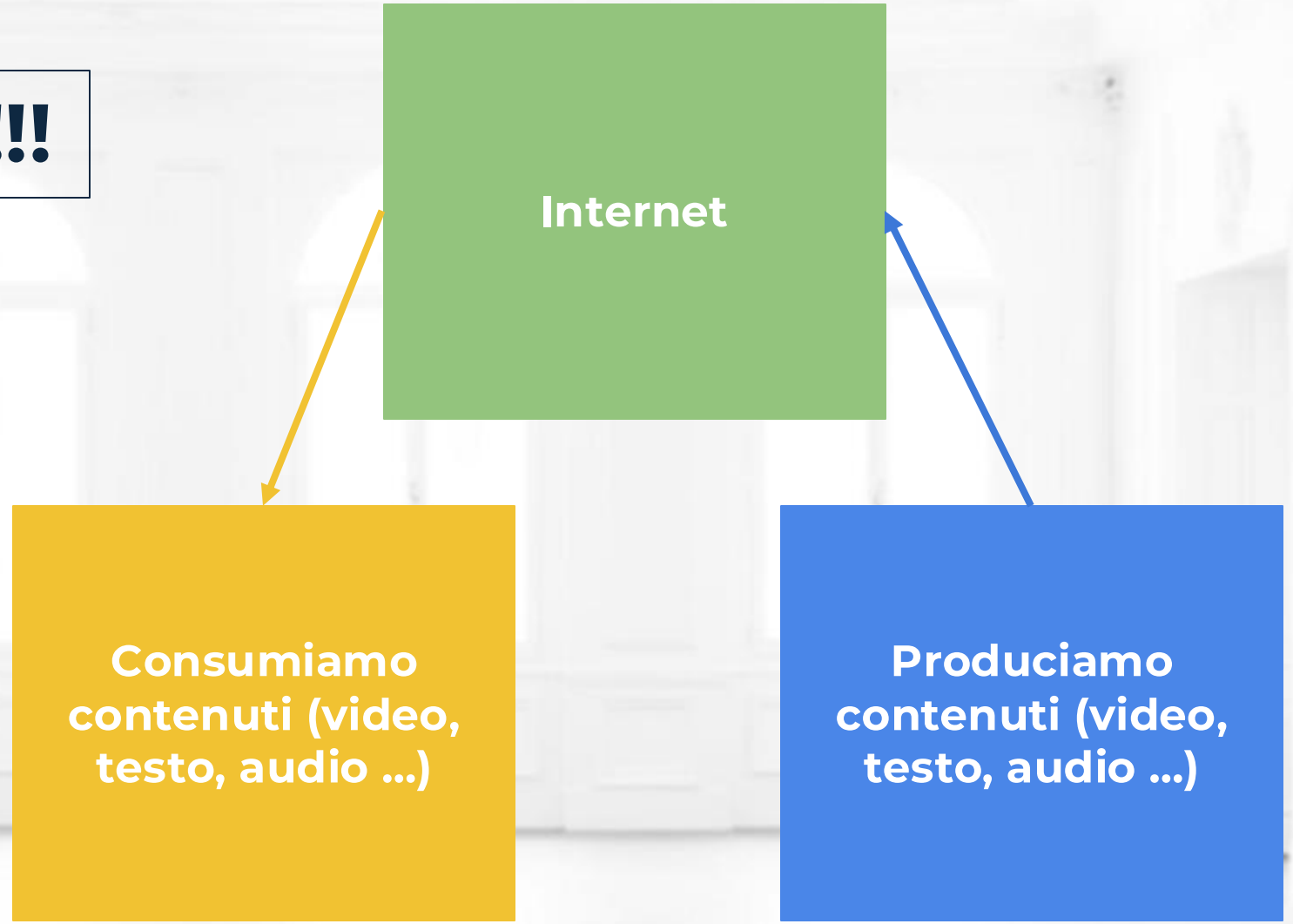
Fonte: https://www.instagram.com/p/C3RmRXvrMEw/

formazionePA

Produttori e Consumatori di Dati

!!! Inforg !!!

Spartiacque anni 2000!



formazionePA

Personaggi Pubblici e Privati

VERO --- L'online influenza l'offline!

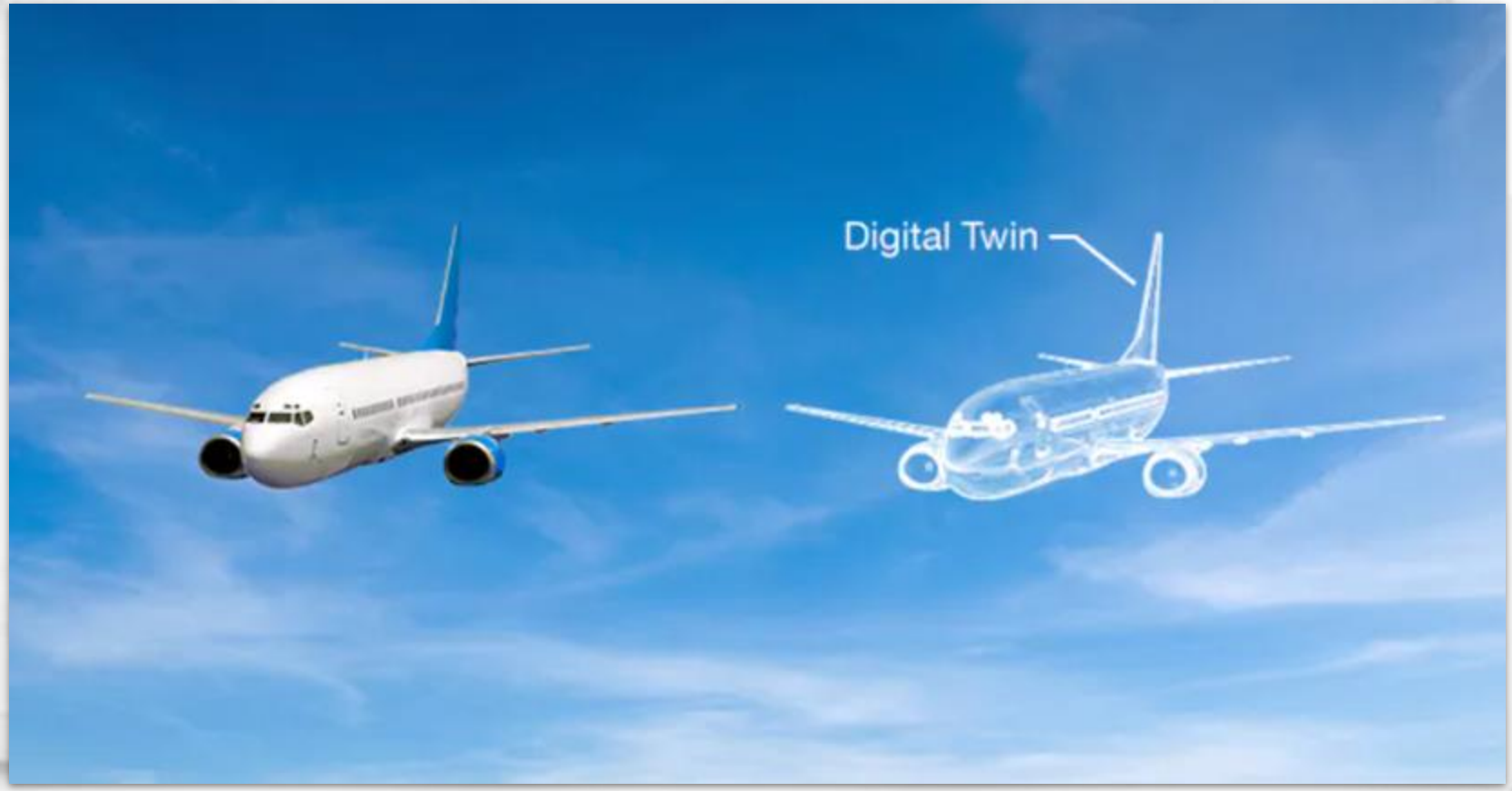
Generazione AO Onlife!

Lifestream

FALSO --- Quello che succede online rimane online!

formazione PA

Gemello digitale



formazionePA

Identità Fisiche e Virtuali

formazionePA

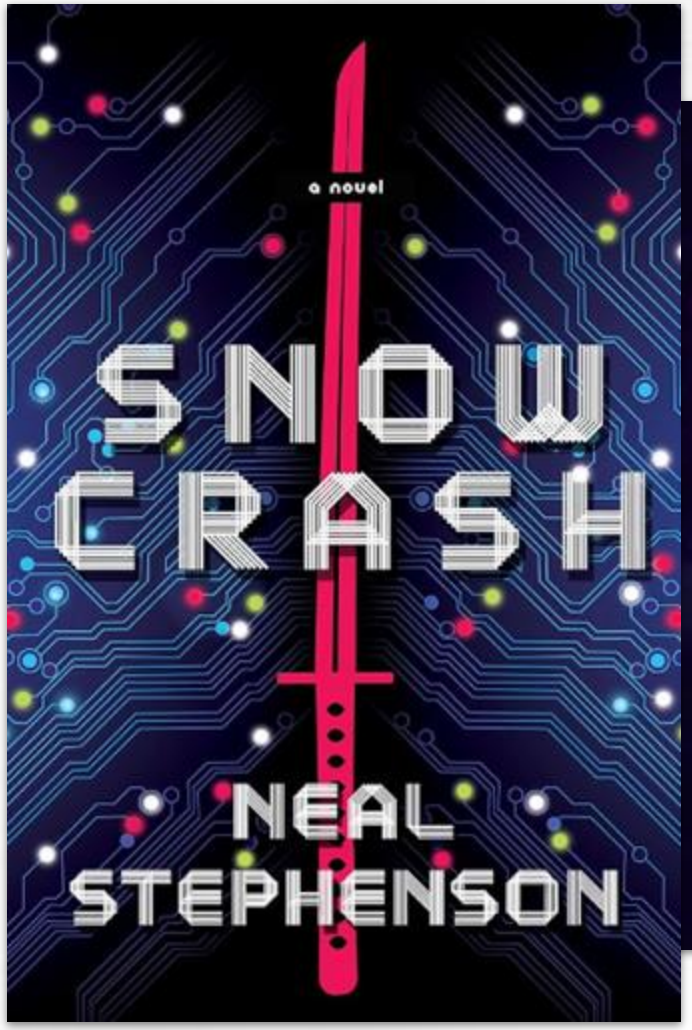
Identità Fisiche e Virtuali

Identità Digitale

Associazione con identità fisica

formazionePA

Metaverso



formazione PA

Intelligenza Artificiale

formazionePA

Quantum Computing

Il quantum computing è un campo avanzato della tecnologia dell'informazione che sfrutta i principi della meccanica quantistica per eseguire operazioni di elaborazione dell'informazione. Ecco i quattro punti fondamentali del quantum computing:

1. Qubit: A differenza dei bit classici, che possono essere in uno stato di 0 o 1, i qubit possono esistere in uno stato di 0, 1 o entrambi contemporaneamente grazie al concetto di sovrapposizione quantistica. Questo permette ai quantum computer di eseguire molte operazioni in parallelo, aumentando significativamente la potenza di calcolo.

2. Entanglement (intreccio quantistico): Gli qubit possono essere intrecciati, il che significa che lo stato di un qubit è direttamente correlato allo stato di un altro, indipendentemente dalla distanza che li separa. Ciò consente una comunicazione quantistica più veloce e la possibilità di eseguire calcoli distribuiti in modo più efficiente.

3. Superposizione e misurazione: Gli qubit sfruttano la superposizione per esistere in più stati simultaneamente, ma **quando vengono misurati, assumono uno stato specifico**. Questa caratteristica è fondamentale per l'esecuzione di algoritmi quantistici e consente ai quantum computer di risolvere alcuni problemi in modo più efficiente rispetto ai computer classici.

formazionePA

Il contesto in cui viviamo

Il mondo digitale della PA

formazionePA

Il quadrilatero

AI

Quantum

NEUROSCIENZA

Cybersicurezza

Metaverse

Connection

PA e Cybersecurity

Il **rapporto Clusit**: fa capire quanto l'Italia e la PA in specifico siano sotto attacco informatico.

L'ACN, agenzia per la cybersicurezza nazionale, istituita nel 2022, e la sua relazione annuale al parlamento, mostrano come l'Italia sia consapevole di essere un bersaglio internazionale e voglia dotarsi di una difesa cybernetica adeguata. L'ACN produce una relazione annuale sulla situazione cyber nazionale.

Acquisti ICT: il nuovo codice degli appalti mette nell'articolo 108 il concetto di sicurezza informatica come premiante nelle gare.

Le misure minime di sicurezza ICT: sono le misure che la PA adotta per difendersi da attacchi cyber. Presentate nel 2018 e in aggiornamento presumibilmente per il 2024, mostrano la consapevolezza della PA delle sue vulnerabilità.

formazione PA

PA e Cybersecurity

Capitolato per la nomina dell'Amministratore di Sistema e per l'affidamento della gestione del sistema informatico

Regolamento comunale per la sicurezza delle informazioni
Esempio di regolamento che stabilisce la policy per la sicurezza delle informazioni

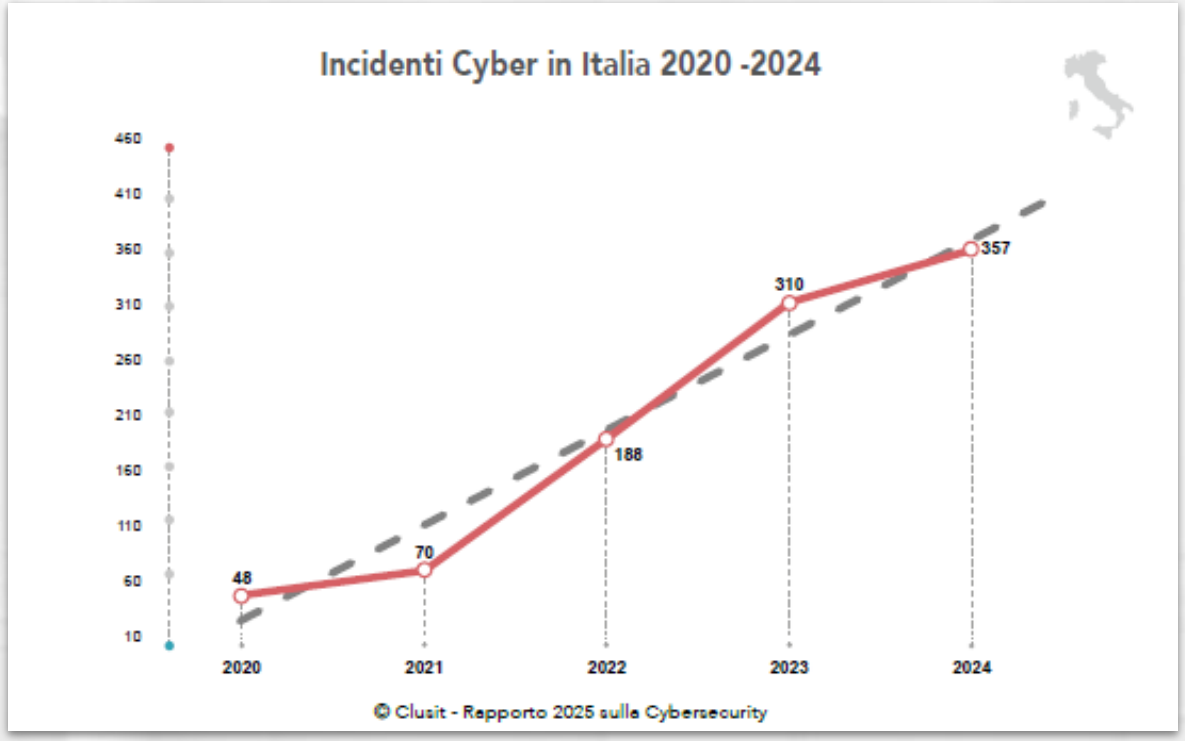
Piano di continuità operativa
Esempio di modello generale

RTD
Responsabile per la transizione al digitale

NIS2
La NIS2 è una **direttiva dell'Unione Europea sulla cybersicurezza** che aggiorna la direttiva NIS originale con l'obiettivo di creare un livello più elevato e uniforme di sicurezza in tutta l'UE.
Amplia l'ambito di applicazione ai settori medi e grandi, introducendo requisiti più stringenti di gestione del rischio, segnalazione degli incidenti e sicurezza della supply chain.
Le organizzazioni appartenenti **ai settori essenziali o importanti** devono conformarsi a queste nuove disposizioni per garantire la resilienza informatica, con sanzioni significative in caso di mancato rispetto. (o **comuni sopra i 100.000 abitanti**)

formazionePA

Rapporto Clusit



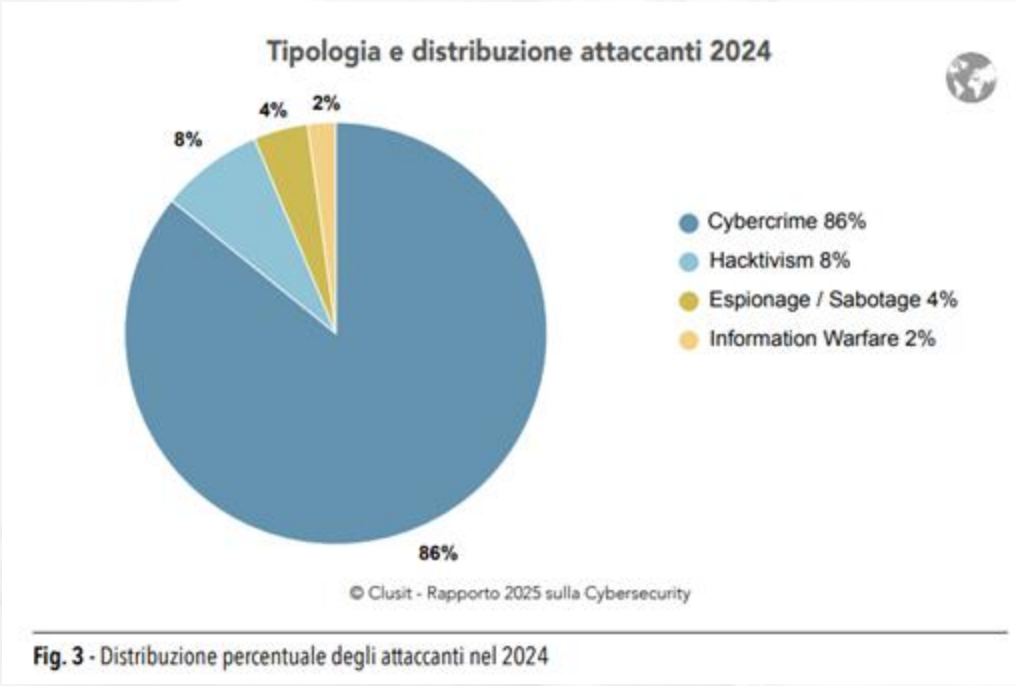


Fig. 3 - Distribuzione percentuale degli attaccanti nel 2024

formazionePA

Gli attaccanti

Cybercrime: Il cybercrime si riferisce a attività criminali che coinvolgono l'utilizzo di computer o reti informatiche come strumenti o obiettivi. Questo include una vasta gamma di reati informatici, come frodi online, furto di identità, attacchi informatici, distribuzione di malware, phishing, truffe finanziarie e molto altro. Gli autori di cybercrime cercano di trarre vantaggio finanziario o causare danni a individui, aziende o organizzazioni.

Hacktivism: L'hacktivism è una forma di attivismo che coinvolge l'uso delle abilità e delle tecniche di hacking per promuovere un messaggio politico o sociale. Gli hacktivist si impegnano in attività informatiche, come attacchi DDoS (Distributed Denial of Service), defacing di siti web, infiltrazioni di database o rilascio di informazioni riservate, al fine di esporre o protestare contro ingiustizie, violazioni dei diritti umani o altre questioni di interesse pubblico.

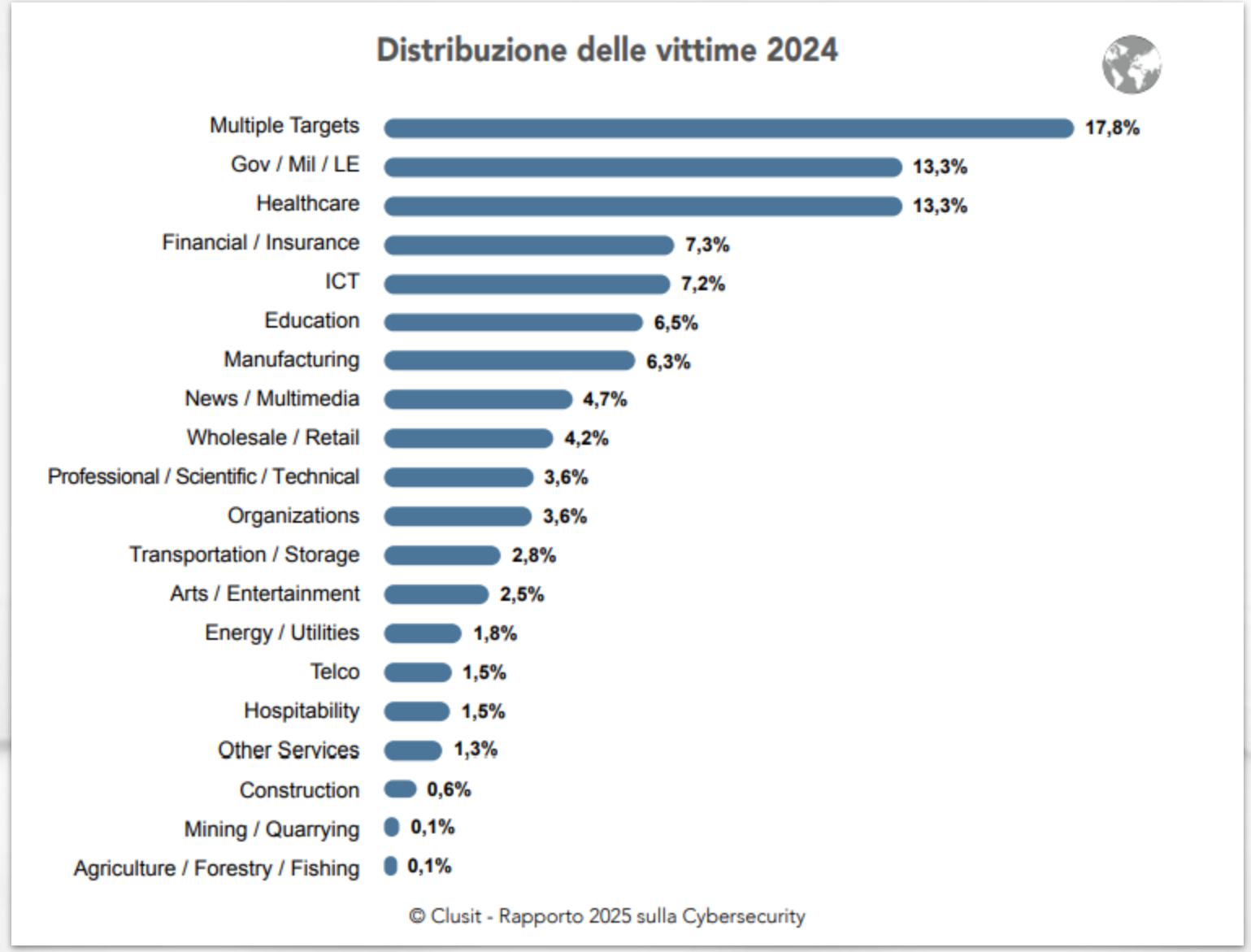
formazionePA

Gli attaccanti

Guerra cibernetica: a guerra cibernetica si riferisce a un conflitto che coinvolge operazioni offensive e difensive nel cyberspazio da parte di governi, organizzazioni o gruppi. In una guerra cibernetica, gli attori cercano di influenzare, danneggiare o distruggere le infrastrutture informatiche avversarie. Ciò può includere attacchi contro reti di comunicazione, sistemi di difesa, infrastrutture critiche o informazioni strategiche. La guerra cibernetica coinvolge spesso attori statali e può avere gravi conseguenze politiche, economiche e sulla sicurezza nazionale.

Cyberspionaggio: Il cyberspionaggio è l'uso di tecniche informatiche per ottenere informazioni riservate o segrete da organizzazioni, governi o individui. Gli attori di cyberspionaggio cercano di infiltrarsi nelle reti informatiche altrui, rubare dati sensibili, svolgere operazioni di sorveglianza o monitoraggio o compromettere la sicurezza delle informazioni. Queste attività sono spesso condotte da servizi di intelligence statali o da gruppi che cercano di ottenere vantaggi politici, militari, economici o di intelligence.

Rapporto Clusit

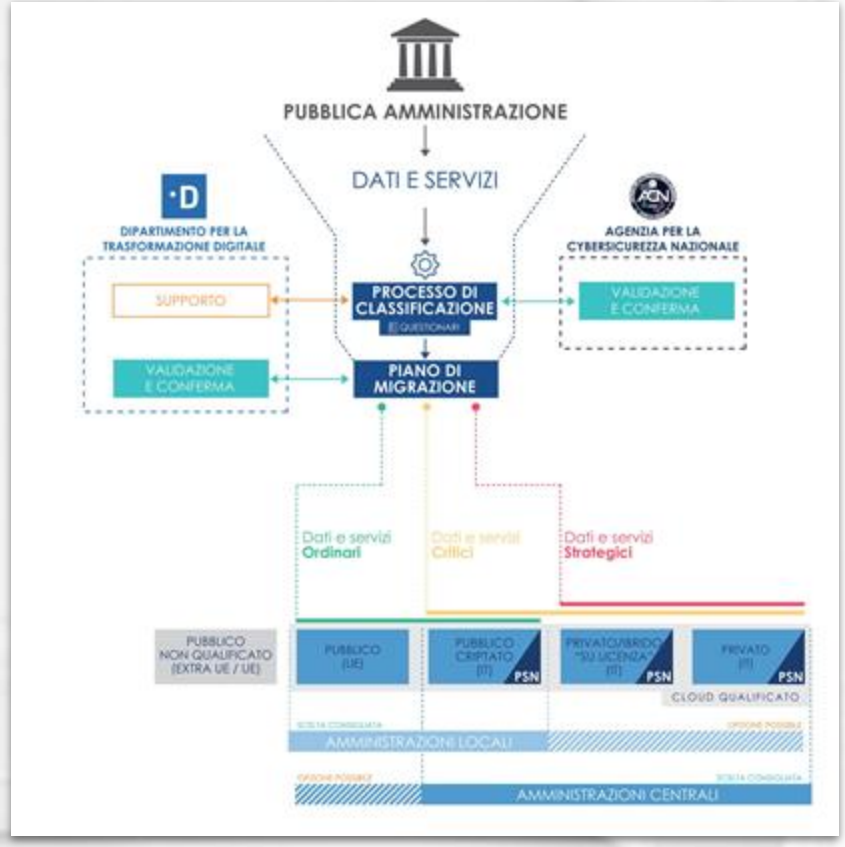


formazionePA

Agenzia Cybersicurezza

Dal 19 gennaio 2023 la **qualificazione dei servizi cloud per la Pubblica Amministrazione** diventa di competenza dell'Agenzia per la Cybersicurezza Nazionale, che subentra all'Agenzia per l'Italia Digitale (AgID). **Attivazione da giugno 2024.**

In corso valutazione di tutti i fornitori della PA per il PNRR!



formazionePA

Acquisti ICT

Nuovo codice Appalti

Il comma 4 del dlgs 36/2023 (Nuovo codice Appalti) contiene una precisazione circa l'approvvigionamento di beni e servizi informatici, all'**articolo 108**.

In queste attività, le stazioni appaltanti devono tenere in considerazione gli elementi di cybersicurezza, sempre circa la valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo.

Devono attribuire ad esso grande rilievo nei casi in cui il contesto di impiego è connesso alla tutela degli interessi nazionali strategici.

Piano triennale 2024-2026

Nel piano triennale 2024-2026 particolare attenzione al Procurement ICT:

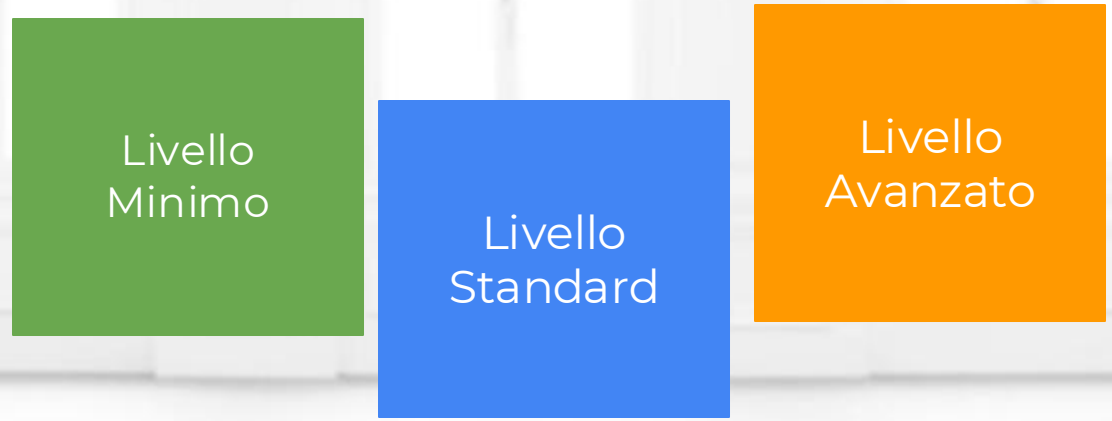
- **Capitolo 2** - Il procurement per la trasformazione digitale
- 1. **Strumento 1** - Approvvigionamento ICT

formazione PA

Misure Minime di Sicurezza ICT

Le misure consistono in controlli di natura **tecnologica, organizzativa e procedurale** utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.

A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione




Furto di Dati

Sicurezza delle informazioni

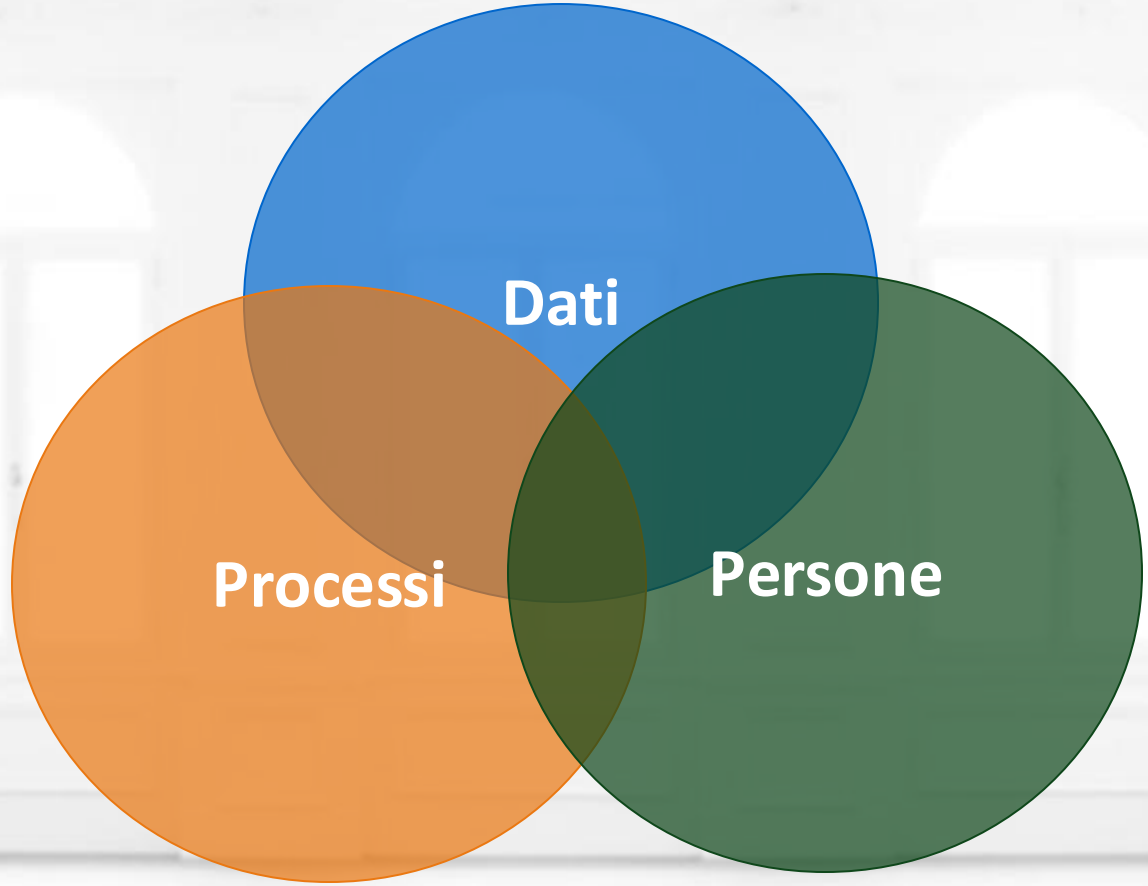
La **Sicurezza Informatica** è la protezione dei sistemi IT contro danni e rischi. Ciò vale per singoli file su computer come per interi data center e comprende database, software, applicazioni, server e dispositivi.

La **Cybersicurezza** estende la sicurezza informatica al cyber spazio complessivo. Ciò include controlli di accesso, crittografia, gestione dei diritti, firewall, proxy, gestione delle vulnerabilità e molto altro; si concentra sulle attività criminali agevolate specificamente attraverso Internet.

La **Sicurezza delle Informazioni** estende la sicurezza al livello fisico,ai dati, all'organizzazione, ai processi e alle persone.

formazionePA

Sicurezza delle informazioni



formazione PA

La azioni

Perché i dati sono importanti per la PA?

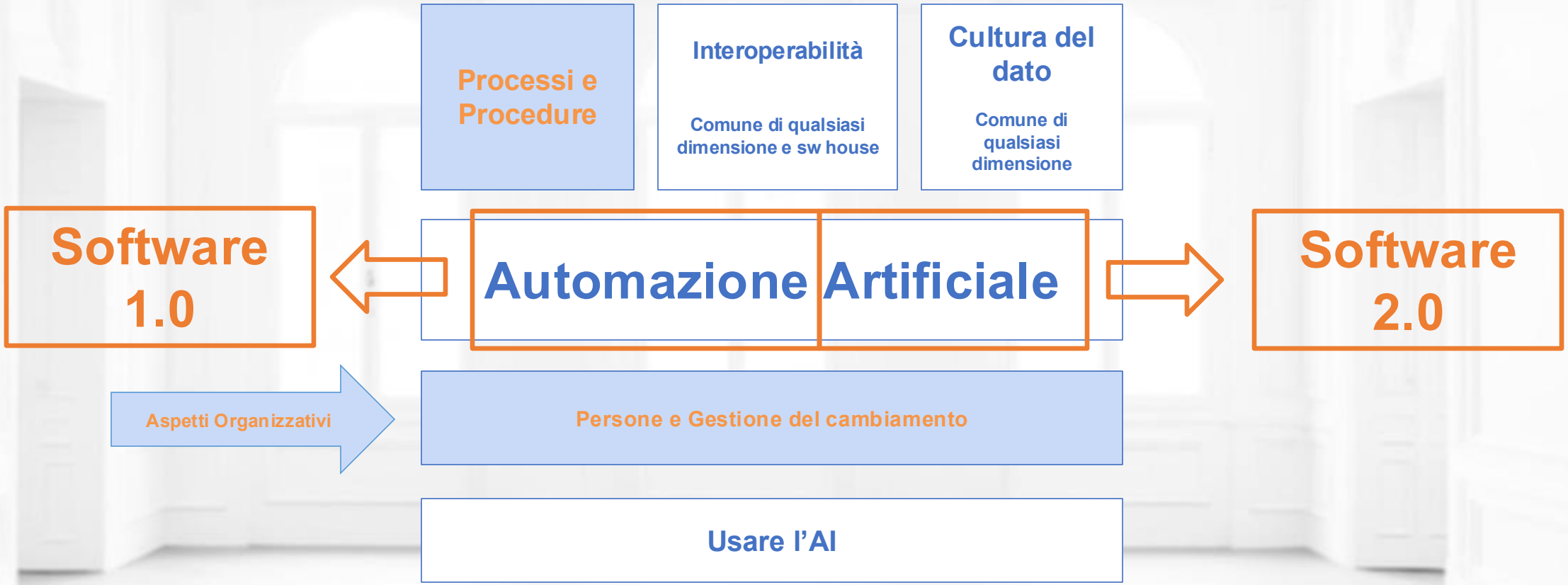
Come dipendenti e
dirigenti pubblici è

fondamentale ragionare sui dati
per
prestare attenzione alla razionalità

nella ricerca della migliore risposta alle esigenze
della struttura e dei cittadini.

formazionePA

Perché i dati sono importanti per la PA?



formazionePA

Dati Informazioni Conoscenza Saggezza

90

90 kg di peso

Andrea pesa 90 kg , la sua altezza è 170 centimetri ed è in sovrappeso

Andrea è in sovrappeso e la sua salute nel medio termine è a rischio

I **dati** valgono di più degli oggetti che li producono

Le **informazioni** estratte valgono più dei dati

La **conoscenza** vale di più delle informazioni

La **saggezza** derivante è inestimabile

5

5 litri di consumo di carburante

Il veicolo consuma 5 litri per fare 5 chilometri

Il veicolo consuma troppo, c'è qualcosa che non funziona

formazionePA

3 Miti e leggende dei dati nella PA

Portare in cloud un applicativo?

“Portare in cloud un applicativo” significa in **verità portare in cloud i dati su cui lavora**.

Un applicativo non è niente altro che un programma per visualizzare, manipolare, modificare dati. Purtroppo solitamente l’applicativo tende anche (anche se non dovrebbe) a codificare i processi di un ente, a seguito dei vincoli che il suo utilizzo impone e quindi il software la fa da padrone, e spesso usa i dati in un solo modo: quello per cui è stato scritto.

Un erp ad esempio nel migliore dei casi fa bene il suo lavoro, ma non rende disponibili i dati con export, open data o api, e quindi riduce il potenziale dei dati raccolti rendendoli prigionieri al suo interno.

formazionePA

3 Miti e leggende dei dati nella PA

Ho usato i dati per quello che serviva, sono a posto!

Non c'è maggior **spreco che <u>non usare i dati</u>** raccolti lasciandoli rinchiusi nel software che li ha prodotti.

formazione PA

3 Miti e leggende dei dati nella PA

IL GDPR blocca la circolazione dei dati?

Infatti come dice l'art. 1 del GDPR, il vero scopo dei dati è la loro condivisione per ottenere informazione, conoscenza e saggezza.

Articolo 1
Oggetto e finalità

1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla ***libera circolazione di tali dati****.*

2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

3. ***La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali****.*

Il GDPR, **usato impropriamente** come ostacolo alla circolazione dei dati da alcuni, ha lo scopo opposto di aumentare la circolazione dei dati, pur nel rispetto dei diritti di protezione dei dati personali.

L'interoperabilità e il #onceonly sono fondamentali.

formazione PA

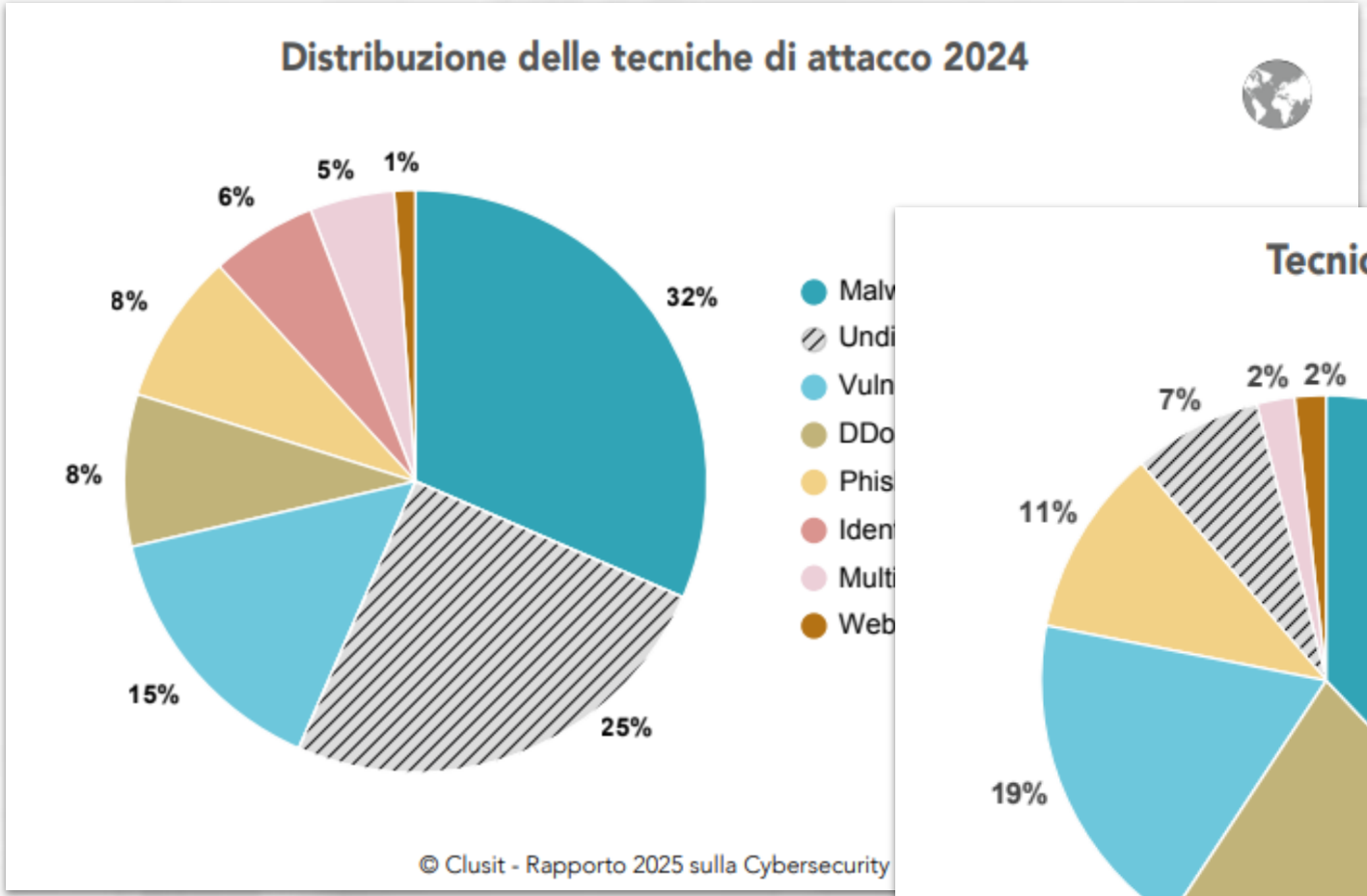
Malware e Social Engineering

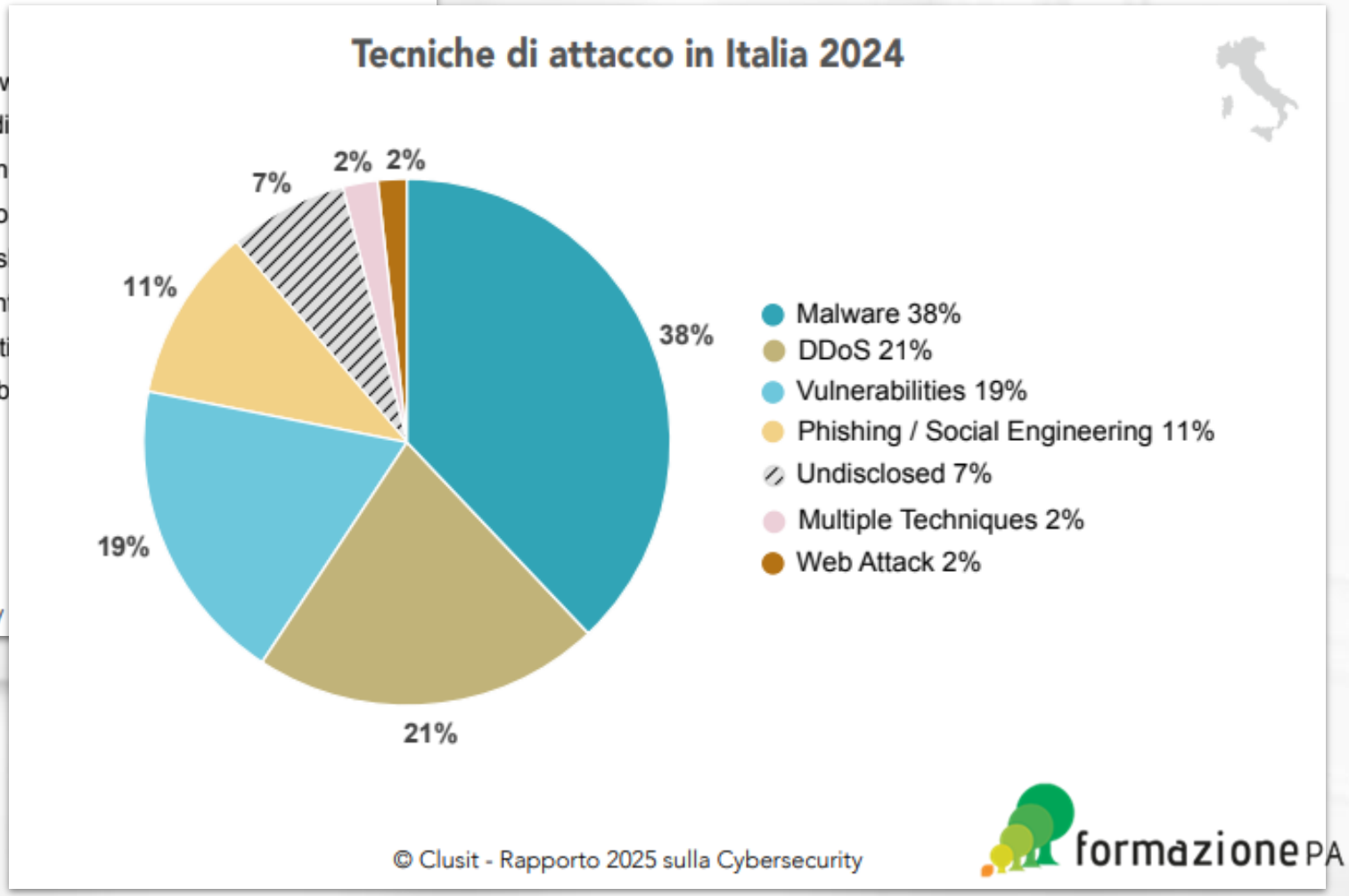
Quali sono gli strumenti di attacco?

I malware

formazionePA

I malware





formazione PA

I malware

Un malware è un tipo di ***software dannoso*** progettato per causare danno o intrusione in un sistema informatico senza il consenso dell'utente.

Il termine "malware" è un'abbreviazione di "*software malevolo*" e comprende una vasta gamma di software dannosi, tra cui virus, worm, trojan, ransomware, spyware e adware.

I malware sfruttano le **vulnerabilità** dei sistemi.

formazionePA

Le minacce

Minaccia = vulnerabilità pesata per il rischio pesata per la severità

Una **vulnerabilità** informatica è una **debolezza o una falla** presente in un sistema informatico o in un software che può essere sfruttata dagli attaccanti per ottenere accesso non autorizzato, danneggiare o manipolare dati, interrompere il funzionamento del sistema o compiere altre azioni malevole. L

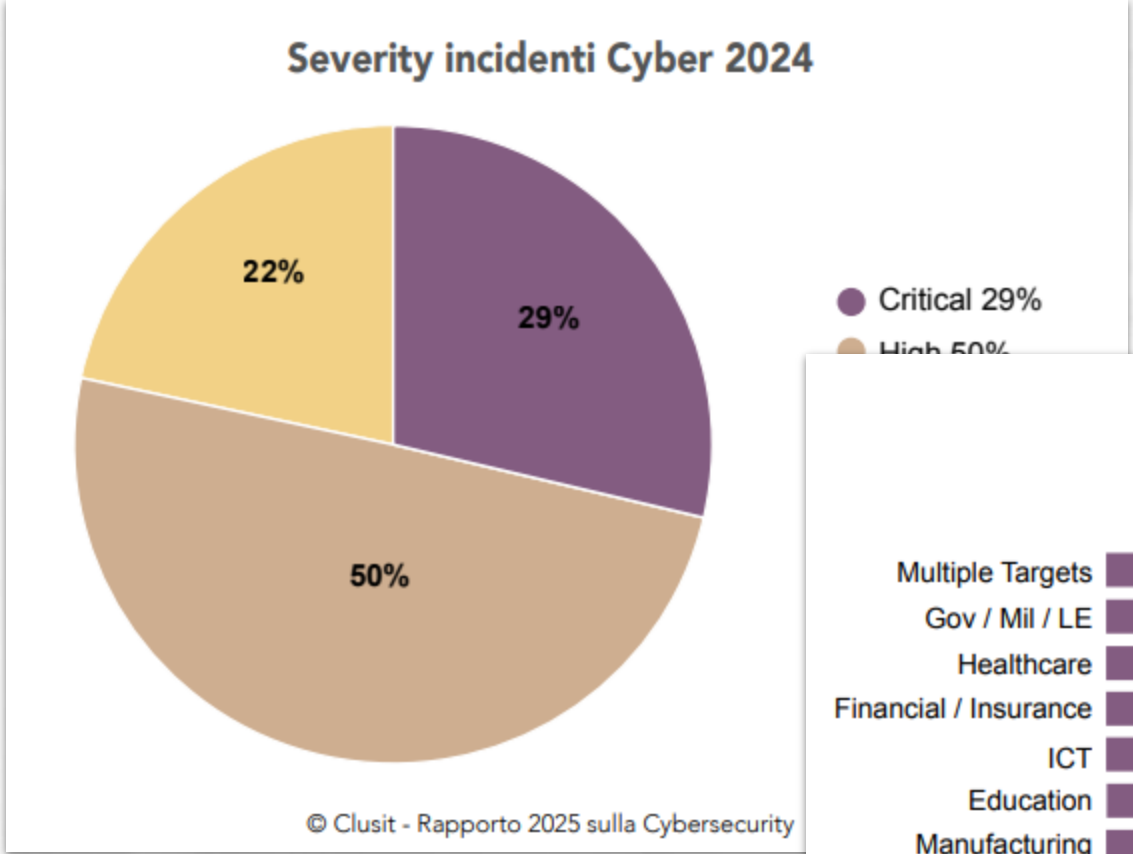
Vulnerabilità

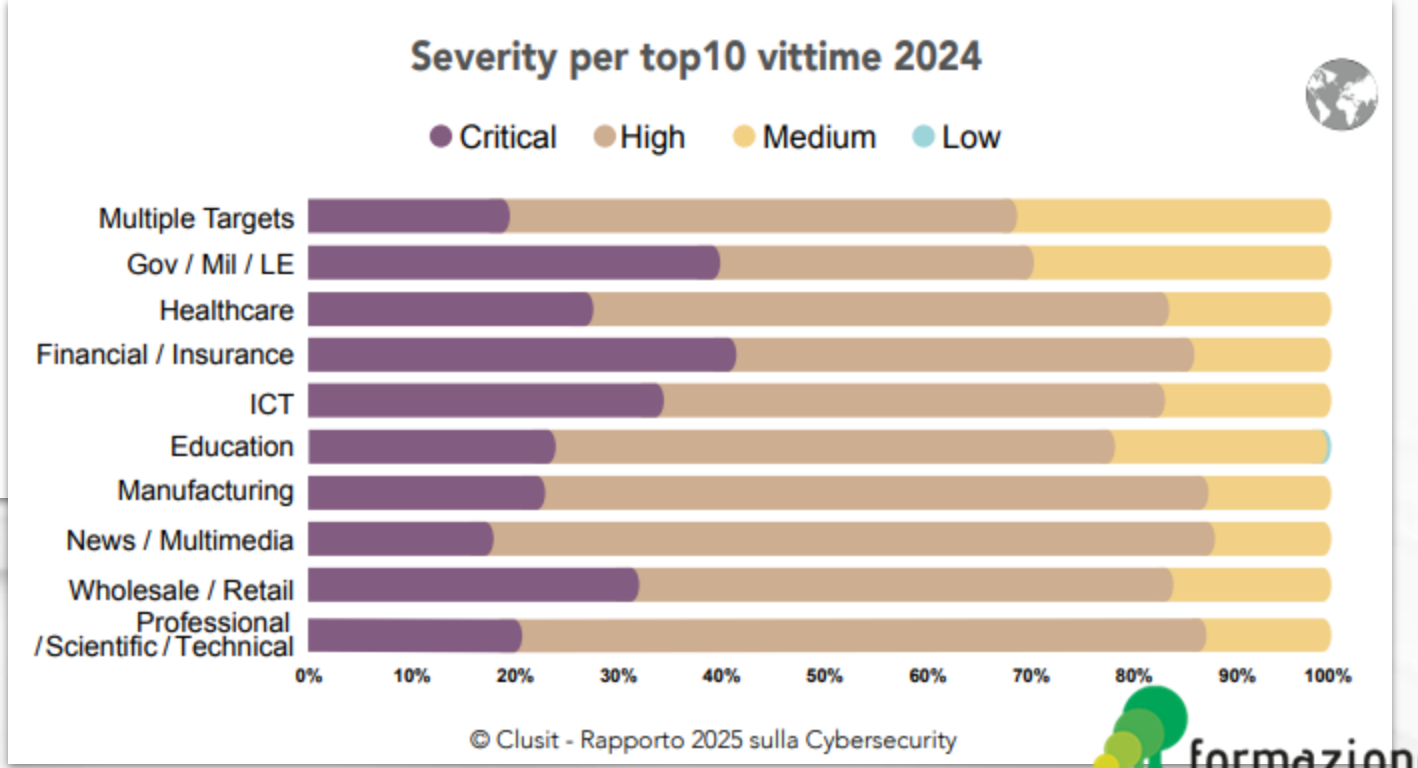
Rischio

Un **rischio** associato a una vulnerabilità informatica è **la possibilità** che un attaccante sfrutti tale vulnerabilità per compromettere la sicurezza di un sistema informatico.

formazionePA

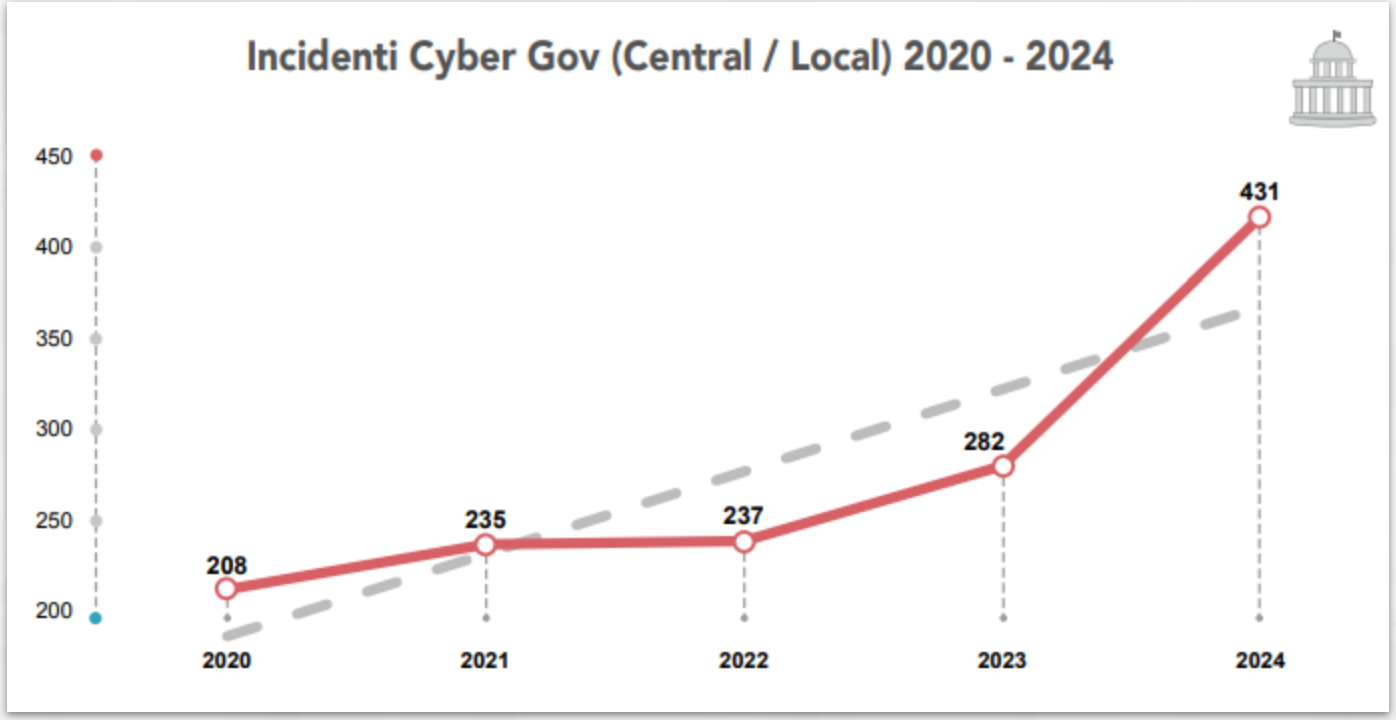
Le minacce





formazione PA

Le minacce


Incidenti Cyber Gov (Central / Local) 2020 - 2024
450
400
350
300
250
200
208
235
237
282
431
2020
2021
2022
2023
2024

Le vulnerabilità

Le vulnerabilità zero day sono quelle per cui il **vendor non ha ancora trovato una patch**. Sono fino al momento della patch indifendibili.

Vulnerabilità Tecnologiche Zero Day

Vulnerabilità Tecnologiche Conosciute

Le vulnerabilità più sfruttate sono quelle conosciute e si basano sul fatto che gli essere umani non patchano i sistemi, per mancanza di conoscenza dell'esistenza di una patch o per mancanza di una policy di patching.

esempi: lasciare la password di default su un dispositivo

Errori di configurazione

Errori nel comportamento umano

formazionePA

Tipi di malware

Adware

Gli adware sono software indesiderati progettati per presentare messaggi pubblicitari sullo schermo, spesso all'interno di un browser web. Generalmente, gli adware si avvalgono di un metodo subdolo, mascherandosi da componenti legittimi o nascondendosi in un altro programma al fine di provocare con l'inganno l'installazione su PC, tablet o dispositivo mobile.

Virus

I virus sono malware che si attaccano ad altri programmi e, quando eseguiti — di solito inavvertitamente — si riproducono modificando altri programmi e infettandoli con il proprio codice. Proprio come i virus del corpo umano. Il virus nel corpo umano viene eseguito ad esempio con uno starnuto ed infetta gli altri umani con questo veicolo di trasporto.

Spyware

Gli spyware sono malware che osservano segretamente le attività dell'utente sul computer, senza autorizzazione, per poi inviare queste informazioni al creatore del software.

formazionePA

Tipi di malware

Worm

I worm sono malware simili ai virus, che si riproducono per diffondersi sugli altri computer di una rete e danneggiandoli, di solito, mediante la distruzione di dati e file.

Trojan

Un trojan o "cavallo di Troia" è uno dei malware più pericolosi. Di solito si presenta sotto forma di qualcosa di utile, per ingannare l'utente. Una volta entrato nel sistema, i criminali ottengono l'accesso non autorizzato al computer della vittima. Da qui, i trojan possono essere utilizzati per rubare dati finanziari o installare altre minacce, come virus e ransomware.

Ransomware

I ransomware sono malware che impediscono all'utente di accedere al proprio dispositivo e/o criptano i suoi file, obbligandolo a pagare un riscatto per ottenerli. I ransomware sono stati definiti "l'arma scelta" dei criminali, perché richiedono un pagamento rapido e ingente in criptovalute difficili da rintracciare. Il codice alla base dei ransomware è semplice da ottenere sui marketplace criminali e difendersi da essi è molto difficile.

formazionePA

Tipi di malware

Keylogger

I keylogger sono malware che registrano la pressione dei tasti degli utenti sulla tastiera, memorizzando le informazioni raccolte e inviandole ai criminali responsabili, che puntano a informazioni sensibili come nomi utente, password o dati delle carte di credito.

Rootkit

I rootkit sono dei malware che forniscono al criminale i privilegi da amministratore del sistema infetto. Generalmente, sono progettati per rimanere nascosti agli occhi dell'utente, degli altri software e del sistema operativo stesso.

Exploit

Gli exploit sono malware che sfruttano i bug e le vulnerabilità di un sistema per consentire al loro creatore di assumere il controllo. Come altre minacce, gli exploit sono legati al malvertising e attaccano attraverso siti web legittimi che lasciano inconsapevolmente penetrare contenuti dannosi provenienti da siti web nocivi. Dopodiché, i contenuti dannosi provano a installarsi sul computer mediante un drive-by download. Non serve alcun clic. È sufficiente visitare un sito legittimo al momento sbagliato.

Cryptomining

Il crypto mining dannoso, noto anche come drive-by mining o cryptojacking, è una tecnica malware sempre più diffusa, che in genere prevede l'installazione da parte di un trojan. Consente a persone estranee di utilizzare un computer per "generare" (mining) criptovalute, ad es. Bitcoin o Monero. Anziché lasciare che gli utenti raccolgano i frutti del lavoro del proprio computer, i cryptominer inviano la valuta raccolta ai propri account. Essenzialmente, un cryptominer dannoso deruba gli utenti delle loro risorse per lucro.

formazionePA

Altri tipi di attacchi

DDOS

Un sistema viene bombardato di richieste fino a che non viene resto talmente lento da risultare irraggiunbile.

Brute force

Tento di attaccare un sistema in maniera frontale, provando ad esempio tutte le combinazioni di password composte da lettere a e b fino a 3 caratteri ovvero:
aaa, aab, abb, aba, bbb, bba, bab, baa

formazionePA

Vettori di attacco

Un **vettore di attacco** è il metodo utilizzato da un criminale per tentare di accedere in modo illegittimo ad un sistema IT e alle informazioni sensibili in esso contenuti, sfruttando di solito una vulnerabilità presente all'interno di una rete, un sistema o un'applicazione.

Email di phishing con link o allegati

Applicazioni per dispositivi mobili

File scaricati da strumenti di file sharing

Tecniche di Social engineering

Dispositivi infetti

Brute force attack

formazionePA

Il mio computer può essere quindi

Attaccato direttamente

Attaccato per rubare dati, accessi, altro

Zombie

Attaccato per diventare parte di un'armata controllata da un server di Command & Control e quindi essere utilizzato in attacchi DDoS o altro

formazionePA

Il più cattivo dei malware

Le fasi di un attacco ransomware sono 4

Infiltrazione
Installazione
Criptazione
Estorsione

Singola Estorsione

i dati vengono cifrati e si chiede un riscatto per decifrarli

Doppia Estorsione

i dati vengono copiati e poi cifrati. Quindi viene chiesto un riscatto sia per decifrarli che per non diffonderli.

formazionePA

10 regole di difesa in ufficio

1. AGGIORNAMENTI DEI SISTEMI

- (io e ICT) Aggiornare costantemente i **sistemi e i software a livello di sistema operativo** (es. windows update)
- (io e ICT) Aggiornare anche l'**hardware del sistema** (es. hp support tool)

- (io e ICT) Aggiornare **tutti i software che utilizzo più spesso**. questo può essere fatto software per software oppure con sistema centralizzati di aggiornamento (es. anche tramite le ultime suite antivirus come WithSecure ad esempio)
- (io e ICT) in particolare tenere aggiornati il **browser** e il **software di email**

2. ANTIVIRUS, ANTI RANSOMWARE

(io e ICT) Avere un **sistema antivirus** e tenerlo aggiornato

Tipicamente gli antivirus di ultima generazione comprendono:

- sistema **antivirus**
- sistema **anti ransomware**
- sistema di **controllo della navigazione internet**
- sistema di **patching degli applicativi più diffusi**

Gli antivirus moderni utilizzando:

- firme
- euristiche
- intelligenza artificiale

3. Firewall attivo

(io e ICT) Avere un sistema **firewall attivo sul computer**

(ICT) Avere un sistema **firewall attivo a livello perimetrale**

4. Backup

(io e ICT) Avere una **copia dei dati**:

- su server
- su cloud
- conoscere la politica di backup
    - full, incrementale
    - periodo di retention dei dati
    - es.
        - ho 12 backup mensili e 30 backup giornalieri

Accorgimenti: **cifrare il backup** e avere una copia in cloud o offline.

5. Gestione delle Password

(io e ICT) Salvare **le password** in un **password manager**

- non tenere le password scritte in chiaro su dei fogli
- non tenere le password scritte in chiaro su post-it
- non dare le password a colleghi e in caso serva poi cambiarle
- attuare **politiche di gestione** delle password
    - cambiarle periodicamente
    - **usare password di almeno 14 caratteri** (meglio più lunghe che più complesse)

6. Pulizia del dispositivo

- (io e ICT) **Rimuovere tutti gli applicativi non più utilizzati**
- (io e ICT) **Rimuovere tutti i dati che non sono più necessari presenti in locale sul dispositivo**
- (io e ICT) **Pulizia file** obsoleti, cookie etc etc

7. Email Social Engineering e Phishing

- Vediamo tra poco …

8. Sicurezza logica e fisica

- **Bloccare il sistema** in caso ci si debba allontanare (WIN+L)
- **Mettere in sicurezza il sistema da furti fisici** di smartphone, portatile, dischi
- **Cifrare i dispositivi** per evitare furti
  - smartphone
  - portatile
  - dischi removibili se utilizzati (incluse schede)

9. Accessi

1. **Lasciare attivi i sistemi di controllo di installazione applicazione:** spesso questi sistemi inclusi nel sistema operativo vengono considerati fastidiosi perché “non ti fanno fare quello che vuoi a meno che confermi o inserisci una password”. Invece aiutano molto perché ti rendono consapevole del fatto che “qualcosa” si sta installando sul tuo dispositivo. E se la scelta non è tua potrebbe essere un attacco derivante da qualche azione che hai fatto.
2. **lavorare con i minimi permessi necessari** (fare tutto con un utente amministratore perchè non si sa mai non è una buona pratica)

10. Altri consigli

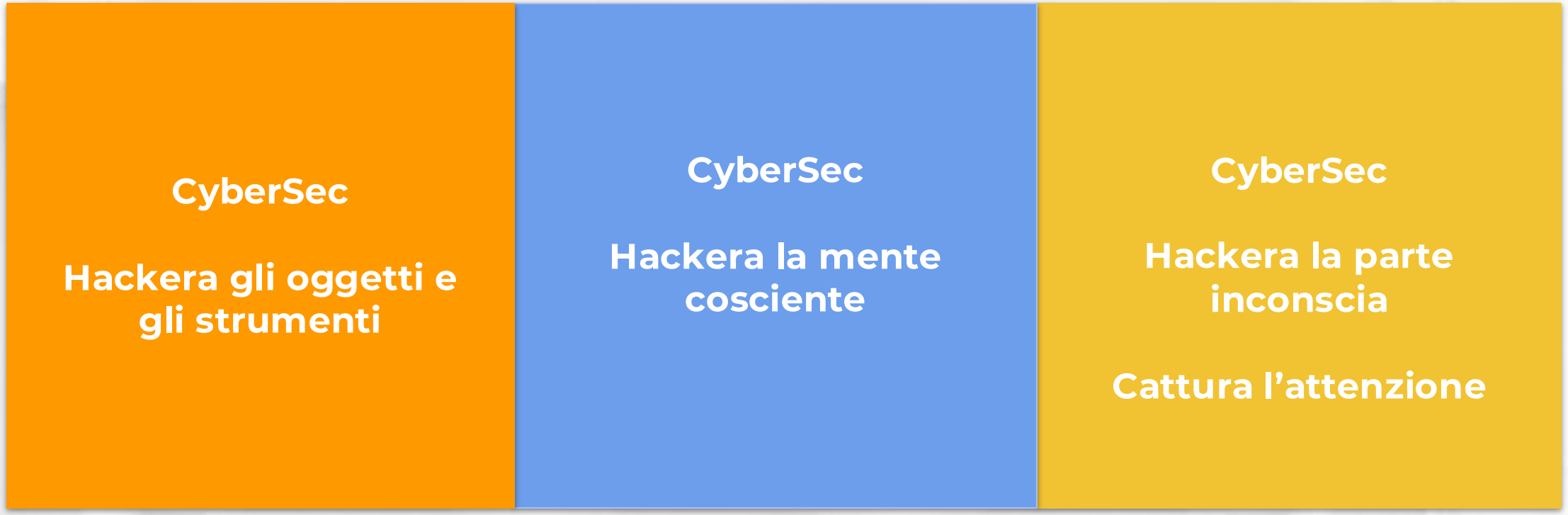
1. **No ai software crackati:** spesso sono vettori di attacco
2. **Separare gli ambienti lavorativi da quelli familiari** (es. portatile di lavoro dal portatile utilizzato dai familiari)

Altri strumenti di attacco!

Il Social Engineering

formazionePA

CyberSecurity Layer



formazione PA

Social Engineering

L'**ingegneria sociale è l'arte della manipolazione per rubare informazioni.**

A differenza dei crimini tecnici che sfruttano vulnerabilità per l'attacco e coinvolgono marginalmente esseri umani, essa si basa su

vulnerabilità del comportamento umano

comportamento umano che è prevedibile per **indurre le vittime a rivelare informazioni volontariamente**.

È importante notare che gli ingegneri sociali utilizzano **tattiche psicologiche** per manipolare le vittime, sfruttando la loro fiducia, emozioni o desiderio di aiutare.

Essi cercano di eludere **le difese sia digitali che umane**, e la consapevolezza di queste tecniche può aiutare a prevenire e rilevare gli attacchi di ingegneria sociale.

formazionePA

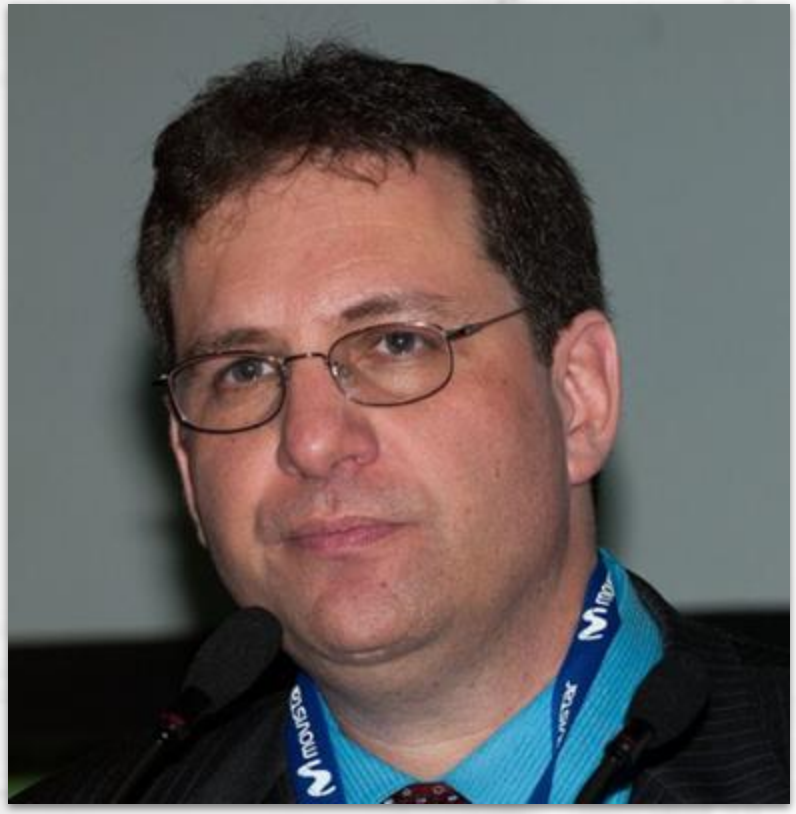
Social Engineering

Il punto più debole nella catena di sicurezza è l'elemento umano.

K. Mitnick

Le persone sono inclini a prendere **scorciatoie mentali**.

Possono essere consapevoli che non dovrebbero divulgare determinate informazioni, ma **la paura di non essere gentili, la paura di apparire ignoranti, la paura di una figura di autorità percepita**: tutti questi sono trigger che possono essere sfruttati da un ingegnere sociale per convincere una persona a ignorare le procedure di sicurezza stabilite.



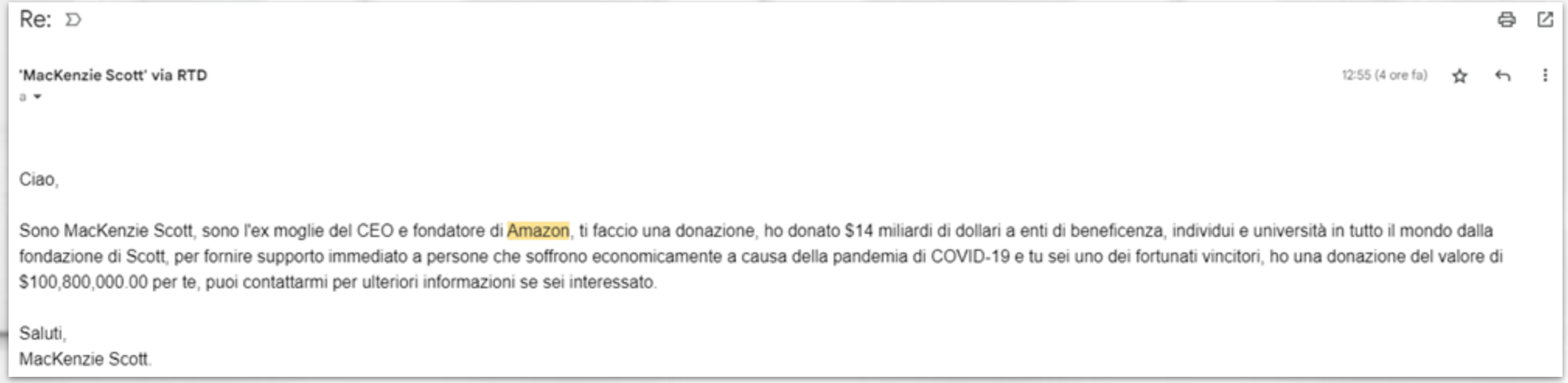
formazionePA

Tecniche di social eng.

Phishing

E' una tecnica di ingegneria sociale in cui gli attaccanti **inviano messaggi falsi, come e-mail o sms o altri messaggi di testo**, fingendo di provenire da fonti affidabili, come istituti finanziari o servizi online popolari.

Questi messaggi spesso cercano di indurre le vittime a rivelare informazioni personali o ad accedere a siti web contraffatti che rubano le credenziali di accesso.



Re:

'MacKenzie Scott' via RTD

a

12:55 (4 ore fa)

Ciao,

Sono MacKenzie Scott, sono l'ex moglie del CEO e fondatore di Amazon, ti faccio una donazione, ho donato $14 miliardi di dollari a enti di beneficenza, individui e università in tutto il mondo dalla fondazione di Scott, per fornire supporto immediato a persone che soffrono economicamente a causa della pandemia di COVID-19 e tu sei uno dei fortunati vincitori, ho una donazione del valore di $100,800,000.00 per te, puoi contattarmi per ulteriori informazioni se sei interessato.

Saluti,
MacKenzie Scott.

Perchè è meglio attaccare umani?

Un umano non si può fixare definitivamente.

Umano	Macchina
Ha una vulnerabilità, spiego come mitigarla. Può dimenticarsi, essere stanco, sbagliare ...	Ha una vulnerabilità: la correggo. Il sistema è sicuro.

formazionePA

Come difendermi? Le domande

Le mie emozioni sono elevate e provo un senso di urgenza?

Questo messaggio proviene da un amico, un conoscente o un mittente legittimo?

Questo sito web non è sicuro o non è quello che mi aspettavo o scritto non correttamente?

Questa offerta sembra troppo buona per essere vera?

Posso verificare l'identità di una persona?

formazionePA

Come difendermi? Le azioni

Agire piano

Non devo avere fretta.
Nel dubbio aspetto.

Verificare l'identità

Utilizzo un secondo canale per verificare che la richiesta venga davvero dalla persona che la richiede. Es. telefono, email, messaggio, altro?

formazionePA

Focus

Phishing

formazionePA

Phishing

Il **phishing** è un termine che indica le truffe online in cui gli aggressori si fingono una persona o un'entità di fiducia della vittima al fine di ottenere accesso a informazioni sensibili, account finanziari e altro ancora.

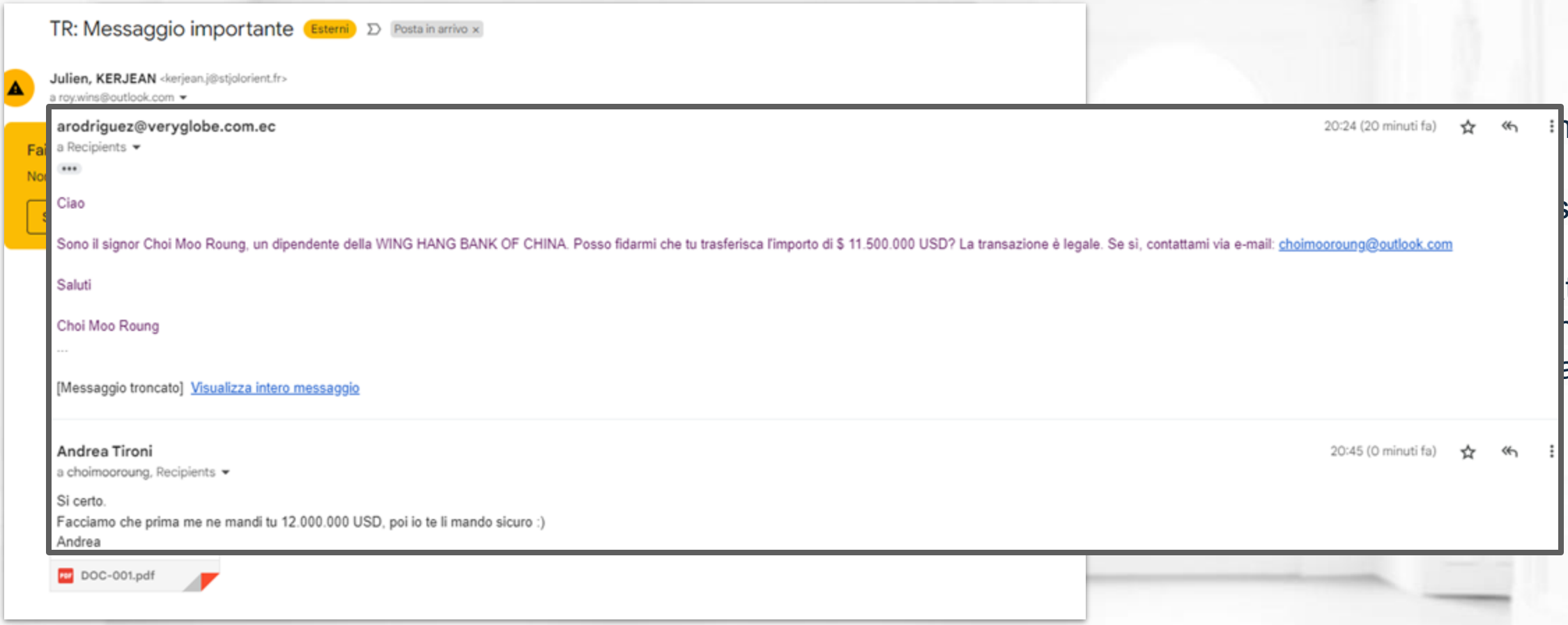
I truffatori si presentano come una società legittima o un amico e manipolano le vittime per compiere azioni specifiche. Ad esempio, potrebbero ingannarti facendoti:

esempi

a. Cliccare su un link maligno o scaricare un allegato contenente malware.
b. Divulgare il tuo nome utente, password o informazioni sull'account.
c. Inviare denaro a un conto controllato dal truffatore.

formazionePA

Phishing



hira a:

sta

to
nziali
ante

formazione PA

Smishing

Un **sms ingannevole**, che mira a far cliccare su un link

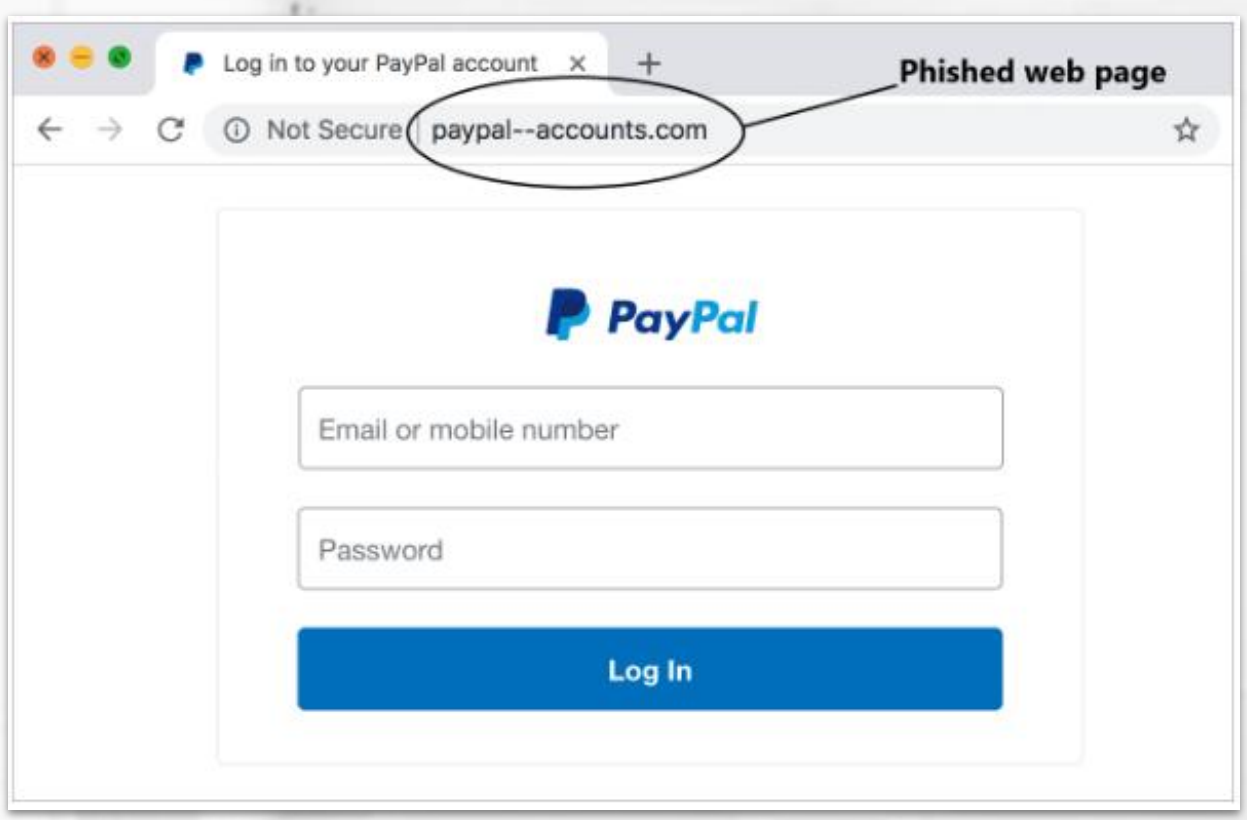
formazionePA

Vishing

Questo tipo di phishing si basa sulle **chiamate telefoniche**.

I truffatori si fingono rappresentanti di istituzioni finanziarie o di altre organizzazioni di fiducia e cercano di ottenere informazioni sensibili dall'utente, come i dettagli della carta di credito o le password.

Pharming

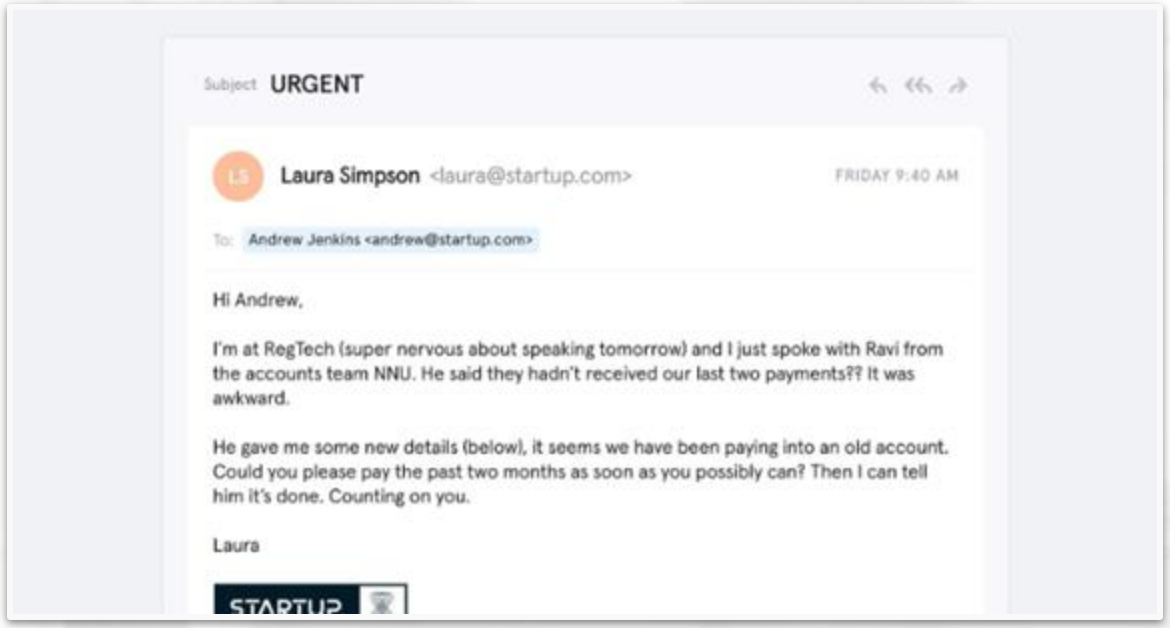


Il **pharming** mira a dirottare il traffico di un sito web verso una **pagina web fraudolenta** senza il consenso dell'utente.

Gli attaccanti manipolano i server DNS o i file di configurazione del router per indirizzare gli utenti verso un sito web contraffatto, dove vengono richieste informazioni personali.

formazionePA

Spear Phishing



Questo tipo di phishing mira a **utenti specifici** o a un'**organizzazione specifica**.

Gli attaccanti raccolgono informazioni dettagliate sugli obiettivi e utilizzano queste informazioni per personalizzare gli attacchi.

Possono utilizzare nomi, titoli di lavoro o altre informazioni rilevanti per rendere i messaggi più credibili.

formazionePA

Domande di difesa

Controllare identità del mittente (indirizzo email, mittente sms, mittente telefonata)

Nome del mittente (verificare che il nome sia corretto)

Il contenuto del messaggio è corretto o presenta “qualcosa di strano” rispetto allo stile abituale del mittente o altri segnali particolari?

Richiesta di informazioni personali e/o sensibili?

Il contenuto presenta link o allegati?

formazionePA

Azioni di difesa

1. Aggiornamento browser, software di posta e sistema operativo

2. Rimani informato su particolari tipologie di attacchi (es. pec finte di AdE)

3. Mantieni un minimo di scetticismo. Nel dubbio verifica l'identità o cestina l'email, ma non agire!

formazionePA

Focus

Smartphone

formazione PA

Smartphone

Tenere aggiornato il telefono: quando viene proposto un aggiornamento effettuarlo sempre.

Porre attenzione alle app che si scaricano.

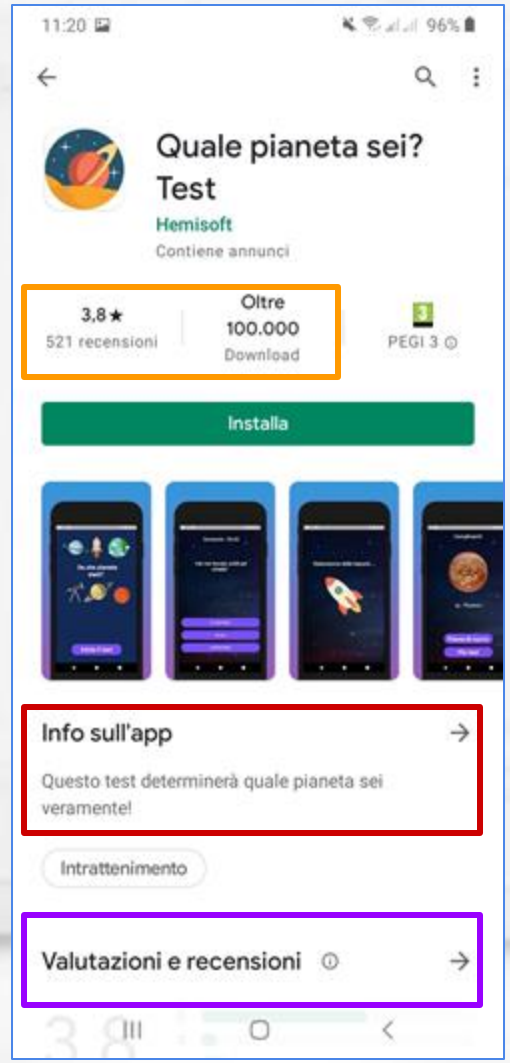
Scaricare il minor numero di app possibile, e eliminare quelle non in uso. Dare solo i permessi necessari.

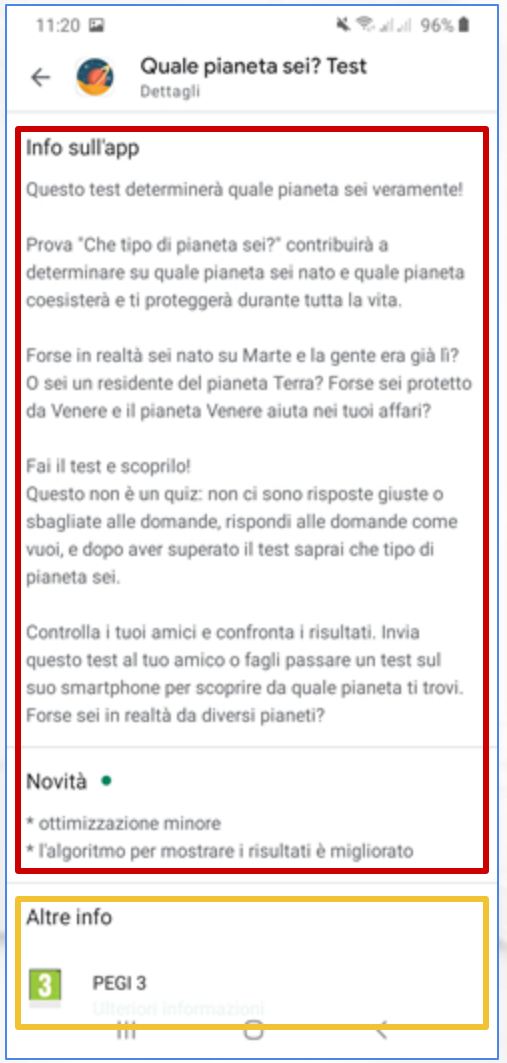
Tenere bloccato il telefono, se non in uso.

Evitare reti wi-fi non sicure.

formazionePA

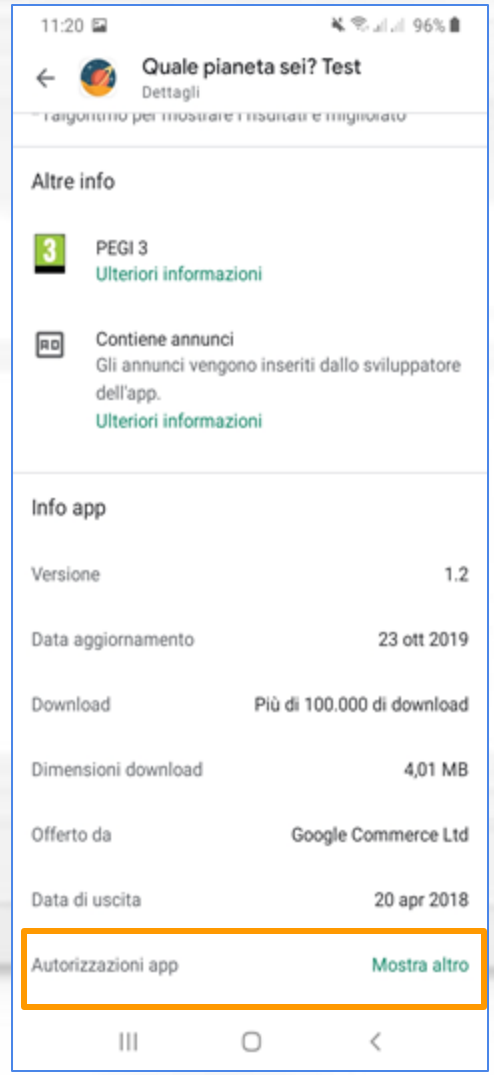
Come difenderci?

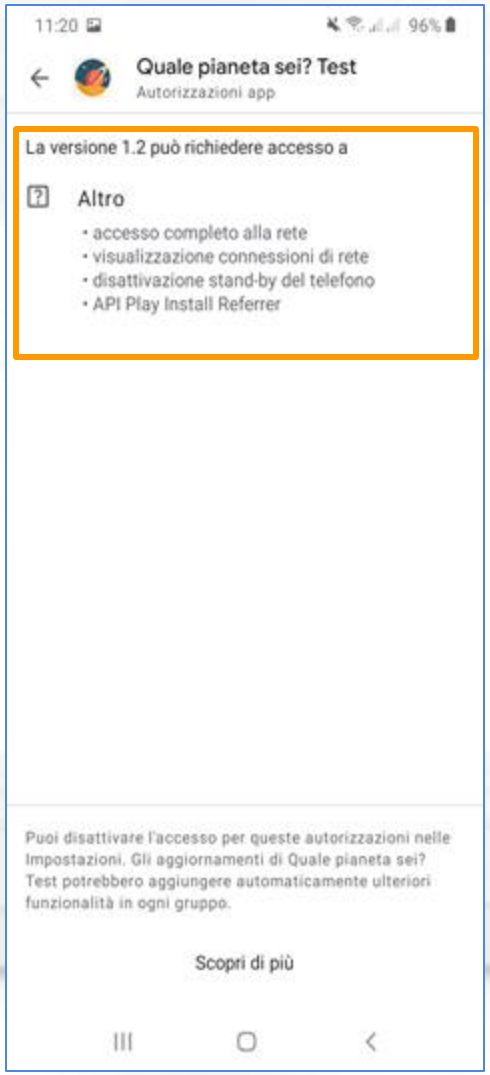




formazionePA

Come difenderci?



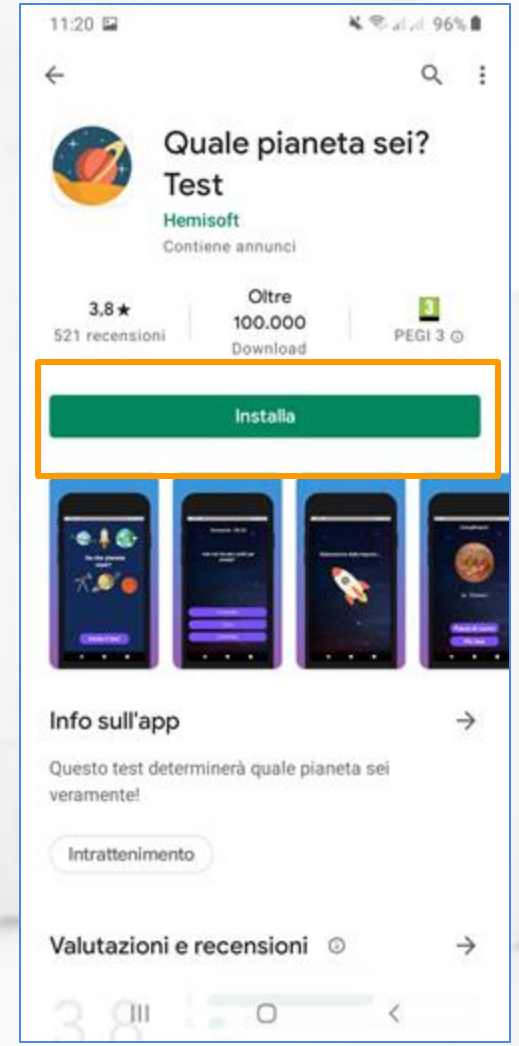


formazionePA

Come difenderci?

Quando si clicca su installa **attenzione a cosa si accetta nei permessi dell'app**.

Esempio: perché un app come "quale pianeta sei?" dovrebbe accedere ai miei files o alle mie foto?



formazionePA


Furto di tempo e
Hacking inconscio

Furto di tempo

Uno degli aspetti più diffusi negli ultimi anni nel mondo cyber è l'aspetto associato **al furto di tempo**. Non vengono infatti rubati solo i dati, anzi spesso **viene rubato tempo per generare dati che sono generati da te ma nascono già di altri**.

Prendiamo un esempio.

Ti colleghi a una piattaforma video per vedere gli highlights della partita di ieri della tua squadra del cuore, visto che hai due minuti prima di andare a fare la spesa. Dopo due ore sei ancora lì a guardare video: non hai fatto la spesa e non hai visto nemmeno i gol della partita della tua squadra del cuore. **Cosa è successo?**

formazionePA

Furto di tempo

Semplicemente in queste due ore è avvenuto un furto di tempo, del tuo tempo. La piattaforma video ti ha presentato, grazie ai suoi algoritmi, dei video che secondo lei potevano essere interessanti in base alle attività che hai fatto nei giorni precedenti, che ha raccolto grazie ai video che hai visto, oppure da altre piattaforme. e quindi è riuscita a catturare la tua attenzione e la tua curiosità presentandoti sequenze di video simpatici o divertenti o seri o professionali e tenerti per due ore “a lavorare per lei”. Ma in che senso lavorare per lei? Sei diventato uno **shadow worker grazie ad un meccanismo bottomless.**

La piattaforma nel presentarti i video **raccoglieva anche i dati del tuo comportamento**: hai guardato un video per intero? E’ un dato. un video l'hai piantato a metà? E’ un dato. In tale modo sei diventato un generatore di dati per la piattaforma che da un lato valida i suoi algoritmi di proposta di video grazie al tuo tempo e al tuo “lavoro”, dall'altro raccogliendo dati su di te migliorando **la tua classificazione**.

formazione PA

Furto di tempo

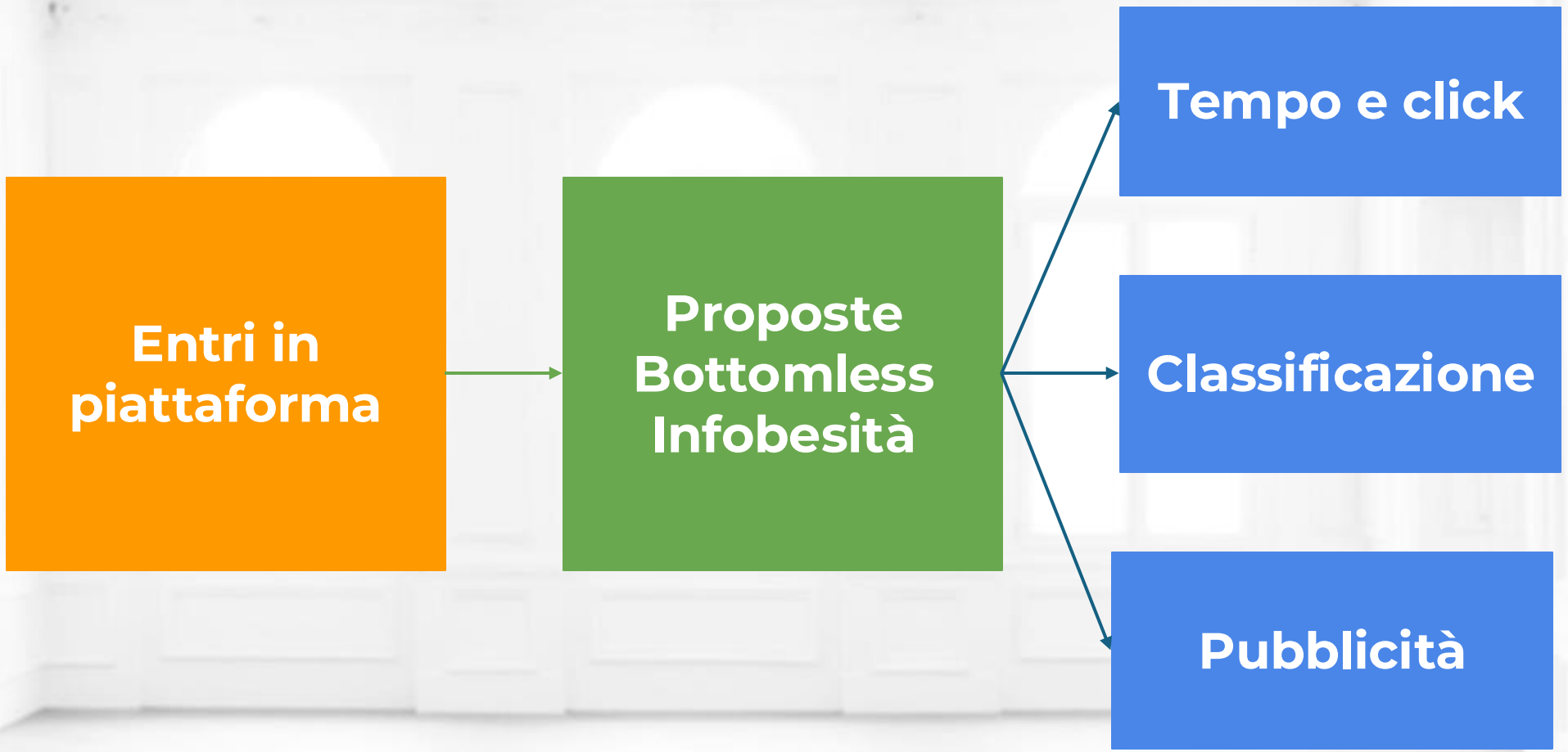
Ad esempio potrebbe capire che sei uno di quelli a cui piace il calcio , piacciono le moto e piacciono i gatti".

Di solito a queste persone piace anche il giardinaggio, quindi ti propone una pubblicità sul giardinaggio. Meglio ti classifica, meglio riesce a mandarti delle pubblicità mirate che per chi fa inserzione sono molto meglio di quelle che possono essere inviate sulla TV generalista dove non si sa quale sarà il pubblico.

Ah, ricorda, **alla piattaforma non interessa chi sei**, interessa che dati produci in modo da classificarti meglio in mezzo ad altri come te e quindi mandarti pubblicità migliori o vendere meglio i tuoi dati o i dati del tuo "gruppo di simili". Che tu ti chiami Mario o Giovanna, cambia molto molto poco.

formazione PA

Furto di dati e di tempo



Social Dilemma

https://www.youtube.com/watch?v=Ko2YcD0iYpc

Youtube

formazionePA

Youtube

formazione PA

Fake News

Cosa sono?

Con fake news intendiamo un'**informazione in parte o del tutto non corrispondente al vero, divulgata in maniera intenzionale e non, attraverso il web o i media**. Le fake news riguardano diversi ambiti, come ad esempio, quello politico, sociale, scientifico fino ad arrivare a cultura e spettacolo.

L'informazione falsa si propaga in modo estremamente veloce, grazie alla condivisione che avviene in maniera molto facile attraverso l'uso dei social network: in questo modo, vengono **messe in circolazione enormi quantità di notizie e diventa estremamente difficile riuscire a riconoscere una notizia vera da una falsa**.

Questo porta con sé delle conseguenze molto gravi poiché **basare il proprio ragionamento su informazioni false porta ovviamente a conclusioni altrettanto false.**

Immagine generata con l'AI

formazione PA

Fake News

Di seguito trovi le caratteristiche più frequenti di una fake news. Conoscerle può aiutarti a evitarle.

1. **Le notizie fake molto spesso fanno leva sui sentimenti e hanno un forte carattere di novità**. Sono costruite ad arte ed in modo da sembrare molto rilevanti e utili nei contenuti che propongono. Ciò cattura l'attenzione del lettore attirandone l'interesse e spingendolo alla condivisione della notizia.

1. Le fake news sono **prive di prove concrete o di riferimenti scientifici**. Spesso nelle notizie false non vengono citate le fonti o vengono citate fonti false o incomplete. Talvolta vengono citati nomi di esperti inventati e istituti di appartenenza inesistenti.

1. **Vengono utilizzate foto e immagini scelte per catturare l'attenzione**, oppure talvolta possono riferirsi a situazioni e contesti diversi da quelli oggetto della fake news.

1. **Spesso recano errori di battitura e grammaticali, con titoli esca**, scritti in maiuscolo e con un uso eccessivo di punti esclamativi

Immagine generata con l'AI

formazionePA

Fake News

Lo scopo:

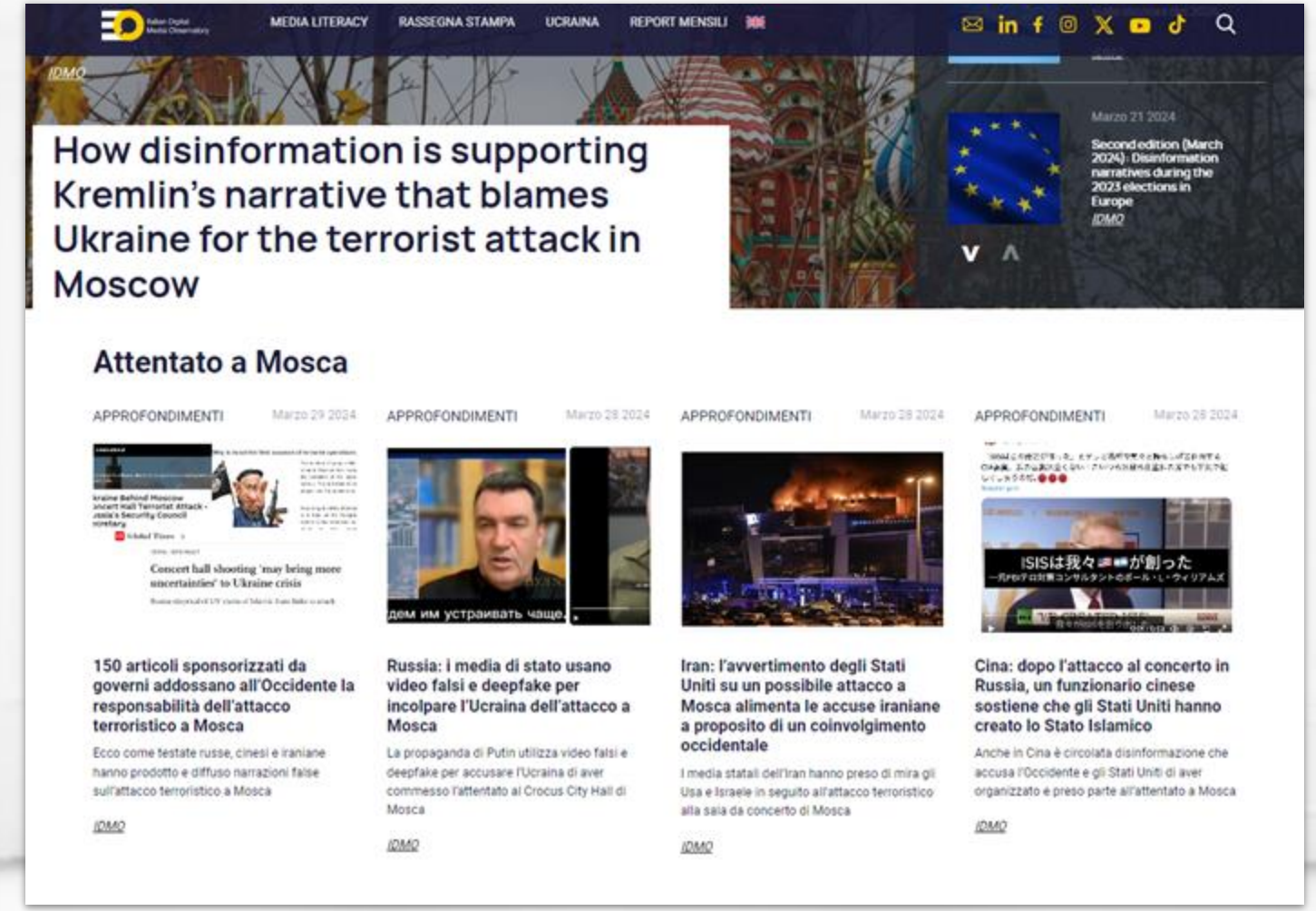
- danneggiare la reputazione
- polarizzare l'opinione pubblica
- distrarre l'attenzione

Come difendersi

- sviluppare spirito critico: cercare i fatti
- cercare fonti attendibili e ufficiali
- cercare conferme su altre fonti
- approfondire approfondire approfondire

Immagine generata con l'AI

formazionePA



https://www.idmo.it/ - Italia Digital Media Observatory

formazionePA

Raiplay- Pillole Contro la Disinformazione

formazione PA

Deep Fake

Lo scopo:

- Un deepfake è una forma di manipolazione multimediale avanzata che utilizza l'intelligenza artificiale, in particolare le reti neurali, per creare contenuti falsi, come video, audio o immagini, che sembrano autentici e reali. Il termine "deepfake" deriva dalla combinazione di "deep learning" (apprendimento profondo) e "fake" (falso).

Immagine generata con l'AI

formazionePA

Deep Fake

Lo scopo:

- Nel contesto dei video, ad esempio, un deepfake può sostituire il volto di una persona in un filmato con il volto di un'altra persona, rendendo la manipolazione difficile da rilevare a occhio nudo. Questa tecnologia può essere utilizzata in modo creativo per scopi di intrattenimento, come creare video umoristici o scene immaginarie, ma può anche essere utilizzata in modo malevolo per diffondere informazioni false, manipolare immagini di personaggi pubblici o creare contenuti dannosi.

formazionePA

Deep Fake

- L'avanzamento delle tecniche di deep learning ha reso più accessibile la creazione di deepfake, aumentando la preoccupazione riguardo alla possibilità di abusi e manipolazioni. Alcuni sforzi sono in corso per sviluppare tecnologie e strumenti per rilevare e mitigare i danni causati dai deepfake.

  http://fal.ai/camera

formazione PA

Focus sulla guerra Cibernetica

Link al post

formazionePA

Focus sulla guerra Cibernetica

Nell'ambiente mediatico attuale la **disinformazione** viene diffusa attraverso algoritmi di intelligenza artificiale, fake news, troll e fantocci digitali, cioè attraverso i moderni strumenti della **propaganda computazionale**.

Una definizione operativa, che ha mostrato negli ultimi anni tutto il suo valore euristico, è quella di Wooley e Howard dell'Università di Oxford, secondo cui "**La propaganda computazionale è l'uso di algoritmi, automazione e cura umana per distribuire intenzionalmente informazioni fuorvianti sui social media**"

Le **campagne di manipolazione** delle percezioni che oggi usano propaganda e disinformazione per seminare dubbio e scontento nella popolazione vengono infatti diffusamente distribuite sui **social network** principali, Facebook, X, Instagram, Truth, e altri ambienti ingegnerizzati per favorire il coinvolgimento delle persone e la polarizzazione delle opinioni. In aggiunta, propaganda e disinformazione sono diventate un problema cibernetico perché i suoi attori usano strumenti digitali automatizzati e interattivi per colpire le certezze dei bersagli con un esercito di troll, di bot , e facendo largo uso di meme e notizie online fasulle, create ad arte da gruppi di guerriglia digitale che usano anche tecniche di software hacking per manipolare l'informazione e i suoi protagonisti, i cui contenuti viaggiano in misura consistente anche su forum come Reddit, Discord, e 4chan.

formazionePA

Focus sulla guerra Cibernetica

In generale, gli autori militari hanno identificato le seguenti caratteristiche che raccomandano i social media come arma informativa:

- il **basso costo** delle operazioni sui social media sia in termini di fondi che personale
- l'**ampia portata** potenziale delle operazioni di informazione online, soprattutto considerando la crescente penetrazione di Internet
- la **capacità di reagire in tempo reale e in luoghi senza presenza fisica**
- la **negabilità delle operazioni** sui social media, data la difficoltà nel distinguere l'attività ordinaria dagli atti di guerra dell'informazione sponsorizzati dallo stato
- la **percezione che gli effetti psicologici dei media online e dei social media siano superiori a quelli forniti dai media tradizionali** a causa del potenziale di confezionare contenuti multimediali in modo da ottenere "**ulteriore influenza emotiva e psicologica**".

Tecnostress e Tecnodieta

Tecnostress

Per **tecnostress** si intende l'eccessivo utilizzo della tecnologia o suo impatto sulla vita che genera ansia e nei casi peggiori depressione, dovuto ad esempio all'eccesso di utilizzo di dispositivi tecnologici o al fatto di dare loro troppa importanza.

Lo sviluppo della tecnologia ha permesso nel corso degli anni di agevolare e migliorare le attività quotidiane. Quando però l'utilizzo della tecnologia diventa **eccessivo** possono scaturire problemi che influenzano il benessere psicofisico. Si parla in questo caso di tecnostress.

Il termine è stato coniato nel 1984 da Craig Broda che l'ha definito come un
"disagio moderno causato dall'incapacità di coabitare con le nuove tecnologie del computer"

Il tecnostress è legato sia agli strumenti tecnologici che al flussi di informazioni a cui siamo esposti, ovvero alla info-obesità.

formazionePA

Tecnostress

info-obesità

Fonti multiple di informazioni

(internet, email, telefono, radio, giornali, televisione, messaggi pubblicitari, notifiche …

Mole di informazioni

non sempre è sinonimo di di ricchezza di informazioni

Difficoltà a gestire le informazioni

Organizzare in maniera razionale così che una volta archiviate sia veloce recuperarle

formazionePA

Tecnostress

Un esempio su tutti

Le notifiche, il padrone del mondo nel XXII secolo

Stress + Distrazione + Controllo del tempo

formazionePA

Tecnostress - Come si manifesta

Tecno Invasion

Tecno Overload

Tecno Complexity

Tecno Insecurity

Tecno Overload

Le persone devono gestire simultaneamente flussi di informazioni da fonti diverse, spesso al di sopra di quelle che sono le loro capacità: in questo caso si sentono sovraccaricati.

info-obesità.

Tecno Overload

formazionePA

Tecno Invasion

Tecno Invasion

Grazie alla tecnologia moderna la persona può essere sempre reperibile e questo **impedisce di separare il lavoro dalla vita privata**: ciò porta a un'invasione tra i due mondi.

formazionePA

Tecno Complexity

I **continui aggiornamenti e sviluppi delle tecnologie ICT** obbligano tutti a impiegare gran parte del proprio tempo nel tentativo di imparare ad utilizzare le nuove tecnologie. Questo può far scaturire avversione alle tecnologie, paura e ansia.

Tecno Complexity

formazionePA

Tecno Insecurity

Tecno Insecurity

I **continui aggiornamenti tecnologici** possono portare le persone a:

- sentirsi insicure e a rischio nel mondo del lavoro, o sentirsi obsolete in generale
- essere stressate dai continui cambiamenti di strumenti

formazionePA

Phubbing

Phubbing

mania di **controllare compulsivamente** il proprio telefonino. Notifiche, chattare, video, tutti catturano la nostra attenzione anche in situazioni inadatte.

Gli **smartwatch** hanno esacerbato questa tendenza associata alla notifiche.

Non è importante con chi l'interlocutore stia comunicando, è importante il fatto stesso che lo faccia e questo porta alla **distruzione della comunicazione e della relazione**.

Di fronte al phubbing, nascono sentimenti di frustrazione, di trascuratezza, di delusione, di tristezza e di solitudine.

formazionePA

TecnoStress vs Flow

Multitasking

vs

SwitchTasking

Stare nel flow

- un grande investimento di attenzione sulla situazione in atto
- una sensazione di **benessere** e di **soddisfazione personale**
- la presenza di un impegno a cui corrispondono capacità personali adeguate

formazionePA

Information Literate

Dobbiamo diventare degli

Information Literate

persona capace di identificare, individuare,valutare, organizzare e utilizzare e comunicare le informazioni.

Obiettivi:

- definire il **fabbisogno** informativo con precisione (per cosa uso lo strumento? per quanto tempo?)
- **ricercare** e **localizzare** informazioni rilevanti, vagliarle criticamente, classificarle e selezionarle efficientemente
- **comprendere** e **interpretare** dati e informazioni per tradurle efficacemente in intuizioni e concetti utili allo scopo definito
- usare le informazioni reperite per creare **nuove ide**e e sviluppare concetti innovativi

formazionePA

TecnoStress - Difesa

Formazione su tecnostress

Riduzione esposizione alla tecnologica

Sfida: provare 24 ore senza tecnologia

Prendersi delle **pause** dalla tecnologia.

formazionePA

Tecno Dieta

Strumenti di difesa:

1. individuare le **fonti attendibili** a livello informativo

1. prendersi delle **pause** (sia nella giornata che nella settimana) disattivando notifiche, spegnendo cellulari, staccando dal lavoro …

   usare **tecniche di rilassamento** muscolare e mentale

1. **alfabetizzazione informatica**

1. **formazione sul tecnostress**

formazionePA

Tecno Dieta

Gestione Delle informazioni

- mi serve davvero questa informazione **adesso**?
- mi serve di **archiviare** l'informazione?
- la **troverò** quando mi servirà?
- è **rumore o segnale?**

formazionePA

Tecno Dieta

Pensare al futuro uscendo dal rumore del quotidiano:

- nessuna notizia è così importante da non poterne fare a meno
- se hai bisogno di informazioni, trova fonti affidabili e concentrati su **notizie importanti e di lungo periodo**
- ti serve davvero la “**fake fame”?**

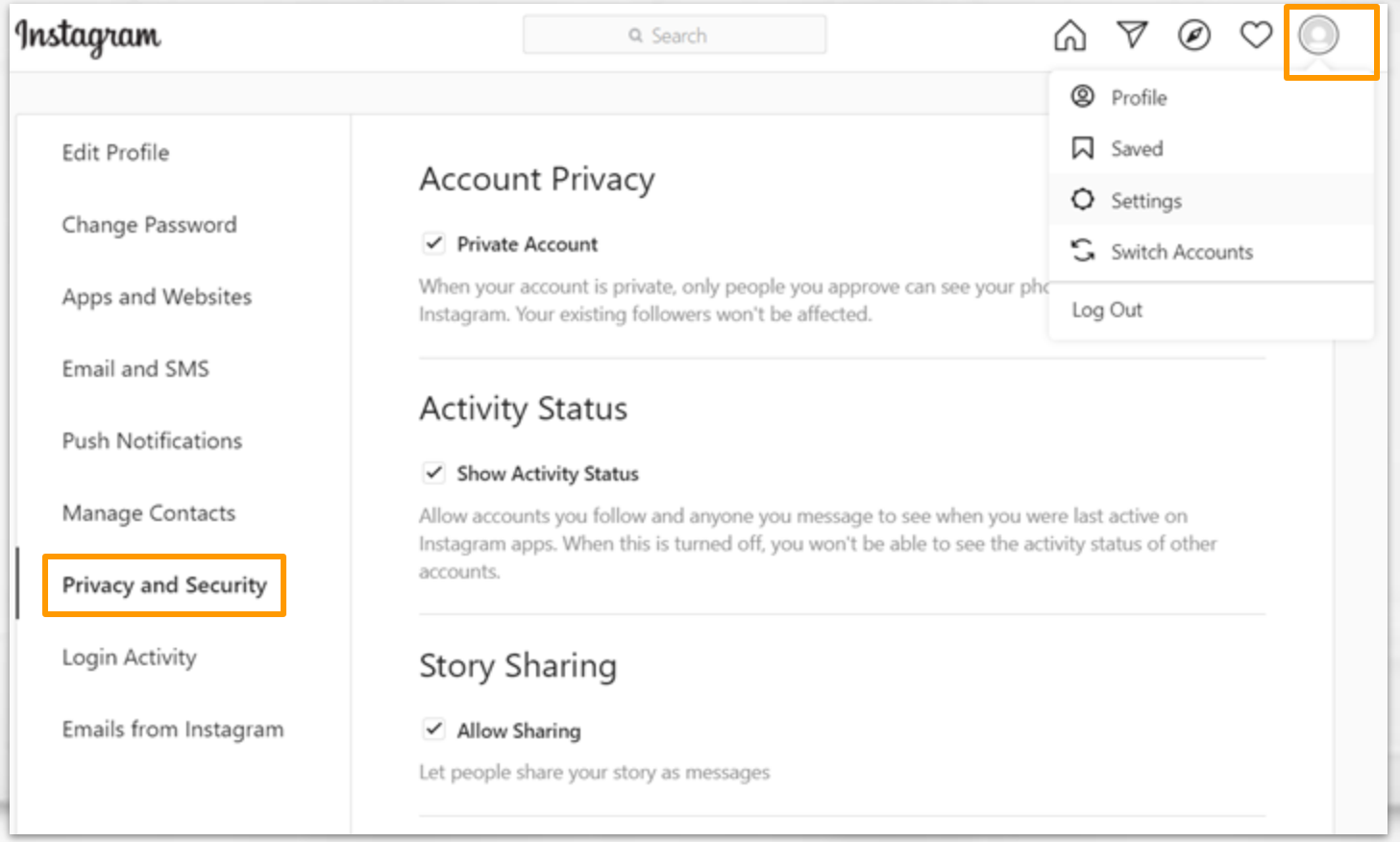
formazionePA


Rischi Cyber e
Nuove Generazioni

Social Media

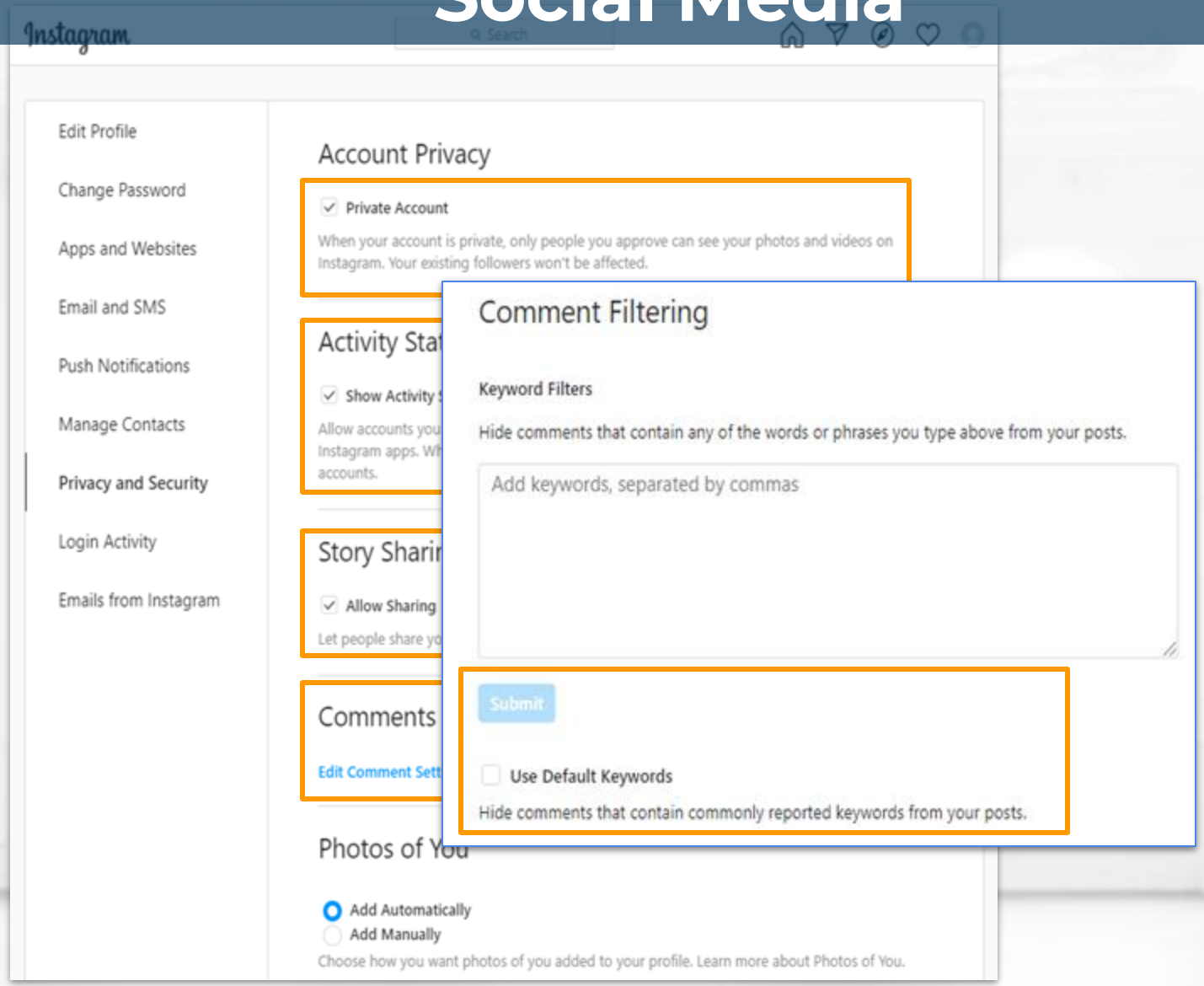
Secondo le statistiche ogni adolescente ha dai 2 ai 10 social media account.

Social Media



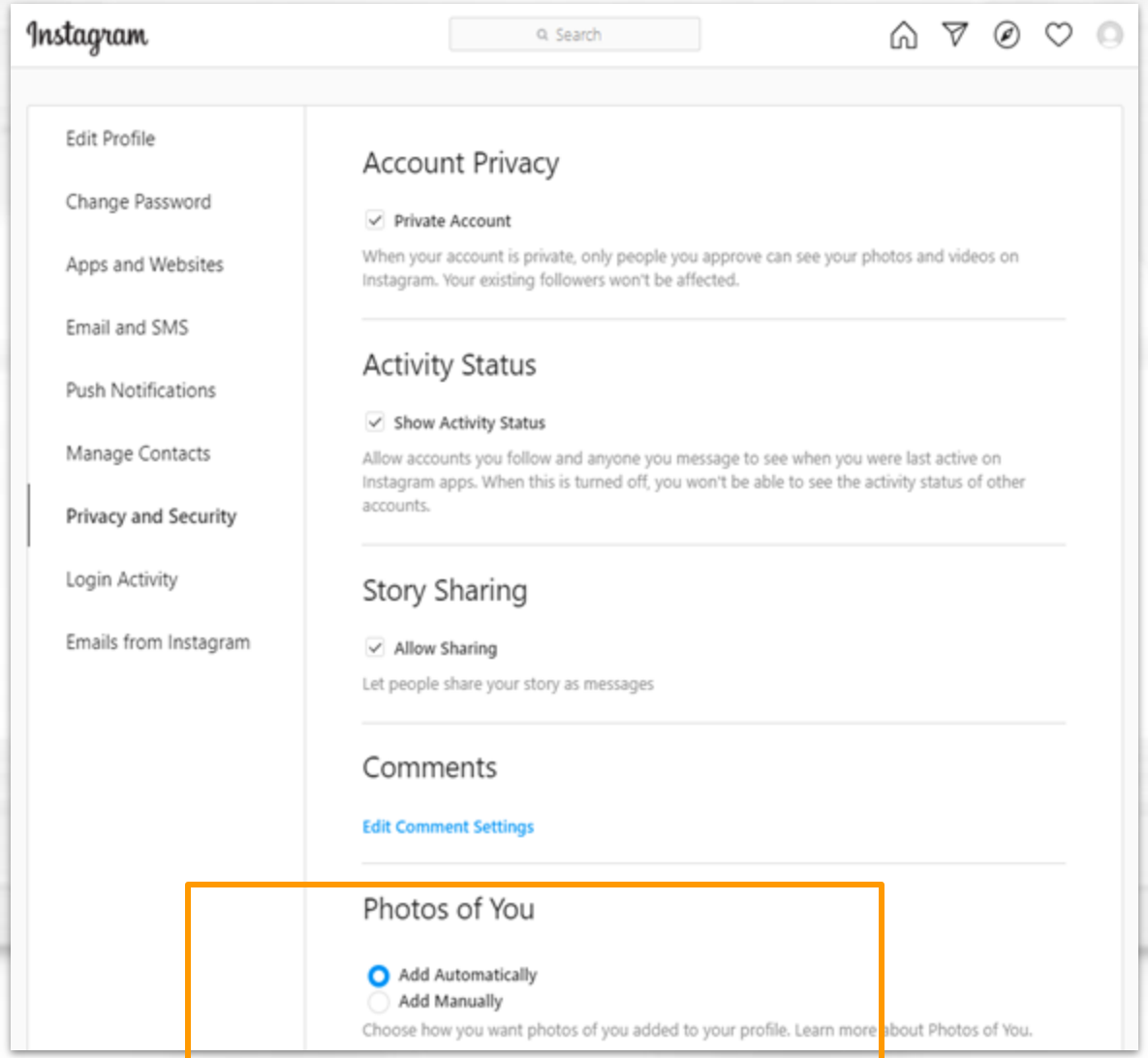
formazione PA

Social Media



formazionePA

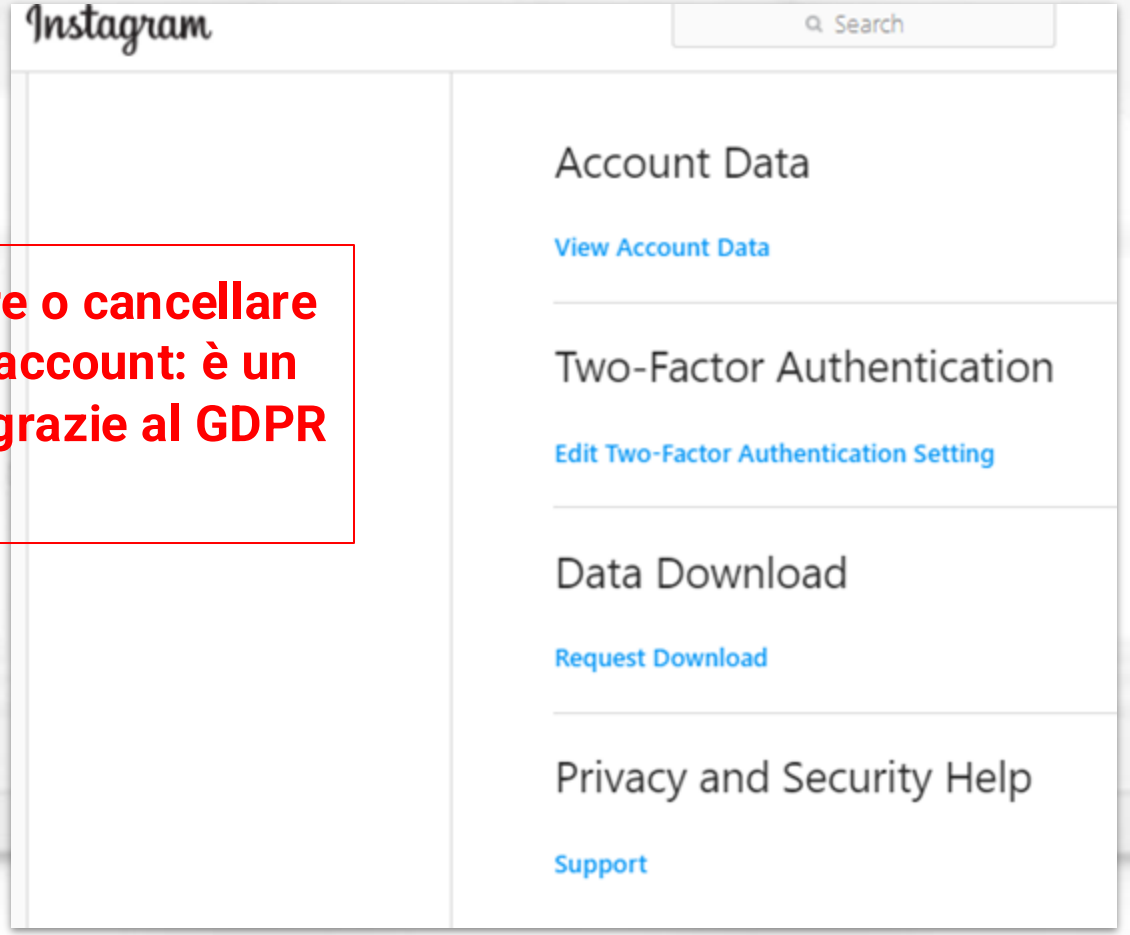
Social Media



formazionePA

Social Media

Si può anche disabilitare o cancellare permanentemente un account: è un diritto (diritto all'oblio) grazie al GDPR (2018)



formazione PA

Social Media

Proteggiti e proteggi gli altri/e.

La maggior parte dei social network ha dei sistemi di reporting: si possono segnalare contenuti/comportamenti offensivi, oltre a bloccare utenti o chiedere rimozioni di pagine. Puoi farlo da solo/a. Se pensi che tu o un tuo amico/a siate in pericolo come conseguenza di ciò che avete visto o condiviso, parlane con i tuoi genitori e contattate la Polizia Postale (recatevi presso un ufficio di Polizia o segnalate i fatti a www.commissariatodips.it; www.facebook.com/commissariatodips/; www.facebook.com/unavitadasocial/)

formazionePA

Cyberbullismo

Cyberbullismo - Cosa é?

Il cyberbullismo ("bullismo elettronico" o "bullismo in internet") è **una forma di bullismo attuata attraverso l'uso dei Nuovi Media** (dai cellulari a tutto ciò che si può connettere a internet).

Come il bullismo tradizionale è una **forma di prevaricazione e di oppressione reiterata nel tempo, perpetuata da una persona o da un gruppo di persone più potenti nei confronti di un'altra persona percepita come più debole**.

Le caratteristiche tipiche del bullismo sono l'intenzionalità, la persistenza nel tempo, l'asimmetria di potere e la natura sociale del fenomeno (Olweus, 1996), ma nel cyberbullismo intervengono anche altri elementi.

Immagine generata con l'AI

formazionePA

Cyberbullismo - Cosa é?

- **L'impatto (viralità)**: la diffusione di materiale tramite internet è incontrollabile e non è possibile prevederne i limiti (anche se la situazione migliora, video e immagini potrebbero restare online.)

- **La possibile anonimità**: chi offende online potrebbe tentare di rimanere nascosto dietro un nickname e cercare di non essere identificabile

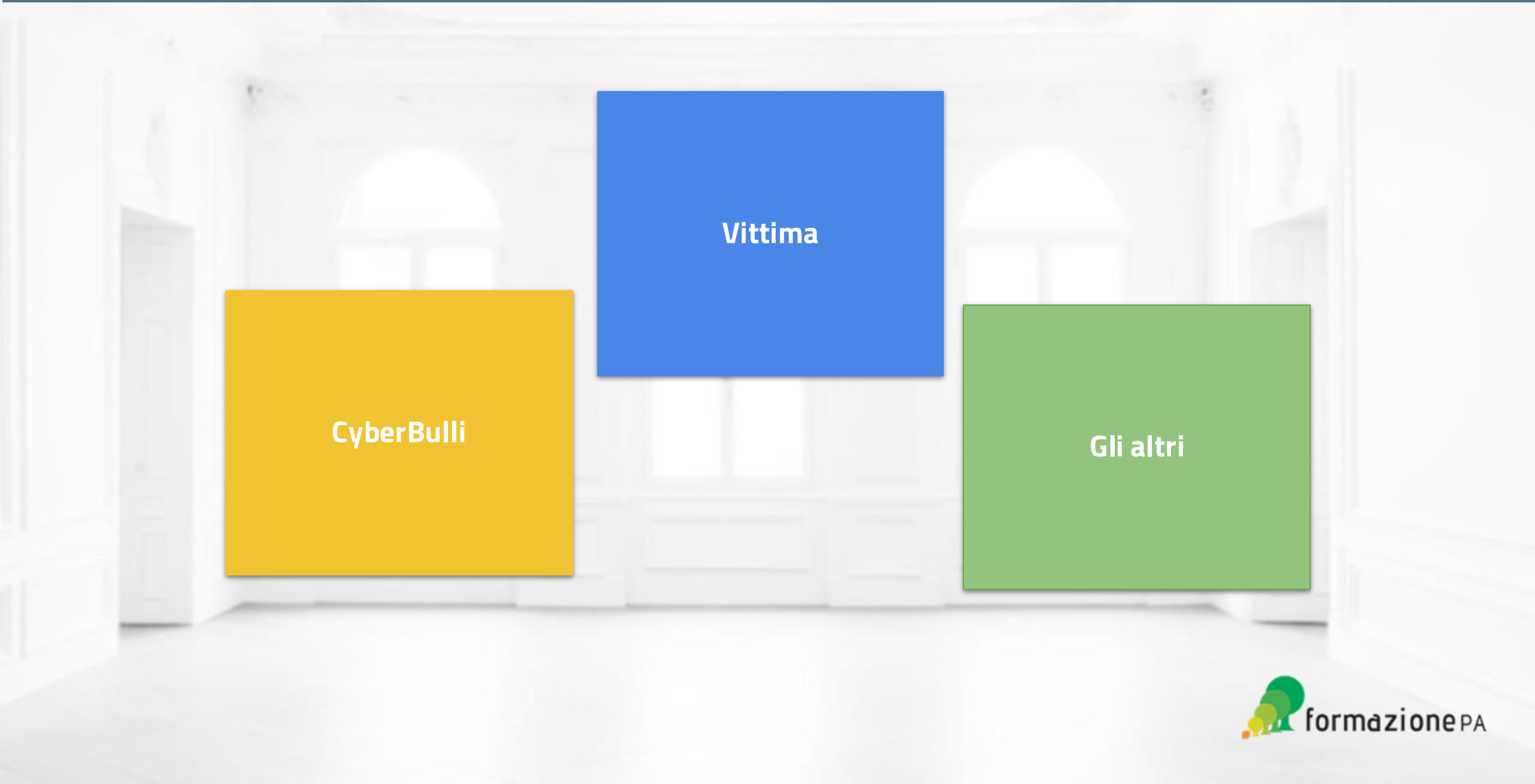
- **L'assenza di confini spaziali**: il cyberbullismo può avvenire ovunque, invadendo anche gli spazi personali e privando l'individuo dei suoi spazi-rifugio (è raggiungibile infatti anche a casa propria).

- **L'assenza di limiti temporali**: il cyberbullismo può avvenire a ogni ora del giorno e della notte.

Immagine generata con l'AI

formazionePA

Gli attori!



CyberBulli

CyberBulli

Il 29 maggio 2017 il Parlamento Italiano ha varato la legge n.71 entrata in vigore il 18 giugno 2017. Tale norma dal titolo “Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo” fornisce una definizione precisa di cyberbullismo, ovvero “qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, furto d'identità, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di isolare un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo.” [art.1 comma 2.]

È interessante notare come tra le fattispecie elencate siano comprese azioni che riconducono al reato penale (ricatto, diffamazione, furto d’identità) e altre che non lo sono (ingiuria, forme di pressione...)

formazionePA

Vittima

Vittima

1. Parlarne ad un **adulto di fiducia**, anche gli adulti una volta sono stati giovani.

1. **Ignorare i bulli**

1. Disattivare/Eliminare l'**app o l'account** con cui si subiscono gli episodi

1. Cambiare **numero di telefono**

1. Chiedere alla **piattaforma di cancellare i contenuti (non sempre facile)**

formazionePA

Vittima

Gli altri

- Se succede a un amico/a, spesso sei tu che puoi fare la differenza: parla con lui/lei, e se la situazione è seria, passa alla soluzione: dillo a un genitore, un fratello/sorella più grande, un insegnante. Non è un tradimento, **stai salvando** qualcuno/a in difficoltà.

- Convincere la vittima a parlare con un adulto di fiducia.

formazionePA

Cyberbullismo - Revenge Porn

Il reato è quello del cosiddetto “**revenge porn**” e lo commette chiunque **diffonda, ceda o invii immagini** o video a contenuto sessuale senza il consenso delle persone interessate.

Prevede la reclusione da 1 a 5 anni.

(Il 9 agosto 2019 è entrata in vigore la legge n. 69 – altrimenti detta “Codice Rosso”)

Immagine generata con l’AI

formazionePA

Cyberbullismo - Revenge Porn

In questo periodo in cui **si trascorre molto tempo on-line**, è bene essere maggiormente prudenti cercando di evitare l'invio di foto o video di contenuti intimi perché, oltre al pericolo di un **uso illecito da parte di chi riceve le immagini,** spesso con il fine di ritorsione o di vendetta, c'è anche un problema legato alla **sicurezza dei dispositivi**. Infatti c'è sempre l'eventualità che malintenzionati possano accedere abusivamente ai vostri cellulari o computer, acquisirne i contenuti per poi divulgarli sul web o utilizzarli come arma di ricatto.

Una volta che le immagini sono state diffuse in Rete diventa difficile, se non impossibile, rimuoverle definitivamente, con gravi conseguenze per la vittima.

Immagine generata con l'AI

formazionePA

Ridurre il rischio di diventare vittima

Ridurre il rischio di diventare vittima

- Utilizzare delle password sicure e non rivelarle a nessuno.
- Proteggere la propria sfera privata. Non divulgare dati e informazioni sensibili.
- Sui social media accettare come amici soltanto le persone che si conoscono veramente.
- Non postare **foto o filmati imbarazzati**.
- Vietato il **sexting** (scambio di testi e/o immagini intimi in rete).
- Togliere riferimento a se stessi nelle foto.
- Bloccare il telefono quando non si è davanti allo schermo

formazionePA

Social Challenge

Challenge

Sfide che mirano a creare momenti o percorsi che possono danneggiare una persona (fino a portarla alla morte).

Si basano **sui meccanismi di accettazione sociale** tipici dell'età adolescenziale.

Immagine generata con l'AI

formazionePA

TikTok

Ridurre il rischio di diventare vittima

Ridurre il rischio di caderci

- Non accettare challenge pericolose
- Non **sentirsi obbligati**
- Parlare con un adulto se ci si sente costretti a fare qualcosa online
- **Aspetti tecnologici**

formazionePA

Vademecum per te e per i colleghi

Vademecum - Cosa fare per prevenire un attacco hacker

Vademecum - Cosa fare per prevenire un attacco hacker?

1. tenere aggiornato il sistema (sia smartphone che computer)
    a. lo smartphone li presenta in automatico
    b. il computer li mostra in automatico oppure periodicamente nella barra di ricerca scegliere aggiornamenti windows e lanciarli
2. tenere aggiornato e attivo l'antivirus
    a. solitamente viene fatto in automatico
3. tenere il firewall attivo di windows
    a. nella barra di ricerca scegliendo windows firewall dovrebbe essere tutto attivo
4. avere un backup dei dati
    a. presso l'ente vengono effettuati salvando i dati del server, a casa utilizzare un servizio cloud oppure un disco esterno cifrato
5. non aprire email strane o con allegati strani
    a. l'80% degli attacchi arrivano mediante le email. Evitare nel dubbio di aprire email che ci creano dubbi sulla provenienza o con allegati che non conosciamo.
6. gestire le password con password manager come ad esempio LASTPASS o KEEPASS
    a. questi permettono di salvare password, generarle, automaticamente riempire moduli online, e soprattutto di ricordarci sollo la password di accesso alle altre e non tutte le password di cui abbiamo bisogno
7. pulire periodicamente il dispositivo ad esempio con CCLEANER
8. Evitare di utilizzare il wi-fi comunale, se non presente una rete Ospiti, con il proprio cellulare personale che potrebbe essere fonte di attacchi mediante app social
9. evitare i software crackati
10. formazione sulla cybersecurity

formazionePA

Vademecum - Come accorgersi di essere sotto attacco?

Vademecum - Come accorgersi di essere sotto attacco?

1. il computer va molto lento
2. ricevo un'email che mi fa venire un dubbio sull'origine della stessa
3. il browser mi manda su siti che non ho digitato o non conosco
4. il browser presenta della barre indesiderate
5. vedo dei popup strani sul computer
6. sui social ricevo richieste di amicizia da persone che non conosco
7. il software antivirus viene disattivato o segnala malfunzionamenti
8. ci sono software installati non conosciuti

formazionePA

Vademecum - Cosa fare in casi si pensi di aver subito un attacco?

Vademecum - Cosa fare in caso si pensi di aver subito un attacco?

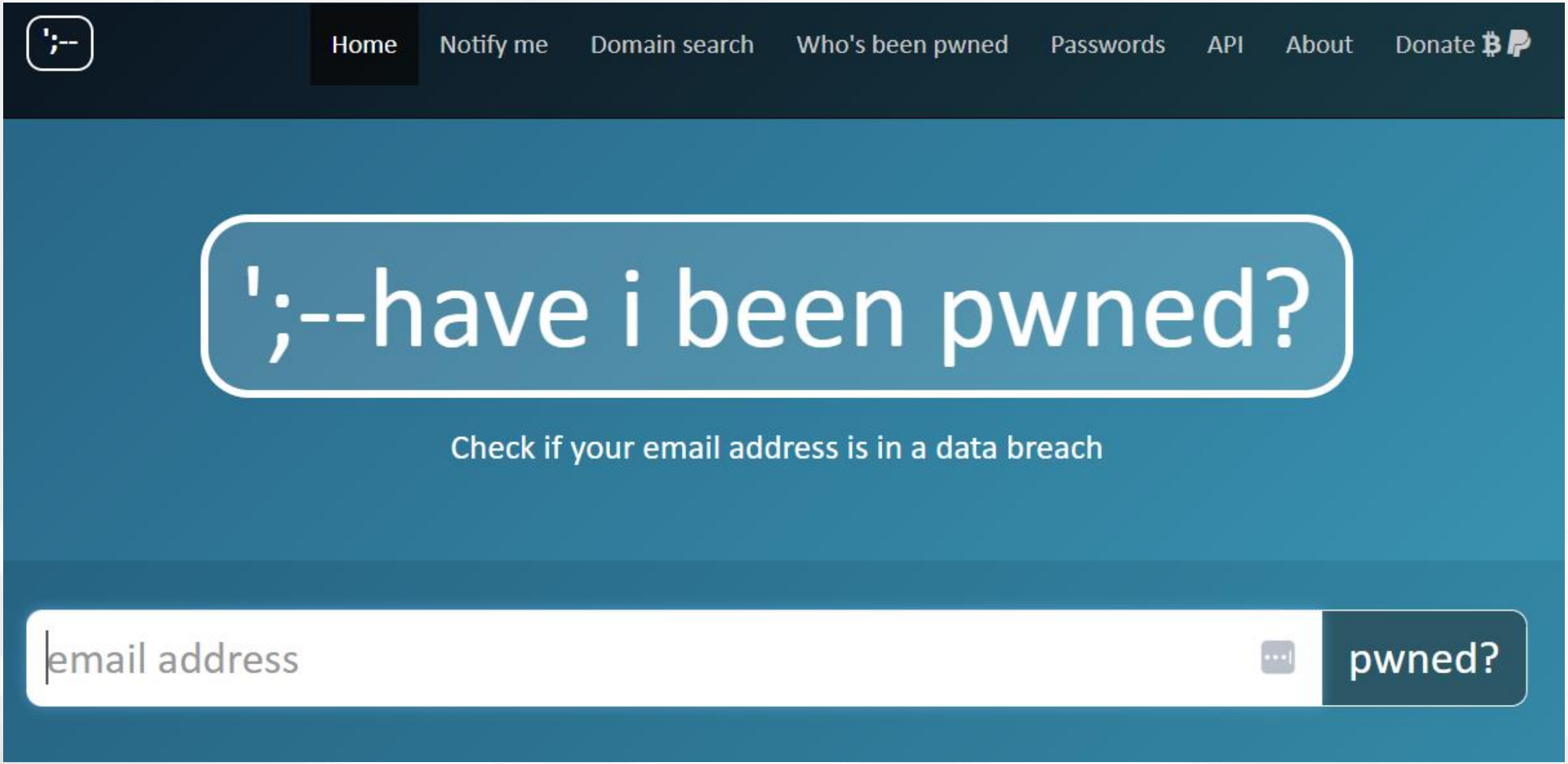
1. disconnettere il dispositivo dalla rete, scollegando l'apposito cavo
2. disconnettere i server dalla rete, scollegando l'apposito cavo
3. se non si riesce a scollegare pc o server, spegnerli con
4. spegnimento normale del sistema
5. se non si riesce nemmeno a spegnerli, togliere corrente anche togliendo l'alimentazione
6. chiamare l'assistenza tecnica

formazionePA


Focus Password

formazione PA

https://haveibeenpwned.com/

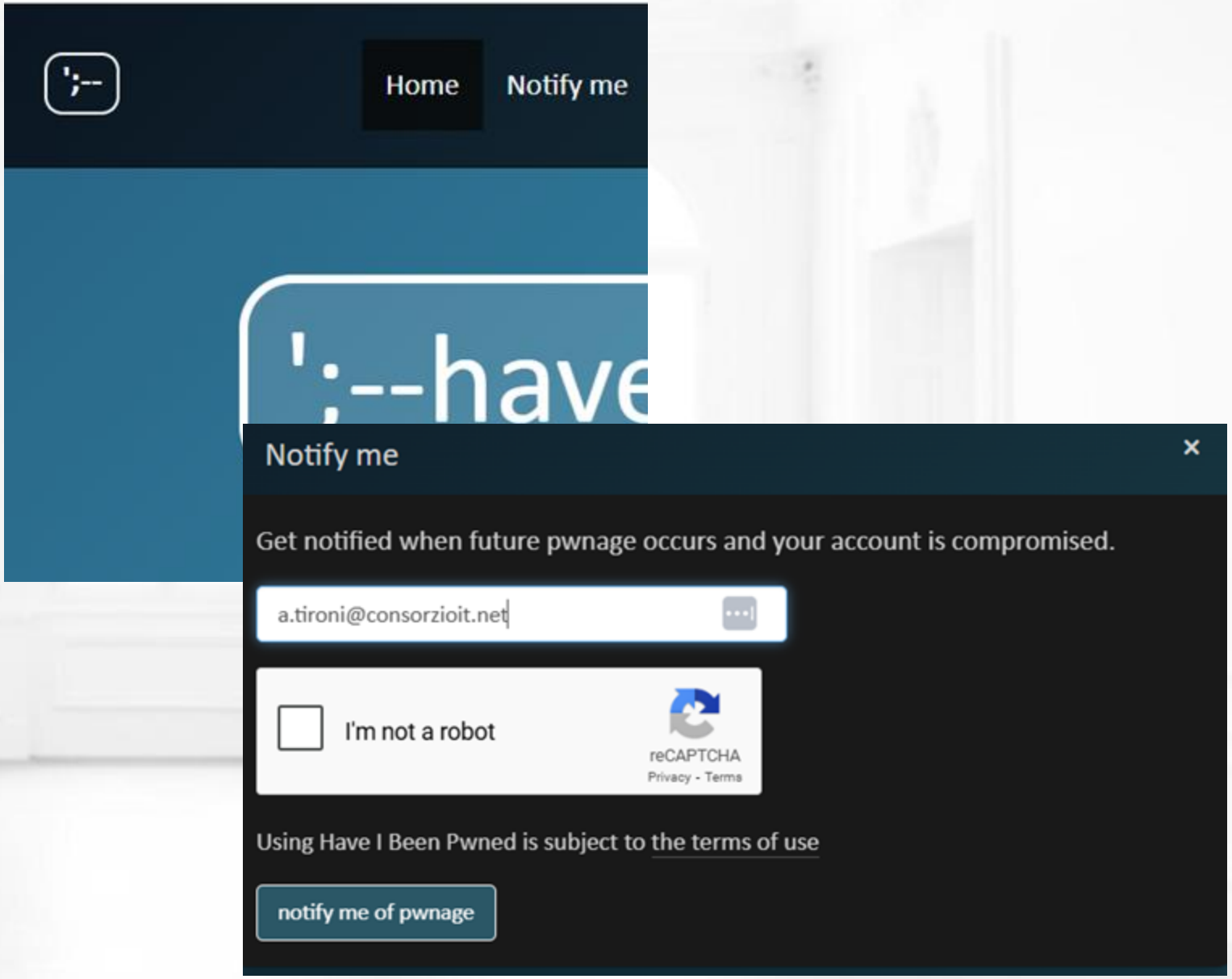


https://haveibeenpwned.com/

Step 1
Proteggiti utilizzando Password Manager per generare e salvare password complesse per ogni sito web.

Step 2
Abilita l'autenticazione a due fattori e salva i codici nel tuo account Password Manager.

https://haveibeenpwned.com/

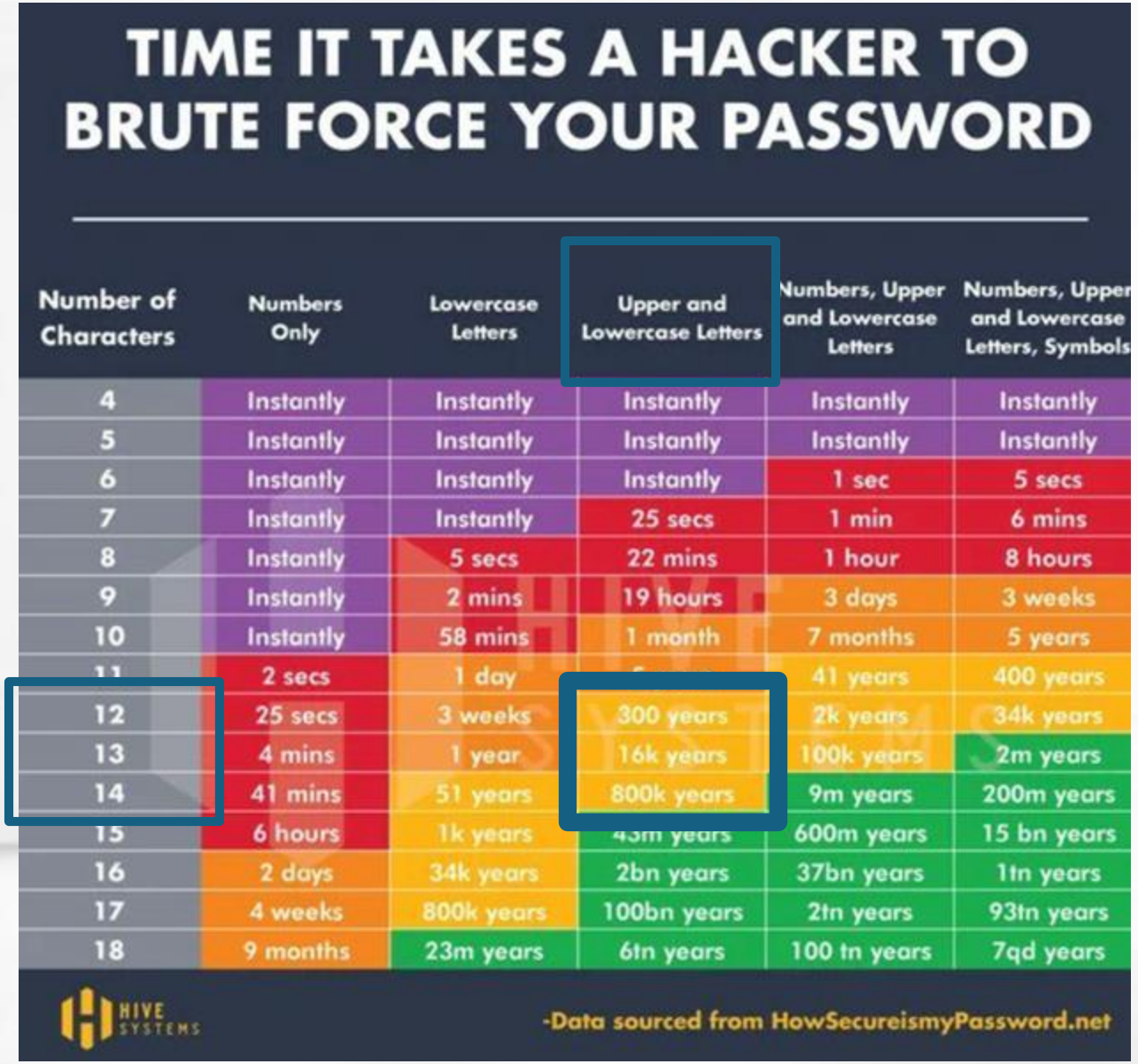


Step 3

Iscriviti alle notifiche per eventuali altre violazioni. Poi sarà sufficiente cambiare quella password univoca.

Come fare una password complessa?

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.1[illegible]%
#5	7777	[illegible]45%
#6	1004	[illegible].616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	69[illegible]	0.512%
#11	[illegible]99	0.451%
#12	3333	0.419%
#[illegible]	5555	0.395%
[illegible]4	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

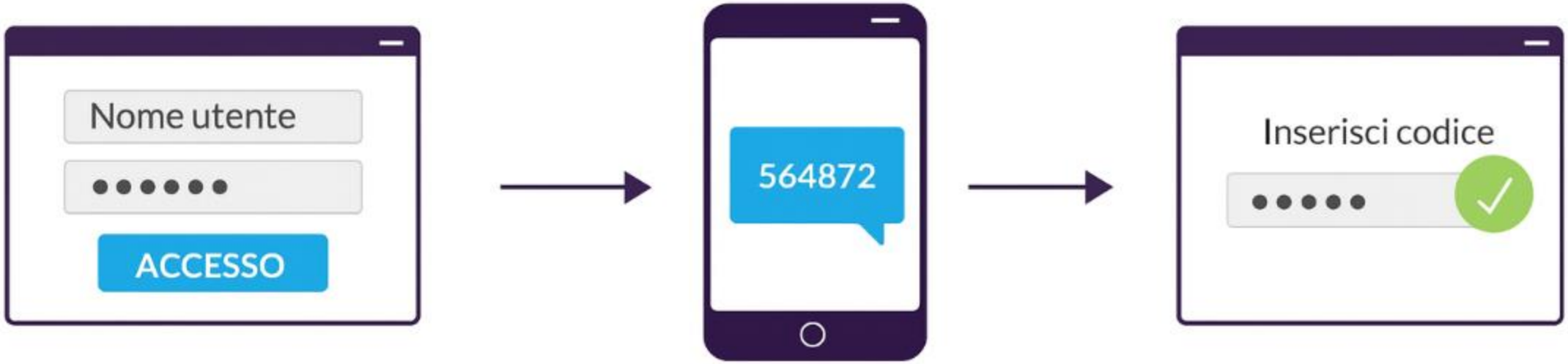


formazione PA

2FA

MFA

2 factor authentication



L''utente inserisce il proprio nome uten e la propria password.

Un codice di autenticazione viene inviato al disposi- tivo mobile dell 'utente.

L'utentie inseriisce il proprio codice di auten- ticazipne per accedere all applicazione.

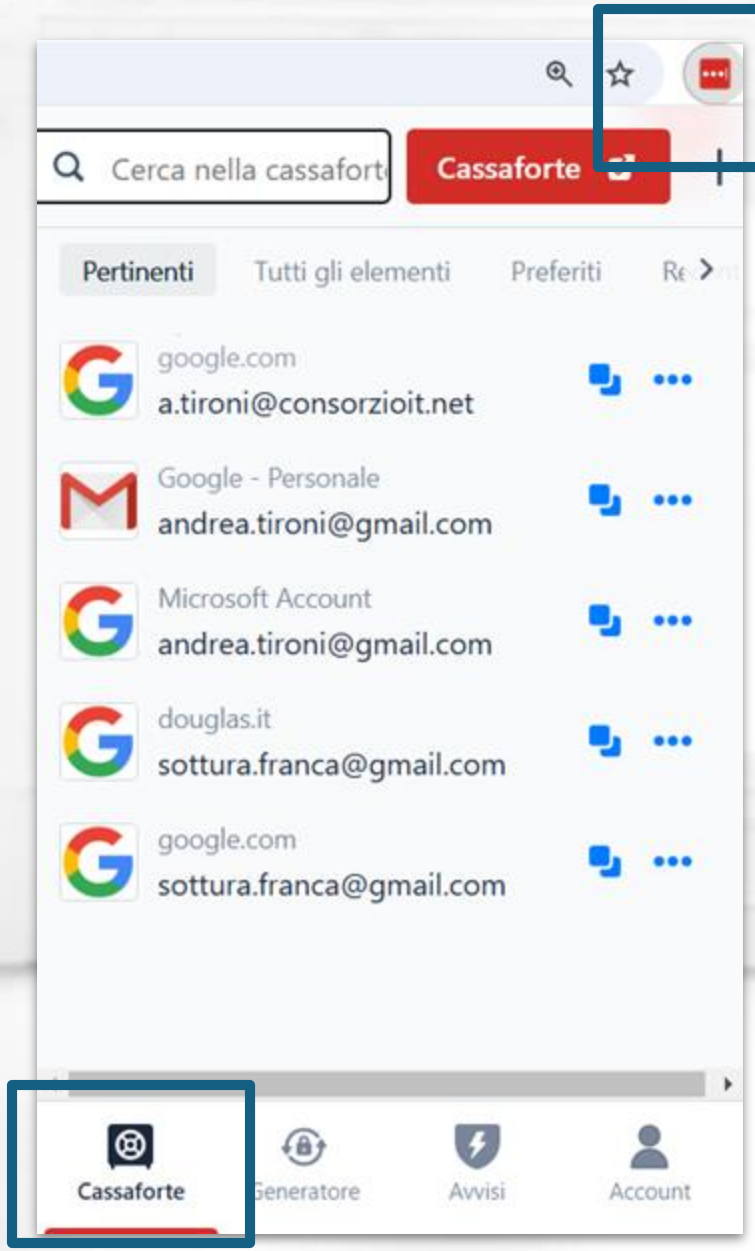
Esempio di 2FA utilizzando un dispositivo mobile.

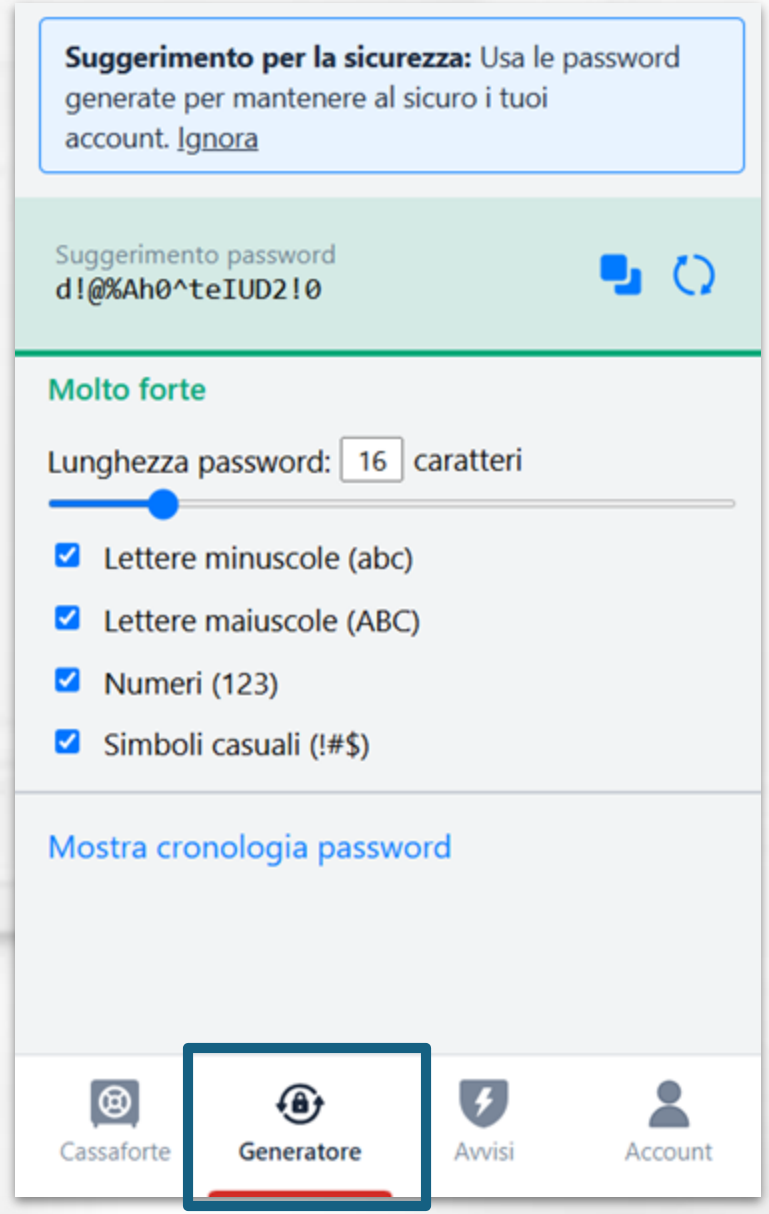
formazione PA

PASSWORD MANAGER

Password Manager

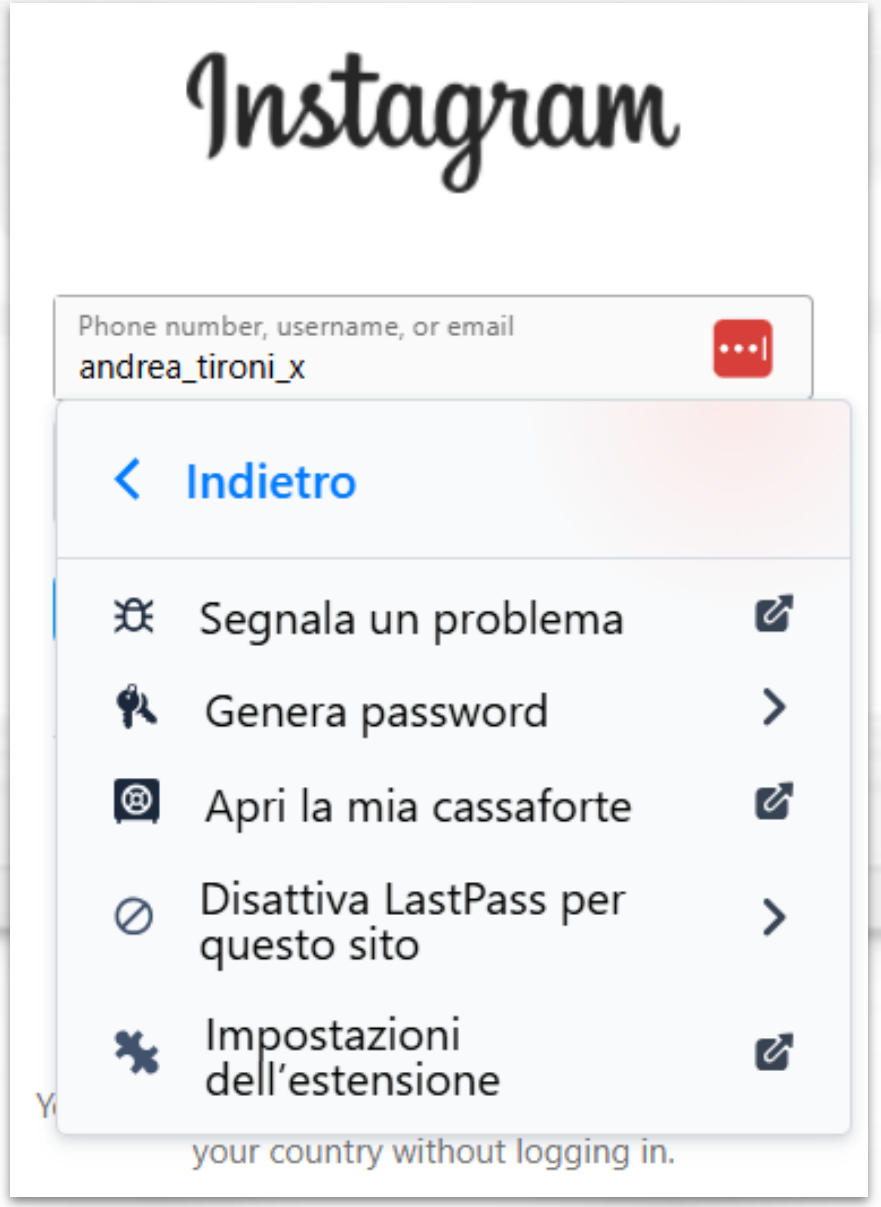
LastPass





Password Manager

LastPass



formazionePA

PASSKEY

PassKey - Cosa è?

Versione digitale e accessibile qui

Google

Come funziona

Una passkey è composta da due parti: una chiave di accesso pubblica sul server per il sito web a cui stai accedendo, e una chiave privata corrispondente sui tuoi dispositivi.

Quando effettui l'accesso, il sito web controlla se la chiave d'accesso pubblica corrisponde a quella privata.

Per farlo, ti viene chiesto semplicemente di sbloccare il tuo dispositivo.

Accederai al tuo account, mentre la tua chiave d'accesso privata e i tuoi dati biometrici rimarranno al sicuro sul tuo dispositivo e non verranno mai condivisi con nessuno.

PassKey - Cosa è?