Immagine creata con AI

ARI TREVISO
IQ3TR
05 giugno 2026

LoTW è stato hackerato!
Tu sei il prossimo bersaglio?

"Non aspettare l'incidente"

Sicurezza informatica pratica per radioamatori:

Riconosci, Previeni, Proteggi

IK3GIG – Fabio Provedel

Immagine creata con AI

Stasera parliamo di: Sicurezza Informatica (mondo digitale) o Cyber Security

Come dice: Alessio Pennasilico (componente del Comitato Scientifico del CLUSIT) nella prefazione al libro "*Cyber Security*" di Giorgio Sbaraglia:

La cybersecurity non è più, e non può più essere, un argomento per esperti.
Se mai lo è stata.
Per questa ragione è indispensabile raccontare a tutti, anche a chi tecnico non è, e non solo deve esserlo, quali rischi corre e come può difendersi.
...
Per comprendere che non ci dobbiamo preparare al futuro, ma cercare di recuperare un enorme ritardo sulla consapevolezza che avremmo dovuto costruire negli anni passati.
E non lo abbiamo fatto.

Scopriamo cosa c'è oltre lo specchio

Immagine creata con AI

Perché i criminali informatici prendono di mira i radioamatori?

Il radioamatore moderno non è più solo un operatore radio.

È una figura ibrida: gestisce apparati digitali, usa software SDR, accede a ripetitori via internet (Echolink, D-STAR, DMR), partecipa a reti di emergenza e comunica su piattaforme digitali.

Questa ricchezza tecnologica espone a rischi specifici che molti sottovalutano.

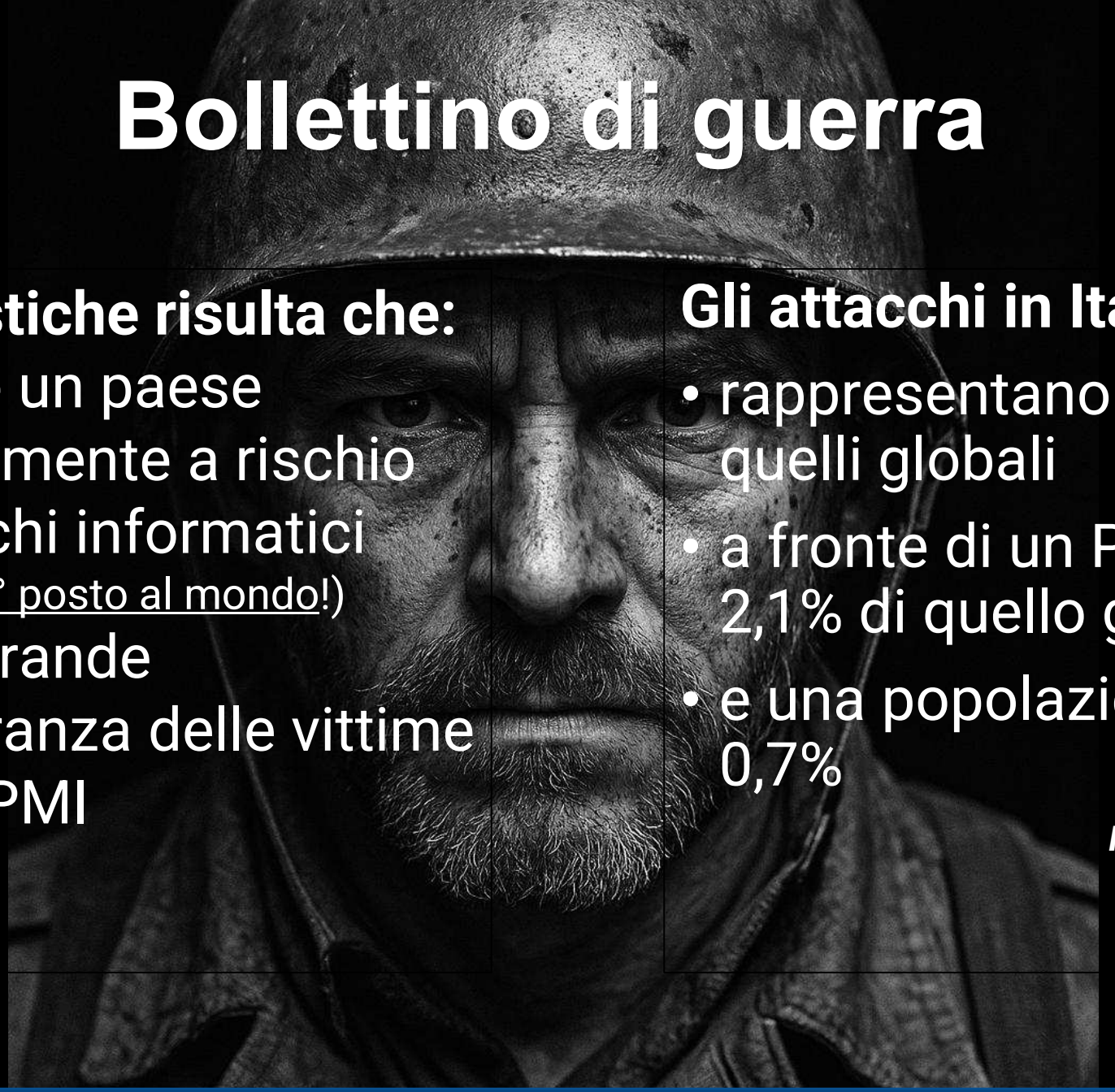
L'attacco ad ARRL/LoTW: cosa è successo davvero e cosa ci insegna


Immagine creata con AI

Perché si parla di sicurezza nel digitale

- Il mondo digitale è **soggetto ad azioni criminali** ben strutturate ed organizzate
- Oggigiorno è un elemento fondamentale della cultura personale e professionale per muoversi nel mondo digitale
- Le aziende ma anche noi dobbiamo aumentare il nostro livello di conoscenze nell'ambito della sicurezza informatica per proteggerci

Bollettino di guerra



Dalle statistiche risulta che:

- L'Italia è un paese estremamente a rischio di attacchi informatici (siamo al 3° posto al mondo!)
- La stragrande maggioranza delle vittime sono mPMI

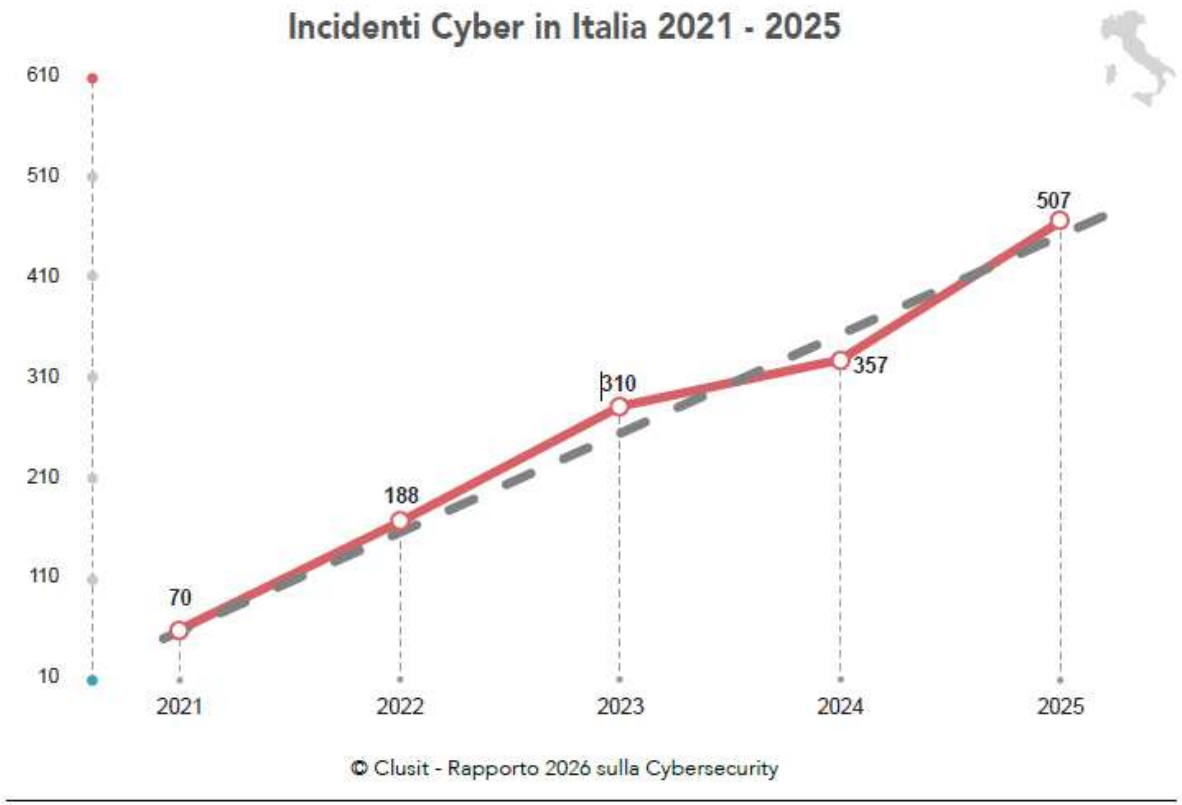
Gli attacchi in Italia:

- rappresentano il 10,1% di quelli globali
- a fronte di un PIL che è il 2,1% di quello globale
- e una popolazione che è lo 0,7%

Fonte: Rapporto Clusit

Immagine creata con AI

Crescita attacchi in Italia



· Distribuzione degli incidenti cyber in Italia nel periodo 2021 - 2025

9,6%
È la percentuale di incidenti cyber avvenuti in Italia rispetto al resto del mondo

61%
È la percentuale di incidenti di matrice Cybercrime in Italia

+66%
È la crescita di incidenti di tipo Phishing / Social Engineering in Italia

+42%
È l'aumento degli incidenti cyber nel 2025 rispetto al 2024 in Italia

16%
Degli incidenti al settore Manifacturing nel mondo avviene in Italia

Fonte Rapporto Clusit 2026 aggiornamento_03_26

Accadde in Veneto:

- **Gruppo Carraro** - (Campodarsego, Padova) settembre 2020
- **Neafidi** - (Vicenza) - febbraio 2024
- **Alf Da Frè** - (Gaiarine, Treviso) Notte tra il 10 e l'11 febbraio 2025
- **31 Piccole e Medie Imprese Venete** - febbraio 2025
- **Fashion Box S.p.A. (Replay)** (Caselle d'Asolo, Treviso) - febbraio 2025
- **Fantin Group** (Istrana, Treviso) - 4 marzo 2025
- **Adrenalina** (Caerano San Marco, Treviso) - 5 marzo 2025
- **Asolo Dolce** (Asolo, Treviso) - aprile 2025
- **Mobilità di Marca (MOM)** Treviso - aprile 2025
- **Siti istituzionali della Regione Veneto** - 24 febbraio 2025
- **Breton S.p.A.** — Castello di Godego, TV - 1 maggio 2025
- ……..

Caso reale nel mondo ham: l'attacco ransomware ad ARRL e LoTW (2024)

- **12 maggio 2024:** LoTW – Logbook of The World – va offline.
- Non per un guasto, ma per un ransomware.
- **Il vettore di ingresso:** credenziali acquistate sul Dark Web da precedenti violazioni di altri servizi.
- **ARRL ha pagato 1.000.000 di dollari** per ottenere la chiave di decifratura.
- **LoTW rimasto offline per quasi 7 settimane** (12 maggio – 1° luglio 2024), sistemi telefonici down, Learning Center irraggiungibile, sistema contabilità colpito
- **Oltre 60.000 log in coda** al momento del ripristino. Diplomi DXCC, WAS, VUCC bloccati per mesi.
- **Dati soci esposti:** nomi, indirizzi, callsign presenti nel database.
- **Lezione:** se ARRL può essere colpita con credenziali riutilizzate, chiunque di noi può esserlo.

Il messaggio chiave:

- Se un’organizzazione come ARRL, con risorse tecniche dedicate, può essere colpita da un ransomware entrato tramite credenziali rubate, chiunque di noi può essere un bersaglio.

- La difesa parte dalle nostre abitudini quotidiane: password uniche, 2FA attivo, aggiornamenti regolari.

Il fattore umano

Il 95% degli attacchi andati a buon fine è dovuto all'**ERRORE UMANO**.

Il problema esiste tra la tastiera e la sedia

La superficie di attacco del radioamatore digitale

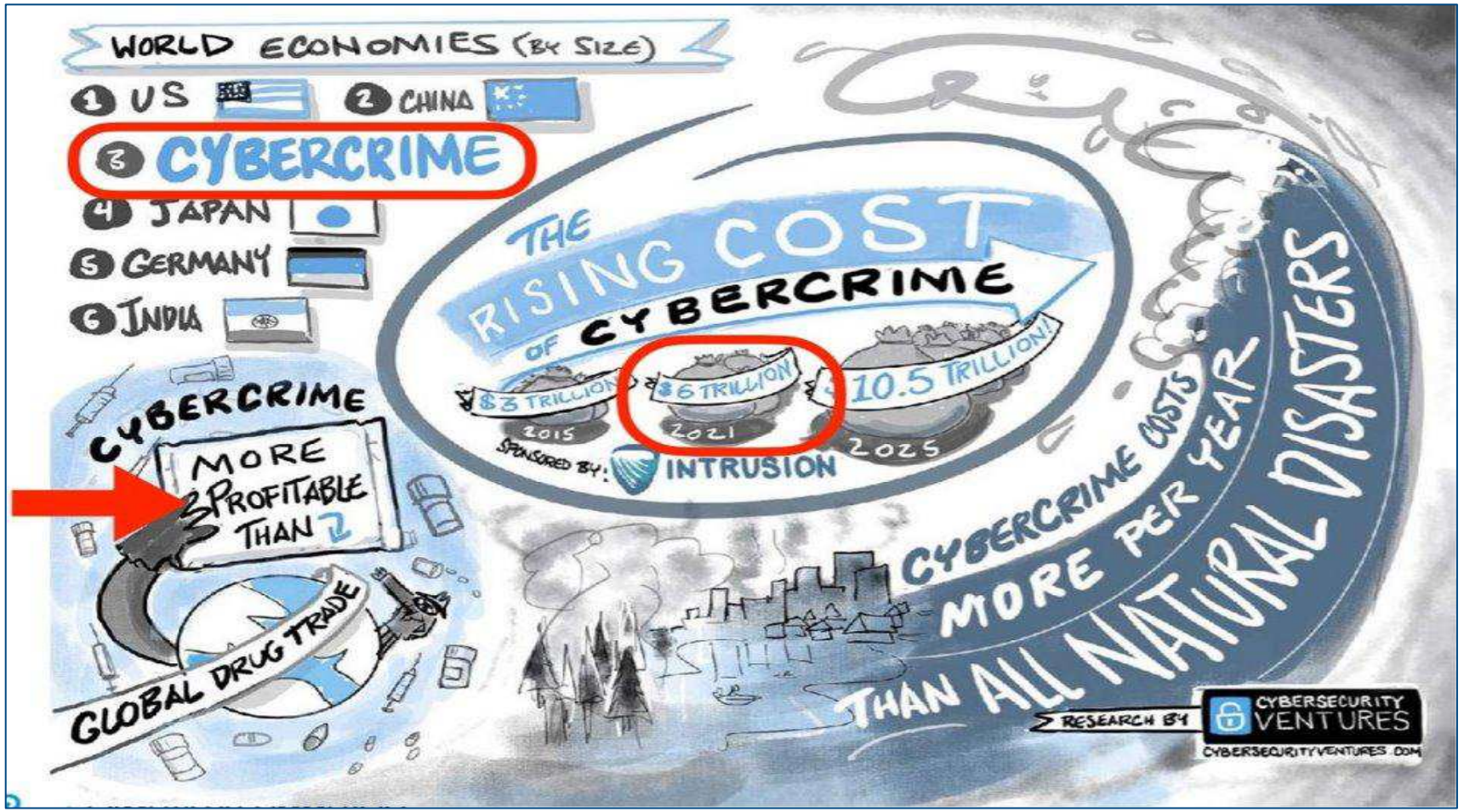
- **Email e comunicazioni:** phishing mirato con callsign, log QSO, referenze a contest reali.
- **Software radio:** malware in versioni false di WSJT-X, CHIRP, SDR#, N1MM scaricate da siti non ufficiali.
- **Ripetitori e nodi:** accesso non autorizzato via Echolink/IRLP, denial of service, intercettazione.
- **Database pubblici:** QRZ, LoTW, eQSL contengono nomi reali, indirizzi, callsign e apparati posseduti.
- **Reti domestiche:** router mal configurato, dispositivi IoT, NAS con log radio esposti.
- **Reti di emergenza:** compromissione di comunicazioni critiche in scenari Protezione Civile (ARES, RACES).

Conoscere il nemico

Non ci sono più gli hacker di una volta…

Giro di affari della criminalità informatica

Fonte: Cybersecurity Ventures



Un trilione (negli USA) corrisponde a **1.000 miliardi** (10^{12}), ovvero un milione di milioni.

Principali settori dell’ecosistema criminale

Fonte: Rapporto Clusit 2023

«L'inferno in Terra»

A lavorare nelle fabbriche di frodi un vero e proprio esercito di sfruttati.
Tra Laos, Cambogia e Myanmar, secondo la United States Institute of Peace, sono **300.000 le persone che giornalmente truffano altre persone online** in luoghi con sbarre alle finestre, telecamere a circuito chiuso e ingressi sorvegliati da personale armato.

Le nostre info sono un bene prezioso

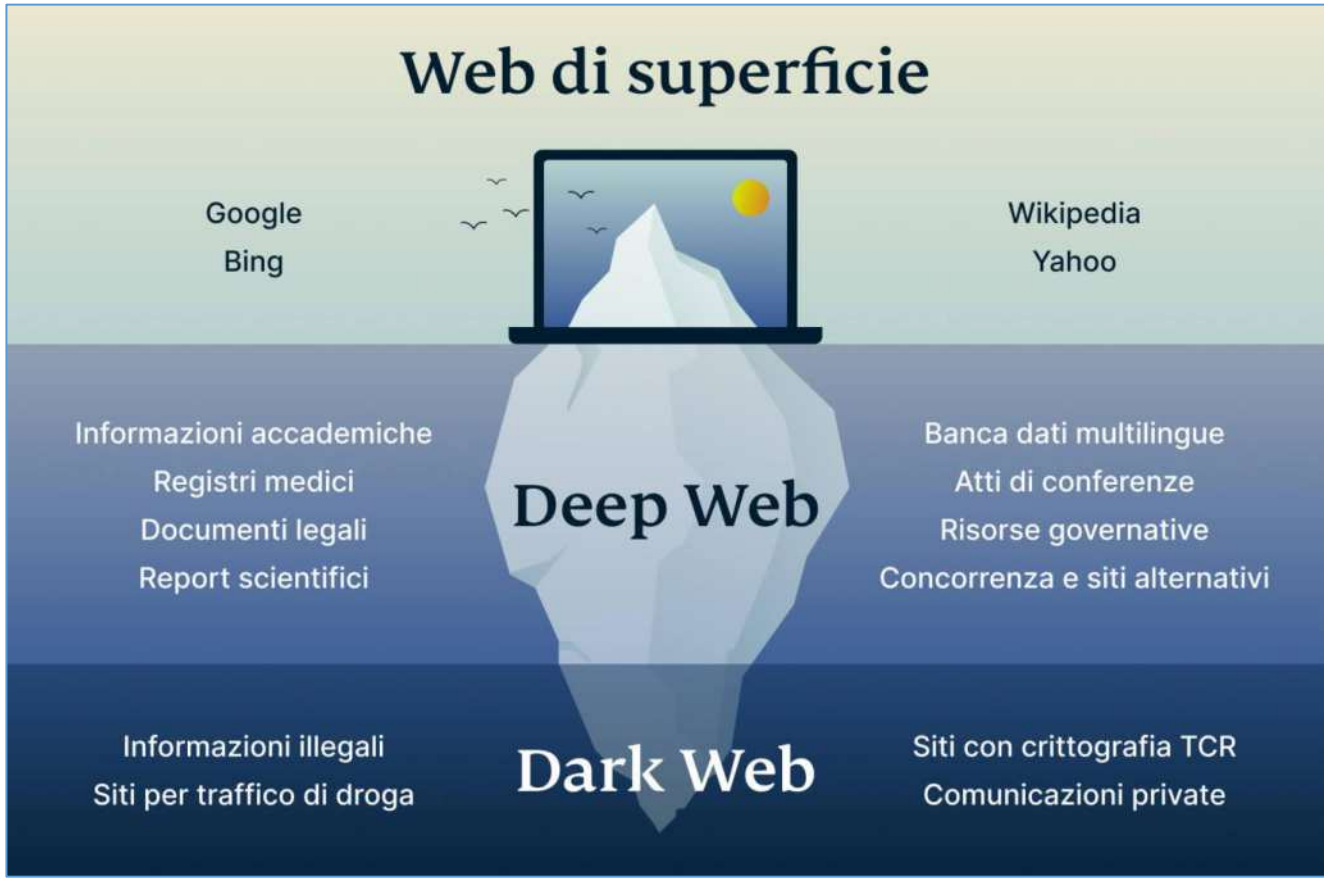
- Le nostre informazioni personali, vengono utilizzate sempre più spesso per verificare la nostra identità, effettuare transazioni online e iscriversi alle piattaforme di social media.
- Visto il valore delle nostre informazioni, hacker e altri malintenzionati che vogliono fare soldi online non si fanno scrupoli a rubarle e venderle sul **dark web**.

Che cosa è il Dark Web?

Il dark web è una **rete nascosta** di siti web non indicizzati dai motori di ricerca.

Dato che tutte le **attività** sul dark web **sono anonime**, sono spesso associate ad **attività illegali**, come la vendita di droga e di armi.

Nel dark web **esistono anche siti web affidabili**, utilizzati per comunicazioni segrete in situazioni di oppressione e per fornire accesso a notizie censurate in alcuni paesi.



Che prezzo hanno i nostri dati nel Dark Web?

Immagine creata com AI

Esempi di vendita dei dati rubati

Post: Selling Network Full Access (Domain Admin)

Electric Power Company - Amman, Jordan - Employees:8,150 Revenue: $719 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 3200$

German Hospitals - Saudi Arabia - Employees: 7,400 Revenue: $1 Billion (Domain Admin+NTDS+Full internall netwrok info) Price: 3500$

Insurance - Thailand - Employees: 520 Revenue: $131 Million (Domain Admin+NTDS+Full internall netwrok info) Price: 1000$

Saudi Arabic governmental health insurance - Full Network Access (Domain Admin+NTDS+Full internall netwrok info) Price: 3000$

Egypt ministry of foreign affairs - Full Network Access(Domain Admin+NTDS+Full internall netwrok info) Price: 5000$

Excerpt of match

I'm selling some logins extraxcted directly from a Juventus database

https://en.wikipedia.org/wiki/[redacted]_F.C.

vulnerability available too.

The records are as follows:

163 employee user – email | password

5 admin user – email | login ! password

Negotiable price.

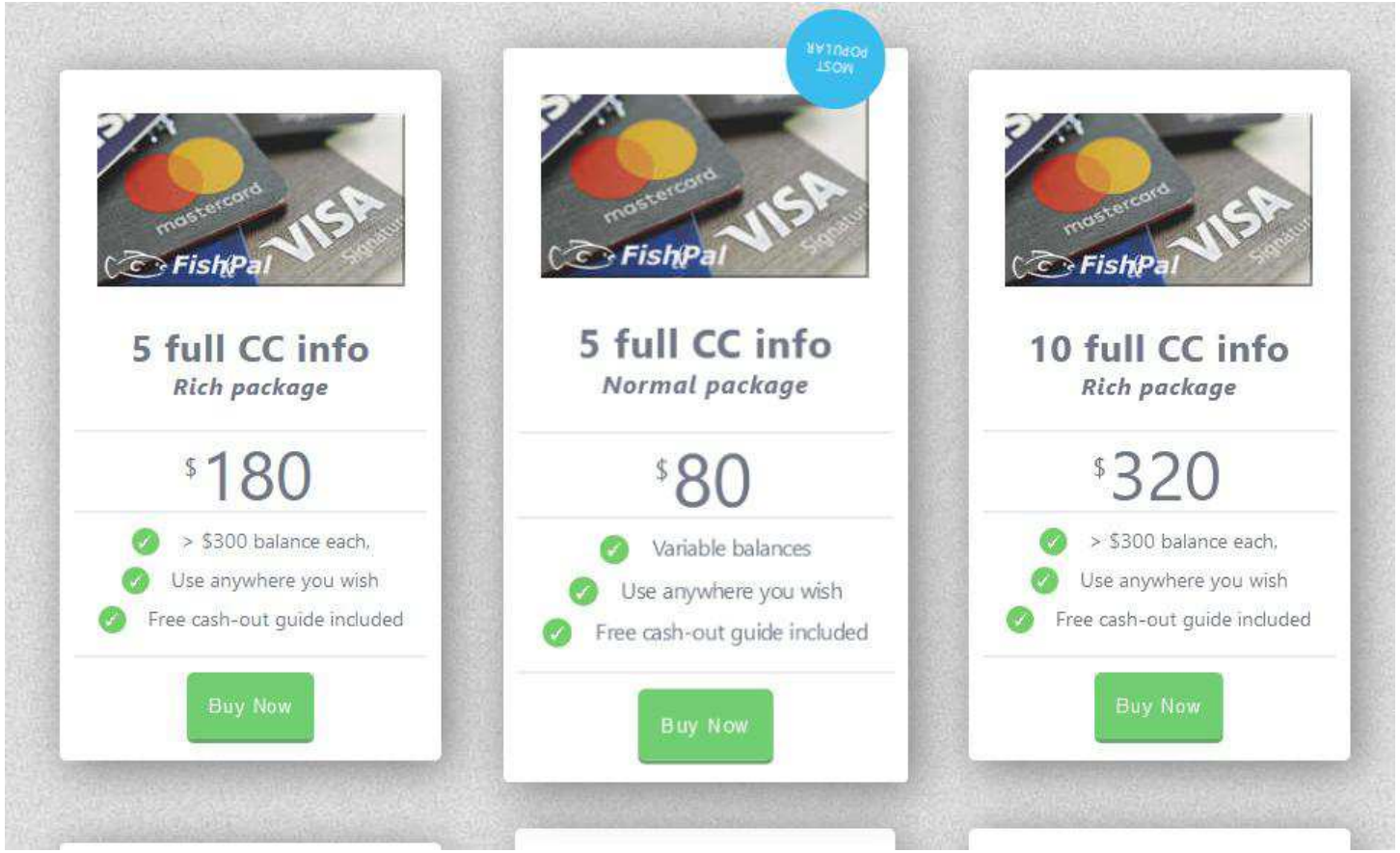
Interess u?

Private

Passports

Indici dei prezzi del Dark web

Product	Price	Quantity
Lithuanian Passport	1350 EUR = 0.01371 Ƀ	1 X Buy now
Netherlands Passport	1500 EUR = 0.01523 Ƀ	1 X Buy now
Denmark Passport	1500 EUR = 0.01523 Ƀ	1 X Buy now
Great Britain Passport	1800 EUR = 0.01828 Ƀ	1 X Buy now
Canada Passport	1250 EUR = 0.01269 Ƀ	1 X Buy now



Pay Pal

Our Classic Paypal Zone

We got fresh new Paypal accounts frequently, as always. Upon buying, you'll receive the Paypal account's details, a matching Socks 5 proxy server det
and a bonus PDF guide for safely cashing out. Click **'Buy this'**, to start the buying procedure! It's simple and only takes a minute.

To prevent double-selling, if you start buying an account, it's state will change to "Locked", so nobody else can buy it again.

Current number of available accounts: **37**
Last updated: 10/28/2025

Internal UID	Balance	Account type	Card	Country	Our Price	Add to cart
UDBTCIQH	1.075 USD	Personal	Yes (confirmed)	United States	$ 118	Buy this!
VXWPLICS	1.859 USD	Personal	Yes (confirmed)	United States	$ 196	Buy this!
PRJGGVHH	1.218 EUR	Premier	Yes (confirmed)	Italy	$ 156	Buy this!
OGPWPGMK	671 USD	Premier	Yes (confirmed)	United States	$ 77	LOCKED
HVFXYMDC	669 GBP	Personal	Yes (confirmed)	United Kingdom	$ 97	Buy this!
LMOWSPCE	706 USD	Personal	Yes (confirmed)	United States	$ 81	LOCKED
XPVENFAZ	1.436 USD	Premier	Yes (confirmed)	United States	$ 154	Buy this!
TSVWIXJL	660 USD	Personal	Yes (confirmed)	United States	$ 76	LOCKED
GTFDTMJV	1.173 USD	Premier	Yes (confirmed)	United States	$ 127	Buy this!
IHAHXRPM	1.776 USD	Personal	Yes (confirmed)	United States	$ 188	Buy this!
MISUKYGY	2.056 USD	Personal	Yes (confirmed)	United States	$ 216	Buy this!

Documenti d'identità

ARTICOLO	*PREZZO
Scansione della patente di guida statunitense	$35
Patente di guida fisica statunitense	$75
Patente di guida fisica UE	$70
Patente di guida fisica non UE (per i paesi europei non appartenenti all'UE)	$65
Scansione del passaporto statunitense	$3
Scansione del passaporto UE	$3

Cybercrime in abbonamento

Ingegneria sociale (Social engineering)

Ingegneria sociale significa l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è, oppure manovrandoli.

Di conseguenza l'ingegnere sociale può usare le persone per strapparle informazioni con o senza l'ausilio di strumenti.

Kevin D. Mitnick – L'arte dell'inganno

Ingegneria sociale: manipolare le persone, non i sistemi

- **Autorità:** “Sono il presidente della vostra sezione, ho bisogno della password del ripetitore con urgenza”
- **Urgenza:** “Devi agire adesso o perdi il callsign”
- **Reciprocità:** qualcuno ti ha fatto un favore e ora chiede qualcosa in cambio
- **Familiarità:** il criminale usa il tuo nome, il tuo callsign, riferimenti al tuo ultimo contest
- **Paura:** “Il tuo computer ha un virus, chiama subito questo numero”

Phishing (ingegneria sociale)

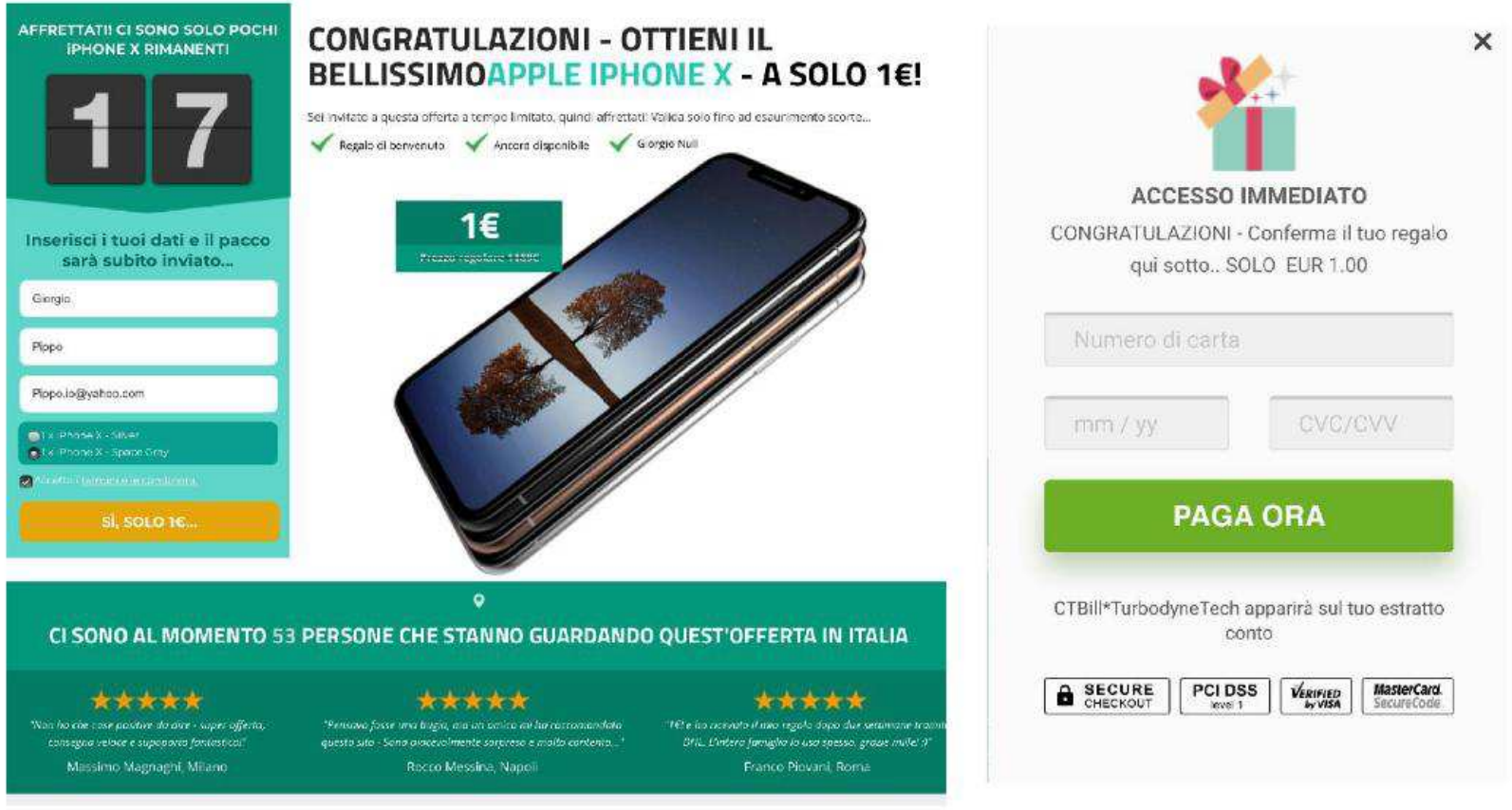
Un attacco di phishing è una **tecnica di ingegneria sociale** utilizzata da cybercriminali **per ingannare gli utenti** e indurli a rivelare informazioni sensibili, come credenziali di accesso, dati bancari o personali.
Questo tipo di attacco **si sviluppa generalmente in più fasi**, che seguono una logica ben precisa, vediamole.

Il ciclo dell'attacco: come si preparano prima di colpire

Gli attacchi mirati non avvengono mai all'improvviso.
I criminali seguono un processo metodico:

1. **Ricognizione:** raccolgono informazioni (QRZ, social, siti club, log contest pubblici)
2. **Costruzione del pretesto**: creano uno scenario credibile usando i dati raccolti
3. **Attacco:** email, messaggio, telefonata o accesso diretto
4. **Sfruttamento:** accesso ai sistemi, furto dati, installazione malware
5. **Persistenza e monetizzazione**: rimangono nascosti o vendono i dati
6. **Cancellazione delle tracce** e installazione software maligno (backdoor)

NON SERVONO TRUCCHI RAFFINATI... PER FARE PHISHING



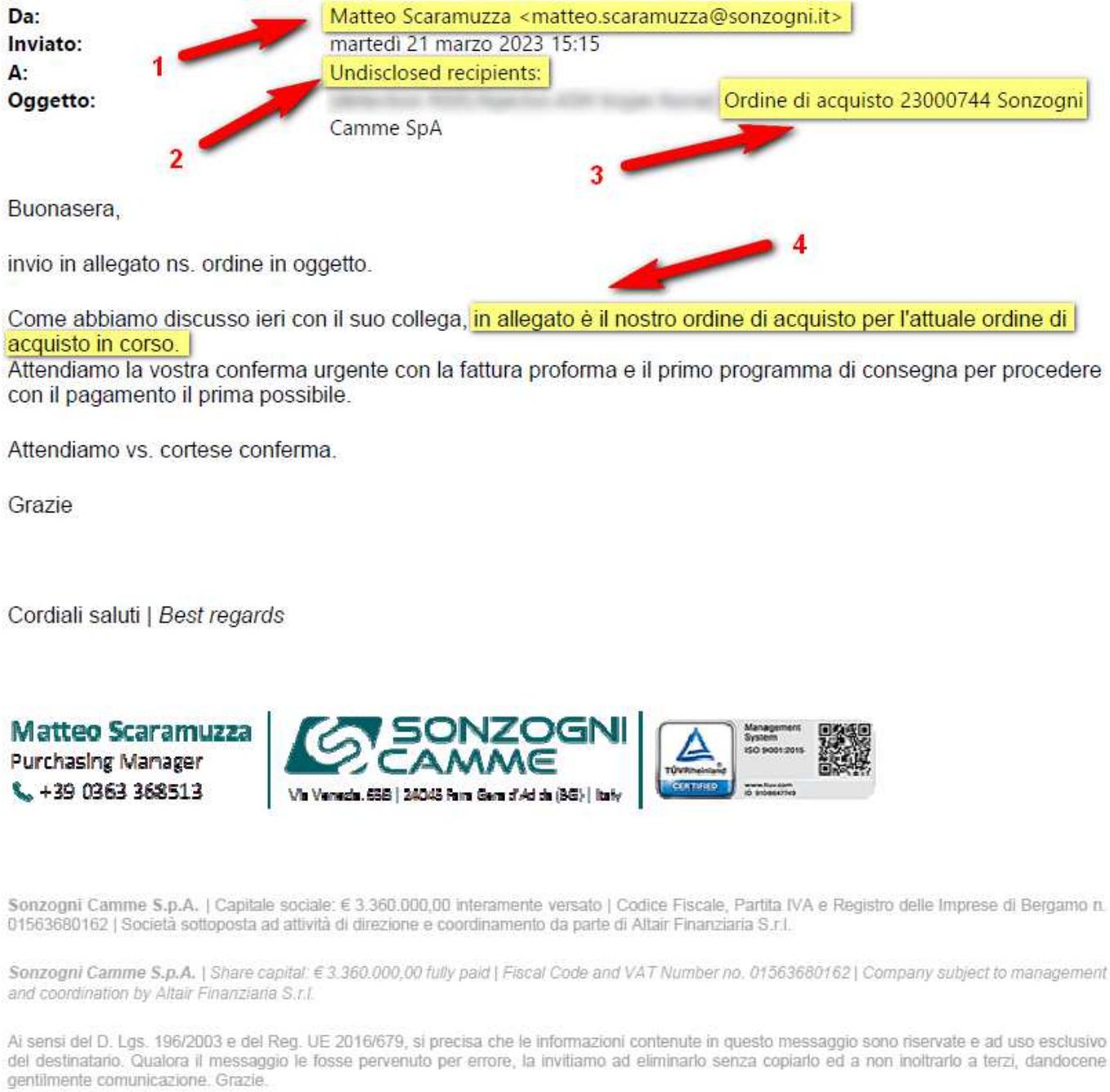
Fonte:
www.giorgiosbaraglia.it

Phishing

Punti da controllare:

1. Nome del mittente (sembra corrispondere)
2. Indirizzo mail (il dominio corrisponde a quello della società mittente)
3. Oggetto (è riferito a qualche ordine/commessa conosciuta?)
4. L'italiano non sembra molto corretto

Il controllo non è stato superato.



Da: Matteo Scaramuzza <matteo.scaramuzza@sonzogni.it>
Inviato: martedì 21 marzo 2023 15:15
A: Undisclosed recipients:
Oggetto: Ordine di acquisto 23000744 Sonzogni Camme SpA

1
2
3
4

Buonasera,

invio in allegato ns. ordine in oggetto.

Come abbiamo discusso ieri con il suo collega, in allegato è il nostro ordine di acquisto per l'attuale ordine di acquisto in corso.
Attendiamo la vostra conferma urgente con la fattura proforma e il primo programma di consegna per procedere con il pagamento il prima possibile.

Attendiamo vs. cortese conferma.

Grazie

Cordiali saluti | *Best regards*

Matteo Scaramuzza
Purchasing Manager
+39 0363 368513

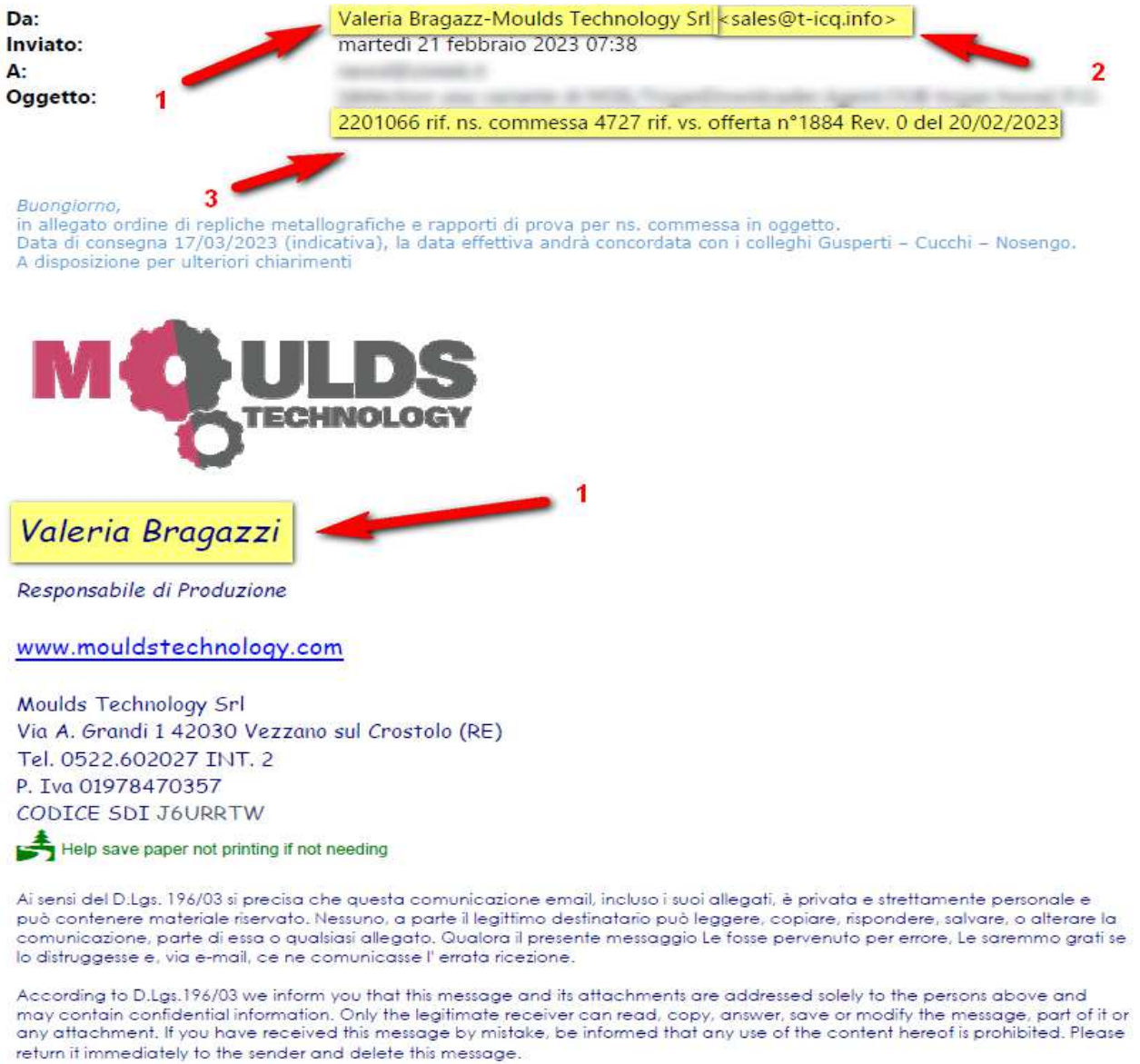
SONZOGNI CAMME
Via Venezia, 55B | 24048 Pena Gera d'Ad da (BG) | Italy

Management System ISO 9001:2015 CERTIFIED

Phishing

- Punti da controllare:
  1. Nome del mittente (sembra corrispondere)
  2. Indirizzo mail (il dominio non corrisponde a quello della società mittente)
  3. Oggetto (è riferito a qualche ordine/commessa conosciuta?)

Il controllo non è stato superato.



📡 Scenario reale per radioamatori:

- **Ricevi una email** apparentemente da QRZ.com:
  "Il tuo account ha rilevato accessi sospetti dalla Cina.
- **Clicca qui** per verificare la tua identità e proteggere il tuo callsign."
- **Il link** porta a un sito identico a QRZ, ma falso.
- **Inserisci le credenziali** e il tuo account è compromesso.

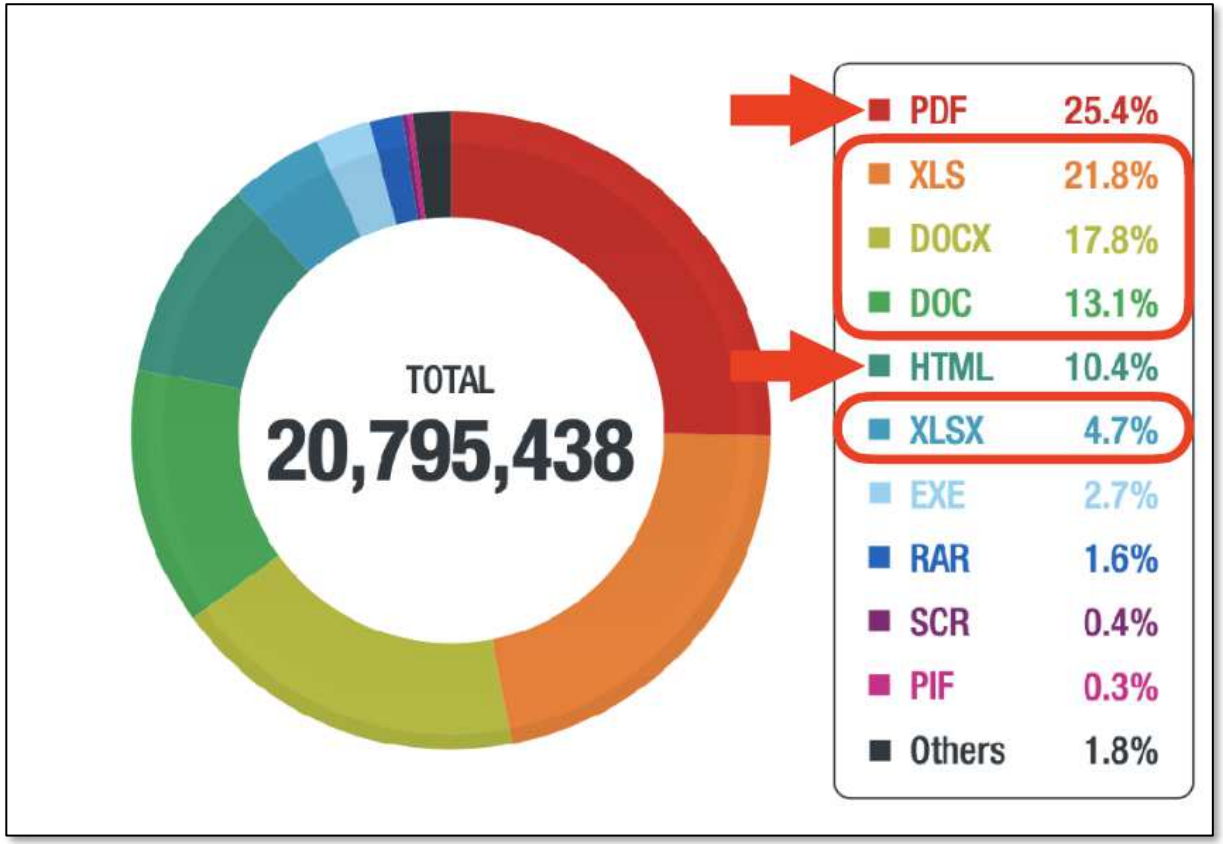
I segnali di allarme da riconoscere sempre:

- **Urgenza artificiale:** “Agisci entro 24 ore o il tuo account sarà sospeso”
- **Indirizzo mittente** con piccole variazioni: qrz-support@qrz.net invece di @qrz.com
- **Link** che al passaggio del mouse mostrano URL diversi dal testo
- **Richiesta di credenziali**, numeri di carta o dati personali via email
- **Allegati non attesi**, anche da mittenti apparentemente noti

I TIPI DI FILE PIÙ USATI COME ALLEGATI

I file più usati come allegati, per inoculare un malware, sono quelli più utilizzati dagli utenti:
Pdf, Excel, Word.

***Attenzione ai file di Office con macro*.**



Importante quindi disabilitare l'uso delle macro in Office

Fonte:
www.giorgiosbaraglia.it

Tipi di attacco:

varianti del phishing

WHALING: dall'inglese whale (balena), per indicare un phishing nel quale si punta a far abboccare un pesce grande

SPEAR PHISHING: attacco mirato verso un «pesce» specifico

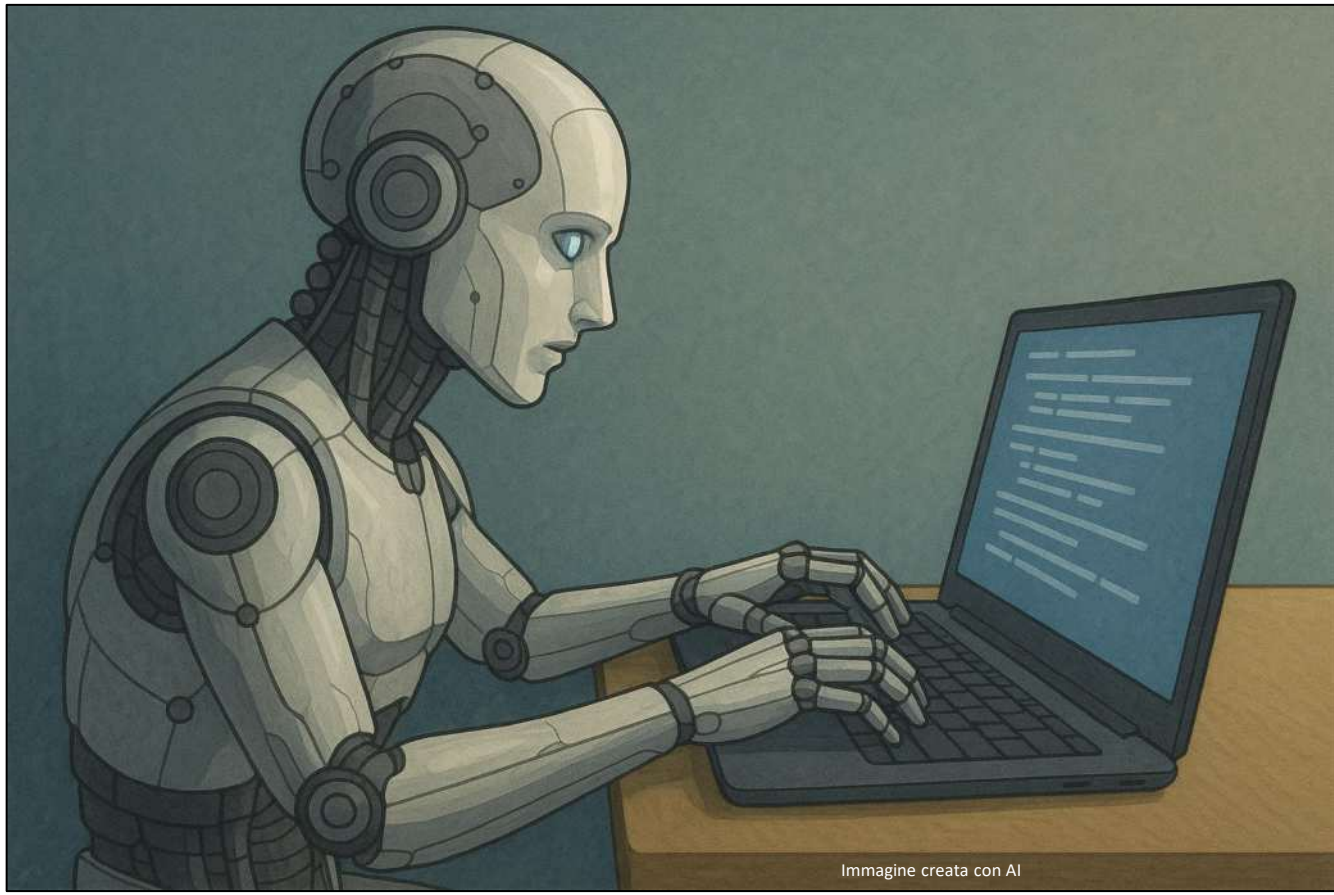
SMISHING: “SMS phishing”, realizzato attraverso l’invio di messaggi su dispositivi mobili.

VISHING: “phishing vocale”. La parola è una crasi tra Voice e Phishing ed indica una truffa telefonica.

QRISHING: “QR Codes+Phishing”. L'attacco è sotto forma di un codice QR, che indirizza a un link web contenente malware.

Phishing con AI

https://www.facebook.com/reel/1988354291929338



Come accedere ai siti - gli URL

Questa forse è la parte più difficile … ma è quella che vi salva la vita!

Un URL, acronimo di Uniform Resource Locator, è un indirizzo web che punta a un sito specifico, a una pagina web o a un documento su internet.

Contiene vari elementi, tra cui il **protocollo di comunicazione di rete**, un **sottodominio**, un **nome di dominio** e la sua estensione.

Esempi di URL

https://www.aritreviso.it

https	protocollo di comunicazione di rete
.it	dominio di 1° livello
.aritreviso	dominio di 2° livello
www	dominio di 3 livello

https://it.wikipedia.org

https://www.aruba.it

Esempi di URL

https://www.microsoft.com/it-it/microsoft-365

/it-it	sezione del sito in lingua italiana
/microsoft-365	sezione del sito relativa al 365

Esempi di URL

https://www.microsoft.com/it-it/microsoft-365?market=it&doc=1

?	inizia la parte dei parametri passati alla pagina
market=it	parametro «market» con valore «it»
&	permette di passare più parametri alla pagina

Esempi di URL

https://www.microsoft.com/it-it/microsoft-365?market=it#Featured-news

#	indica una sezione della pagina
Featured-news	nome della sezione della pagina

URL falsificati: il typosquatting

Il typosquatting è la registrazione in malafede di un nome di dominio molto simile ad uno famoso. Deriva dalla crasi di «typo» (errore di battitura) e «squat» (occupare abusivamente).

Questi link NON SONO LA STESSA COSA:

https://account.google.com/ServiceLogin

https://account.google.com.ServiceLogin.it/

dove:

- .com – dominio di 1° livello
- .google – dominio di 2° livello
- account – dominio di 3 livello
- ServiceLogin – pagina del sito

Fonte: www.giorgiosbaraglia.it

URL falsificati

Originale	google.com	microsoft.com	facebook.com	domus.it
FALSO	go0gle.com	mlcrosoft.com	facebo0k.com	dornus.it
FALSO	gooogle.com	microsoff.com	facebbok.com	domus.lt

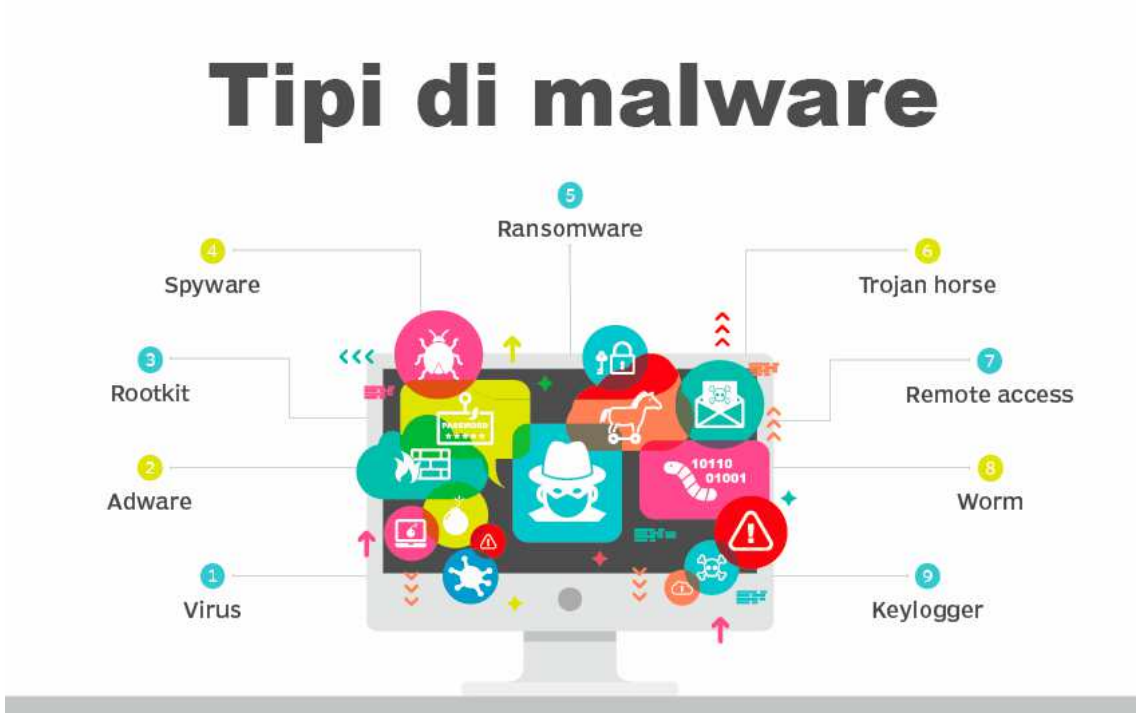
Fonte:
www.giorgiosbaraglia.it

Come tutelarsi?

- **Leggere attentamente l'URL** a cui stiamo accedendo
- **Digitare direttamente l'URL** nella barra degli indirizzi del browser e non fare clic sul link nella mail
- Fare **clic con il pulsante destro** sul link e scegliere «Copia collegamento ipertestuale» dal menu che si apre; copiare il link in un documento word o del blocco note per esaminare il link

Malware

Malicious software, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.



Ransomware la minaccia più temibile

È un tipo di malware che limita l'accesso del dispositivo che infetta, **richiedendo un riscatto** (ransom in inglese) da pagare per rimuovere la limitazione.

Ad esempio alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altre invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro.

RANSOMWARE: I vettori d’infezione

I vettori d’infezione utilizzati dai ransomware sono sostanzialmente i medesimi usati per gli altri tipi di attacchi malware:

1) Email di phishing: il più diffuso, oltre il 75% degli attacchi è portato con messaggi di posta elettronica.
2) Navigazione su siti compromessi: il cosiddetto “drive-by download” da siti nei quali sono stati introdotti exploit kit che sfruttano vulnerabilità dei browser, di Flash Player o altri.
3) Utilizzando un supporto rimovibile: per esempio una chiavetta USB armata con il software malevolo. Questa tecnica si chiama “Baiting” (esca).
4) All’interno (in bundle) di altri software che vengono scaricati: programmi gratuiti che ci promettono di “crackare” software costosi per utilizzarli senza pagare (per esempio: Microsoft Office e Adobe Photoshop CC).

Fonte:
www.giorgiosbaraglia.it

RANSOMWARE: Come difendersi

- **Non aprire mai gli allegati** di email di dubbia provenienza
- Trattare le **email anche di mittenti conosciuti** come **potenzialmente sospette**: potrebbero essere state compromesse.
- Abilitare l'opzione "**Mostra estensioni nomi file**" nelle impostazioni di Windows.
- Attenzione alle **chiavette USB** e altri supporti rimovibili.
- **Disabilitare l'esecuzione di macro** da parte di componenti Office (Word, Excel, PowerPoint ecc...).

Fonte (Sbaraglia): https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/#Come_proteggersi_dai_ransomware_tre_punti_chiave

Dopo il Dark Web arriva la Dark AI

https://www.facebook.com/reel/809352471580967

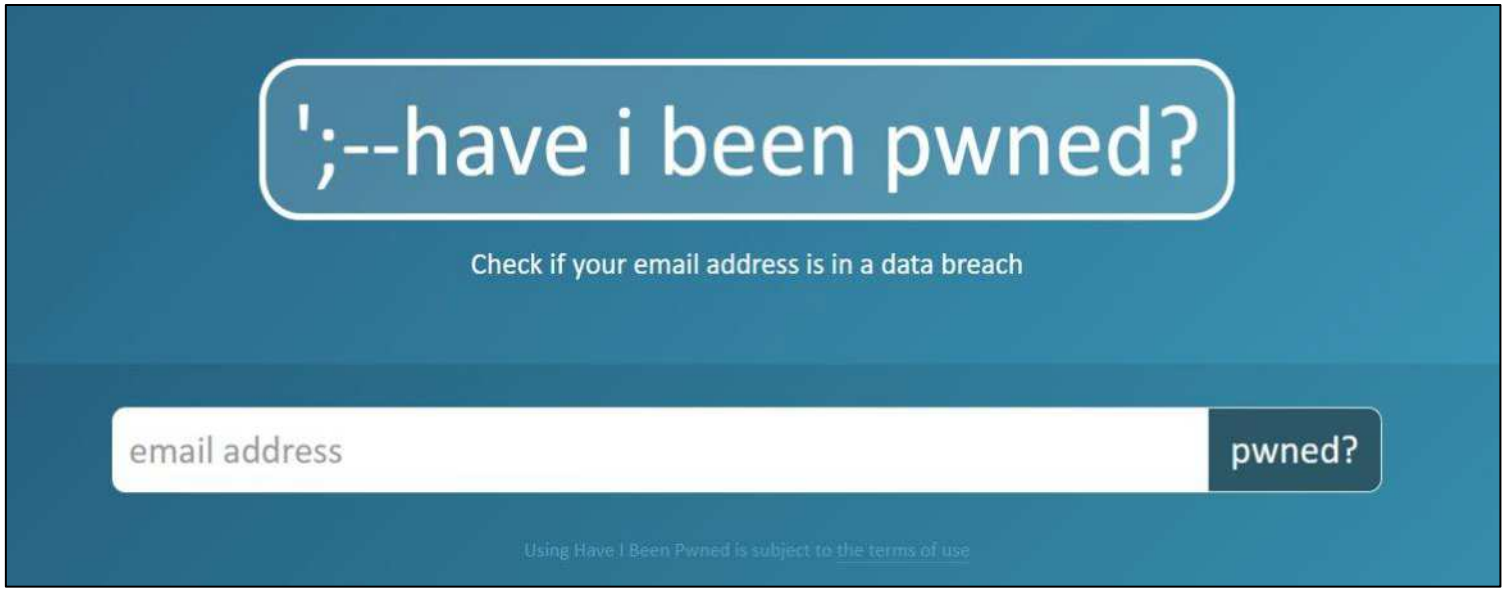
Immagine creata con AI

Un aiuto per controllare virus e file sospetti

https://www.virustotal.com/gui/home/url

https://www.virustotal.com/gui/home/upload

Un aiuto per verificare se la propria mail è compromessa



https://haveibeenpwned.com/

PASSWORD

Password – Come renderle sicure

I tempi per il successo di un attacco di forza bruta **dipendono dalla potenza dei computer usati**; maggiore la potenza usata, minore il tempo di individuazione della password.

Oltre alla lunghezza, non si devono usare nomi o parti di parole che si possono trovare in un dizionario

12 caratteri!
Sono la soluzione corretta
OGGI

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS

› Learn how we made this table at hivesystems.io/password

Password – I password manager

I password manager sono dei servizi cloud (esistono anche da installare in locale ma sono limitati al singolo dispositivo) che memorizzano le credenziali dei nostri account ed anche altre informazioni utili (ad es. carte di credito).

Vantaggi:

- Occorre ricordare una sola password molto complessa (master password)
- I dati sono cifrati con algoritmi forti (AES 256)
- Possono generare password complesse in automatico
- Riempiono in automatico i moduli web

Password- L’autenticazione a più fattori

L’autenticazione a più fattori (MFA – Multi Factor Authentication) si basa *sull’utilizzo congiunto di due o più metodi di autenticazione* indipendenti tra di loro:

1. Una cosa che conosco (password o PIN)
2. Una cosa che ho (app certificata, smartphone per gli SMS, token fisico)
3. Una cosa che sono (riconoscimento biometrico di impronta digitale, volto, retina, voce, ecc.)

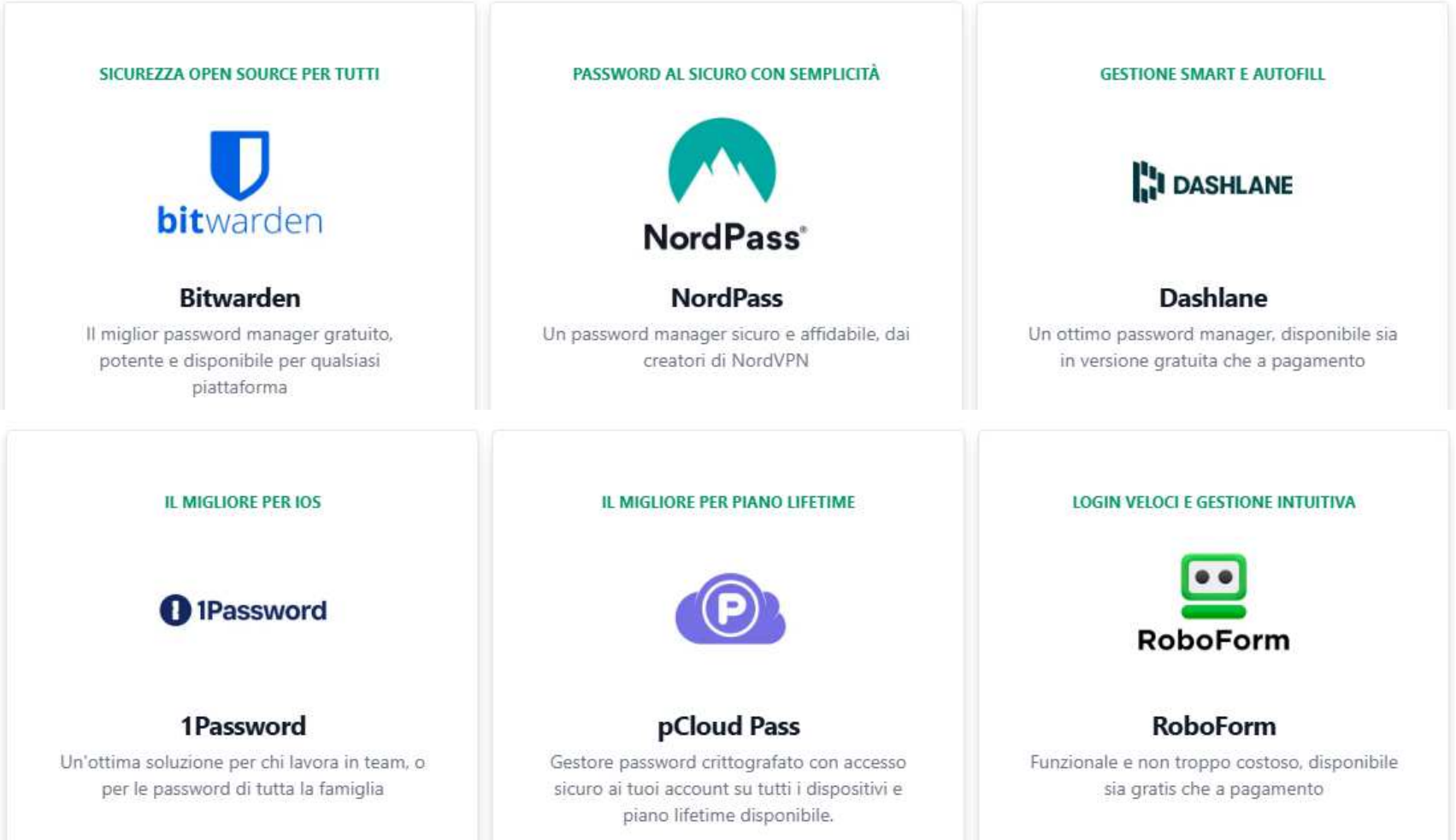
La combinazione di due metodi è la cosiddetta 2FA (autenticazione a due fattori), quella che li utilizza tutti e tre è la 3FA (autenticazione a tre fattori).

Password- L’autenticazione a più fattori

Alcuni metodi utilizzati:

- *Invio di SMS con un codice usa e getta*: vulnerabile perché facilmente intercettabile e soggetto a frodi
- *Invio di una MAIL con un codice usa e getta*: meno vulnerabile ma soggetto comunque ad attacchi
- *Applicazioni certificate e dedicate*: Microsoft Authenticator, Google Authenticator, ArubaOTP, ecc.); viene creata una chiave univoca che permette di associare la specifica istanza dell’app con l’utente ed il dispositivo
- **Potete attivarla su:** qrz.com clublog.com …

Migliori password manager gratis



A sinistra alcuni esempi.
Ma basta cercare sui motori di ricerca o chat gpt con:
«*i 10 migliori password manager gratis*»

Password e autenticazione
La gestione delle password è il fondamento di ogni difesa personale.

Le regole essenziali:

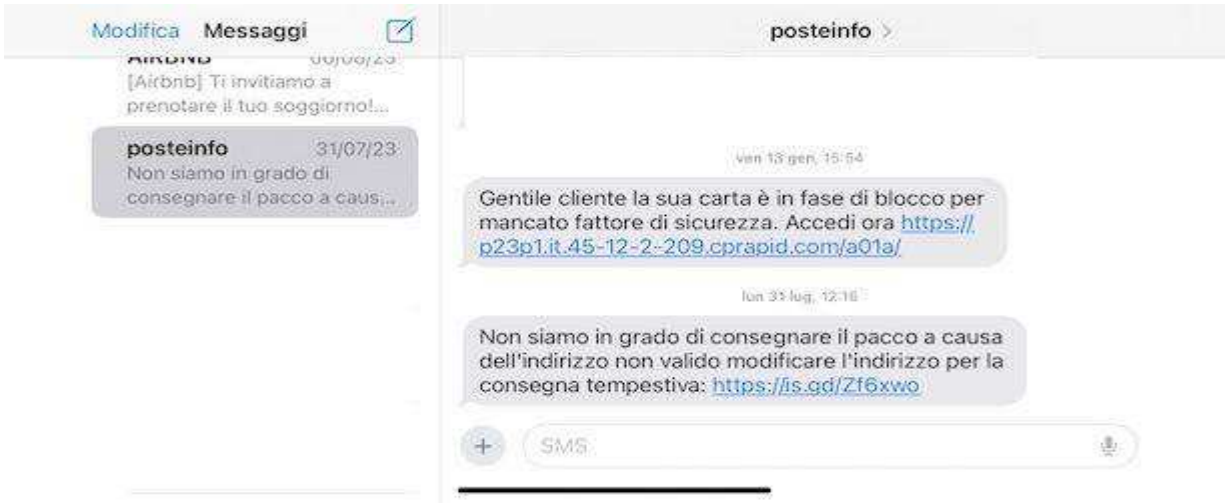
- **Usa password diverse** per ogni account – senza eccezioni
- **Usa un password manager** (Bitwarden, KeePassXC): ricorda solo una master password
- **Abilita l'autenticazione a due fattori** (2FA) su tutti i servizi critici: email, LoTW, QRZ, PayPal
- **Preferisci app authenticator** (Google Authenticator, Aegis) all'SMS che può essere intercettato
- **Verifica periodicamente se le tue credenziali** sono trapelate su haveibeenpwned.com

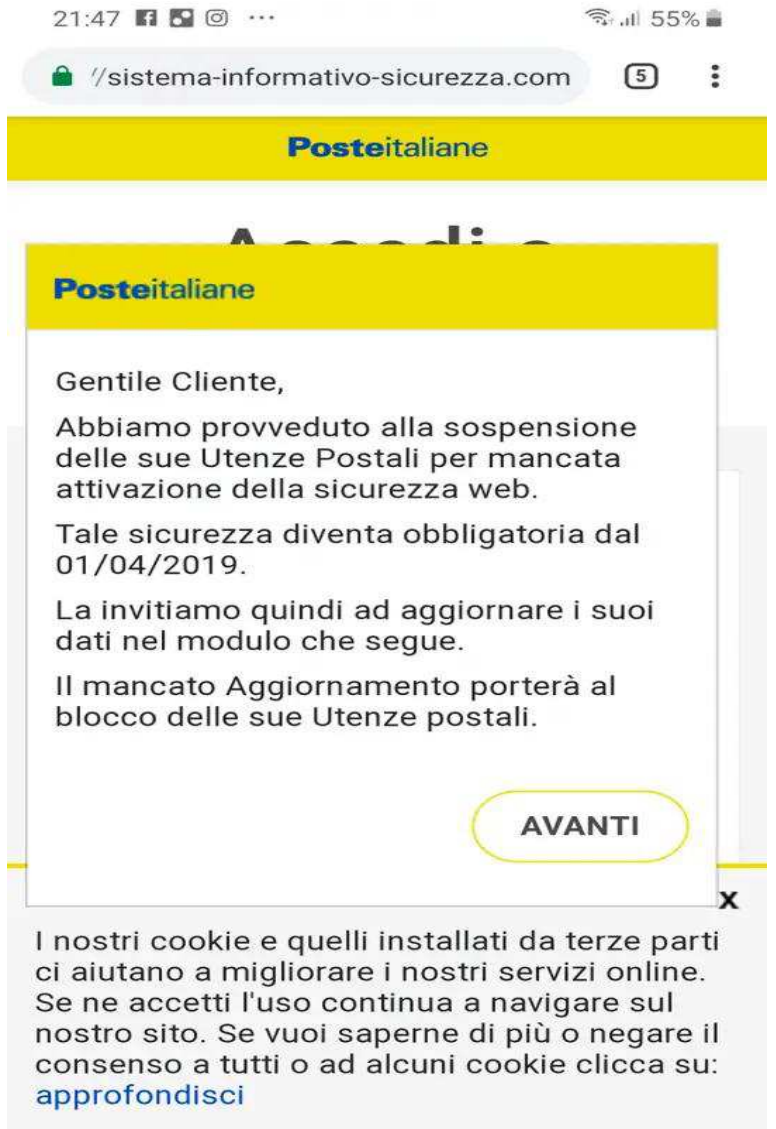
DISPOSITIVI MOBILI

SMishing


SMS
oggi 16:55
Banca N26
ATTENZIONE! il Suo Conto Verra' Sospeso Per Evitare La Sospensione Clicca Su' https://banca-n26-sicuro-com.preview-domain.com (N26)


ALERT BNL
Spoofing
Giovedì 29 Febbraio
BNL: é stato effettuato un pagamento di 256,47 EUR con la tua carta **** presso PayPal. Se non riconosci questo pagamento, bloccalo: https://bit.ly/interBNPP
14:46


Modifica
Messaggi
posteinfo
[Airbnb] Ti invitiamo a prenotare il tuo soggiorno!...
posteinfo 31/07/23
Non siamo in grado di consegnare il pacco a caus...
posteinfo
Gentile cliente la sua carta è in fase di blocco per mancato fattore di sicurezza. Accedi ora https://p23p1.it.45-12-2-209.cprapid.com/a01a/
Non siamo in grado di consegnare il pacco a causa dell'indirizzo non valido modificare l'indirizzo per la consegna tempestiva: https://is.gd/Zf6xwo
SMS


21:47
55%
//sistema-informativo-sicurezza.com
5
Posteitaliane
Posteitaliane
Gentile Cliente,
Abbiamo provveduto alla sospensione delle sue Utenze Postali per mancata attivazione della sicurezza web.
Tale sicurezza diventa obbligatoria dal 01/04/2019.
La invitiamo quindi ad aggiornare i suoi dati nel modulo che segue.
Il mancato Aggiornamento porterà al blocco delle sue Utenze postali.
AVANTI
I nostri cookie e quelli installati da terze parti ci aiutano a migliorare i nostri servizi online. Se ne accetti l'uso continua a navigare sul nostro sito. Se vuoi saperne di più o negare il consenso a tutti o ad alcuni cookie clicca su: approfondisci

Phishing su WhatsApp

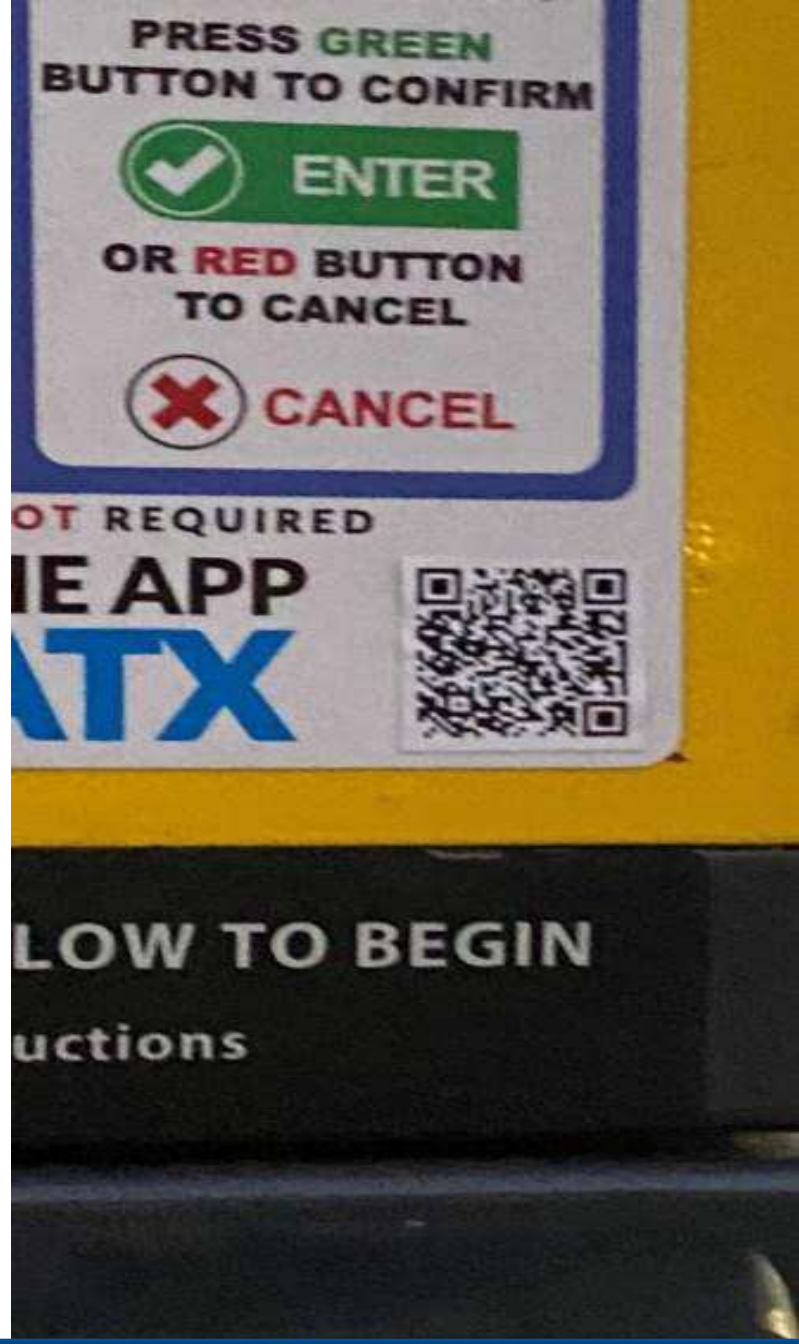
Truffa del figlio in difficoltà

QRishing

Il Dipartimento di Polizia di Austin (Texas) ha comunicato che sono stati apporti dei QRCode fraudolenti su alcuni parchimetri.

Le persone pagavano un sito truffa e non il parcheggio.

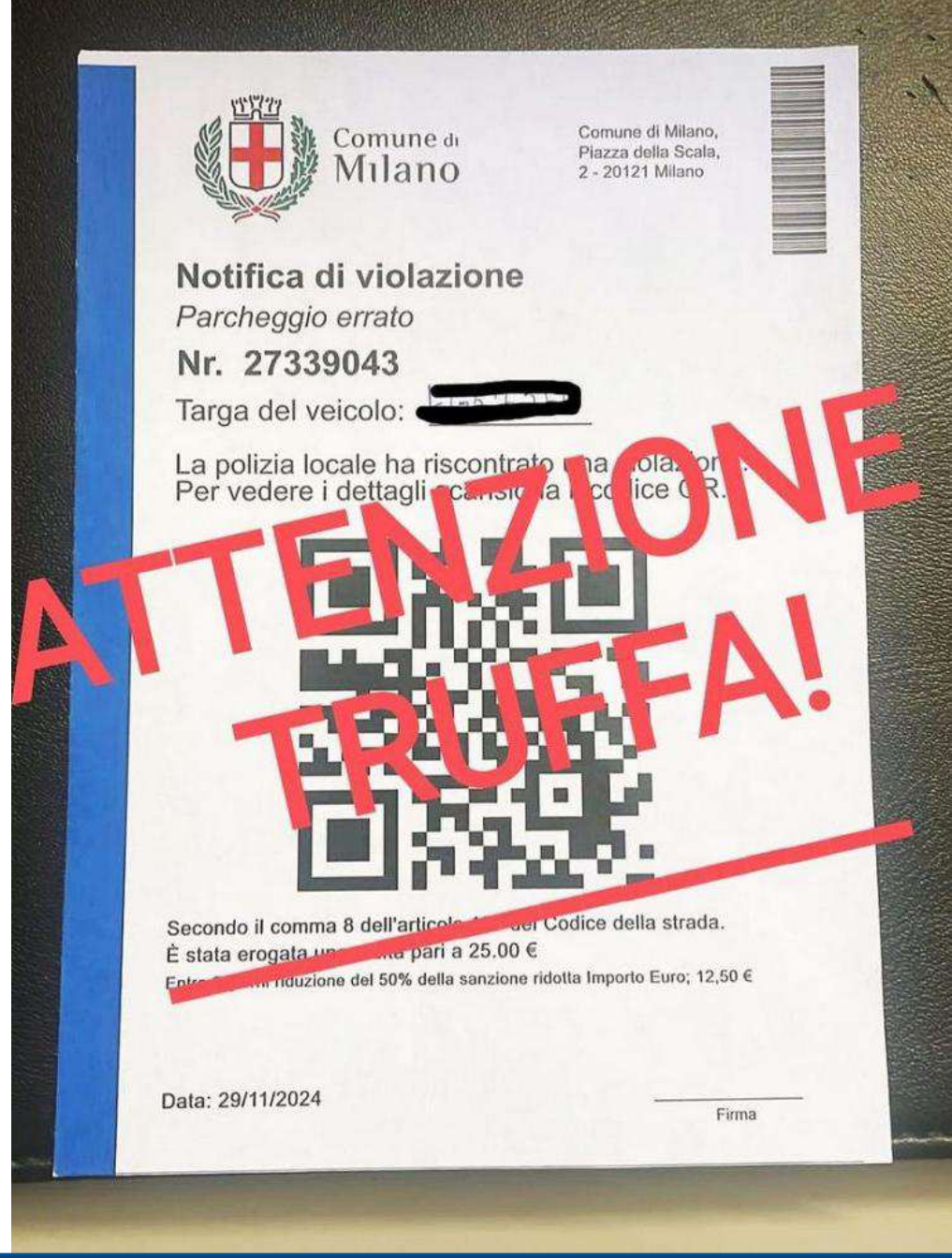
(soldi rubati e multa per mancato pagamento del parcheggio…)



QRishing
Multa Comune Milano

In diverse zone di Milano, sono state individuate multe false sui parabrezza delle vetture in sosta.

Sui fogli era ben visibile un QR code, con tanto di stemma del Comune di Milano, e la dicitura “notifica di violazione – parcheggio errato”.



Juice Jacking

- I criminali hanno trovato il modo di **infettare i dispositivi** mobili tramite le **porte USB di ricarica** disponibili in luoghi pubblici (aeroporti, treni, centri commerciali, ecc.).
- Il Juice Jacking consiste nel tentativo di accedere ai dati contenuti nello smartphone utilizzando come canale di comunicazione il cavo (jack) di alimentazione (juice) usb. Infatti, c'è un dettaglio che non va mai dimenticato: il cavo usb non serve soltanto per ricaricare, ma viene utilizzato anche per la trasmissione di dati e per sincronizzare uno smartphone e un computer.

Juice Jacking

Come proteggersi?

- ricaricare il dispositivo mobile **usando l'alimentatore** in dotazione collegato a una presa di energia elettrica;
- in alternativa all'alimentatore, è consigliabile utilizzare una batteria di riserva (**power bank**);
- se proprio non si può fare a meno di utilizzare una porta USB pubblica per la ricarica dello smartphone, è consigliabile usare un **cavo USB per sola alimentazione/ricarica**, quindi privo dei "fili" utilizzati per la trasmissione di dati;
- come ultima alternativa, **spegnere il telefono prima di metterlo in carica.**

Le nuove truffe che non immaginate e come non caderci

https://www.facebook.com/reel/747866948278221

Immagine creata con AI

Decalogo di sicurezza per i dispositivi mobili

1. Richiedere l'autenticazione dell'utente (PIN, password, biometria, …); non usare PIN facili
2. Crittografare i dati sui dispositivi mobili
3. Mantenere aggiornati il sistema operativo e le applicazioni
4. Evitare il collegamento a reti Wi-Fi pubbliche, libere o gratuite (se lo fate usate una VPN)
5. Limitare il download di applicazioni alle sole fonti affidabili (Google Play Store o Apple Store)
6. Non dimenticate di attivare il backup

Decalogo di sicurezza per i dispositivi mobili

7. Attivare l’accesso remoto ai dati e la loro cancellazione
8. Navigare solo su siti web sicuri
9. Non ricaricare il telefono via USB da porte sconosciute (es. treno, aeroporti, hotel, ecc.) (Juice Jacking)
10. Non collegare il dispositivo via bluetooth o altro a periferiche sconosciute o non di proprietà (es. auto a noleggio, stampanti)
11. In caso di vendita, cessione o rottamazione riportarlo alle condizioni di fabbrica e cancellare tutti i dati presenti anche su eventuali memorie esterne

Decalogo di sicurezza per i dispositivi mobili

12. Non fare clic sui link nei messaggi a meno che non si possano verificare o si è assolutamente certi del mittente
13. Utilizzare i QRCode sole se provengono da fonti affidabili
14. Effettuare il logout dai siti web e dalle applicazioni dopo l'utilizzo
15. Non fornire MAI informazioni personali tramite messaggi
16. Per i dispositivi mobili aziendali utilizzare un MDM (Mobile Device Management)

Fonte: www.giorgiosbaraglia.it

Abbiamo parlato di VPN ma cosa è?

Cos’è

- Un tunnel sicuro che protegge la connessione Internet
- Cifra i dati e nasconde l’indirizzo IP
- Permette di collegarsi alla rete aziendale da remoto in modo sicuro

Perché è importante

- Previene intercettazioni su Wi-Fi pubblici
- Riduce il rischio di accessi non autorizzati
- Garantisce privacy e protezione dei dati

Quando usarla

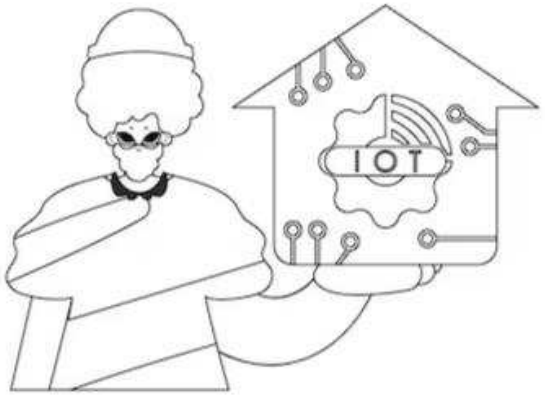
- Smart working / accesso ai servizi interni
- Connessioni da hotel, aeroporti, bar
- Ogni volta che serve proteggere informazioni sensibili

Immagine creata con AI

IOT – Internet Of Things

IOT – Dal Microsoft Digital Defense Report

- Nel 78% dei device IoT con Vulnerabilità conosciute, abbiamo il 46%, quasi la metà, senza possibilità di patch (ovvero il 36% in assoluto);
- 25% dei dispositivi OT usa software non supportato (senza possibilità di patch);
- 96% delle applicazioni usa componenti software Open Source;
- Registrato un +742% dal 2010 degli attacchi su software Open Source;
- 57% dei firmware device OT risulta esposto a più di 10 CVE conosciute.



Come avviene il furto di un’auto

Ham Radio

Software radio: il vettore nascosto

- **I criminali caricano versioni modificate dei programmi più usati su siti di terze parti e forum**.
- **WSJT-X e JTDX (FT8/FT4):** i più scaricati al mondo nel digitale HF – bersaglio principale.
- **CHIRP**: programmazione ricetrasmettitori – versioni false diffuse su gruppi Telegram e forum.
- **Driver SDR:** RTL-SDR, SDR#, GQRX – spesso scaricati da siti specchio non verificati.
- **Software contest:** N1MM, Log4OM, DXKeeper – installatori con malware incluso.
- **Regola d'oro:** scarica SEMPRE dai siti ufficiali degli sviluppatori. Verifica il checksum MD5/SHA256.
- Non installare mai software 'pre-attivato' o con 'patch' da forum o gruppi social.

Ripetitori e reti digitali: infrastruttura a rischio

- **I ripetitori connessi a internet (Echolink, IRLP, D-STAR, DMR) sono infrastrutture critiche per la comunità.**
- Accesso non autorizzato ai nodi Echolink con credenziali deboli o di default mai cambiate.
- Denial of Service: saturazione del ripetitore con trasmissioni continue – blocco totale del servizio.
- Compromissione del controller via interfaccia web esposta direttamente su internet.
- Durante attivazioni di emergenza, un ripetitore compromesso può interferire con Protezione Civile.
- Difendersi: cambia sempre le credenziali di default, non esporre la gestione su internet, usa VPN.
- Monitora i log di accesso ai nodi Echolink/IRLP. Limitare i comandi DTMF critici con codici robusti.

Decalogo di sicurezza per il radioamatore digitale

- **Usa password diverse** per ogni account (QRZ, LoTW, eQSL, email, router) – senza eccezioni.
- **Attiva l'autenticazione a due fattori** (2FA) su tutti i servizi critici: email, LoTW, QRZ.
- **Usa un password manager** (Bitwarden, KeePassXC) – ricorda solo una master password.
- **Scarica software radio SOLO dai siti ufficiali**. Verifica sempre il checksum MD5/SHA256.
- **Aggiorna firmware del router**, **cambia le credenziali di default**, segmenta la rete radio.
- Cambia le credenziali di default del controller del ripetitore. Non esporlo su internet.
- **Verifica se le tue email sono state compromesse**: haveibeenpwned.com.
- **Prima di cliccare un link,** verifica sempre l'URL reale. Diffida delle urgenze via email.
- **Non condividere mai credenziali** via WhatsApp, Telegram o email, neanche con 'amici'.
- **In caso di attacco:** disconnetti, cambia password da altro dispositivo, segnala a Polizia Postale.

Aggiornamenti e sicurezza dei dispositivi

- **Aggiorna sempre il sistema operativo**, il browser e il software radioamatoriale
- **Aggiorna il firmware del router** di casa e cambia le credenziali di default
- **Disabilita servizi di gestione remota** non utilizzati (Telnet, UPnP)
- **Segmenta la rete**: metti gli apparati radio su una VLAN separata dalla rete di casa
- **Fai backup regolari** dei log radio, configurazioni e dati importanti (regola 3-2-1)

I primi passi in caso di compromissione

- **Disconnetti il dispositivo dalla rete** (non spegnere: potresti perdere prove forensi)
- **Cambia le password** da un dispositivo diverso e sicuro
- **Avvisa gli altri utenti** che potrebbero essere stati coinvolti (soci del club, ripetitore)
- **Segnala l'incidente** alla Polizia Postale (www.commissariatops.it)
- **Contatta la tua banca** se dati finanziari potrebbero essere stati compromessi
- **Documenta tutto**: screenshot, email, orari degli eventi anomali

IL SUCCO DEL DISCORSO..

Fonte:
www.giorgiosbaraglia.it

Links

I video di Marco Camisani Calzolari su Facebook: https://www.facebook.com/marcocamisanicalzolari

Rapporto Clusit – www.clusit.it (per richiedere copia dell'ultimo rapporto Clusit)

Agenzia per la Cybersicurezza Nazionale – www.acn.gov.it

www.giorgiosbaraglia.it (una miniera di informazioni)

www.cybersecurity360.it (la rivista italiana online migliore per la Cybersecurity)

https://www.nomoreransom.org/it/index.html (sito creato dalla polizia olandese e altri per difendersi)

https://www.cybersecurity360.it/nuove-minacce/ransomware/ransomware-cose-come-rimuoverlo-e-come-difendersi/ (un articolo molto dettagliato sul ransomware)

https://www.virustotal.com/gui/home/upload (sito per controllo files)

https://www.virustotal.com/gui/home/url (sito per controllo URL)

https://sitecheck.sucuri.net/ (malware scanner per verificare siti web)https://haveibeenpwned.com/ (per verificare se la propria mail è compromessa)

https://www.youtube.com/watch?v=qYnmfBiomlo (spot belga su ingenuità gente)

https://cert-agid.gov.it/statistiche/ (Statistiche CERT-AGID attacchi in corso)

https://www.cybersecurity360.it/nuove-minacce/ransomware/attacchi-ransomware-alle-aziende-italiane-2023-in-aggiornamento/ (Attacchi rivendicati nell'anno)

https://www.gpdp.it/web/guest/temi/cybersecurity/smishing (guida del Garante Privacy allo SMSishing

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (attacco a Maersk)

NON IMPORTA CHI SEI

NON IMPORTA COSA FAI

NON IMPORTA
CON COSA LO FAI

PRIMA O POI
TI ATTACCHERANNO...

(cit. Alessio L.R. Pennasilico, membro comitato scientifico CLUSIT)

Immagine creata con AI

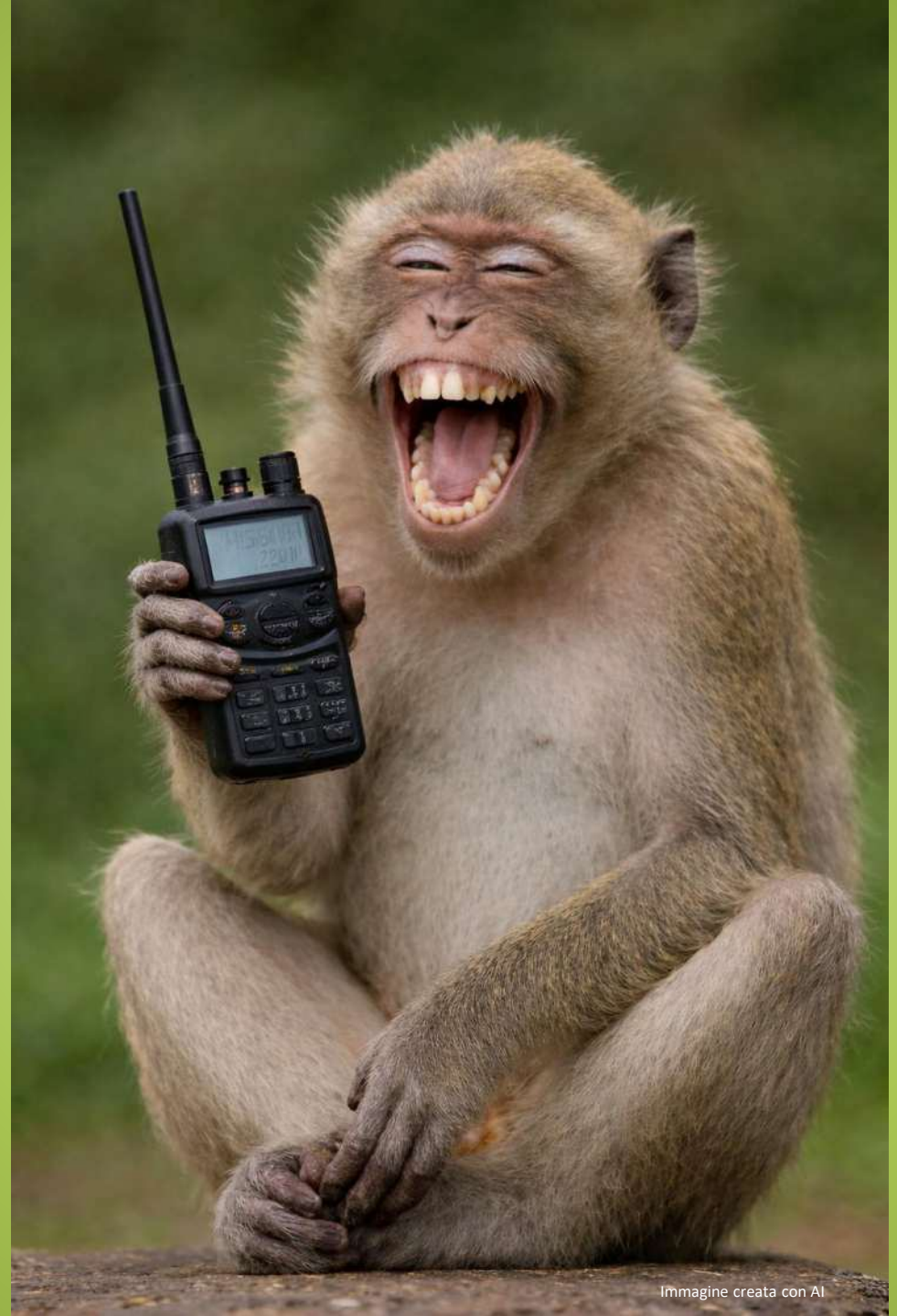


Immagine creata con AI

73 de ARI TREVISO
Buoni DX e navigazione sicura!