



«I sabati di AICIM»

La Cybersecurity nel processo di digitalizzazione di una PMI

18 marzo 2023
h. 10-12

10.00: Apertura lavori

Gianmarco Biagi, Presidente AICIM-AISOM e Holding 7p9

10.10: consapevolezza e sviluppo della sicurezza informatica nelle PMI

Michele Vanzi, Coordinatore Team Innovazione & ITC,
Founder Michele Vanzi&Partners

10.20: studio ed attuazione di un progetto di sicurezza informatica

Giulio Valeri, Founder Software Solutions S.r.l.

10.35: implementazione di sistemi per la protezione dei dati: aspetti legali ed operativi

Maria Clara Piatti, Innovaton Manager/ **William Di Cicco**, Avvocato

10.55: Le insidie informatiche di oggi e di domani: come difendersi

Giorgio Sbaraglia, Information & Cyber Security Advisor | DPO |
Docente 24 Ore Business School | Comitato Direttivo CLUSIT

11.55: Q&A - conclusione

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).

.....

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.



CHI SONO

Giorgio Sbaraglia, ingegnere

☑ Information & Cyber Security Advisor

☑ DPO (Data Protection Officer)

☑ Membro del Comitato Direttivo



☑ Coordinatore scientifico del Master “Cybersecurity e Data Protection” della 24Ore Business School

☑ Scrivo per: www.ictsecuritymagazine.com
www.agendadigitale.eu/
Rivista CLASS

☑ Collaboratore redazione www.cybersecurity360.it CYBERSECURITY360



I MIEI LIBRI



NON CI SONO PIÙ GLI HACKER DI UNA VOLTA...



IL PESO DEL CYBERCRIME SULL'ECONOMIA MONDIALE



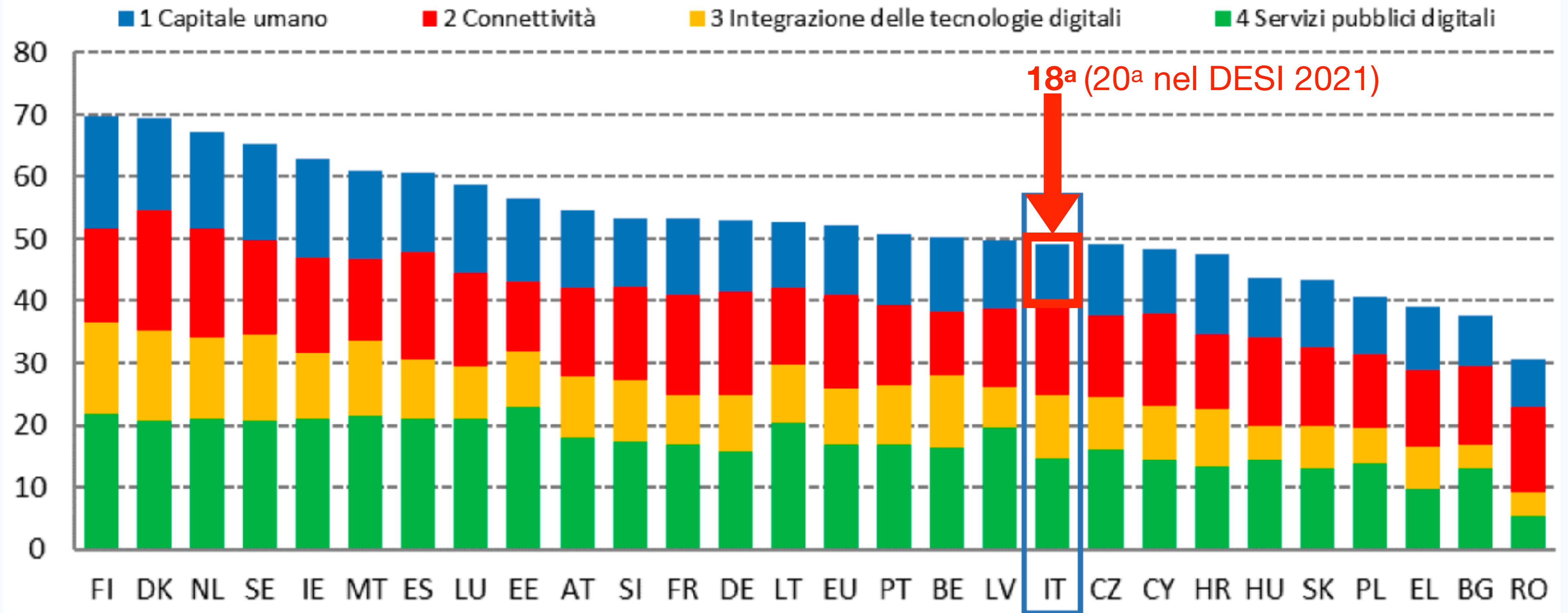
Cybersecurity Ventures prevede che i costi globali del crimine informatico cresceranno del 15% all'anno nei prossimi cinque anni, raggiungendo 10,5 trilioni di dollari all'anno entro il 2025, dai 3 trilioni di dollari del 2015,

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

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

DESI 2022: DIGITAL ECONOMY AND SOCIETY INDEX

Indice di digitalizzazione dell'economia e della società (DESI), Ranking 2022



<https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022>

DESI 2022: DIGITAL ECONOMY AND SOCIETY INDEX

	Italia	UE
	posizione in classifica	punteggio
DESI 2022	18	49,3

	Italia	UE
	posizione in classifica	punteggio
1 Capitale umano	25	36,6
DESI 2022	25	45,7

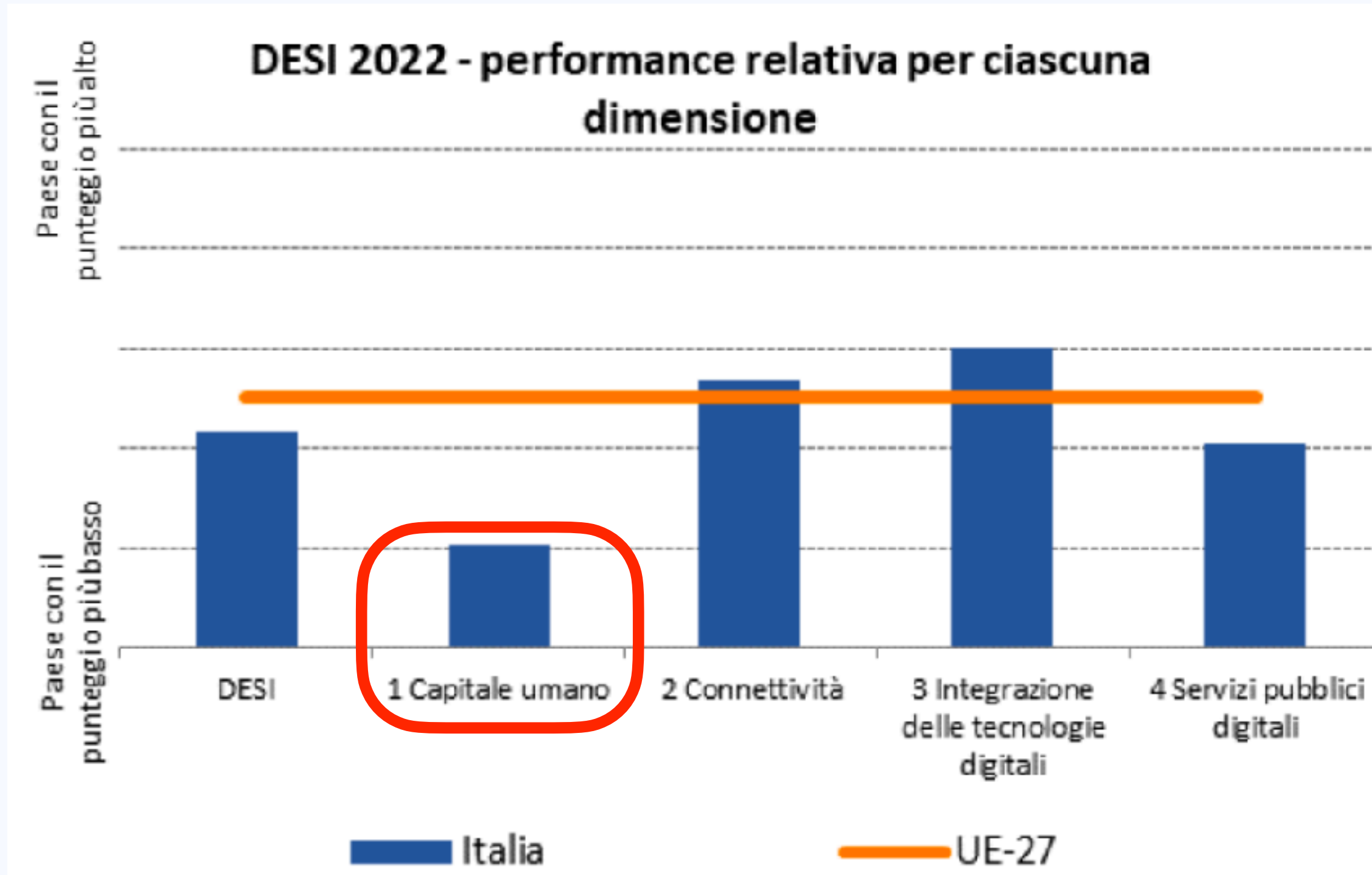
Indice di digitalizzazione dell'economia e della società (DESI), Ranking 2022

L'Italia sta guadagnando terreno e, se si considerano i progressi del suo punteggio DESI negli ultimi cinque anni, sta avanzando a ritmi molto sostenuti.

Per quanto riguarda il capitale umano, l'Italia si colloca (ancora!) al **25° posto su 27 paesi dell'UE**.

Solo il 46% delle persone possiede perlomeno competenze digitali di base, un dato al di sotto della media UE pari al 54%.

Il divario rispetto alla media UE è più ridotto quando si tratta di persone in possesso di competenze digitali superiori a quelle di base (**23% in Italia rispetto al 26% nell'UE**).



Il Rapporto CLUSIT

Rapporto Clusit 2023

sulla sicurezza ICT
in Italia



IL RAPPORTO CLUSIT 2023

CLUSIT: Associazione Italiana per la Sicurezza Informatica

Obiettivi:

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello comunitario che italiano.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza ICT.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

<https://clusit.it>

IL RAPPORTO CLUSIT 2023: “ITALIA NEL MIRINO ”

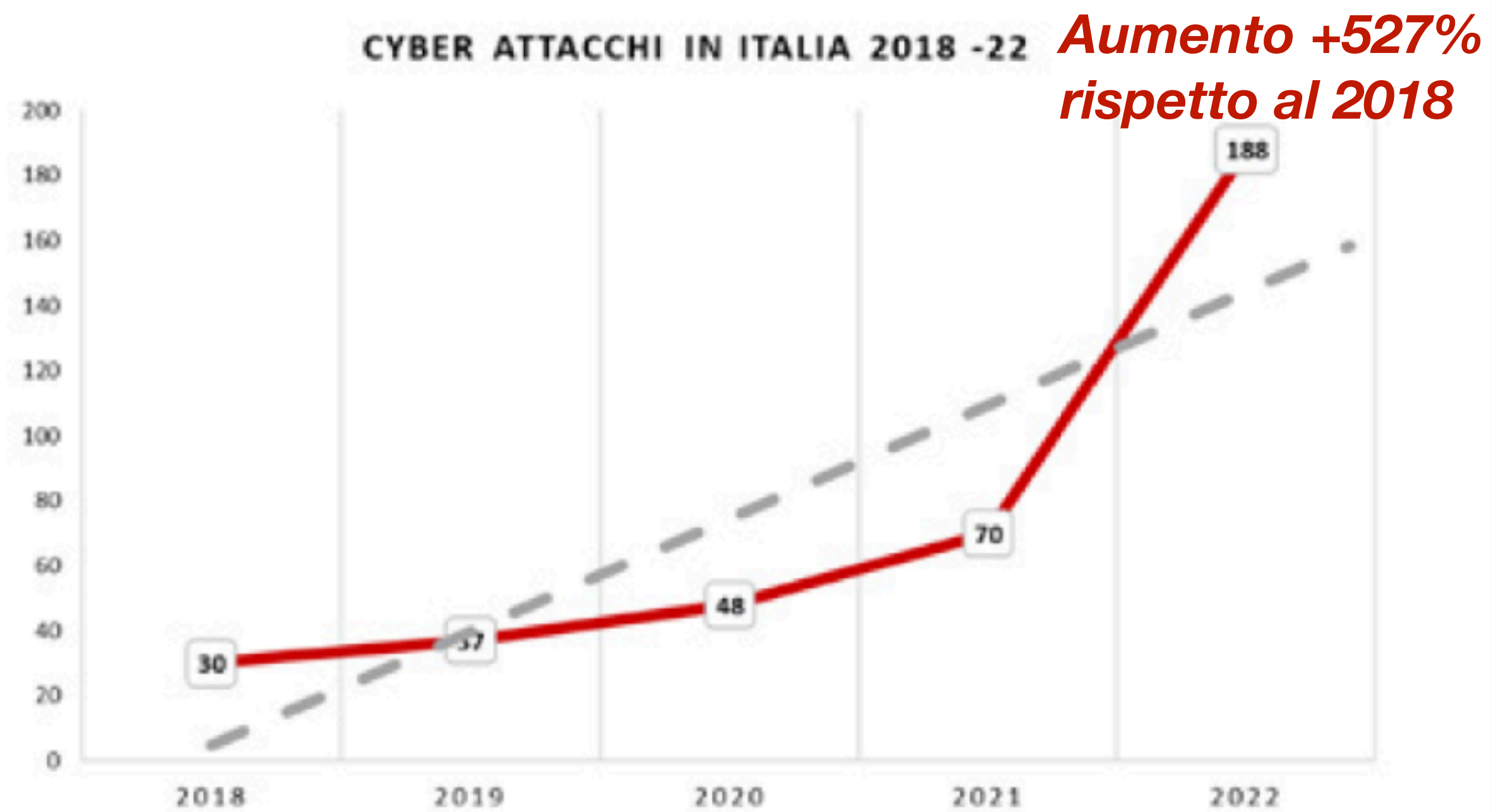


Fig. 23: Distribuzione dei cyber attacchi in Italia nel periodo 2018-2022



Fig. 24: Crescita percentuale degli attacchi Italia vs. global - 2018-2022

L'Italia è sovraesposta in termini di attacchi, rispetto alla sua dimensione nazionale: in pratica nel 2022 il dato italiano sui cyber attacchi rappresenta il 7,6% del totale del campione complessivo considerato a livello mondiale, a fronte di un PIL italiano che rappresenta appena il 2% del PIL mondiale (che è pari a 102 trilioni di dollari)

LE MINACCE PIÙ DIFFUSE:

IL SOCIAL ENGINEERING,

IL PHISHING,

I RANSOMWARE,

LE PASSWORD DEBOLI...

ANCHE I DISPOSITIVI MOBILI SONO A RISCHIO

IL SOCIAL ENGINEERING

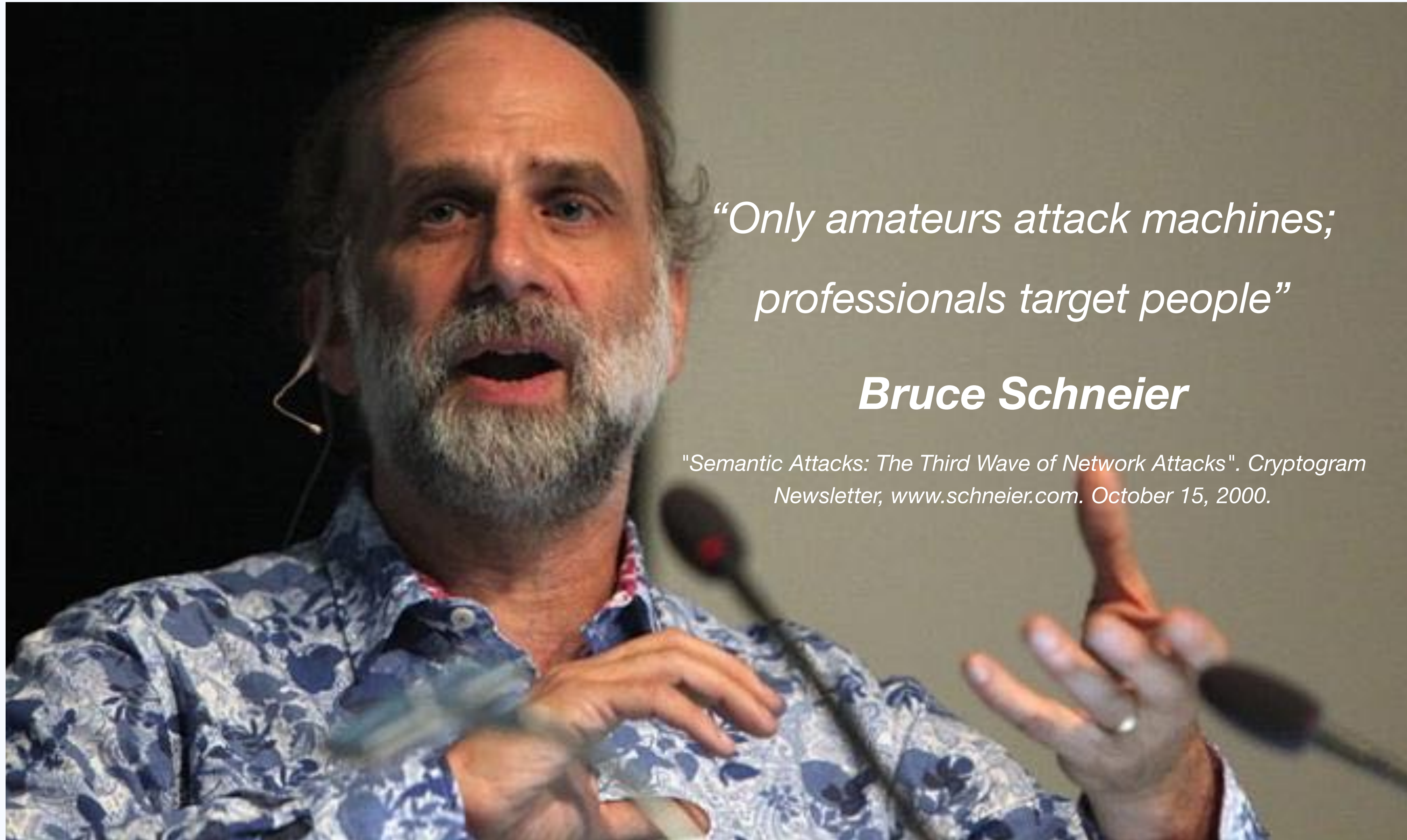
Cos'è il social engineering? (*human hacking*)

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 vulnerabilità dell'essere umano.**



*“Only amateurs attack machines;
professionals target people”*

Bruce Schneier

*"Semantic Attacks: The Third Wave of Network Attacks". Cryptogram
Newsletter, www.schneier.com. October 15, 2000.*



95% of cybersecurity breaches are caused by human error.

Cybint



<https://www.varonis.com/blog/cybersecurity-statistics/>

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 80% 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.

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.



Austin Police Department ✓
@Austin_Police

🚨 Scam Alert 🚨

APD Financial Crimes detectives are investigating after fraudulent QR code stickers were discovered on City of Austin public parking meters. People attempting to pay for parking using those QR codes may have been directed to a fraudulent website and made a payment.

[Traduci il Tweet](#)



10:55 PM · 3 gen 2022 · Twitter Web App

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.

Attenzione ai link!

URL FALSIFICATI: ATTACCHI OMOGRAFICI O TYPOSQUATTING

Originale	<u>google.com</u>	<u>microsoft.com</u>	<u>bankofamerica.com</u>	<u>domus.it</u>
FALSO	<u>go0gle.com</u>	mlcrosoft.com	<u>bankofarnerica.com</u>	<u>dornus.it</u>
FALSO	<u>goooogle.com</u>	<u>microsoft.co</u>	<u>bank-of-america.com</u>	<u>domus.It</u>

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!).

L'EMAIL NON È UNO STRUMENTO SICURO: LA BUSINESS EMAIL COMPROMISE (BEC)

LA TRUFFA: "CEO FRAUD"



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!

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@pippodornus.it

Oppure potrebbe essere modificata in info@pipp0domus.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

RANSOMWARE: LA MINACCIA PIÙ TEMIBILE PER LE AZIENDE

27 GIUGNO 2017: ATTACCO NOTPETYA

NotPetya cyber attack on TNT Express cost FedEx \$300m

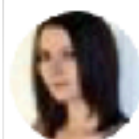
Falling victim to global ransomware attack "posed significant operational challenges", the company says in its latest financial report.



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

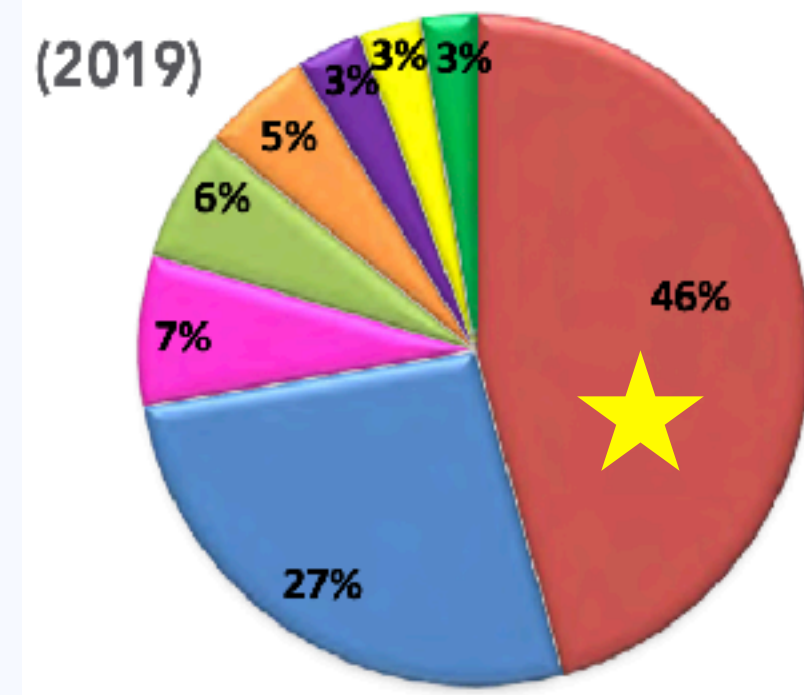
NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs

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

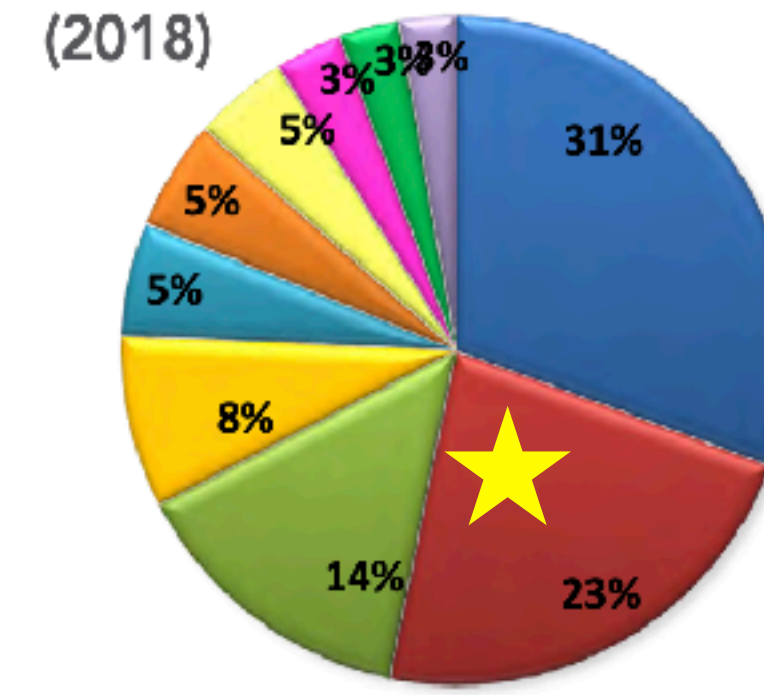


By [Charlie Osborne](#) for [Zero Day](#) | January 26, 2018 -- 10:25 GMT (10:25 GMT) | Topic: [Security](#)

Tipologia e distribuzione Malware



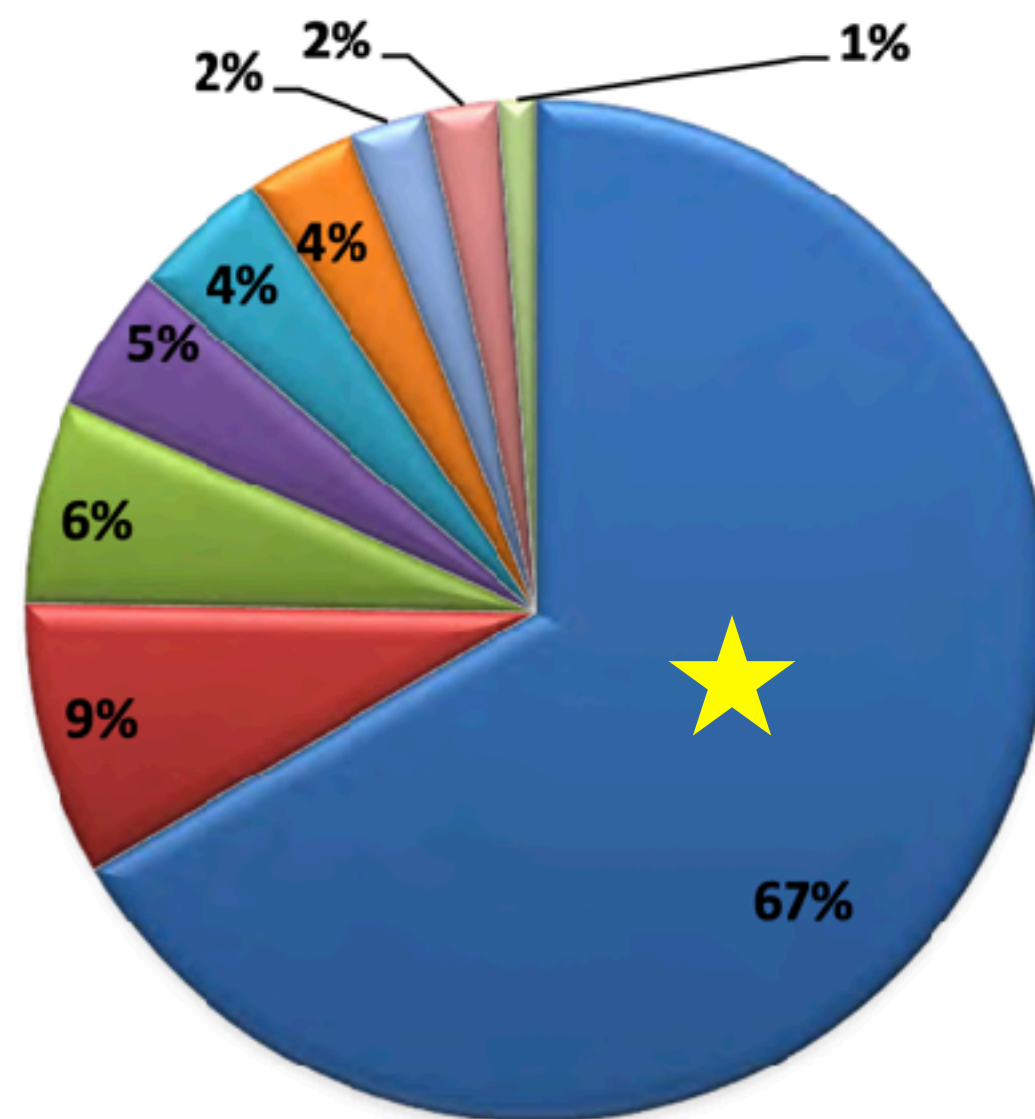
■ Ransomware
 ■ Generic malware
 ■ RAT
 ■ Crypto*
 ■ Android malware
 ■ Banking trojan
 ■ Botnet
 ■ Apple malware



■ Other
 ■ Ransomware
 ■ Cryptominers
 ■ Android
 ■ RAT
 ■ Botnet
 ■ Backdoor
 ■ Banking Trojan
 ■ Apple
 ■ Spyware

© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Tipologia Malware (2020)



■ Ransomware
 ■ RAT
 ■ Others
 ■ Magecart
 ■ Crypto*
 ■ Backdoor
 ■ POS
 ■ Botnet
 ■ spyware

© 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

- 📌 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).
- 📌 Su 793 incidenti di ransomware segnalati a **FinCEN** (Financial Crimes Enforcement Network) nella seconda metà del 2021, il **75% aveva un legame con la Russia.**

I RANSOMWARE

- 📌 Il 93% di chi subisce attacchi accusa **downtime** e/o **perdita di dati**.
- 📌 Il tempo medio di downtime è di **9,6 giorni**.
- 📌 I più recenti, oltre a criptare i file, fanno **Upload**: esfiltrazione dei dati sensibili, minacciandone la divulgazione pubblica (GDPR?!).

Double Extortion!

Ransomware: Maze (dal 2019), NetWalker, RagnarLocker, Conti, LockBit, 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*).
- 📌 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*).
- 📌 2021: riscatto richiesto ad ACER 50 milioni di dollari, a Kaseya 70 M\$, 200M\$ a Media World.

I RANSOMWARE

- 📌 **Riscatto in Bitcoin (o altra criptovaluta).**
- 📌 Il 75% delle aziende che hanno pagato il riscatto avevano avuto il **backup compromesso**.
- 📌 Il 27% delle piccole e medie imprese italiane non possiede un backup, dato che sale fino al 43% tra le sole piccole imprese.

**Se paghiamo il riscatto,
qual è la probabilità di riavere indietro i propri dati?**

**La percentuale di dati ripristinati dopo il pagamento è diminuita:
61% dei dati criptati ripristinati dopo il pagamento del riscatto**
(fonte Sophos: The State of Ransomware 2022)



**Tra le organizzazioni che hanno scelto di pagare un riscatto,
l'80% ha subito un altro attacco**



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**

COME PROTEGGERSI

- 1) Attenzione alle **email**: link e allegati possono essere pericolosi!
- 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** e altri supporti rimovibili (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 maggior elemento di rischio

L'IMPORTANZA DELLE PASSWORD

VERIZON DATA BREACH INVESTIGATIONS REPORT



What tactics do they use?

62% of breaches featured hacking.

51% over half of breaches included malware.

81% of hacking-related breaches leveraged either stolen and/or weak passwords.

43% were social attacks.

14% Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% Physical actions were present in 8% of breaches.

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

MA LE PERSONE CONTINUANO AD USARE PASSWORD MOLTO BANALI...

- | | | |
|--|----------------|---------------|
| 1. password | 12. 1234 | 23. 110110jp |
| 2. 123456 (<i>al primo posto dal 2013</i>) | 13. 1234567890 | 24. 1111 |
| 3. 123456789 | 14. 000000 | 25. 987654321 |
| 4. guest | 15. 555555 | 26. 121212 |
| 5. qwerty | 16. 666666 | 27. Gizli |
| 6. 12345678 | 17. 123321 | 28. abc123 |
| 7. 111111 | 18. 654321 | 29. 112233 |
| 8. 12345 | 19. 7777777 | 30. azerty |
| 9. col123456 | 20. 123 | 31. 159753 |
| 10. 123123 | 21. D1lakiss | 32. 1q2w3e4r |
| 11. 1234567 | 22. 777777 | 33. 54321 |



La classifica delle password più utilizzate in **ITALIA** nel 2022:

(Fonte: **NordPass**)



- | | | |
|--------------------|---------------------|-----------------------|
| 1. 123456 | 12. 1234 | 23. federica |
| 2. 123456789 | 13. amoremio | 24. chiara |
| 3. password | 14. porcodio | 25. napoli1926 |
| 4. ciao | 15. francesca | 26. 1350865 |
| 5. juventus | 16. francesca | 27. 000000 |
| 6. napoli | 17. 1234567890 | 28. antonio |
| 7. ciaociao | 18. alessia | 29. vaffanculo |
| 8. 12345 | 19. qwerty | 30. valentina |
| 9. 12345678 | 20. andrea | 31. giorgia |
| 10. martina | 21. alessandro | 32. 1234567 |
| 11. giulia | 22. giuseppe | 33. simone |

CARATTERISTICHE DI UNA PASSWORD

1. **NUMERO** di caratteri usati: da 12 a 20 (non serve andare oltre)

2. **TIPI** di caratteri usati:

☒ Numeri (0-9) = **10**

☒ Lettere (a-z, A-Z) = **52** (26 minusc. + 26 maiusc.)

☒ caratteri speciali da tastiera (# &%?^ ecc.) = **33**


TOTALE = 95 caratteri (codici ASCII dal 32 al 126)

Purtroppo in alcuni siti – irragionevolmente - vengono imposte delle LIMITAZIONI al numero dei caratteri e NON sono permessi i caratteri speciali

QUANTE SONO LE COMBINAZIONI POSSIBILI?

Consideriamo – per semplicità - una Password di 4 caratteri:

Solo NUMERI: $10^4 =$	10.000 combinazioni
Solo LETTERE MINUSC.: $26^4 =$	456.976 combinazioni
LETTERE MIN.+MAIUSC.: $52^4 =$	7.311.616 combinazioni
NUMERI+LETTERE: $62^4 =$	14.766.366 combinazioni
NUM.+LETT.+CAR.SPEC.: $95^4 =$	81.450.625 combinazioni



**Aumentando i tipi dei caratteri, il numero
delle combinazioni cresce in modo
ESPONENZIALE**

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/>)

Home Notify me Domain search Who's been pwned Passwords API About Donate ₿

';--have i been pwned?

Check if your email or phone is in a data breach



mario.rossi@gmail.com pwned?

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

Why 1Password?

646 pwned websites	12,441,647,441 pwned accounts	115,580 pastes	227,246,091 paste accounts
-----------------------	----------------------------------	-------------------	-------------------------------

<https://haveibeenpwned.com>


[Home](#) [Notify me](#) [Domain search](#) [Who's been pwned](#) [Passwords](#) [API](#) [About](#) [Donate](#) 

'--have i been pwned?

Check if your email or phone is in a data breach

Oh no — pwned!

Pwned in 56 [data breaches](#) and found 4 [pastes](#) ([subscribe](#) to search sensitive breaches)

 3 Steps to better security

<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 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, che non consiglio) 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, quindi proteggiamolo con una password forte, in fondo è l'unica che dovremo veramente ricordare.

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



**In ogni cyber attacco
c'è sempre almeno un
ERRORE UMANO**

PEBKAC: “Problem Exists Between Keyboard And Chair”

Grazie per l'attenzione

cybersec@giorgiosbaraglia.it

www.giorgiosbaraglia.it

