PROGRAMMA
INFRASTRUTTURE
Fondo di Perequazione
2019-2020

Cybersecurity: meglio pensarci prima

A cura di

Giorgio Sbaraglia

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica

UNIONTRASPORTI

27 giugno 2022

La presente documentazione è sottoposta alla licenza sul diritto d'autore **Creative Common CC BY-NC-ND**.

È permessa la ridistribuzione solo in forma intera ed invariata, citando espressamente l'autore.

Non può essere modificata o distribuita commercialmente.

Qualsiasi utilizzo diverso dalla succitata licenza potrà essere fatto solo previa richiesta all'autore Giorgio Sbaraglia (cybersec@giorgiosbaraglia.it).

CHI SONO

Giorgio Sbaraglia, ingegnere

- ☑ Information & Cyber Security Advisor
- ☑ DPO (Data Protection Officer)
- ☑ Membro del Comitato Scientifico Socio Clusit Associazione Italiana per la Sicurezza Informatica
- ☑ Coordinatore scientifico del Master “Cybersecurity e Data Protection” della 24Ore Business School
- ☑ Scrivo per: www.ictsecuritymagazine.com
  www.agendadigitale.eu/
  Rivista CLASS
- ☑ Collaboratore tecnico www.cybersecurity360.it CYBERSECURITY360

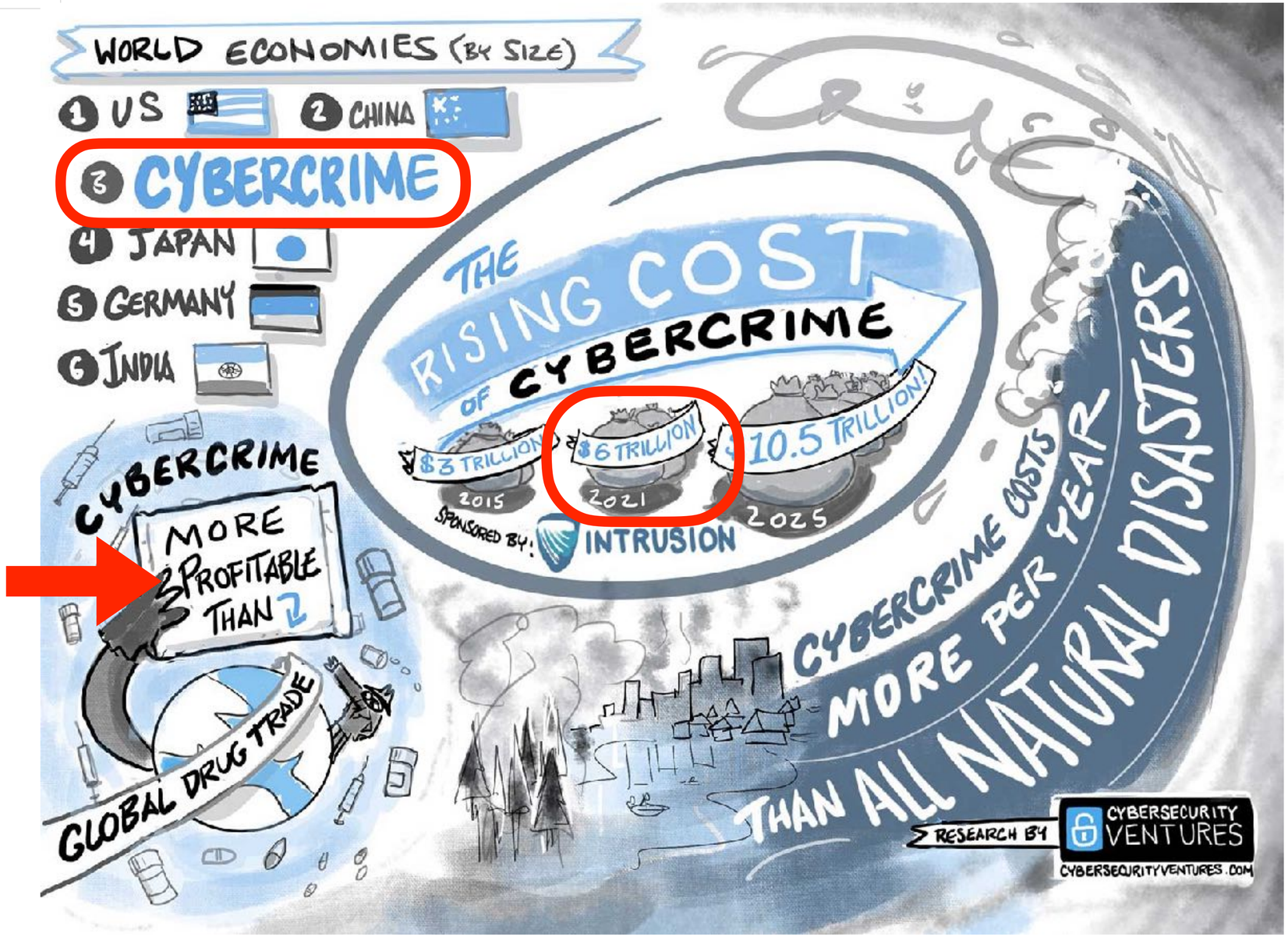
I MIEI LIBRI

www.giorgiosbaraglia.it

UNIONTRASPORTI

NON CI SONO PIÙ GLI HACKER DI UNA VOLTA…

IL PESO DEL CYBERCRIME SULL'ECONOMIA MONDIALE

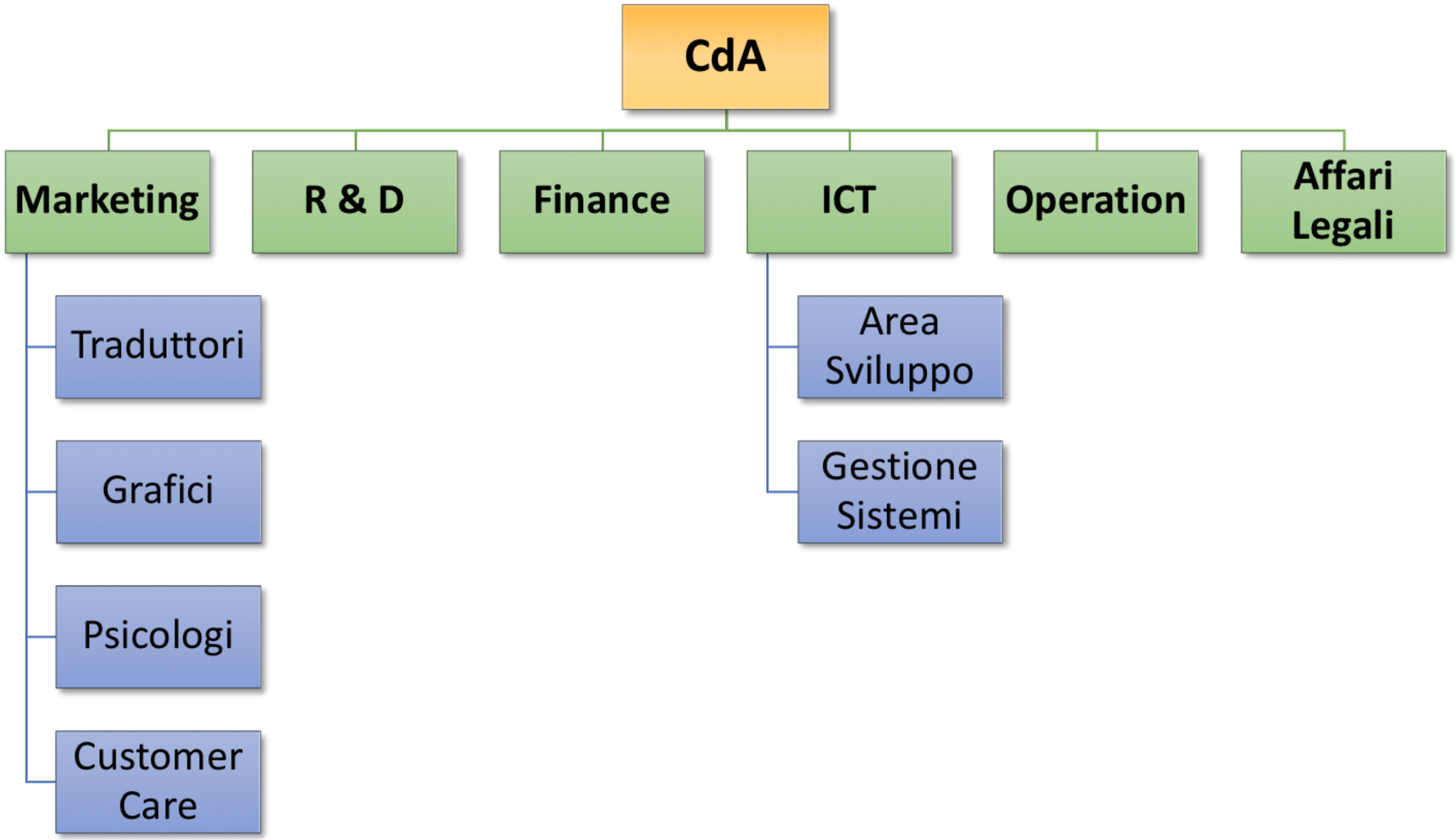


Cybersecurity Ventures prevede che i costi globali del crimine informatico cresceranno del 15% all'anno nei prossimi cinque anni, raggiungendo 10,5 trilioni di dollari all'anno entro il 2025, dai 3 trilioni di dollari del 2015,

più grande del danno inflitto dai disastri naturali in un anno,

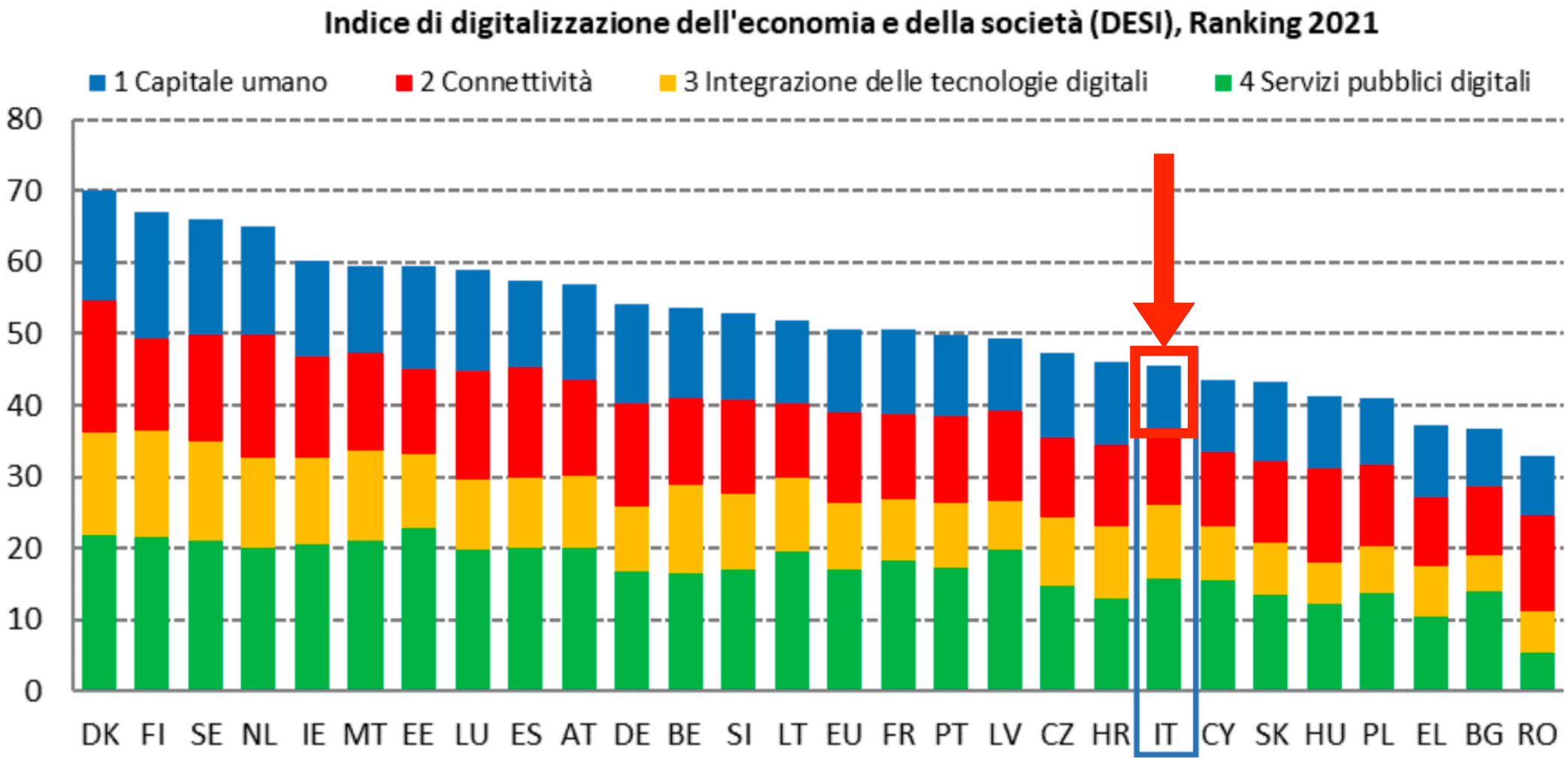
più redditizio del commercio globale di tutte le principali droghe illegali messe insieme.

CYBER CRIME S.P.A.



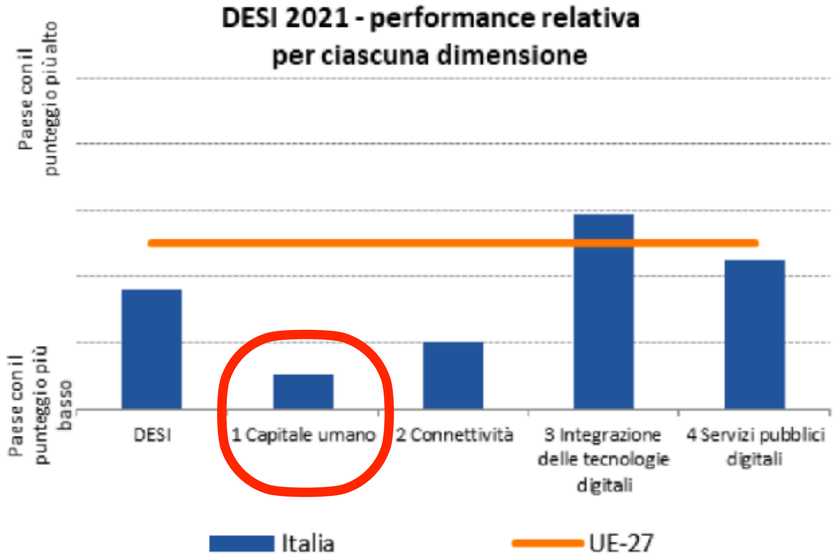
(cit. Alessio Pennasilico - CLUSIT)

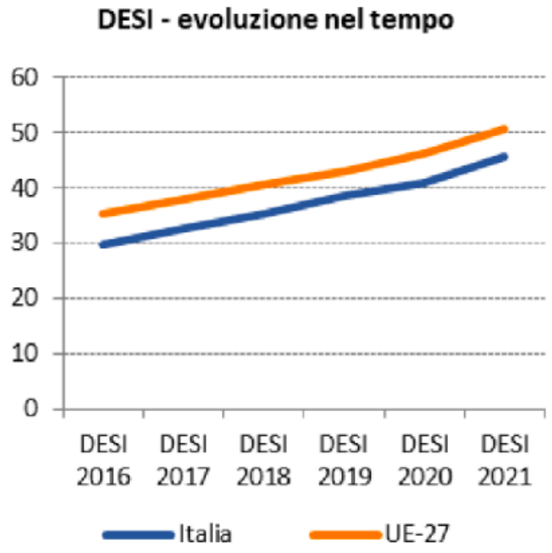
DESI 2021: DIGITAL ECONOMY AND SOCIETY INDEX (EU COMM.)



https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

DESI 2021: DIGITAL ECONOMY AND SOCIETY INDEX (EU COMM.)





L'Italia è significativamente in ritardo rispetto ad altri paesi dell'UE in termini di capitale umano. Rispetto alla media UE, registra infatti **livelli di competenze digitali di base e avanzate molto bassi.**

1 Capitale umano

1 Capitale umano	Italia		UE
	posizione in classifica	punteggio	punteggio
DESI 2021	25	35,1	47,1

Solo il 42% delle persone di età compresa tra i 16 e i 74 anni possiede perlomeno competenze digitali di base **(56% nell'UE)** e **solo il 22% dispone di competenze digitali superiori a quelle di base (31% nell'UE).**

https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

TIPOLOGIA DI ATTACCHI/INCIDENTI

ATTACCHI OPPORTUNISTICI

PHISHING
SMISHING
RANSOMWARE
ecc.

ATTACCHI MIRATI

SPEAR PHISHING
DDoS
APT
BEC
RANSOMWARE
ecc.

ATTACKER MINDSET:
PENSA COME PENSA L'ATTACCANTE

LE MINACCE PIÙ DIFFUSE:

IL SOCIAL ENGINEERING,

IL PHISHING,

I RANSOMWARE,

LE PASSWORD DEBOLI…

ANCHE I DISPOSITIVI MOBILI SONO A RISCHIO

IL SOCIAL ENGINEERING

Per violare un sistema ci possono volere settimane, mentre per violare il "sistema operativo uomo" possono bastare pochi minuti.

Cos'è il social engineering? *(human hacking)*

Semplicemente:

"FREGARE IL PROSSIMO CON LA PSICOLOGIA"

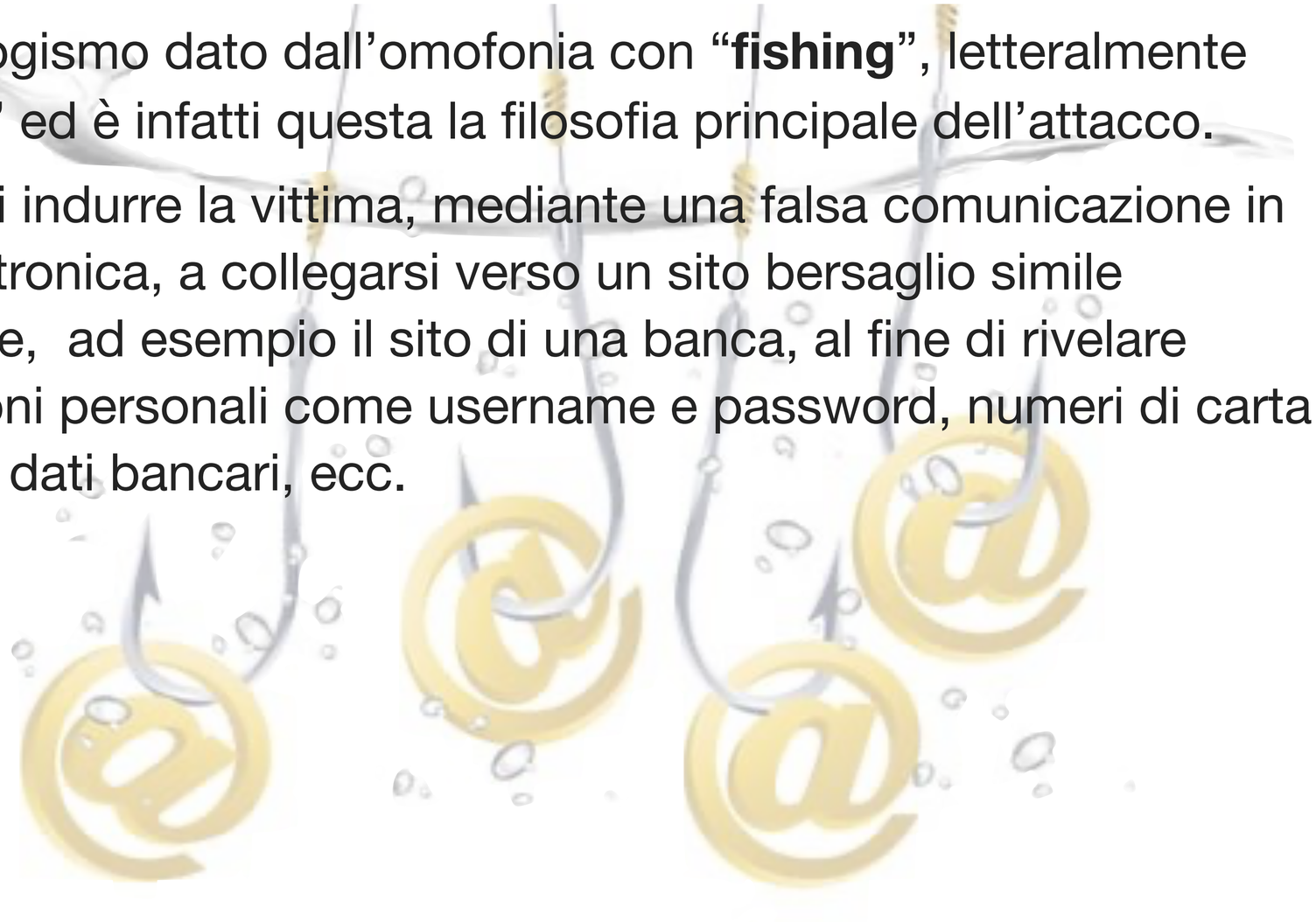
Scopo degli aggressori è indurre l'utente a fidarsi del *contenuto* del messaggio che mandano e quindi eseguirne i comandi.

Il social engineering è fatto apposta per aggirare Antivirus, Firewall, ecc.: quando il sistema non ha bugs da sfruttare, **si punta sulle debolezze e sulla curiosità delle persone.**

CHE COSA È IL PHISHING

È un neologismo dato dall'omofonia con "**fishing**", letteralmente "**pescare**" ed è infatti questa la filosofia principale dell'attacco.

Si cerca di indurre la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale, ad esempio il sito di una banca, al fine di rivelare informazioni personali come username e password, numeri di carta di credito, dati bancari, ecc.



CHE COSA È IL PHISHING

Le e-mail di phishing rappresentano circa il 90% dei vettori di attacco. Nella maggioranza dei casi le e-mail di phishing sono create per:

- **veicolare un malware**
- **rubarci le credenziali.**

La maggioranza di queste e-mail viene bloccata dai sistemi antispam dei nostri computer, ma qualcuna, perché confezionata con più cura, passa.

A questo punto tutto è nelle mani (e nella testa) degli utenti.

Si stima che circa il 97% degli utenti di Internet non sappia riconoscere una mail di phishing.

IL PHISHING: LE VARIANTI

È stato coniato anche il termine “**WHALING**” dall'inglese whale (balena), per indicare un phishing nel quale si punta a far abboccare un pesce grande (un **C-Level**).

Altre forme di Phishing:

- **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. Così si evitano i controlli antispam. È una variante dell’attacco “**watering hole**”.

A PROPOSITO DI “QRISHING”

Austin Police Department informa che adesivi fraudolenti del codice QR sono stati scoperti sui parchimetri pubblici della città di Austin.

Le persone che tentano di pagare il parcheggio utilizzando quei codici QR vengono indirizzati a un sito web fraudolento al quale daranno i dati della carta di credito ed i soldi…

La difesa consiste quindi nel fare sempre molta attenzione prima di accettare l’azione conseguente alla lettura di un QRcode.

SPAM … E PHISHING

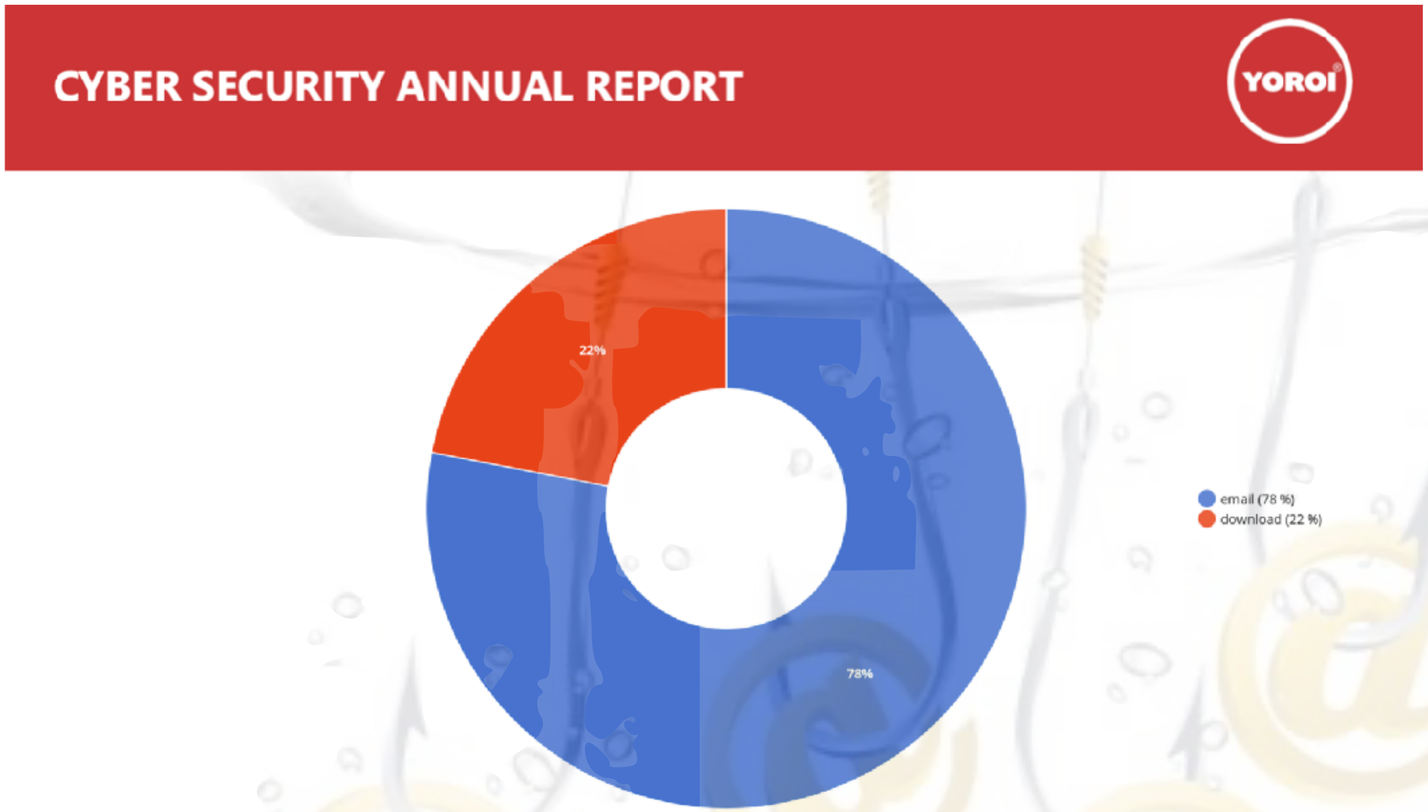


Figura 4. Distribuzione attack vectors

Il Phishing e lo Spear Phishing sono i vettori più adottati nel 2021 come inizio di una catena di attacco

(YOROY CYBERSECURITY ANNUAL REPORT 2022)

PHISHING E SPEAR PHISHING

Alcuni numeri per capire la dimensione del fenomeno.

L'attaccante invia un milione di email di phishing (“a strascico”), sapendo che il 10% di queste email verrà aperto ed almeno l’1% delle persone cliccherà sul link e/o sull’allegato.

La figura a fianco (tratta dal Verizon DBIR) ci mostra il **click rate** (tasso di click) nel phishing.

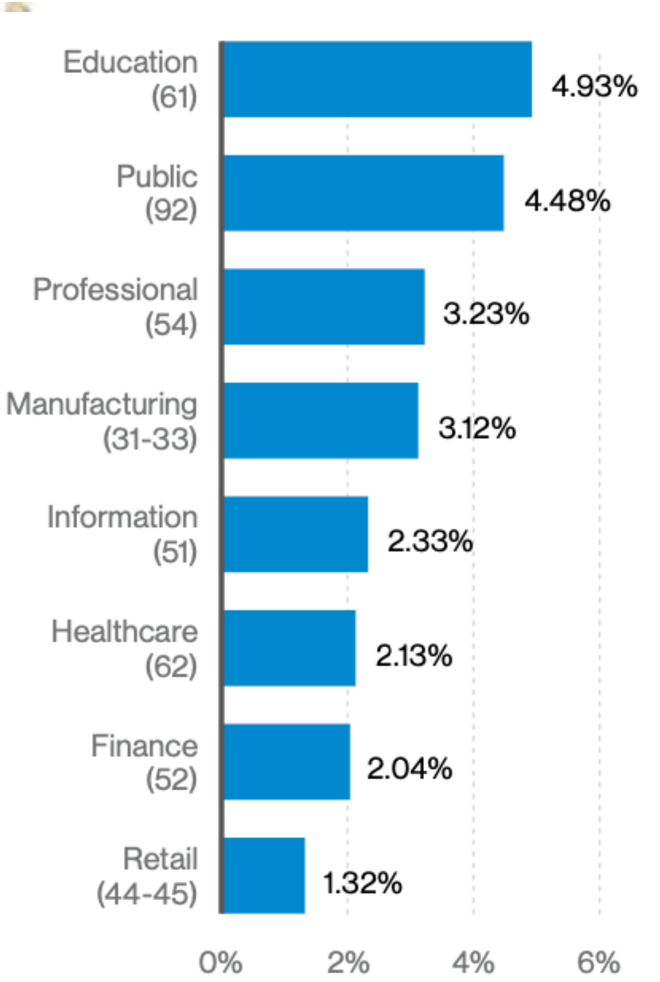
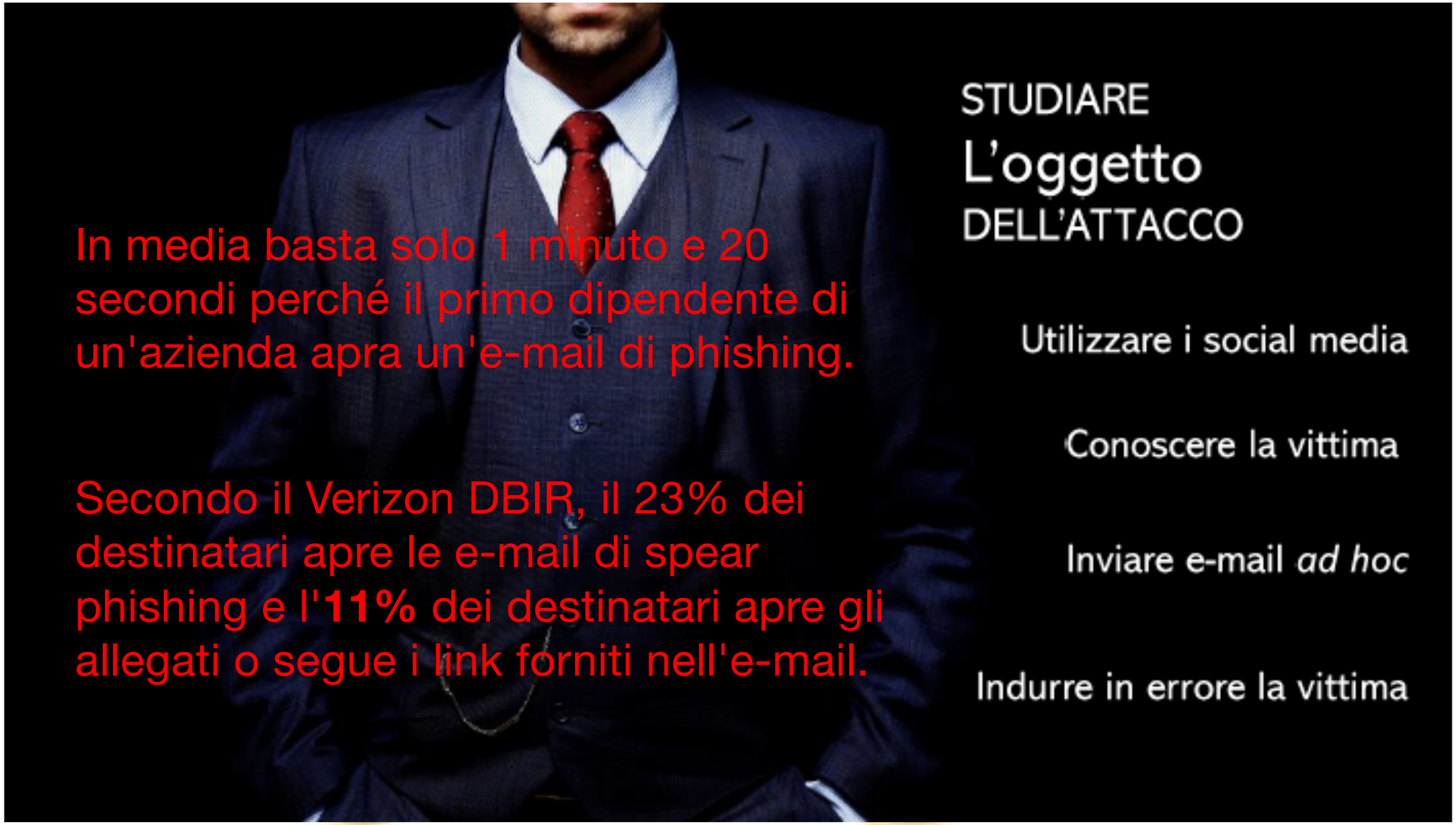


Figure 41. Click rate in phishing tests by industry

PHISHING E SPEAR PHISHING

PHISHING E SPEAR PHISHING



In media basta solo 1 minuto e 20 secondi perché il primo dipendente di un'azienda apra un'e-mail di phishing.

Secondo il Verizon DBIR, il 23% dei destinatari apre le e-mail di spear phishing e l'**11%** dei destinatari apre gli allegati o segue i link forniti nell'e-mail.

Attenzione ai link!

URL FALSIFICATI: ATTACCHI OMOGRAFICI O TYPOSQUATTING ESEMPI

Originale	google.com	microsoft.com	bankofamerica.com	domus.it
FALSO	go0gle.com	mIcrosoft.com	bankofarnerica.com	dornus.it
FALSO	goooogle.com	microsoff.com	bank-of-america.com	domus.lt

I trucchi esemplificati nella tabella sono banali, ma spesso riescono ad ingannare l'utente appena un po' distratto.

URL FALSIFICATI: ATTACCHI OMOGRAFICI O TYPOSQUATTING

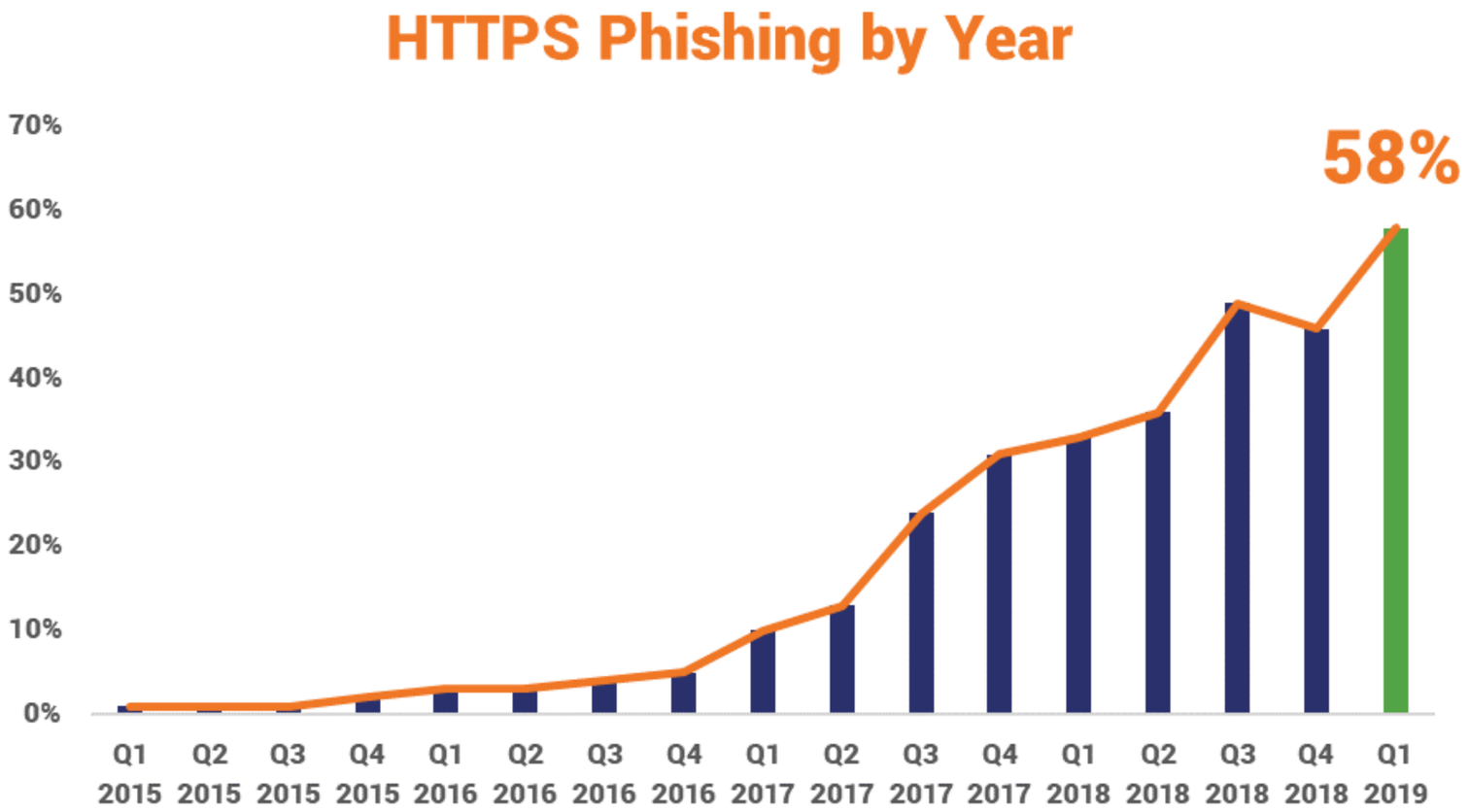
Typo è una parola inglese che può essere tradotta come errore di battitura, refuso. Il **typosquatting** è un trucco che prende di mira gli utenti più distratti.

Il typosquatting consiste nella **registrazione di domini-civetta**, il cui nome varia di una lettera (o al massimo due) rispetto al nome di un sito web molto conosciuto.

COME DIFENDERSI

Per scoprire se un sito web è vittima di typosquatting: digitare direttamente il sito che sappiamo essere corretto (non seguire il link!).

ATTENZIONE ANCHE A HTTPS...



Si utilizzano certificati di tipo **Domain Validation (DV)**, che garantiscono comunicazioni criptate attraverso connessioni HTTPS.

Ma poco o nulla dicono sulla autenticità di chi possiede il sito web al quale siamo collegati.

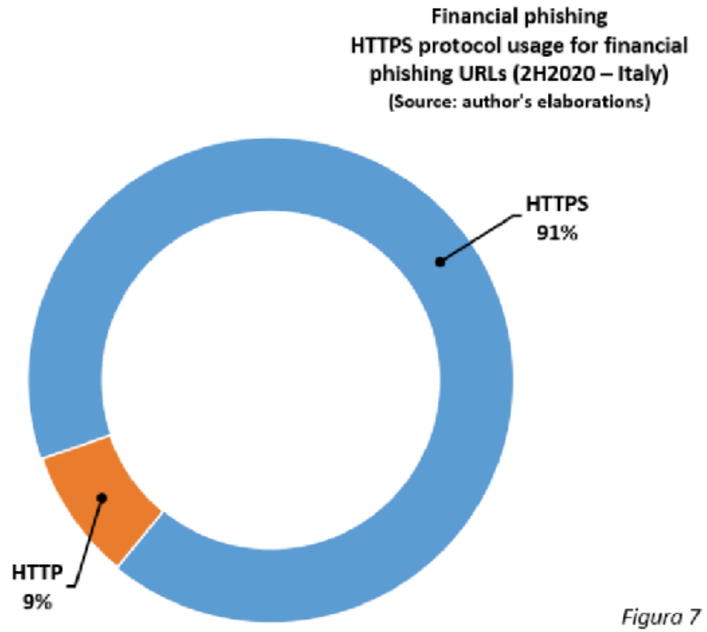
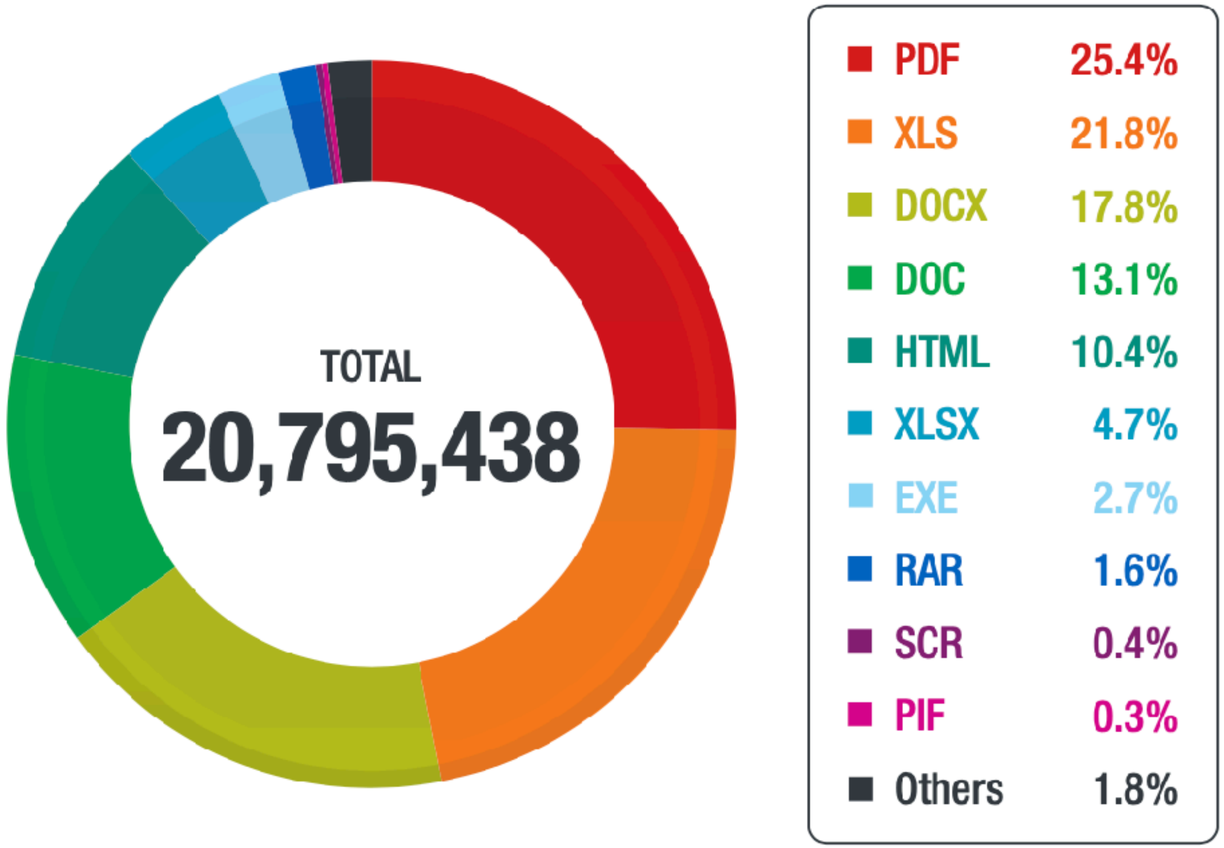


Figura 7

Nel phishing finanziario il 91,2% delle URL di phishing usa il protocollo HTTPS

Fonte: Rapporto Clusit 2021

ATTENZIONE ANCHE AGLI ALLEGATI: I PIÙ PERICOLOSI



I file più usati come allegati malevoli, per inoculare un malware, sono quelli più comuni e più utilizzati dagli utenti: **pdf, Excel, Word.**

Circa il 13÷20% degli allegati in format word (doc e docx) ed Excel (xlsx e xls) sono malevoli.

I file Word ed Excel vengono **"armati" con macro (in VBA: Visual Basic for Applications) al loro interno (con la funzione "Auto_Open")**: importante quindi disabilitare l'uso delle macro in Office.

Figure 24. A quarter of the attachments in detected email threats were PDFs:
Distribution of file types used as attachments in spam emails detected in 2019

Source: Trend Micro Smart Protection Network infrastructure

RANSOMWARE: LA MINACCIA PIÙ TEMIBILE PER LE AZIENDE

27 GIUGNO 2017: ATTACCO NOTPETYA

NotPetya cyber attack on TNT Express cost FedEx $300m

Falling victim to global ransomware attack "posed significant operational challenges", the company says in its latest financial report.

By Danny Palmer | September 20, 2017 -- 16:12 GMT (17:12 BST) | Topic: Security

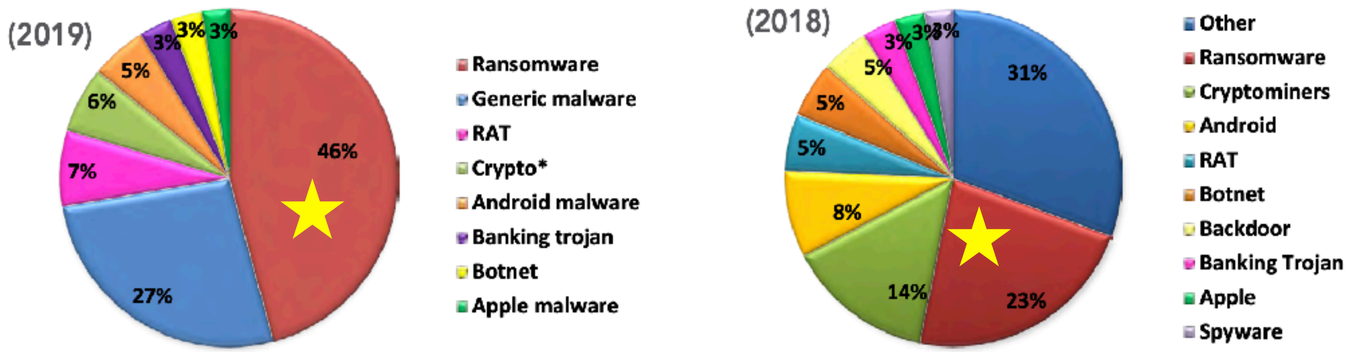
NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

The shipping giant has suffered millions of dollars in damage due to the ransomware attack.

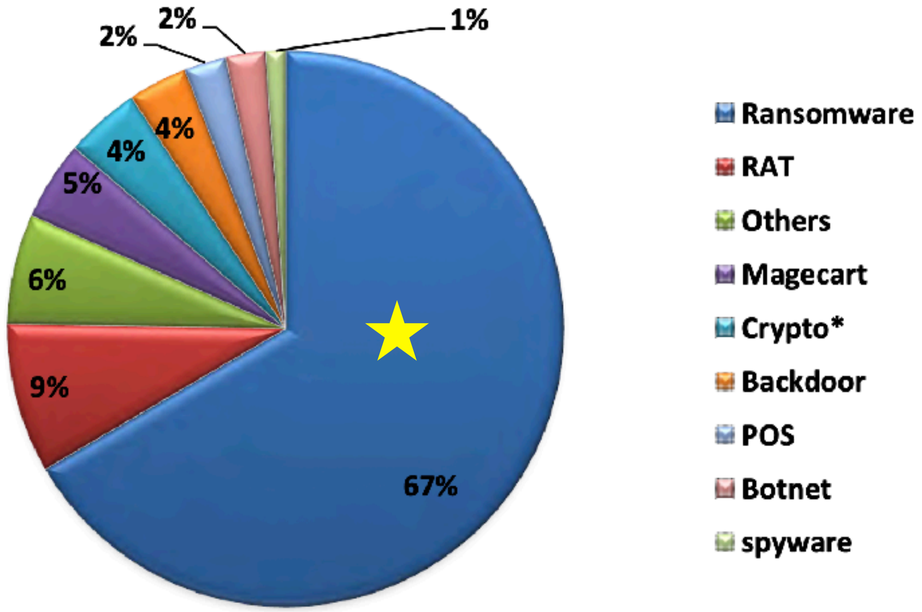
By Charlie Osborne for Zero Day | January 26, 2018 -- 10:25 GMT (10:25 GMT) | Topic: Security

RAPPORTO CLUSIT 2021: RANSOMWARE IN CRESCITA

Tipologia e distribuzione Malware



Tipologia Malware (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

I Ransomware erano:

- un quarto del malware nel 2018,
- nel 2019 quasi la metà del totale,
- **nel 2020 sono il 67%**

I RANSOMWARE

- Categoria: **Trojan horse crittografico.**
- Scopo: **ESTORSIONE.**
- Il Paese più colpito nel 2020 sono gli Stati Uniti (18.2% secondo Symantec). L'Italia è al quarto posto in Europa, dopo Germania, Regno Unito e Francia (fonte Mandiant, società gruppo FireEye).
- Il volume degli attacchi ransomware nei primi tre trimestri del 2021 ha raggiunto 470 milioni, un **aumento del 148%** rispetto allo stesso periodo dello scorso anno (fonte SonicWall).
- Il 90% di chi subisce attacchi accusa **downtime** e/o **perdita di dati**.
- Il tempo medio di downtime è di **9,6 giorni,** ma può arrivare ad **un mese.**
- I più recenti, oltre a criptare i file, fanno **Upload**: esfiltrazione dei dati sensibili, minacciandone la divulgazione pubblica (GDPR?!).
  Double Extorsion!
  Ransomware: Maze (dal 2019), NetWalker, RagnarLocker, DoppelPaymer, ecc.

I RANSOMWARE

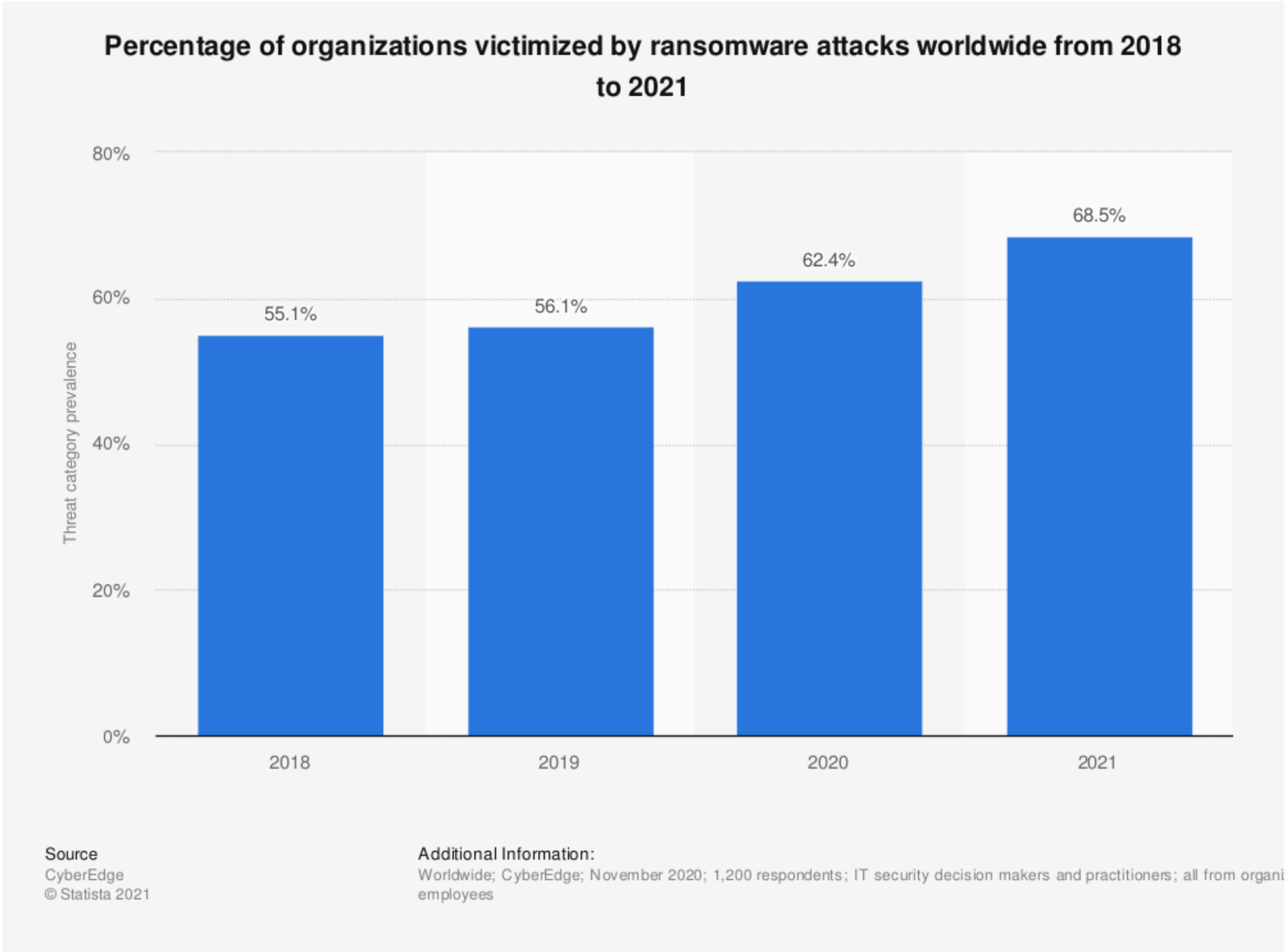
- Nel 2021 il 32% delle aziende dichiara di aver pagato il riscatto. Nel 2022 sono cresciute al 46% *(fonte Sophos: The State of Ransomware 2022).*
- Riscatto richiesto: da poche centinaia, fino a milioni di euro.
- Nei primi anni (2014-2017), nell'81% dei casi il riscatto non supera(va) i 1.000 $.
- Negli anni più recenti, il riscatto medio pagato è passato da **115.123 dollari nel 2019** a **312.493 dollari nel 2020** (**+171% anno su anno**).
- **Anno 2022: riscatto medio 812.360 $ (mondo), 709.746 $ (Italia)** *(fonte Sophos: The State of Ransomware 2022).*
- Dal 2015 al 2019, la richiesta più elevata è stata di 15 milioni di dollari, mentre nel 2020 ha raggiunto i 30 milioni di dollari. *(Fonte: "Unit 42 Ransomware Threat Report 2021" di Palo Alto Networks).*
- 2021: riscatto richiesto ad ACER 50 milioni di dollari, a Kaseya 70 M$.
- Riscatto in Bitcoin (o altra criptovaluta).

I RANSOMWARE: I DANNI CHE L'AZIENDA RISCHIA DI SUBIRE

Non è solo il riscatto, ce ne sono anche altri, non meno gravi:

- ☑ Fermo attività durante le operazioni di ripristino
- ☑ Costi di ripristino dell'infrastruttura
- ☑ Costo per indagine forense
- ☑ Pubblicazione di dati critici e riservati
- ☑ Eventuali spese legali per perdita dati sensibili utenti/clienti
- ☑ Danno reputazionale
- ☑ **CHIUSURA DELL'AZIENDA**

ORGANIZZAZIONI VITTIME DI ATTACCHI RANSOMWARE IN TUTTO IL MONDO DAL 2018 AL 2021



RANSOMWARE: I VETTORI D'INFEZIONE

A) IL FATTORE UMANO

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**).

RANSOMWARE: I VETTORI D'INFEZIONE

B) ERRORI TECNICI

5) Attacchi brute force attraverso **desktop remoto (RDP)**: attacchi con furto di credenziali per accedere ai server e prenderne il controllo. Incremento del 197% nel 2021 su anno precedente (anche a causa dello smart working).
6) Sfruttando **vulnerabilità** dei sistemi. Casi: WannaCry, MS Exchange 2021 (ProxyLogon, ecc.).
7) **Supply Chain Attack** (caso Solar Winds 2020, Kaseya 2021).

E-MAIL “MALIGNE”… COME SI SONO EVOLUTE

Campagna di Phishing 2021 su tutto il territorio nazionale: l’obiettivo dei cybercriminali è quello di veicolare il malware **URSNIF.**

Le mail recapitate in questa campagna sfruttano tutte il tema “**BRT**”: il mittente appare come **ammXXX@brt.it** (con XXX un numero di 3 cifre iniziante per 0).

L’oggetto è **“BRT S.P.A. – fatture scadute XXXXX (IDXXXXX)”**.

16.03.2021

Oggetto: Sollecito pagamento fatture

Gentile cliente,
con la presente Le segnaliamo che non ci risulta pervenuto il pagamento delle fatture scadute di seguito riportate:

Data Documento	Numero Documento	Data Scadenza	Importo
15.02.2021	02891	15.03.2021	1.002,00

Entro e non oltre 5 giorni dalla data di ricevimento della presente, La invitiamo a predisporre il pagamento dell'importo complessivo di Euro 1.002,00

Il pagamento può essere effettuato con bonifico bancario a favore di BRT S.p.A., usando le coordinate IBAN di una delle Banche di seguito elencate riportando nella descrizione il codice cliente 01164433.

Istituto	IBAN	BIC
BNL	IT05 C010 0502 5980 0000 0011 453	BNLIITRRXXX
Monte Paschi Siena	IT51 T010 3002 4020 0000 0378 047	PASCITM1BO2
Banco BPM	IT27 R050 3402 4100 0000 0111 323	BAPPIT21586
Intesa Sanpaolo	IT55 R030 6902 5060 7400 0000 178	BCITITMM
UniCredit	IT81 R020 0805 3640 0000 1097 497	UNCRITMMORR

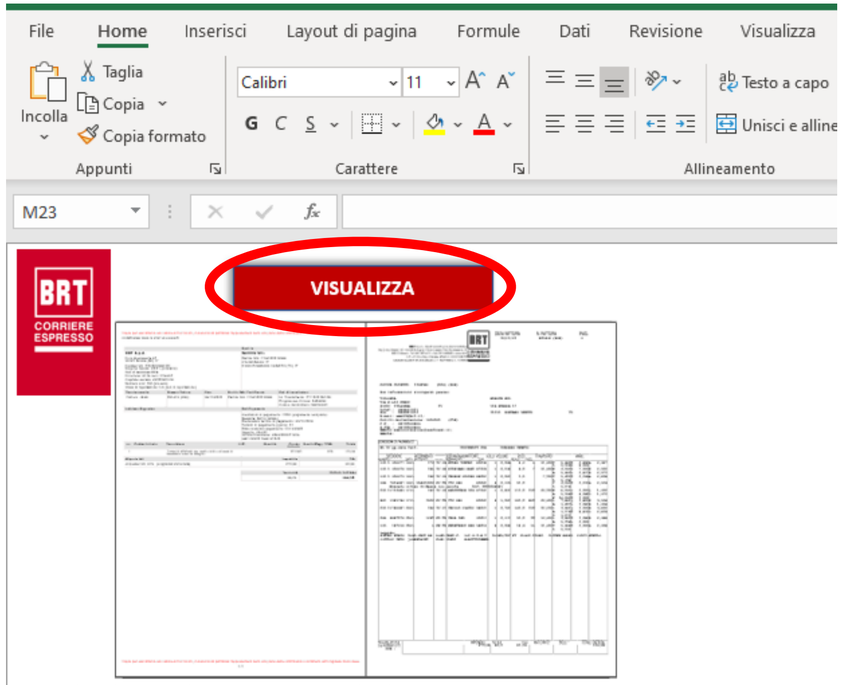
Nel caso abbia già provveduto al pagamento, può considerare nulla la presente comunicazione.
Per eventuali informazioni può contattarci al numero di telefono 0422702311.

Cogliamo l'occasione per inviarLe distinti saluti.

BRT S.p.A.

In allegato è presente un file Excel nominato “**Fattura_XXXXX.xlsm**”.

Aprendo il file allegato, viene mostrata una finta fattura Bartolini ed un pulsante “**VISUALIZZA**”:



Premendo il tasto “Visualizza”, dopo 8 secondi di blocco il file Excel viene automaticamente chiuso ed il PC risulta ormai infetto…

Ransomware…
non è un malware,
è un DISASTRO

RANSOMWARE: LA MINACCIA PIÙ TEMIBILE PER LE AZIENDE

COME PROTEGGERSI

1) Attenzione alle email!
2) Trattare le email di **mittenti conosciuti** come eventualmente sospette, (potrebbero essere stati **spoofate**!)
3) Installare servizi **Antispam** efficaci ed evoluti
4) Disabilitare **l'esecuzione di macro** da parte di componenti Office (Word, Excel, PowerPoint ecc…)
5) Fare **Backup e proteggerli** in modo che non siano accessibili dal ransomware
6) Attenzione alle **chiavette USB** (o CD/DVD) e altri supporti esterni (c.d. Baiting)
7) Adottare sistemi di protezione avanzati: EDR, XDR, IPS, SIEM…
8) Mantenere i sistemi sempre aggiornati
9) **Formare il personale**, il fattore umano è il primo fattore di rischio

L’EMAIL NON È UNO STRUMENTO SICURO:

LA BUSINESS EMAIL COMPROMISE (BEC)

LA TRUFFA: “CEO FRAUD”

R.it Cronaca

Mr. Confindustria a Bruxelles truffato da un hacker: persi 500mila euro. Licenziato

"Sposta subito mezzo milione su questo conto estero". Ma la mail era di un hacker. E i soldi sono spariti. Il finto ordine a firma della direttrice Panucci: "Esegui e non mi chiamare che sto fuori col presidente"

di ROBERTO MANIA

LA BUSINESS EMAIL COMPROMISE (BEC)

La BEC si declina in diverse modalità, le più utilizzate sono:

1) **“CEO Fraud”**: una richiesta di esecuzione di bonifico bancario viene inviata dall'account compromesso di un dirigente aziendale di alto livello (CEO o Chief Financial Officer) ad un dipendente all'interno dell’azienda, incaricato ai pagamenti.

2) **“The Man in the Mail”**: nel business tra cliente e fornitore viene fatta richiesta di pagamento con e-mail falsificata, indicando il c/c del malfattore. Colpisce soprattutto aziende di import/export… ma non solo!

BEC: LA VARIANTE “CEO FRAUD”

1) **“CEO Fraud”**: richiesta di esecuzione di bonifico bancario viene inviata dall'account compromesso di un dirigente aziendale di alto livello (CEO o Chief Financial Officer) ad un dipendente all'interno dell’azienda, incaricato ai pagamenti.

COME FUNZIONA?

- **Contatto diretto da un top manager** tramite e-mail o chiamata inattesa.
- Si utilizzano espressioni come: “La società si fida di te”, “Non sono al momento disponibile”, “Non posso rispondere”.
- Minacce o adulazioni inusuali e/o promesse di ricompensa.
- Richiesta di assoluta **riservatezza**.
- Pressione e **senso di urgenza**.
- Riferimento ad una situazione delicata (ad es. un controllo fiscale, una fusione, un’acquisizione).
- Richiesta anomala che **non segue le procedure interne**.

BEC: LA VARIANTE “THE MAN IN THE MAIL”

2) **“The Man in the Mail”**: nel business tra cliente e fornitore viene fatta richiesta di pagamento con e-mail falsificata, indicando il c/c del malfattore.

COME FUNZIONA?

- Il ladro viola la casella di posta (quella del mittente oppure quella del destinatario) mediante: phishing, social engineering, furto delle credenziali o attacco “brute force”, keylogger.
- Studia le comunicazioni dell’azienda, la carta intestata, le firme dei responsabili, lo stile della corrispondenza.
- Poi si inserisce in conversazioni già in corso comunicando coordinate bancarie diverse (le sue!) su cui eseguire i pagamenti. Per fare questo usa lo “**spoofing**” (imbrogliare), usando un indirizzo email appena diverso, oppure accede direttamente all’email violata.

I NUMERI DELLA BUSINESS EMAIL COMPROMISE

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

September 10, 2019

Alert Number
I-091019-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office.**

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

Tra Ottobre 2013 e Luglio 2019:

Domestic and international incidents: 166.349

Domestic and international exposed dollar loss: **$ 26.201.775.589**

Secondo l'FBI, le truffe BEC sono state segnalate in USA ed in altre 177 nazioni.

Tra il maggio 2018 e il luglio 2019, si è registrato un aumento del 100% delle perdite, rispetto all'intero periodo precedente.

Fonte: https://www.ic3.gov/media/2019/190910.aspx

PROTEGGERSI DA “THE MAN IN THE MAIL”

- Usare credenziali di accesso alle mail robuste e sicure.
- Non utilizzare in azienda indirizzi email gratuiti basati su webmail.
- Leggere le mail con attenzione, soprattutto quelle che si riferiscono a pagamenti. Nel dubbio fare verifiche con mezzi diversi (per es. il telefono, oppure un’altra email).
- **Controllare bene il mittente delle email: un dettaglio (anche solo una lettera!) potrebbe fare la differenza.**
- Implementare sistemi di ANTISPAM avanzati.
- E soprattutto: **Essere consapevoli dell’esistenza di questo tipo di attacchi e saperli riconoscere.**

https://www.giorgiosbaraglia.it/truffe-via-mail-la-business-email-compromise/

PROTEGGERSI DA “THE MAN IN THE MAIL”

- **Controllare bene il mittente delle email: un dettaglio (anche solo una lettera!) potrebbe fare la differenza.**

l’email vera info@pippodomus.it potrebbe essere trasformata dal truffatore in: info@pippodo**rn**us.it

Oppure potrebbe essere modificata in info@pipp**0**domus.it sostituendo la lettera “o” con il numero “0”, pressoché identico.

O anche: info@pippo-domus.com

O anche: info@pippodomus.**lt** (TLD della Lituania).

In sintesi: gli attacchi BEC sono altamente personalizzati, normalmente non contengono alcun tipo di malware e sono in grado di superare i filtri antispam

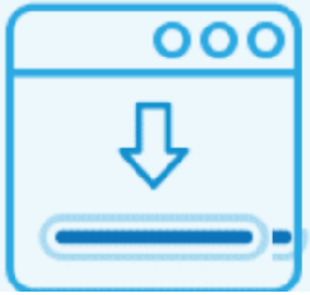
COME PROTEGGIAMO
I NOSTRI DATI?

31 MARZO:
GIORNATA MONDIALE DEL BACKUP

30% of people
have never backed up [1]

113 phones
lost or stolen every minute [2]

29% of disasters
are caused by accident [3]



1 in 10 computers
infected with viruses each month [4]

L’IMPORTANZA DEL BACKUP

Per prevenire perdite di dati per qualsiasi ragione, fare sempre **copia di sicurezza dei propri dati (almeno il 30% degli utenti NON lo fa!).**

3-2-1 BACKUP STRATEGY:

✅ **3** copie di ogni dato che si vuole conservare (L’errore più frequente è la presenza di un’unica copia di backup)

✅ **2** copie ”onsite” ma su storage differenti (HD, NAS, Cloud,…)

✅ **1** copia in sito remoto “off-site” (ev. Cloud)

L’IMPORTANZA DEL BACKUP

Recovery Point Objective (RPO)

Recovery Time Objective (RTO)

SLO (Service Level Objective) comprende RPO + RTO

Ridurre RPO e RTO ha un costo

L'IMPORTANZA
DELLE PASSWORD

VERIZON DATA BREACH INVESTIGATIONS REPORT 2017

81% delle violazioni degli account sono realizzate con **password rubate** e/o **password deboli**.

MA LE PERSONE CONTINUANO AD USARE PASSWORD MOLTO BANALI…

La classifica delle password più utilizzate nel **mondo** (ed anche le peggiori!) nel 2021:

(Fonte: **NordPass**, su un database di 4 TB in 50 nazioni)

1. **123456** *(al primo posto dal 2013, presente 2.543.285 di volte)*
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567
11. qwerty123
12. 000000
13. 1q2w3e
14. aa12345678
15. abc123
16. password1
17. 1234
18. qwertyuiop
19. 123321
20. password123
21. 1q2w3e4r5t
22. iloveyou
23. 654321
24. 666666
25. 987654321
26. 123
27. 123456a
28. qwe123
29. **1q2w3e4r**
30. 7777777
31. 1qaz2wsx
32. 123qwe

MA LE PERSONE CONTINUANO AD USARE PASSWORD MOLTO BANALI…

La classifica delle password più utilizzate in **ITALIA** nel 2021:

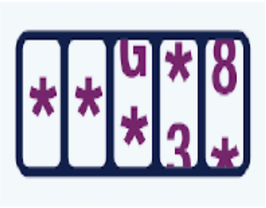
(Fonte: **NordPass**, password violate: 260.463.991

1. **123456** *(al primo posto dal 2013, presente 2.543.285 di volte)*
2. 123456789
3. 12345 *(le prime 3 sono uguali)*
4. 12345678
5. qwerty
6. **juventus**
7. 000000
8. password
9. andrea
10. **napoli**
11. francesco
12. 111111
13. 1234567
14. **cambiami**
15. giuseppe
16. alessandro
17. antonio
18. **ciaociao**
19. **amoremio**
20. francesca
21. 1234567890
22. valentina
23. stella
24. giovanni
25. martina
26. 1234
27. ciccio
28. federica
29. stellina
30. giulia
31. simone
32. alessia

COME VENGONO SCOPERTE (RUBATE) LE PASSWORD?

1) **INGEGNERIA SOCIALE** (ad esempio phishing, Password Sniffing).

2) **INDOVINANDO LE PASSWORD** (utilizzando informazioni personali come nome, data di nascita o nomi di animali domestici).



3) **“BRUTE FORCE ATTACK”**: la prova automatica di un gran numero di password fino a quando viene trovata quella giusta.

4) **INTERCETTAZIONE** di una password mentre viene trasmessa su una rete.

https://www.giorgiosbaraglia.it/attacco-alle-password-tecniche-di-cracking-e-consigli-per-metterle-al-sicuro/

COME VENGONO SCOPERTE (RUBATE) LE PASSWORD?

5) **“SHOULDER SURFING”**: osservando qualcuno mentre digita la password.

6) **INSTALLANDO UN KEYLOGGER** per intercettare le password quando vengono digitate in un dispositivo.

7) **PASSWORD MEMORIZZATE IN MODO NON SICURO**, come scritte a mano su carta e nascoste vicino a un dispositivo (“idiocy attack”).

8) **COMPROMETTENDO UN DATABASE** contenenti un gran numero di password utente, quindi utilizzando queste informazioni per attaccare altri sistemi dove gli utenti hanno riutilizzato le stesse password (“credential stuffing”).

https://www.giorgiosbaraglia.it/attacco-alle-password-tecniche-di-cracking-e-consigli-per-metterle-al-sicuro/

LE REGOLE PER UNA PASSWORD SICURA

✅ **SEMPRE DIVERSA:** Non utilizzare la stessa password in account diversi (*"non puoi evitare che il tuo provider venga violato, ma puoi evitare che tutti i tuoi account vengano hackerati in un colpo solo a causa dell'utilizzo di una sola password"*).

✅ **LUNGA**: utilizzare almeno dodici caratteri.

✅ **MISTA:** lettere maiuscole e minuscole, numeri e caratteri speciali.

✅ **SENZA SENSO:** Non utilizzare nomi, parole o parti di parole che possono essere ritrovati automaticamente in un dizionario.

The only secure password is the one you can't remember

(https://www.troyhunt.com/only-secure-password-is-one-you-cant/)

ERRORI COMUNI DA EVITARE

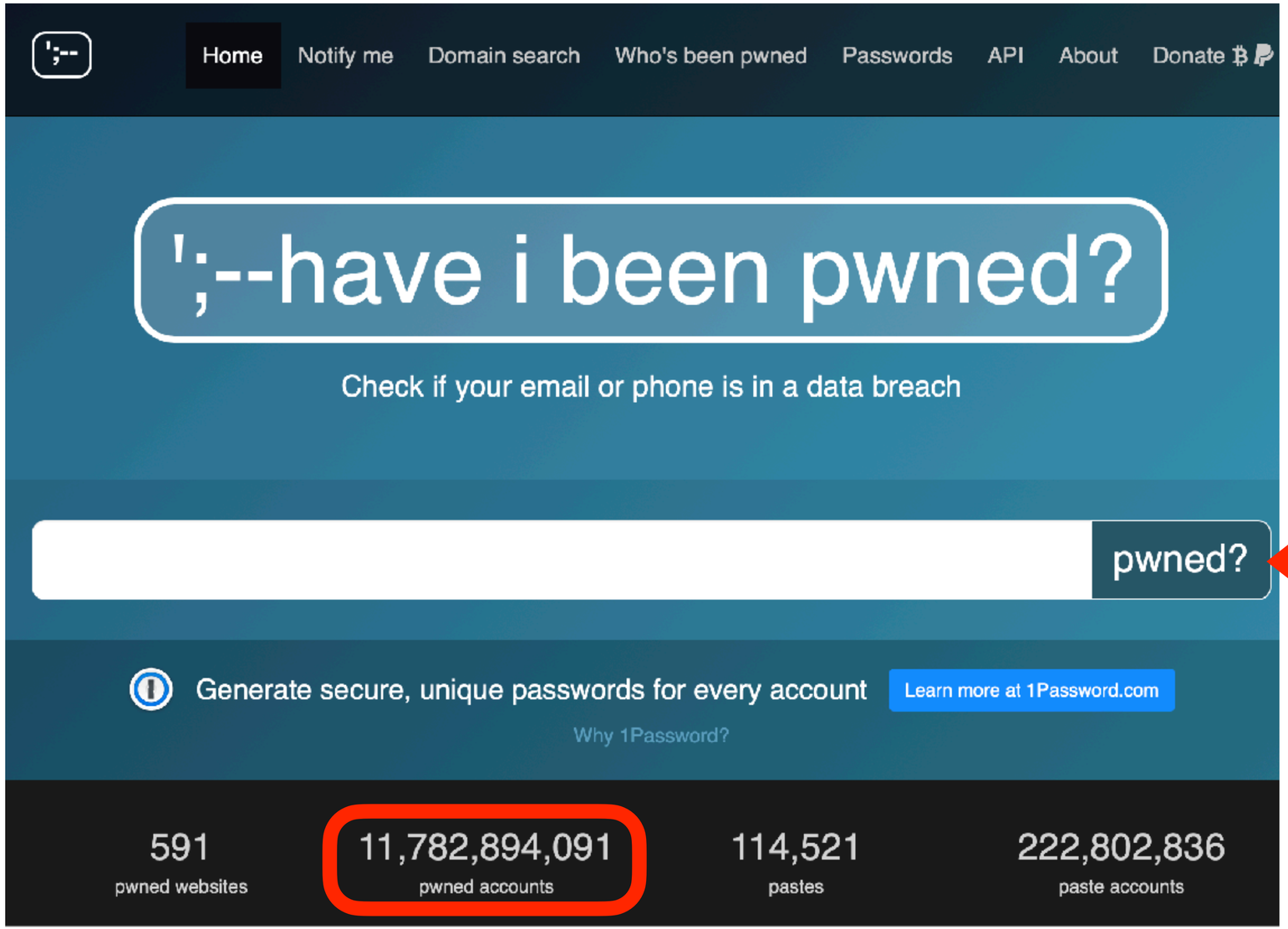
Password contenenti:

- Parole presenti su un dizionario in qualsiasi lingua.
- Sequenze o caratteri ripetuti. Esempi: 12345678, 222222, abcdefg, o lettere adiacenti sulla tastiera (qwerty).
- Parole scritte al contrario, errori comuni di ortografia e abbreviazioni.
- Modificazioni ovvie alla password.
- Informazioni personali o di familiari: nome, compleanno, numero di patente e di passaporto o informazioni analoghe.

The only secure password is the one you can’t remember

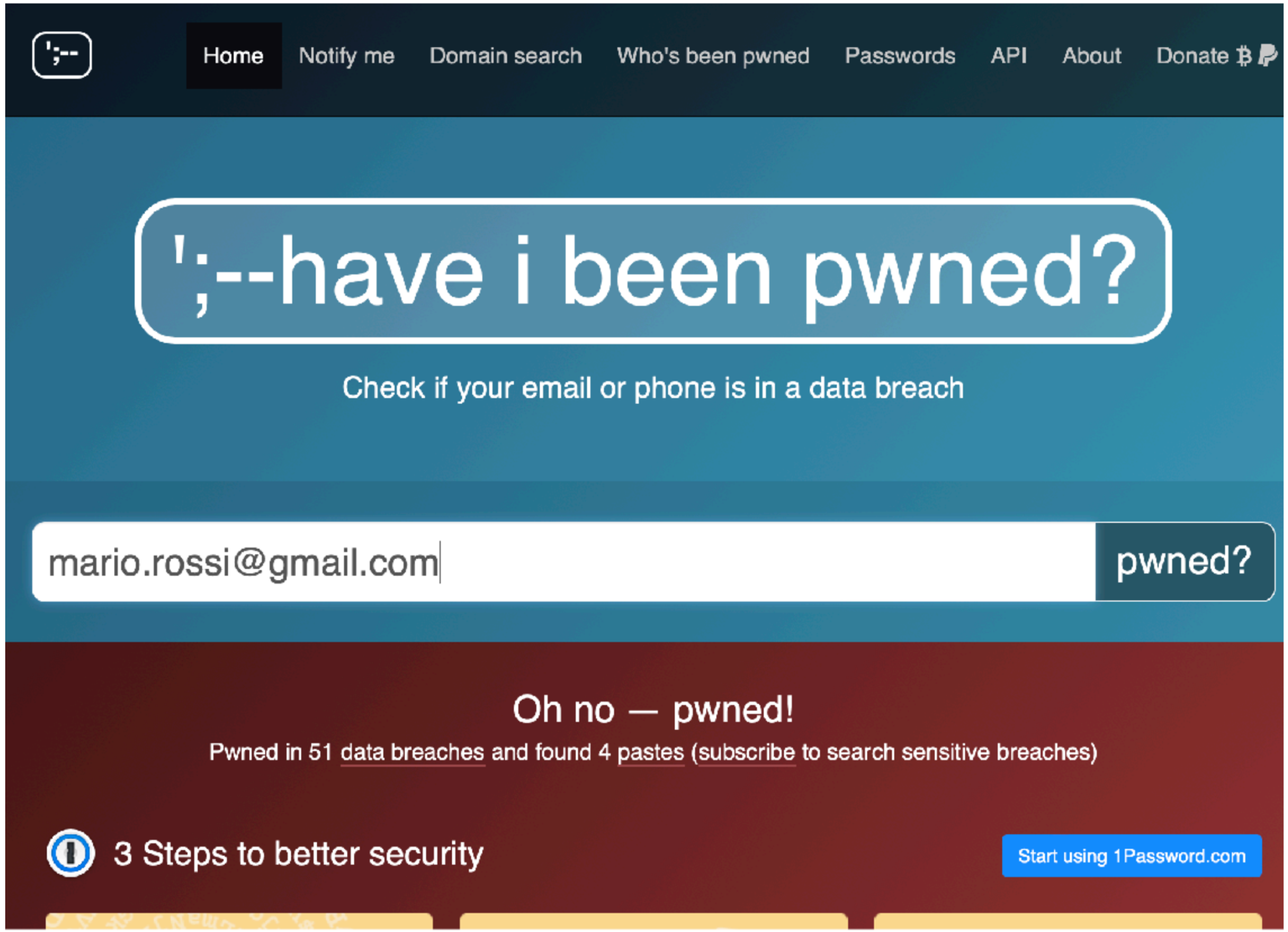
(https://www.troyhunt.com/only-secure-password-is-one-you-cant/)

HAVE I BEEN PWNED? (BY TROY HUNT)



https://haveibeenpwned.com

HAVE I BEEN PWNED? (BY TROY HUNT)



https://haveibeenpwned.com

QUAL È LA SOLUZIONE?

The only secure password is the one you can't remember
(Troy Hunt)

Se, come abbiamo spiegato:

☑ **dobbiamo usare password lunghe e complesse,**

☑ **sempre diverse,**

ed inoltre…

☑ **l'unica password sicura è quella che non si può ricordare,**

qual è il modo più pratico e sicuro per gestire le proprie passwords?

Usare un PASSWORD MANAGER

I PASSWORD MANAGER

✅ I migliori PM sono “multipiattaforma”: disponibili per i sistemi Mac, Windows, iOS ed Android. Questo permette (ma non è un obbligo) di sincronizzare attraverso il Cloud (p.es. Dropbox) le password su ogni dispositivo su cui sono installati (computer, laptop o smartphone che sia).

✅ Protetti da una MASTER PASSWORD, che diventa perciò l’UNICA password che occorre ricordare.

✅ Rappresentano il miglior compromesso tra sicurezza e praticità

https://www.giorgiosbaraglia.it/password-manager-la-guida-completa/

I VANTAGGI DEI PASSWORD MANAGER

- ☑ L'UNICA password che occorre ricordare è la **MASTER PASSWORD** per aprirli.
- ☑ Si possono memorizzare: username, password, dati delle carte di credito e molti altri dati.
- ☑ I dati memorizzati vengono crittografati con sistema di cifratura AES 256 bit (*Advanced Encryption Standard*), una tecnologia crittografica utilizzato come standard dal governo USA e che la NSA ritiene adatta per proteggere i documenti TOP SECRET.
- ☑ Hanno la capacità di generare automaticamente password sicure e complesse.
- ☑ Hanno un sistema intelligente di riempimento automatico dei moduli nei siti web (non occorre perciò fare "copia/incolla" delle password).
- ☑ Quindi… proteggono dal Phishing scam.

https://www.giorgiosbaraglia.it/password-manager-la-guida-completa/

GLI SVANTAGGI E RISCHI DEI PASSWORD MANAGER

- **Scegliere un Password Manager non sicuro**: potrebbe essere pericoloso affidare le proprie password ad un software creato da altri, perché un hacker potrebbe confezionare e mettere in commercio un PM appositamente per rubarci le password. Per evitare questo rischio - che esiste - consiglio di scegliere solo PM di aziende note ed affidabili.
- **Dimenticare la Master Password**: sui PM (tranne qualche eccezione) non esiste il solito pulsante *“Ho dimenticato la password”* per recuperare la chiave d'accesso, proprio per ragioni di sicurezza. Quindi dimenticare la master password significa non avere più l’accesso al PM e perdere irrimediabilmente tutte le proprie password!
- **Farsi rubare la Master Password**: conservare tutte le password in un unico archivio può essere rischioso, (*“all your eggs in one basket”*) quindi proteggiamolo con una password forte, in fondo è l’unica che dovremo veramente ricordare.

https://www.giorgiosbaraglia.it/password-manager-la-guida-completa/

I MIGLIORI PASSWORD MANAGER A PAGAMENTO

LastPass ••• | https://www.lastpass.com/it

1Password https://1password.com

DASHLANE https://www.dashlane.com/it/

KEEPER® https://keepersecurity.com/it_IT/

https://www.giorgiosbaraglia.it/password-manager-la-guida-completa/

I MIGLIORI PASSWORD MANAGER GRATUITI

KeePass https://keepass.info

App per smartphone: https://keepass.info/download.html

Bitwarden https://bitwarden.com

Il codice sorgente è pubblico, disponibile su GitHub (https://github.com/bitwarden), quindi accessibile per audit da parte di chiunque. Esiste anche versione Enterprise a pagamento.

passbolt https://www.passbolt.com

"Made in Luxembourg
where data privacy matters"

Password Safe
Simple & Secure Password Management

https://pwsafe.org

Progettata da Bruce Schneier

IN CONCLUSIONE…

COSA ABBIAMO DIMENTICATO?

IL “FATTORE UMANO”

"Il fattore umano è veramente l'anello più debole della sicurezza”

(“The Art of Deception”

Kevin Mitnick - 2002)

IL “FATTORE UMANO”

Oltre il 90% degli attacchi informatici sono causati dall’ERRORE UMANO

…quindi…

FARE FORMAZIONE !

FARE FORMAZIONE !

GDPR 39 - Compiti del responsabile della protezione dei dati (DPO)

Il responsabile della protezione dei dati è incaricato almeno dei seguenti compiti:

b) …la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

FARE FORMAZIONE !

… e poi istituire un **regolamento aziendale (Policy)** sull'uso delle risorse informatiche aziendali che stabilisca in modo chiaro cosa è permesso e cosa è vietato (perché pericoloso per l'azienda).

E prevedere sanzioni per chi viola tale regolamento

LA SICUREZZA
NON È UNA TECNICA,
È UN PROCESSO

IL SUCCO DEL DISCORSO…

?

QUALCHE DOMANDA

GRAZIE
DELL'ATTENZIONE

cybersec@giorgiosbaraglia.it

www.giorgiosbaraglia.it

SOCIO Clusit
Associazione Italiana per la Sicurezza Informatica