IL DIGITALE CONSAPEVOLE

Sicurezza digitale per tutti, conoscere per evitare

#25NOVEMBRE
Giornata internazionale contro la violenza sulle donne

CHI SONO?

Enrico Catalano

Libero professionista, consulente senior per la normativa sulla protezione dei dati personali e per la gestione della sicurezza delle informazioni, docente per la formazione professionale in materia di privacy & Information Security.

Auditor qualificato per i sistemi di gestione della sicurezza delle informazioni conformi alla norma standard ISO 27001.

Socio di LUGMan APS dal 2006 e dal 2016 membro del Consiglio Direttivo dell'associazione

COSA VI RACCONTO?

- Introduzione alla Cybersecurity e sicurezza delle informazioni;
- Il quadro attuale sul Cybercrime e sui crimini informatici;
- Le minacce informatiche e gli attacchi più comuni:

  Malware, Ransomware, DDoS, Vulnerabilities
- Social Engineering e Phishing:

  le tecniche d'attacco con casi ed esempi pratici
- Social Media, Cyber Risk e Revenge Porn
- Alcune misure di prevenzione.

INFORMATION TECHNOLOGY, CYBERSECURITY, INTERNET OF THINGS… CONOSCIAMO QUESTI TERMINI?

Information Technology (IT)
Questo termine si riferisce all'insieme dei metodi e delle tecnologie che compongono i sistemi (informatici) usati per l'elaborazione, l'archiviazione, la trasmissione, l'utilizzo di dati e informazioni.

Operation Technology (OT)
Il termine intende una categoria di sistemi informatici e di comunicazione adibiti alla gestione, al monitoraggio e controllo dei processi industriali e delle apparecchiature di produzione.

Internet of Things (IoT)
Il termine intende una rete di oggetti fisici ("cose") dotati di sensori, software e tecnologie per raccogliere e scambiare dati in rete.
La connessione permette agli oggetti di comunicare tra loro e con sistemi e persone, abilitando le automazioni e gli scambi di dati.

Cybersecurity
Detta anche cybersicurezza o anche sicurezza informatica, consiste nell'insieme di tecnologie, processi e misure di protezione, progettati ed attuati per ridurre il rischio di attacchi informatici.

Resilienza (digitale)
Con questo termine ci si riferisce alla capacità di prevenire, rilevare, rispondere e riprendersi prontamente da interruzioni dei sistemi informatici, dovute ad incidenti o attacchi.

DIFFERENZA TRA INFORMATION SECURITY E CYBERSECURITY

Il termine **Information Security** rappresenta l'insieme di metodi, tecnologie e regole che sono attuate per garantire la **sicurezza delle informazioni**: si riferisce alla protezione globale delle informazioni e riguarda tutte le forme e modi in cui vengono gestite, anche le informazioni stampate e trasmesse a voce.

La **Cybersecurity** invece si concentra sulla protezione delle informazioni digitali, dei sistemi informatici e delle reti per prevenire possibili minacce informatiche e incidenti informatici, con il principale obiettivo di mantenere al sicuro le risorse digitali e i dati trattati con questi sistemi.
La Cybersecurity può essere vista come una sottocategoria dell'Information Security.

Cybersecurity e sicurezza informatica sono concetti sovrapposti, perché entrambe affrontano le minacce ai sistemi digitali di un'organizzazione e i dati che vi sono trattati.

COSA DEFINISCE LA SICUREZZA DELLE INFORMAZIONI?

Integrità

Con questo termine si intende, nell'ambito della sicurezza informatica, garantire la protezione delle informazioni nei confronti di modifiche accidentali (involontarie) oppure effettuate volontariamente da un attaccante attraverso una minaccia. L'integrità rappresenta la garanzia che le informazioni sono accurate, complete e coerenti in qualsiasi momento del loro ciclo di vita.

Riservatezza (confidenzialità)

Significa che l'informazione deve essere accessibile solo a chi è autorizzato a conoscerla, ovvero deve essere protetta da un accesso non autorizzato o illecito. Può essere sinonimo di privacy e segretezza, che a volte sono utilizzati per distinguere tra protezione dei dati personali degli utenti (privacy) dalla protezione dei dati appartenenti all'organizzazione (segretezza).

Disponibilità

Con questo termine si intende la proprietà delle informazioni di essere accessibili ed utilizzabili da parte di chi è autorizzato a conoscerle, quando necessario e senza eccessivi ritardi.

LA RESPONSABILITÀ DELLE PERSONE PER LA CYBERSECURITY

«CONOSCERE PER EVITARE»

Ogni persona che usa strumenti informatici deve essere istruita e consapevole delle proprie azioni, con lo scopo di prevenire e ridurre le minacce informatiche. Il concetto di «responsabilità» significa anche controllare le informazioni in modo selettivo e protetto, in modo che le azioni che influenzano la sicurezza delle informazioni siano riconducibili al diretto responsabile.

CONOSCIAMO I RISCHI INFORMATICI?

CYBERCRIME E RISCHI INFORMATICI – LA SITUAZIONE EUROPEA

ENISA Report 2024
sullo stato della
Cybersecurity
In Europa
i 21 rischi informatici più importanti ed attuali
(nei primi tre posti della classifica vi sono due rischi relativi alle persone)

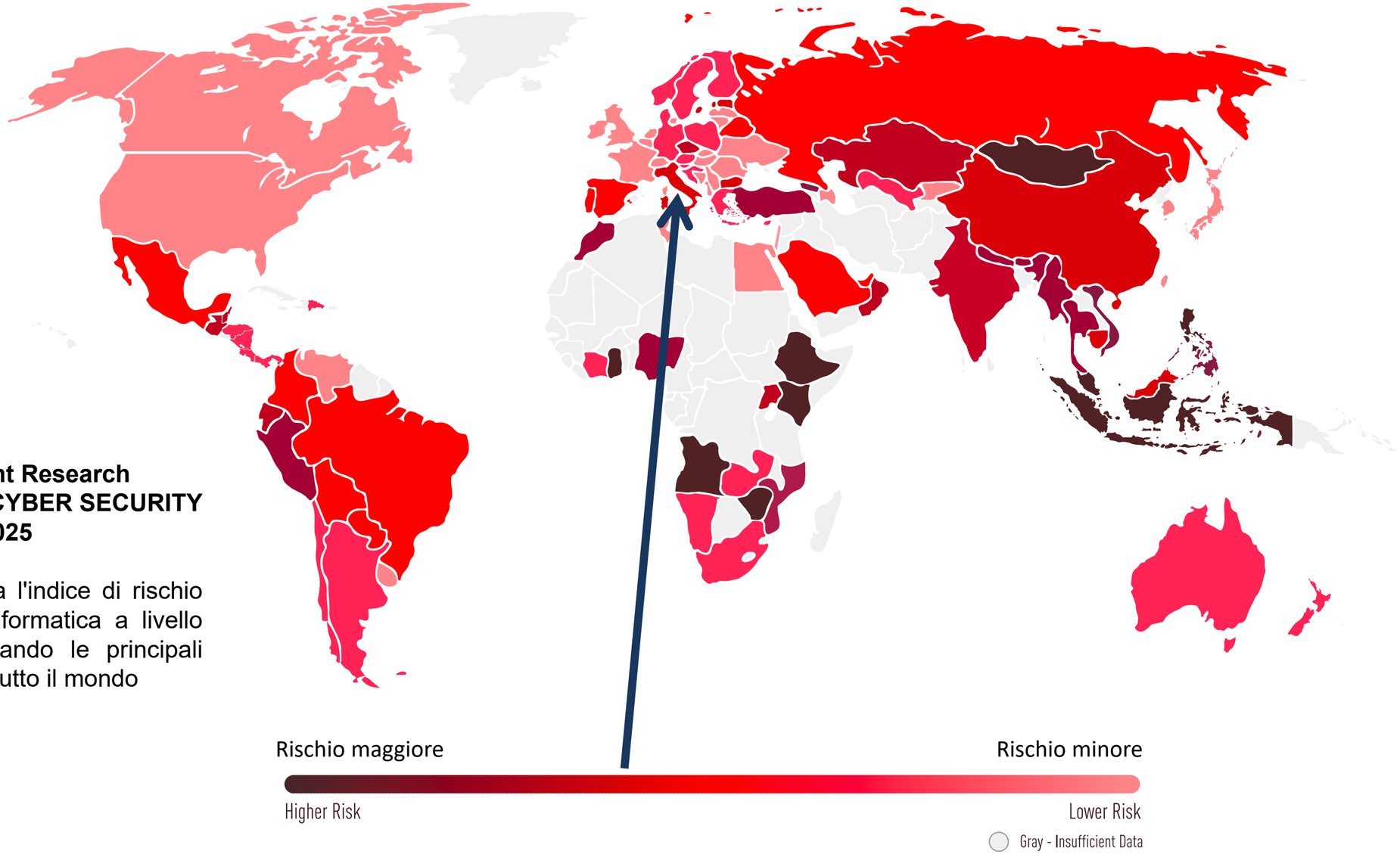
1. Compromissione della Supply Chain informatizzata
2. Carenza di competenze
3. Errore umano e sistemi legacy sfruttati all'interno di ecosistemi cyber-fisici
4. Sfruttamento di sistemi non patchati e obsoleti all'interno dell'ecosistema tecnologico attaccato
5. Ascesa dell'autoritarismo della sorveglianza digitale / perdita della privacy
6. Fornitori di servizi ICT transfrontalieri come singolo punto di errore
7. Campagne avanzate di disinformazione / operazioni di influenza
8. Ascesa di minacce ibride avanzate
9. Abuso di Intelligenza Artificiale
10. Impatto fisico di interruzioni naturali/ambientali su infrastrutture digitali critiche
11. Mancanza di analisi e controllo delle infrastrutture e degli oggetti basati sullo spazio
12. Attacchi mirati potenziati dai dati dei dispositivi intelligenti
13. Aumento della criminalità informatica abilitata dalla valuta digitale
14. Manipolazione dei sistemi necessari per la risposta alle emergenze
15. Manomissione della catena di fornitura del software di verifica deepfake
16. L'intelligenza artificiale interrompe/potenzia gli attacchi informatici
17. Inserimento di malware per interrompere la catena di fornitura della produzione alimentare
18. Sfruttamento dei dati di e-health (e genetici)
19. Attacchi tramite elaborazione quantistica
20. Interruzioni nelle blockchain pubbliche
21. Incompatibilità tecnologica delle tecnologie blockchain

LUGMan

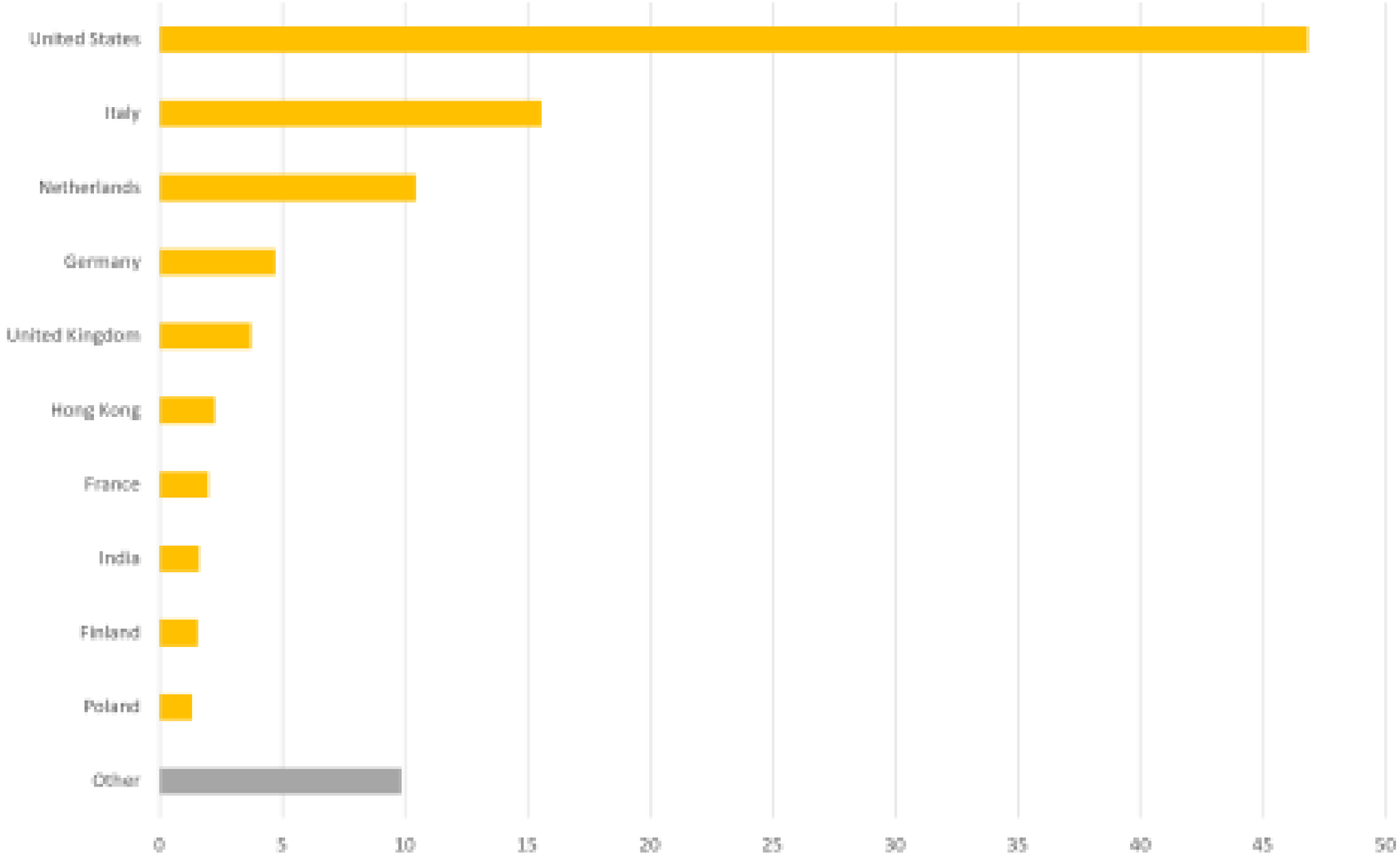
CYBERCRIME E CYBER RISK – LO SCENARIO NEL MONDO

CheckPoint Research
THE STATE OF CYBER SECURITY 2025

La mappa mostra l'indice di rischio della minaccia informatica a livello globale, evidenziando le principali aree di rischio in tutto il mondo



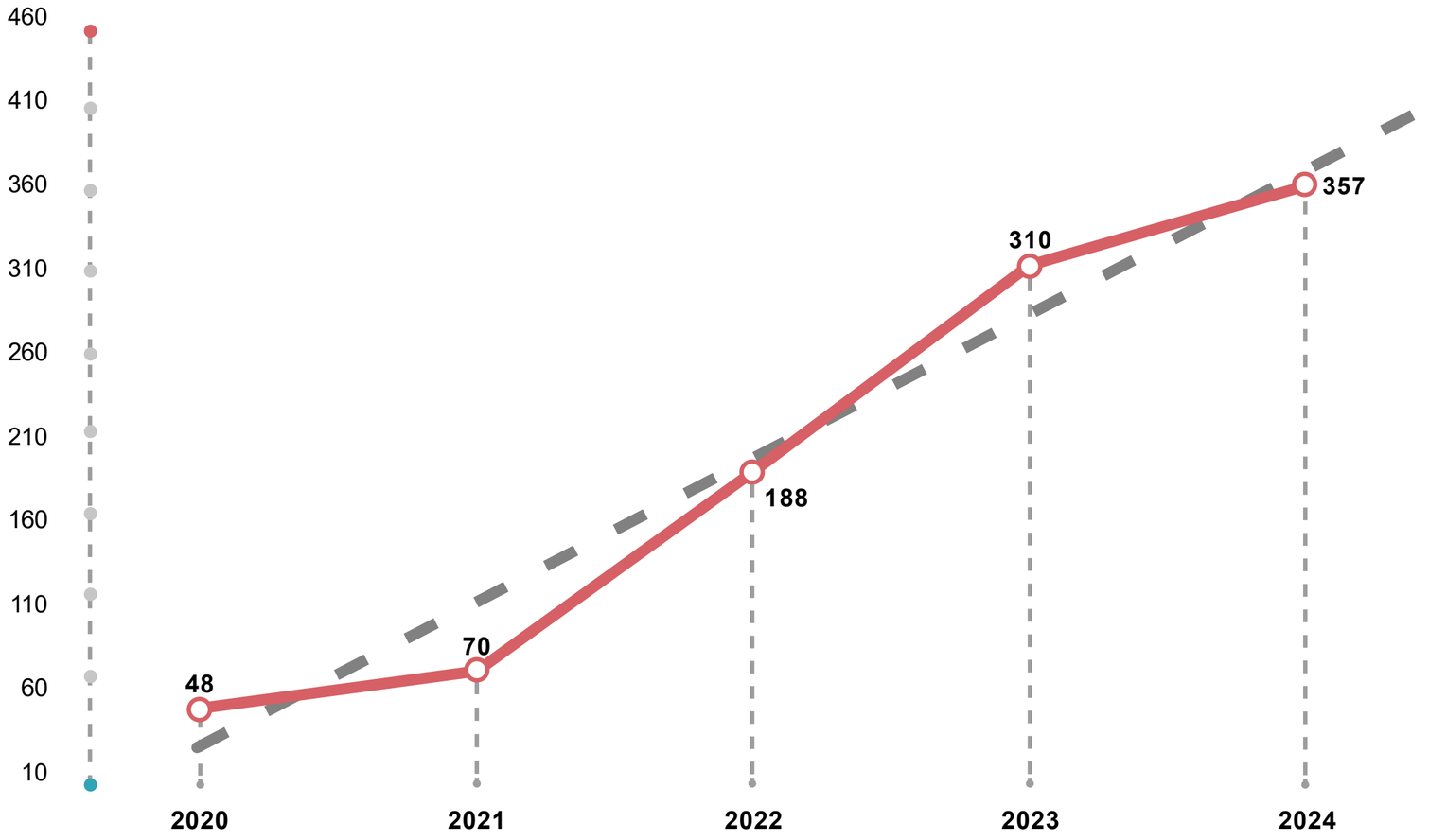
CYBERCRIME E ATTACCHI CYBER – LO SCENARIO NEL MONDO



Dislocazione delle sorgenti di attacco rilevate dai Web Application Firewall *(Dati Fastweb, anno 2024)*

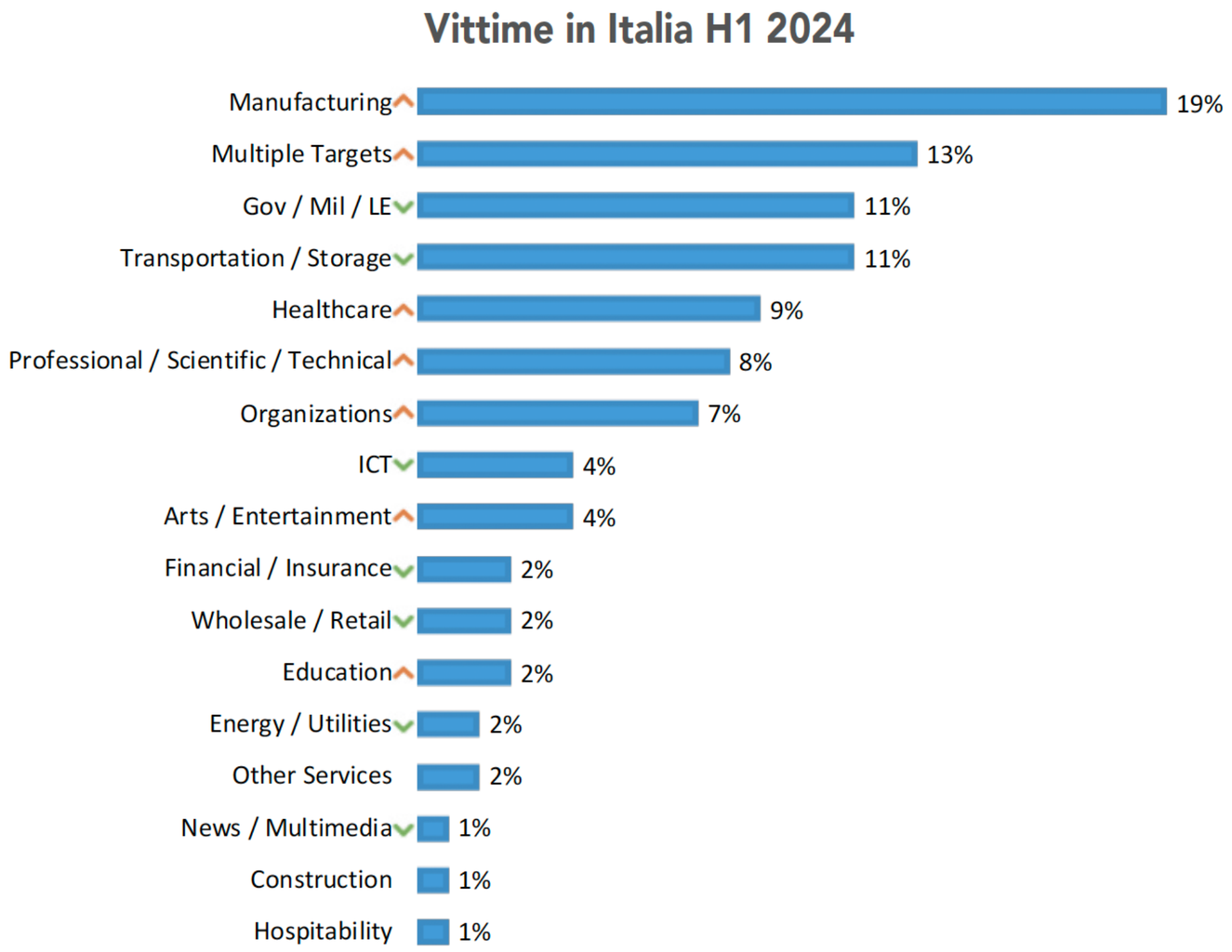
CYBERCRIME – LA SITUAZIONE ITALIANA

Incidenti Cyber in Italia 2020 -2024



© Clusit - Rapporto 2025 sulla Cybersecurity

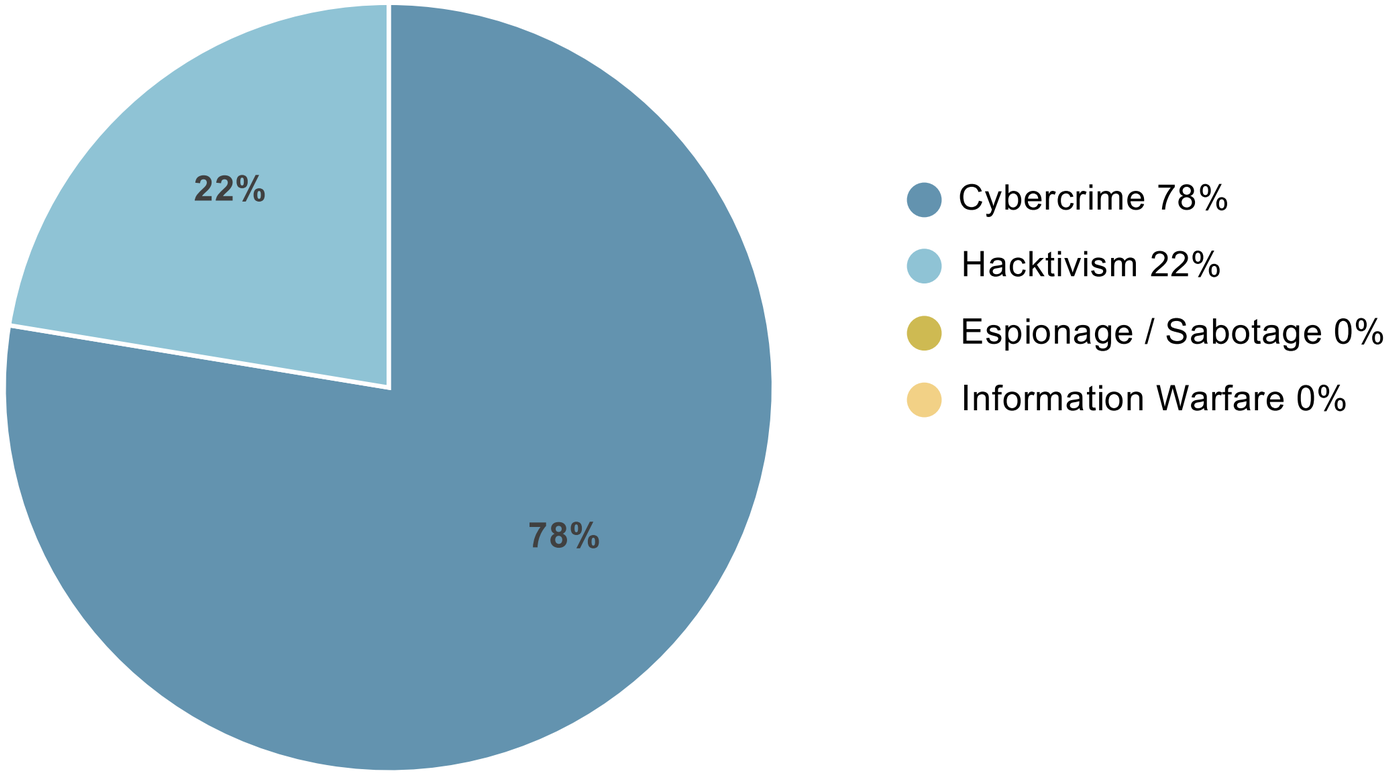
CYBERCRIME – LA SITUAZIONE ITALIANA



© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia - Aggiornamento giugno 2024

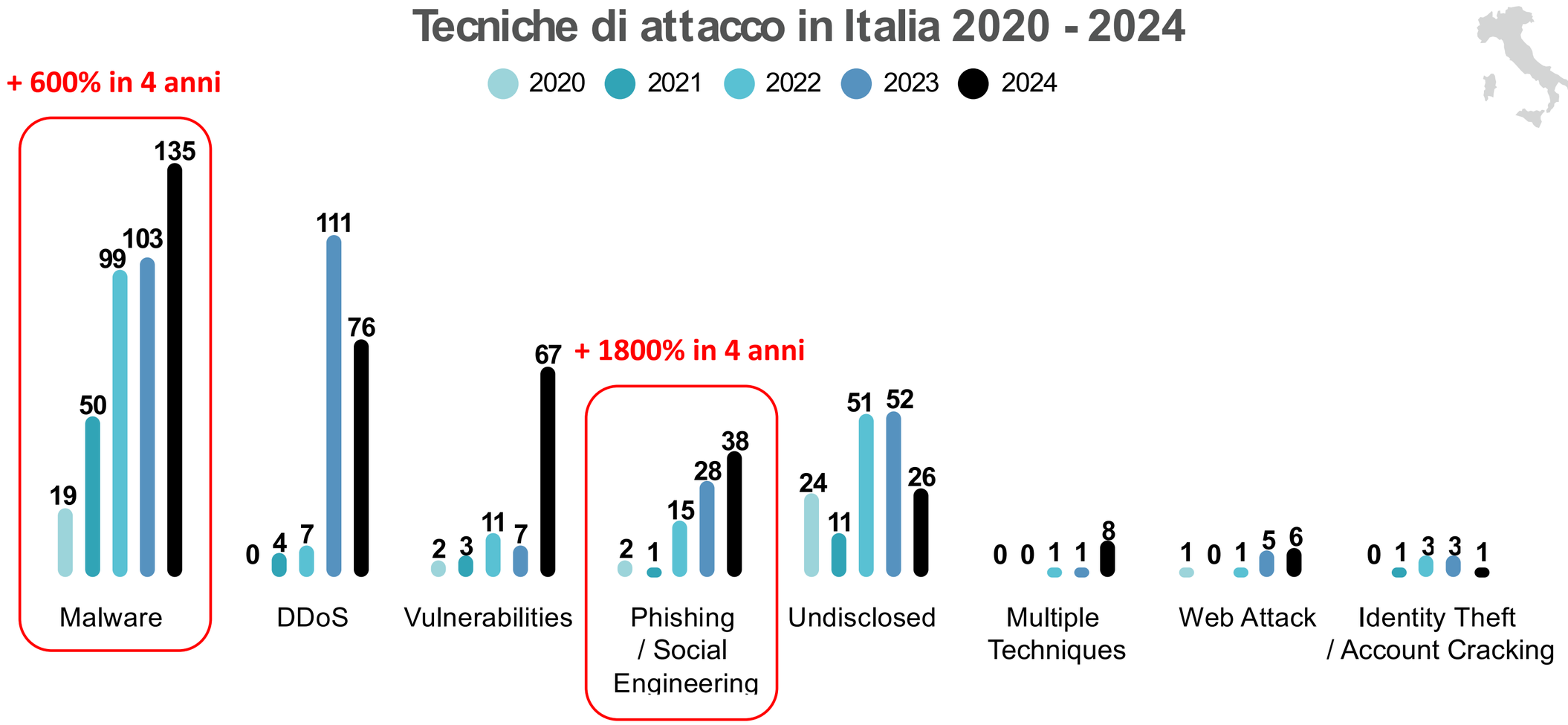
CYBERCRIME – LA SITUAZIONE ITALIANA

Attaccanti in Italia 2024



© Clusit - Rapporto 2025 sulla Cybersecurity

CYBERCRIME – LA SITUAZIONE ITALIANA



CYBERCRIME E MINACCE INFORMATICHE – LE VULNERABILITÀ

Una **vulnerabilità informatica** è un difetto o una debolezza nella progettazione, nella realizzazione o nel funzionamento e nella gestione di un sistema informatico, un software o una rete, che può essere sfruttata dagli aggressori per ottenere un accesso non autorizzato, interrompere le operazioni o rubare informazioni sensibili. Le vulnerabilità possono derivare da varie fonti, come bug del software, configurazioni errate o pratiche di sicurezza inadeguate.

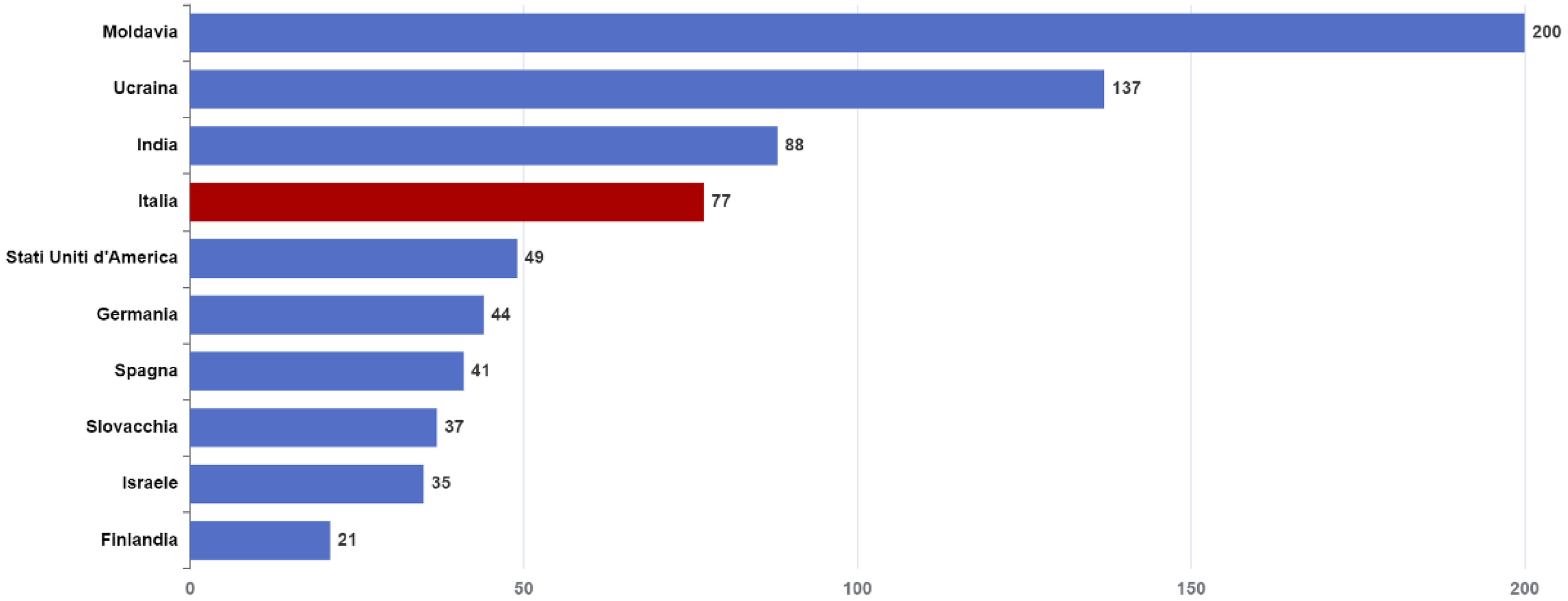
Il concetto di vulnerabilità non va confuso con la minaccia, che è l'elemento attivo di potenziale innesco di un rischio: la minaccia è l'agente che, sfruttando una vulnerabilità, può arrecare un disturbo, un attacco, un danno al sistema ed alle informazioni che vi sono gestite.
In pratica, la minaccia è la causa scatenante (spesso non controllabile direttamente), la vulnerabilità è la concausa (questa sì controllabile) che consente l'azione della minaccia in funzione della probabilità con cui può manifestarsi e generare il rischio con relativo impatto.

CYBERCRIME E MINACCE INFORMATICHE – ATTACCHI DDOS

Denial Of Service – Distributed Denial Of Service (DOS o DDOS)

Questo termine, la cui traduzione significa «*negazione del servizio*», descrive un tentativo ostile di bloccare il normale traffico di un server, di un servizio internet o di una rete esaurendo le risorse del sistema o sovraccaricando l'infrastruttura di rete.
Gli attacchi DDoS vengono realizzati sfruttando come fonti di attacco più sistemi informatici compromessi (da cui «*distributed*») i cosiddetti *botnet* che sono dei gruppi di computer o dispositivi IoT o apparecchiature OT che sono stati infettati da malware e sotto il controllo di un criminale informatico mentre i possessori/utenti ne sono completamente ignari.
Un attacco DDoS è paragonabile a un ingorgo autostradale che impedisce al traffico regolare di arrivare a destinazione.

CYBERCRIME E MINACCE INFORMATICHE – ATTACCHI DDOS

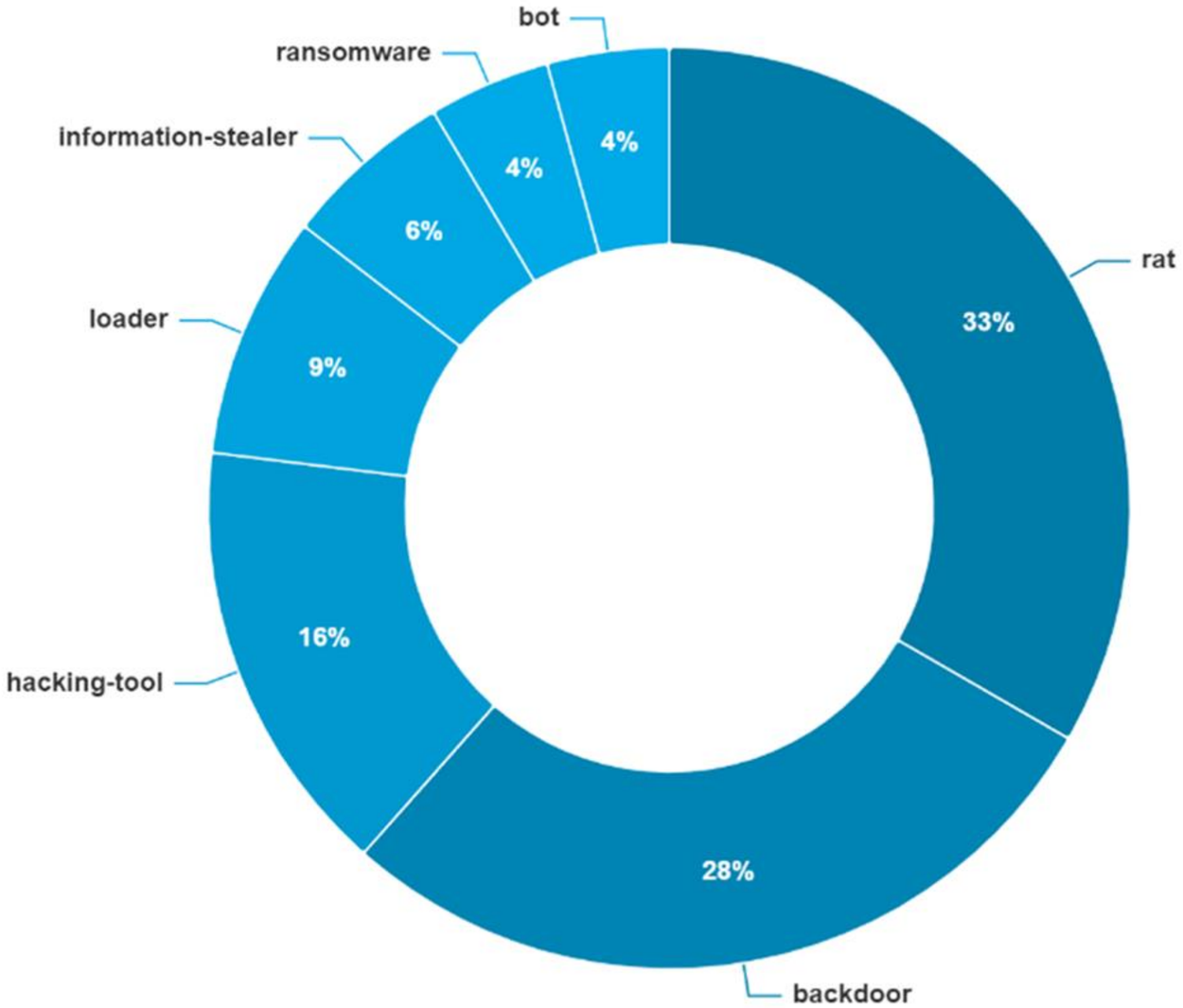


Numero di rivendicazioni degli attacchi DDoS per nazione a maggio 2024 (fonte: ACN)

CYBERCRIME E MINACCE INFORMATICHE – IL MALWARE

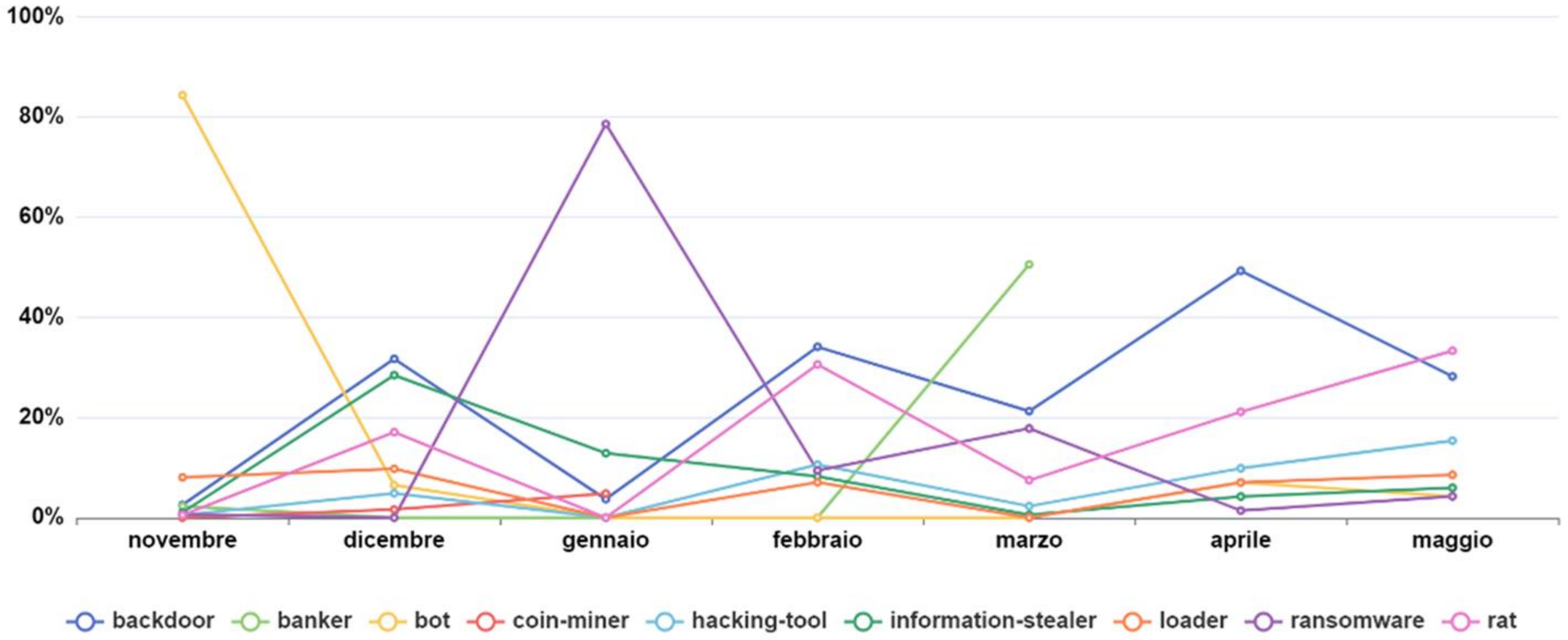
Con il termine generico **Malware** si intende un software dannoso che può essere utilizzato per raggiungere diversi obiettivi su un sistema infetto, ovvero qualsiasi software o firmware destinato a eseguire un processo non autorizzato che avrà un impatto negativo sulla riservatezza, l'integrità o la disponibilità delle informazioni all'interno di un sistema.
Esempi di Malware includono virus, worm, trojan horse o altre entità basate su codice che infettano un host.
A seconda dell'obiettivo dell'autore della minaccia, le funzionalità del malware possono variare dall'ottenere il controllo su sistemi e reti (ad esempio botnet), sui dati (ad esempio furto di informazioni), al consentire l'accesso remoto a reti infette (ad esempio Remote Access Trojan, RAT) e all'installazione di altri software dannosi sui dispositivi delle vittime (ad esempio downloader).

CYBERCRIME E MINACCE INFORMATICHE – IL MALWARE



tipologie di malware più diffuse in Italia a maggio 2025 (fonte: ACN)

CYBERCRIME E MINACCE INFORMATICHE – IL MALWARE



andamento semestrale della diffusione della tipologia di malware in Italia a maggio 2025 (fonte: ACN)

CYBERCRIME E MINACCE INFORMATICHE – IL MALWARE

ALCUNI TRA I MALWARE PIÙ PERICOLOSI DEL 2025

- **Lumma**: è un malware noto per la sua capacità di rubare informazioni sensibili: credenziali di accesso (username e password), informazioni finanziarie (dati di carte di credito, conti bancari), dati personali. La sua diffusione è avvenuta con pagine CAPTCHA false, download da Torrent e attacchi phishing mirati.
- **XWorm, controllo da remoto**: è un malware che consente ai criminali informatici il controllo remoto dei computer infetti, può monitorare le attività delle vittime (registra schermo e tastiera), installare ulteriori malware e utilizzare il computer infetto per lanciare attacchi verso altri sistemi.
- **AsyncRAT, il Trojan multifunzione**: un trojan di accesso remoto (RAT) diffuso con email di spam, può registrare lo schermo della vittima e il keylogging (sequenze di tasti), spiare le attività dell'utente, rubare password, accedere a file e cartelle, controllare webcam e microfono.
- **FakeUpdates**: sfrutta delle finte pagine di aggiornamento del browser, servite da siti legittimi compromessi, è progettato per bypassare i sistemi di sicurezza basati su firme, eludere il rilevamento grazie a tecniche di offuscamento. Gli attaccanti iniettano script malevoli che reindirizzano l'utente verso una pagina falsificata

(www.akamai.com, www.noisicurezza.com, www.cybersecurity360.it)

CYBERCRIME E MINACCE INFORMATICHE – IL RANSOMWARE

Il termine **ransomware** descrive un tipo di attacco dannoso in cui gli aggressori prendono il controllo degli asset (*beni informativi di valore*) di un bersaglio (*l'azienda*) e richiedono un riscatto in cambio della restituzione della disponibilità degli asset; generalmente, gli aggressori crittografano i dati aziendali e richiedono un pagamento per ripristinare l'accesso ai dati.
I cybercriminali possono anche rubare le informazioni e richiedere un pagamento aggiuntivo in cambio della mancata divulgazione dei dati alle autorità, ai concorrenti o al pubblico.

Gli attacchi ransomware sono una minaccia persistente con un tasso di incidenti costante, tuttavia le misure di sicurezza informatica messe in atto, tra cui (soprattutto) delle solide strategie di backup e ripristino, hanno consentito alle organizzazioni di resistere agli attacchi ransomware senza dover pagare dei riscatti per ripristinare l'accesso ai dati.
La decisione di pagare o meno è influenzata da vari fattori, tra cui la natura dell'attività, la criticità dei dati crittografati e la tolleranza al rischio dell'organizzazione.

CYBERCRIME E MINACCE INFORMATICHE – SOCIAL ENGINEERING

Con il termine **Social Engineering** ci si riferisce a tutte le tecniche di attacco che sono volte a convincere una vittima a rivelare informazioni specifiche o a compiere un'azione specifica per motivi illegittimi.

Rispetto alle altre modalità di cybercrime, questa tecnica non sfrutta le falle dei sistemi informatici: nel Social Engineering l'attaccante per i suoi scopi malevoli sfrutta il fattore umano, che di fatto è quasi sempre l'anello debole di qualsiasi catena di sicurezza.

Per ingannare le persone sfruttando i loro aspetti psicologici e comportamentali, l'attaccante spesso si spaccia per una persona o una fonte nota e conosciuta (impersonandola o persuadendoci di esserla) allo scopo di ottenere la fiducia della vittima.

CYBERCRIME E MINACCE INFORMATICHE – SOCIAL ENGINEERING

L'Intelligenza Artificiale entra negli attacchi di Social Engineering

Gli attacchi cyber di Social Engineering diventano sempre più sofisticati grazie all'Intelligenza Artificiale generativa, in grado di colpire direttamente persone o dipendenti di un'azienda, ad esempio con la falsificazione della voce di una persona conosciuta.

Oggigiorno L'AI generativa viene sfruttata anche dai cybercriminali per la creazione di campagne di phishing personalizzate, in cui gli aggressori sfruttano le informazioni rese pubbliche delle loro vittime o dalle loro organizzazioni per creare testi esca accattivanti e convincenti, attraverso la generazione di deep fake, immagini, audio e video sintetici che sono praticamente indistinguibili dalla realtà.

CYBERCRIME E MINACCE INFORMATICHE – SOCIAL ENGINEERING

L'Intelligenza Artificiale negli attacchi di Social Engineering – UN CASO REALE

Nel febbraio 2024, durante il primo furto di questo tipo, un dipendente di una multinazionale è stato ingannato a versare 25 milioni di dollari ai truffatori. Gli aggressori hanno utilizzato la tecnologia deepfake per fingersi il direttore finanziario della società durante una videochiamata, inducendo il dipendente a partecipare a una videochiamata con quelli che pensava fossero altri membri del personale, ma che in realtà erano tutti ricostruzioni deepfake.

Il dipendente era diventato sospettoso dopo aver ricevuto un messaggio presumibilmente dal direttore finanziario britannico della società. Inizialmente, pensava che fosse una mail di phishing, poiché parlava della necessità di una transazione segreta. Tuttavia, ha messo da parte i dubbi dopo la videochiamata, poiché le altre persone presenti sembravano e suonavano proprio come colleghi che riconosceva.

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

Gli attacchi di **phishing** utilizzano e-mail fraudolente, SMS, telefonate o link ingannevoli a siti web apparentemente legittimi per indurre le persone a rivelare informazioni sensibili come password, numeri di carte di credito o dati personali, scaricare malware o esporsi in altro modo al crimine informatico. Gli attacchi di phishing sono una forma di Social Engineering.

Lo **spear-phishing** è un phishing altamente mirato, eseguito anche attraverso la compromissione delle email aziendali (*Business Email Compromise, BEC*) : gli aggressori personalizzano i messaggi in base a informazioni specifiche sull'organizzazione e sulle persone che vi lavorano oppure sul target specifico.

Il Phishing via email è la principale causa di incidenti di sicurezza informatica ed è responsabile del 73% delle violazioni di Social Engineering. (*fonte: Verizon*)

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

I dati mostrano che il Credential Phishing rappresenta la minaccia più diffusa, costituendo il 71,7% delle attività malevole analizzate.
L'attacco si basa su siti web falsi che simulano portali legittimi per sottrarre credenziali di accesso, sfruttando l'ingenuità e la fiducia delle vittime.

CYBERCRIME E MINACCE INFORMATICHE – LO SMISHING

Gruppi di cybercriminali organizzano una nuova truffa che prende di mira la principale app di messaggistica

La nuova truffa su Whatsapp con prefisso +91: cosa fare se si viene adescati

Vi arriva una **notifica su Whatsapp**, ed aprendola vi trovate davanti ad un **messaggio** da un numero sconosciuto con **prefisso 91** che recita "**ciao, posso parlarle un attimo?**". Immaginiamo che sia un'esperienza capitata a molti nell'ultimo periodo: si tratta infatti della **nuova truffa che prende di mira praticamente chiunque utilizzi la famosissima app di messagistica**. Vediamo di cosa si tratta, come evitare problemi, e cosa fare nel caso in cui si commetta un errore e quindi si venga effettivamente truffati.

Lo **SMiShing**, attraverso messaggi SMS che arrivano sul telefono e invitano a visitare un link, è ancora uno dei metodi più usati per infettare i dispositivi mobili.

Anche piattaforme di messaggistica come WhatsApp o Telegram sono usate per il Phishing

CYBERCRIME E MINACCE INFORMATICHE – LO SMISHING

venerdì • 17:15

Invio di SMS/MMS a 353 492 5578

NEXI: Gentile cliente, e stato effettuato un tentativo di pagamento da 1880 EUR se non sei tu bloccalo al numero

de di allert: 3446937045

0762039

mercoledì • 18:39

Invio di SMS/MMS a 353 492 5469

NEXI: Gentile cliente, e stato effettuato un tentativo di pagamento da 1880 EUR se non sei tu bloccalo al numero verde di allert: 3500762039 3446937045

18:39

CYBERCRIME E MINACCE INFORMATICHE – LO SMISHING

Truffa dello Spid, falso sms Inps per duplicare l'identità digitale

MANTOVA Gli specialisti delle truffe online non vanno mai in vacanza e tantomeno fanno il ponte per Pasqua o 25 Aprile. È infatti di questi giorni l'allarme per la truffa dello Spid lanciato dalla Cna. I truffatori inviano un falso Sms facendo apparire come mittente l'Inps che invece è completamente estraneo. Come spiega **Franco Bruno**, responsabile dello sportello anti truffa della Cna, che mette in guardia le imprese e i cittadini, "la comunicazione fraudolenta invita a cliccare su un link per aggiornare i propri dati: il sito su cui si viene reindirizzati è una copia di quello ufficiale, ma non è autentico - avverte Bruno -. A questo punto viene chiesto di inserire informazioni personali sensibili come dati anagrafici, codice fiscale, Iban, copia di documenti, un selfie o un video. Con il materiale raccolto viene creato un falso sistema pubblico di Identità Digitale(Spid) - conclude Bruno - poi usato dai truffatori per compiere azioni illegali nei confronti degli utenti".

L'allarme sui falsi sms dell'Inps lanciato dalla Cna

La Voce di Mantova – 4 maggio 2025

CYBERCRIME E MINACCE INFORMATICHE – VISHING

Il **vishing** è una forma di phishing tramite comunicazioni vocali (Vocal Phishing), di solito chiamate telefoniche, dove gli aggressori si spacciano per entità affidabili e convincono le vittime a rivelare informazioni sensibili.
I sistemi telefonici attuali (VoIP) consentono la configurazione del numero chiamante in uscita, non c'è da sorprendersi se alcune delle chiamate dai finti operatori arrivano da un numero di telefono che è proprio quello della banca.
Ad esempio, i falsi operatori bancari richiamano il numero di telefono che spesso viene chiesto nella pagina di phishing, presentandosi come addetti della banca che hanno notato movimenti sospetti o che richiedono urgenti aggiornamenti dell'App bancaria. Si può ipotizzare che, mentre è al telefono con noi, il finto addetto faccia login sul sito vero della banca e per questo ha bisogno dei codici one-time che proprio in quel momento la banca invia al nostro cellulare o alla App installata sul nostro smartphone, e che lui non può avere senza il nostro aiuto.

CYBERCRIME E MINACCE INFORMATICHE – SMISHING + VISHING

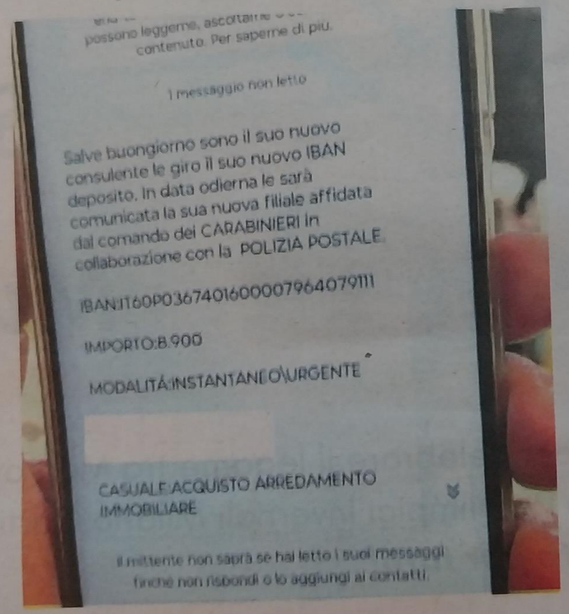
sarà diretto sui bracci della rotatoria completata.

DENTRO IL RAGGIRO
MESSAGGI INGANNEVOLI

Truffa del finto bonifico: come funziona e come difendersi

Il racconto di una vittima che è stata al gioco: tutto inizia con un Sms e finisce su un conto di una banca con solo uno sportello virtuale

MANTOVA Negli ultimi tempi sono aumentati in maniera esponenziale i casi di truffa tramite falso bonifico. Il meccanismo è semplice: arriva un Sms in cui viene segnalato un movimento sospetto sul conto corrente, e un numero da contattare. Risponde un funzionario che dice che passerà la segnalazione ai carabinieri. Poco dopo chiama un carabiniere che fa spostare il denaro dal conto della vittima a un conto più sicuro, dove i soldi poi spariscono. Ma come funziona veramente questo raggiro? Lo spiega un nostro lettore che si occupa di sistemi di sicurezza bancari e che è stato contattato da questi truffatori. «Il mese scorso mi è arrivato questo Sms in cui mi avvisavano di una mia fantomatica autorizzazione a un pagamento di 4.700 euro con la carta di credito - spiega il nostro lettore -. Ho subito intuito che era una truffa e ho deciso di stare al gioco per vedere come funziona". L'uomo ha così chiamato il numero indicato in Sms. "Mi ha risposto un tizio che si è presentato come Assistenza Nexi - racconta ancora -. Per stare al loro gioco ho disconosciuto l'operazione e ho dato un nome di fantasia e ho detto che risiedo in provincia di ferrara. Un minuto dopo mi ha chiamato un sedicente brigadiere dei carabinieri con il numero del comando provinciale dell'Arma di Ferrara". Il finto carabiniere ha spiegato alla sua "vittima" che il denaro che aveva sul suo conto corrente era a rischio e che era quindi opportuno trasferire il tutto temporaneamente su un conto corrente "secretato dello Stato" intestato a un agente della Polizia Postale, in modo da fare trovare il conto azzerato al momento in cui avrebbe dovuto partire il bonifico da 4.700 euro. "L'iban del conto su cui avrei dovuto far confluire i miei soldi - racconta ancora il nostro lettore -. A quel punto non ho dato seguito alle istruzioni dei truffatori, però ho cercato di contattare telefonicamente la banca indicata per il bonifico, ma ho scoperto che non è possibile telefonare, anche perché non ha filiali in Italia, se non una sede operativa a Milano con uno sportello virtuale. Ho inviato una mail a questa banca e mi hanno risposto che offrono assistenza solo tramite una App telefonica. Ho cercato di scaricare questa App ma poi ho desistito perché sarei stato costretto ad aprire un rapporto con la banca al momento dell'attivazione dell'App". Ferma restando l'estraneità di questo istituto di credito alla truffa che è stata tentata, si tratta comunque di una baca ideale per questo tipo di raggiri; praticamente impossibile da contattare quando tutti i soldi trasferiti sul conto indicato spariscono.



IL PRESIDENTE IERI HA FATTO TAPPA IN CITTÀ

San Francesco tra

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

Aruba

Gentile cliente,

Desideriamo informarla che il suo dominio [redacted]it è scaduto e necessita di un rinnovo immediato per evitare l'interruzione dei servizi associati, inclusa la webmail.

importo da versare: **€5,99**

in assenza di rinnovo tempestivo, si potrebbero verificare le seguenti conseguenze:
***Disattivazione del sito web**
***interruzione del servizio email**
***perdita definitiva del dominio**

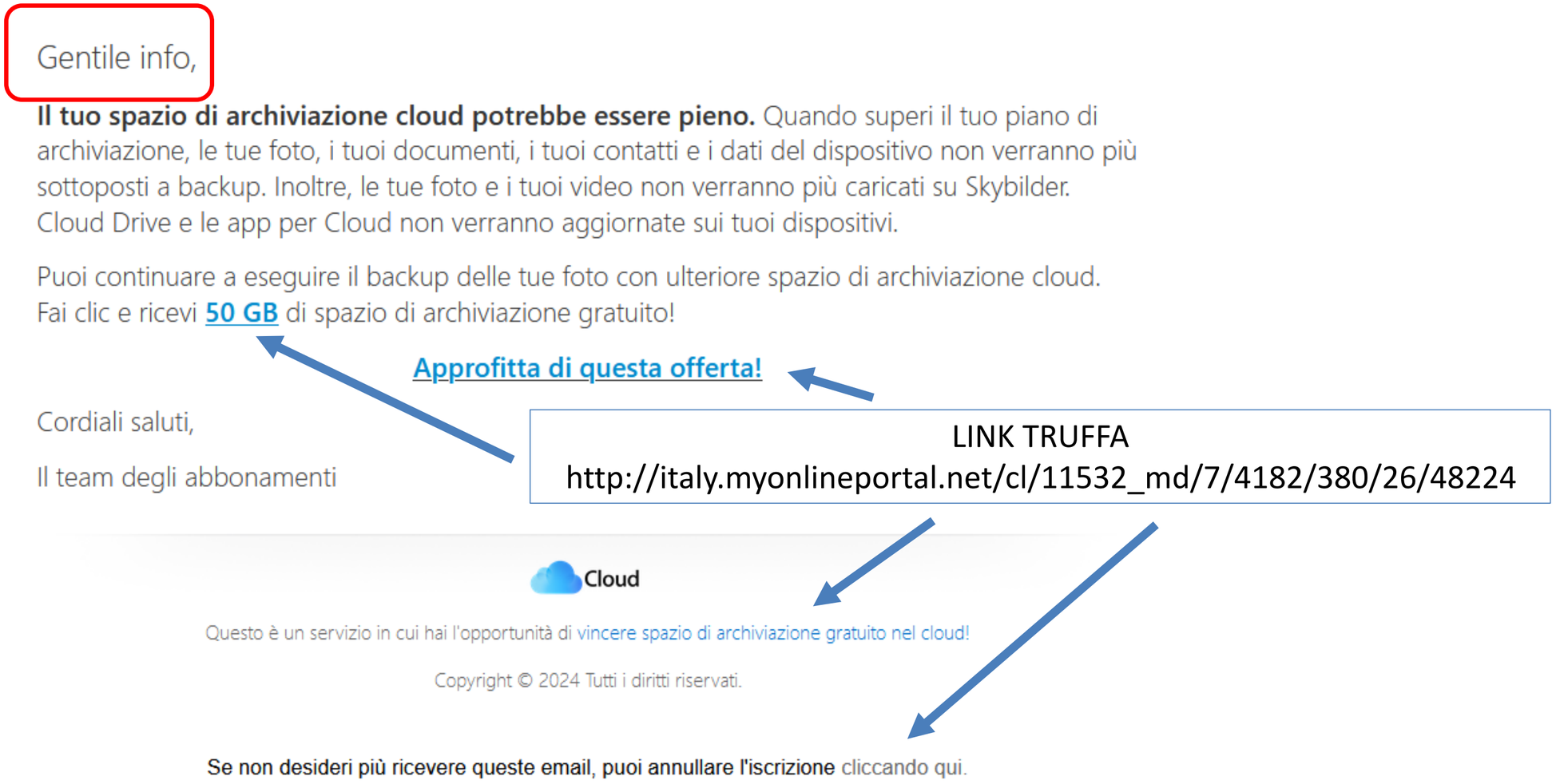
Link truffa: https://ow.ly/M7WQ50Xuuy3

Rinnova Ora

per qualsiasi domanda o necessità di assistenza, il nostro servizio clienti è a sua completa disposizione.

cordiali saluti,
Team assistenza clienti

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING



CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

Gazzetta di Mantova Venerdì 4 ottobre 2024

Il furto d'identità a un venditore di macchine

Attacco hacker a un'azienda di auto Decine i truffati per oltre 100 mila euro

• Rubati i dati di un dipendente: persone raggirate nel Mantovano e nel Bresciano Denuncia contro ignoti in Procura

VALERIO MORABITO

MANTOVA Quello che si è consumato negli ultimi mesi nel Mantovano sembra un crimine informatico compiuto nei confronti di una nota azienda che commercializza automobili. Un fenomeno che negli ultimi anni è in preoccupante crescita. La persona che si è vista sottrarre dati sensibili è un venditore, residente in provincia di Mantova, che lavora in una ditta con sedi tra il Mantovano e altre province.

Il raggiro

A ingannarlo sarebbe stato un finto cliente che in un primo momento si è mostrato interessato all'acquisto di un'Audi. Così i due hanno iniziato ad interagire, ma quando il salone di auto ha inviato il contratto da sottoscrivere e ha chiesto una caparra da cinque mila euro, il finto acquirente è scomparso. In sostanza è stato un escamotage, quello del truffatore, per entrare in possesso di alcuni dati sensibili (compreso il modello contrattuale dell'azienda) e avviare successivamente una miriade di truffe online che, fino ad oggi, avrebbero fruttato almeno 100 mila euro.

Reati *Tra le ipotesi c'è quella di frode informatica e sostituzione di persona*

I numeri

Le persone raggirate, in generale in giro per l'Italia, sono sette. C'è chi, nel Mantovano e nel Bresciano, avrebbe provato ad acquistare un'Audi Q2, Q3 e una Bmw X4. Ma l'impressione è che i truffati siano molti di più. Nel frattempo, il dipendente continua a essere contattato dai carabinieri, in quanto diverse persone lo denunciano per i raggiri commessi, in realtà, da un'altra persona che gli ha rubato l'identità. Così per tutelarsi, il venditore della nota ditta ha sporto denuncia-querela nei confronti di ignoti. Diversi i reati ipotizzati: dalla frode informatica alla sostituzione di persona, fino al trattamento illecito dei dati personali e accesso abusivo a un sistema informatico.

Venditore Al dipendente del salone è stato sottratto anche il modello contrattuale della ditta FOTO D'ARCHIVIO

IL FENOMENO

In aumento i cyber attacchi alle imprese: incubo furti d'identità

Crimini informatici Nel mirino le ditte

Negli ultimi anni c'è stata una impennata dei crimini informatici. Nella maggior parte dei casi gli hacker, tramite l'haching, ovvero l'uso di mezzi non convenzionali o illeciti per ottenere l'accesso non autorizzato a un dispositivo digitale o una rete informatica, riescono a rubare i dati delle ditte o dei singoli dipendenti. Oppure, c'è la minaccia "ransomware", vere e proprie estorsioni che preoccupano le aziende che gestiscono dati sensibili, che consiste nel blocco dell'accesso ai file sul computer infetto, al quale segue la richiesta di un riscatto per ripristinare l'accesso ai dati.

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

Generali: Kit Emergenza Auto gratuito, solo per oggi!	Offerta Generali <andrewh@myt.mu>
Prendete il vostro zaino Knipex oggi stesso	Il tuo zaino Knipex <infoXJAI@forgetme.ovh>
Il tuo caffè, fatto alla perfezione	De'Longhi per la Tua Cucina <infoelOf@forgetme.ovh>
Avviso di archiviazione Cloud GRATUITA	Avviso di limite del cloud <infoTGTz@forgetme.ovh>
Offerta Limitata – Tumbler Termico Nespresso in Regalo!	Esclusiva Offerta Nespresso <infoTLqW@forgetme.ovh>
Premio esclusivo da Shein	Premio esclusivo Shein <infozneL@forgetme.ovh>
Partecipa ora e ottieni Lavazza	Offerta Lavazza Caffè <infoYWhB@forgetme.ovh>

Offerta Generali <andrewh@myt.mu>

Rispondi | Inoltra | Archivia

Recipients <andrewh@myt.mu>

Generali: Kit Emergenza Auto gratuito, solo per oggi!

GENERALI

Gentile cliente Generali ,

Congratulazioni! Sei stato selezionato tra i fortunati per un'opportunità esclusiva: ricevere un kit di emergenza per auto!!

Per ottenerlo, ti basterà rispondere a poche semplici domande sulla tua esperienza con il Touring Club Belgium.

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

Generali: Kit Emergenza Auto gratuito, solo per oggi!	Offerta Generali <andrewh@myt.mu>
Prendete il vostro zaino Knipex oggi stesso	**Il tuo zaino Knipex <infoXJAI@forgetme.ovh>**
Il tuo caffè, fatto alla perfezione	**De'Longhi per la Tua Cucina <infoelOf@forgetme.ovh>**
Avviso di archiviazione Cloud GRATUITA	**Avviso di limite del cloud <infoTGTz@forgetme.ovh>**
Offerta Limitata – Tumbler Termico Nespresso in Regalo!	**Esclusiva Offerta Nespresso <infoTLqW@forgetme.ovh>**
Premio esclusivo da Shein	**Premio esclusivo Shein <infozneL@forgetme.ovh>**
Partecipa ora e ottieni Lavazza	**Offerta Lavazza Caffè <infoYWhB@forgetme.ovh>**
Pacco Quechua in Arrivo	**Decathlon Premi Outdoor <infoMizj@forgetme.ovh>**
Partecipa al programma fedeltà di Netflix	**Iscrizione a Netflix <infolKhi@forgetme.ovh>**
🚙 Un'opportunità imperdibile! Ricevi il tuo nuovo Kit di emergenza per auto!	**Novità da Telepass! <Telepass-ebu@sandtediaoda.top>**
Warning: message 1sZTII-0006Xz-Sk delayed 6456 hours	Mail Delivery System <Mailer-Daemon@posta.kosmosoft.eu>
Azione necessaria: completa le informazioni per la tua spedizione FedEx 987...	FedEx Servizio Clienti <nasar.nabeebaccus@myt.mu>
*****SPAM*** La tua opinione conta: vinci un kit di emergenza per auto rispondendo al nostro son...**	**Team premi ACI <cQWErE@laperouse.ovh>**
Partecipa al nostro sondaggio per avere la possibilità di vincere un set di utensili Dexter da Leroy ...	**Promozioni per i clienti Leroy Merlin <itEXXF@ieaf.ovh>**
Offerta esclusiva! Rispondi al sondaggio, ottieni il Kit Emergenza!	Telepass Avviso <PBAwLK@laperouse.ovh>
Sondaggio Generali – Ottieni oggi il tuo Kit Emergenza Auto gratuito!	**Sondaggio Generali <infoFQIT@laperouse.ovh>**
Condividi la tua esperienza e ricevi un premio!	Sorpresa Esselunga <infovOPK@ieaf.ovh>
De'Longhi: La qualità che meriti	**Solo per Tempo Limitato <infoDFUp@laperouse.ovh>**
*****SPAM*** info, La Tua Tazza Termica Perfetta – Gratis!**	**Esclusiva Offerta Nespresso <infopXvU@laperouse.ovh>**
Premio esclusivo da Shein	Premio esclusivo Shein <infoUTQF@laperouse.ovh>
Pacco Quechua in Arrivo	Kit Escursionismo Quechua <infoZurc@damien-bourcy.ovh>
Partecipa al programma fedeltà di Netflix	**Iscrizione a Netflix <infocjxP@laplage.ovh>**
Il Tuo Regalo è in Consegna	Il Tuo Kit Avventura <infochRF@martinezmarin.ovh>
La tua iscrizione è scaduta!	Rinnovo Netflix <infoyhIB@laperouse.ovh>
Il tuo codice di monitoraggio: IPHON-1312-KL10	Assistenza clienti SHEIN <infoEtzd@mytestdomain.ovh>
*****SPAM*** Messaggio sullo spazio di archiviazione GRATUITO su iCloud**	**Messaggio importante per iCloud <infoMMTq@gift.nron13.ovh>**
Avviso di archiviazione Cloud GRATUITA	Grazie! Premi iCloud <infogtRr@gift.steno.ovh>

CYBERCRIME E MINACCE INFORMATICHE – IL PHISHING

LINK TRUFFA

https://firebasestorage.googleapis.com/v0/b/hsfh1-cc45f.appspot.com/o/itconad-yw1.htm?alt=media&token=61e479c6-4785-4f3f-b15d-e3f3bc397457

CYBERCRIME E PRIVACY – FURTO DI IDENTITÀ

Nel mirino gli hotel a 4 stelle

Passaporti hackerati e messi in vendita La truffa sul dark web

Oltre 70mila i documenti rubati e offerti alla rete. Da 800 a 10mila euro il listino prezzi fissato dai cybercriminali per averli

ROMA Hanno preso di mira alberghi a quattro stelle in tutta Italia per hackerare migliaia di documenti di riconoscimento: scansioni ad alta risoluzione di passaporti e carte di identità che venivano carpite agli ignari clienti durante le operazioni di check-in. Autore dell'attività illecita su larga scala è il gruppo di cybercriminali «Mydocs», che ha messo, poi, in vendita il materiale su un forum del dark web. L'attività illecita è iniziata nel giugno scorso.

Il caso Un passaporto ANSA

tel italiani. Tra le strutture colpite dai blitz telematici figura l'hotel Cà dei Conti a Venezia, al quale, a luglio, sarebbero state sottratte illecitamente 38.000 immagini. Altri furti di dati sarebbero avvenuti negli alberghi Casa Dorita di Milano Marittima (2.300 documenti), Regina Isabella di Ischia

IN ALBERGO
NON DOVETE MAI PERMETTERE
CHE SIA FATTA
LA COPIA DEL VOSTRO
DOCUMENTO DI IDENTITÀ!!!

SE RIFIUTANO DI DARVI LA CAMERA SENZA LA COPIA DEL DOCUMENTO, CHIAMATE LA POLIZIA LOCALE

LUGMan

SOCIAL ENGINEERING & PHISHING – TECNICHE DI ATTACCO

Tecniche comuni di Social Engineering e come sfruttano la natura umana

- **Uso dell'autorità**: Le organizzazioni sono costruite come gerarchie, dove le persone in cima sono al comando. Un Social Engineer può impersonare una persona autorevole e ordinare al suo obiettivo di compiere un'azione.
- **Accendere il fascino**: Le persone sono più propense a fare cose per le persone che amano: un Social Engineer può cercare di usare il proprio carisma per influenzare qualcuno a fare ciò che vuole.
- **Dare e ricevere**: i Social Engineer possono dare gratis al loro bersaglio qualcosa di poco conto; poi, approfitteranno di un senso di obbligo per ottenere ciò che vogliono.
- **Cercare appoggi**: Le persone sono più propense a fare qualcosa che qualcuno chiede dopo aver appoggiato pubblicamente quella persona o quella causa. Un Social Engineer potrebbe cercare un'approvazione pubblica da parte della sua vittima e poi chiedere qualcosa.
- **Fare ciò che è popolare**: alle persone piace essere popolari, un Social Engineer farà in modo che sembri che "tutti facciano" ciò che sta cercando di ingannare un obiettivo.
- **Offerta scarsa o limitata**: i Social Engineer possono far sembrare scarso o limitato nel tempo ciò che offrono, questo fa sì che le persone si affrettino a cercare di approfittare dell'offerta senza riflettere.

SOCIAL ENGINEERING & PHISHING – TECNICHE DI ATTACCO

Gli attacchi di Phishing più comuni

- **Problemi con l'account**: Una tattica di Phishing comune è quella del problema con gli account online (Amazon, Netflix, PayPal, ecc.). Quando si affrettano a cliccare sul link e a risolvere il problema, l'aggressore raccoglie le loro credenziali di accesso.
- **Business Email Compromise (BEC)**: Un attacco BEC è un classico esempio di utilizzo dell'autorità. L'aggressore impersonerà una persona importante all'interno di un'organizzazione (direzione, ecc.) e istruirà l'obiettivo a compiere un'azione dannosa, come l'invio di denaro a un conto controllato dall'aggressore.
- **Fattura falsa**: l'aggressore può mascherarsi da venditore per ottenere il pagamento di una fattura in sospeso. Questo scam è progettato per far sì che la vittima invii denaro all'aggressore o per farle scaricare e aprire un allegato contenente malware.
- **Documenti condivisi nel cloud**: I cybercriminali sfruttano la condivisione di documenti nel cloud per aggirare la sicurezza di Office 365 e altre soluzioni di sicurezza: spesso questi strumenti verificano che un link sia legittimo, ma non verificano eventuali contenuti dannosi nel documento condiviso. In alternativa, l'aggressore può fingere di condividere un documento e mostrare una pagina che richiede alla vittima di inserire le proprie credenziali di accesso per accedere al documento

SOCIAL ENGINEERING & PHISHING – TECNICHE DI ATTACCO

Che cosa cercare in un messaggio e-mail sospetto

- **Indirizzo del mittente**: gli attaccanti utilizzano comunemente indirizzi e-mail che sembrano affidabili o legittimi nei loro attacchi. Verificate sempre che l'indirizzo del mittente non contenga errori, ma ricordate che un aggressore potrebbe aver compromesso l'account reale e lo sta utilizzando per il suo attacco.
- **Saluto**: La maggior parte delle aziende personalizza le proprie e-mail indirizzandole al destinatario per nome, ma un phisher potrebbe non conoscere il nome che accompagna un determinato indirizzo e-mail. Se una formula di apertura – come "Gentile cliente" - oppure un saluto di chiusura sono eccessivamente generici e non personali – ad esempio "Saluti" - potrebbe trattarsi di un'e-mail di phishing.
- **Tono e grammatica**: spesso un'e-mail di phishing non suona bene e presenta problemi di ortografia e grammatica. Se un'e-mail sembra inconsueta rispetto al solito per quel mittente, forse è phishing.
- **Collegamenti non corrispondenti**: Può verificare la destinazione di un link in un'e-mail su un computer passandoci sopra con il mouse. Se il link non va dove dovrebbe, è probabile che l'e-mail sia dannosa.
- **Allegati strani**: le e-mail di phishing sono spesso utilizzate per diffondere malware. Se ricevete una "fattura" che è un file ZIP, un file Excel o qualcos'altro di insolito, quasi sicuramente si tratta di malware.
- **La necessità o l'urgenza**: le e-mail di phishing sono progettate per indurre la vittima a fare qualcosa; se un'e-mail suscita un senso di urgenza o spinge a un'azione particolare, potrebbe essere dannosa.

SOCIAL ENGINEERING & PHISHING – MISURE DI PROTEZIONE

- Utilizzare strumenti di filtraggio e protezione della navigazione web.
- Usare strumenti di filtraggio e protezione del traffico e-mail da malware e spam.
- Utilizzare un software anti-malware («antivirus») con caratteristiche avanzate in grado di rilevare determinare azioni pericolose, che in caso di rilevamento o di infezione da malware può inviare messaggi di alert.
- Attivare un sistema firewall di tipo avanzato a protezione delle rete che sia in grado di rilevare traffico anomalo, configurato per trasmettere le notifiche di problemi, tentativi di intrusione , traffico anomalo, attacchi DDoS.
- Attivare il firewall del sistema operativo sugli endpoint (personale computer)

SOCIAL ENGINEERING & PHISHING – MISURE DI PROTEZIONE

- Non salvate mai le password nei computer e soprattutto dispositivi mobili (notebook, tablet, telefoni): è scomodo digitare una password complessa, ma se il dispositivo mobile viene rubato o preso in prestito, altre persone avranno accesso ai dati aziendali.
- Configurate il browser per fare in modo che alla chiusura della sessione cancelli tutta la cronologia, i files temporanei, la cache, i cookies, SOPRATTUTTO NON SALVATE MAI LE PASSWORD DEI SITI WEB!
- Usate sempre password forti, scritte con un mix di maiuscole/minuscole, numeri e caratteri speciali; è meglio una password molto lunga ma facile da ricordare (ad esempio 'Credenziale_numero_01_del_2025') piuttosto che una password complessa ma difficile da ricordare e che è necessario scrivere.
- Non usate sempre la stessa password ovunque, bisogna sceglierne una diversa per ogni ambito di accesso: se un hacker violerà un vostro account, si limiterà solo a quello.

SOCIAL ENGINEERING & PHISHING – MISURE DI PROTEZIONE

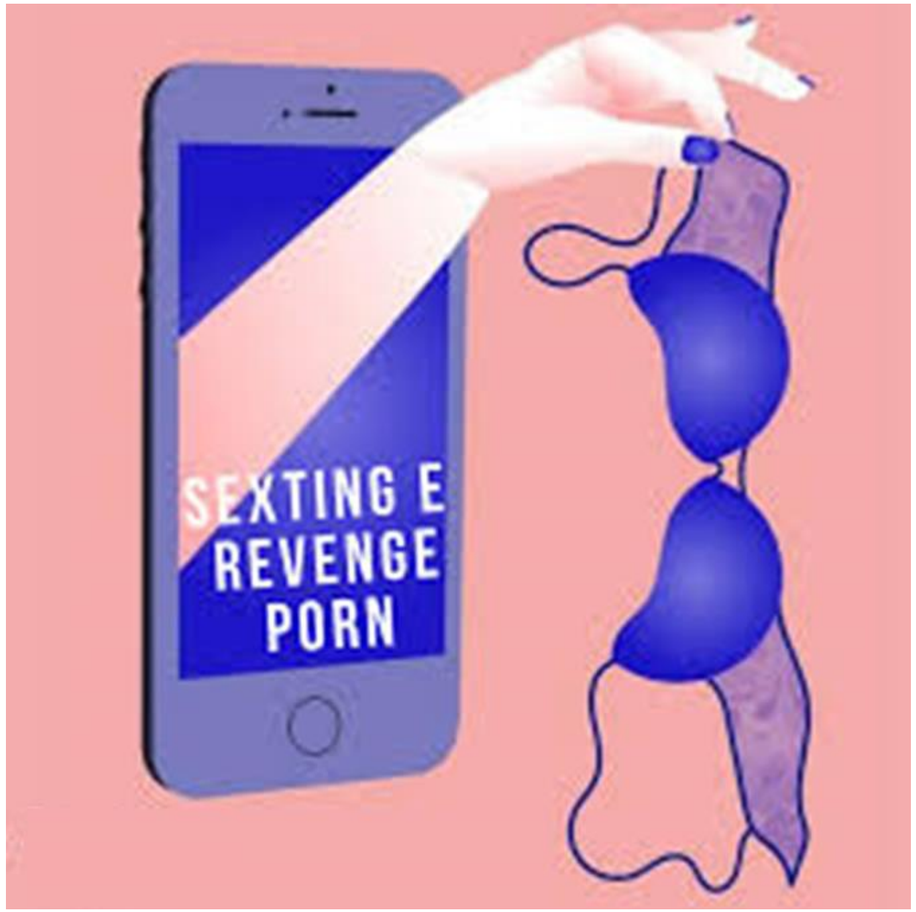
- Non fidatevi dei link che trovate nelle mail, possono essere falsi e portarvi ad un sito-truffa; usate il metodo del copia-incolla dentro un documento Word per verificare l'esatto indirizzo, oppure digitateli a mano nel campo indirizzo del browser;
- Fate attenzione a chi spedite le e-mail: non è possibile sapere quanta cura avrà il destinatario delle informazioni contenute nel vostro messaggio.
- Evitate di inoltrare all'infinito i messaggi e-mail con tutto il loro contenuto e gli indirizzi altrui, copiate e trasmettete solo il contenuto necessario tralasciando tutto quello che non serve.
- Quando dovete mandare un messaggio e-mail a più destinatari che magari non si conoscono, mettete gli indirizzi nel campo Ccn (copia nascosta) così nessuno vedrà gli indirizzi degli altri destinatari

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

#25NOVEMBRE

Giornata internazionale contro la violenza sulle donne

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE



La diffusione non consensuale di immagini o video a contenuto sessualmente esplicito è una orrenda piaga contemporanea: parliamo del Revenge Porn, che letteralmente significa “vendetta pornografica”.
Spesso, questi contenuti sono stati realizzati all’interno di una relazione intima e consensuale e successivamente sono divulgati da uno degli stessi protagonisti, in seguito a una rottura o ad un conflitto nella relazione, con l’intento di vendicarsi, umiliare o danneggiare la vittima.

Si tratta di UN CRIMINE GRAVE perseguibile penalmente !!!

E’ penalmente perseguibile anche “Chiunque” diffonda successivamente tale materiale pur non essendo coinvolto nella sua creazione.

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

Revenge Porn e Pedo Pornografia: i collettivi hacker si mobilitano

Anonymous e LulzSec_ITA
https://twitter.com/LulzSec_ITA/status/1247958118933372928?s=20

Anonymous Italia (gruppo collettivo di hacker italiani) da tempo ha in corso una nuova operazione denominata OpRevengeGram per smascherare e rivelare pubblicamente gli utenti di queste chat che scambiano contenuti illeciti: il nome prende spunto dalle parole Revenge-Porn e Telegram, la nota piattaforma di chat sul quale si stanno diffondendo questi contenuti.
Si sommano, alle azioni regolari delle forze dell'ordine, anche quelle della comunità di internet, capitanate da collettivi di hackers e volontari tesi a far emergere questo "sottobosco illegale".

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

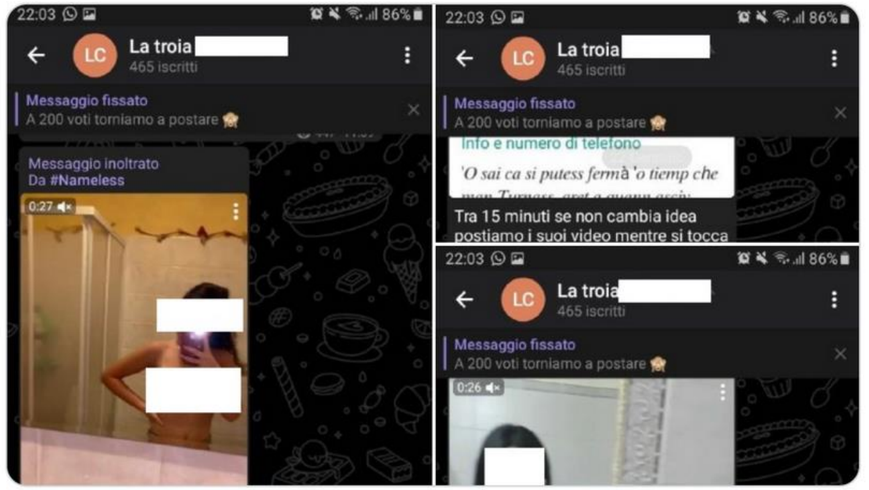
LulzSecITA
@LulzSec_ITA

Pasquale, 17 anni, minaccia ragazzine 2006/2008 di diffondere contenuti privati se non gli inviano nudes. Cellulare: 351131**** Instagram: @mister_bape_shark Ha molti account telegram che crea ed elimina in continuazione. #OpRevengeGram

· Twitter Web App

LulzSecITA
@LulzSec_ITA

Rosario, minacciare una ragazzina di divulgare le sue foto se non fa un video mentre sp*mpina il suo cane.. è abbastanza da malati non credi? Sappiamo che stai a Milano, username telegram: @jklsq numero di telefono 388734****! Dormi sonni tranquilli cucc.



· Twitter Web App

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

I giudici tendono a reprimere con estrema severità i casi di pornografica, con interpretazioni restrittive. Ad esempio, la pronuncia della Cassazione n.5522 depositata il 12.02.2020 nella quale si afferma che :

La diffusione via WhatsApp a un solo destinatario delle fotografie pornografiche minorili, anche se originate da selfie, rientra nell'ipotesi di reato prevista dall'articolo 600-ter, comma 4, del Cp, che punisce con la reclusione fino a tre anni la cessione, anche a titolo gratuito, di materiale pedopornografico, a prescindere da chi abbia scattato le fotografie. Ai fini della configurabilità del reato non rileva che le fotografie siano autoscattate oppure no. Il caso riguardava uno studente che dopo essere venuto in possesso del cellulare di una amica per scattare una foto collettiva, aveva a sua insaputa fotografato dei selfie pornografici della stessa, presenti nel telefono, inviandoli a un amico via whatsapp che poi a sua volta li aveva divulgati. (fonte: Guida al diritto 2020, 13, 105)

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

Come proteggersi dal Revenge Porn con misure di cybersecurity?

La prima e più importante forma di difesa sono sempre la consapevolezza e la prudenza. Spesso accade che i dati personali vengano immessi dagli stessi interessati nel circuito di messaggistica e social network, sfuggendo così ogni controllo e rendendone impossibile la cancellazione una volta diffusi.
Se sei un genitore, evita di far utilizzare dispositivi digitali ai tuoi figli piccoli se sono da soli, monitora il loro comportamento online e spiega con chiarezza perché è bene evitare di interagire con sconosciuti e diffondere informazioni personali, soprattutto foto e filmati, tramite messaggi e social network.
(PAGINA INFORMATIVA DEL GARANTE PRIVACY: www.gpdp.it/minori)

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

Come prevenire la diffusione di immagini private con misure di cybersecurity?

Limitiamo la nostra impronta digitale:

- Privacy settings: Configuriamo i nostri profili social in modo che solo i nostri contatti approvati possano vedere i nostri contenuti.
- Limitazione delle informazioni: Evitiamo di condividere troppi dettagli personali online, come il nostro indirizzo o il luogo di lavoro, la palestra frequentata, ecc.
- Immagini: Utilizziamo immagini che non ci ritraggono in situazioni compromettenti e riflettiamo attentamente prima di condividere contenuti intimi.
- Accertiamoci della affidabilità e dell'integrità etica del destinatario: evitiamo di intrattenerci online con persone che non conosciamo personalmente e, se lo facciamo, mettiamoci nella condizione che abbia qualcosa da perdere anche l'altro nel divulgare contenuti sconvenienti.

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

Come prevenire la diffusione di immagini private con misure di cybersecurity?

Monitoriamo la nostra presenza online:

- Google Alerts: impostiamo avvisi per il nostro nome e altre informazioni che ci identificano per essere avvisati di nuovi contenuti che ci riguardano.
- Social listening tools: esistono strumenti che permettono di monitorare le conversazioni online che parlano di noi. Sui Social, rimuoviamo l'autorizzazione ai tag senza la nostra autorizzazione.

Proteggiamo nostri dispositivi:

- Password forti: utilizziamo password complesse per tutti i nostri account, evitiamo date di nascita, compleanni, nomi del cane, amico, nonna etc..
- Impostiamo i nostri dispositivi per poterli bloccare o cancellare da remoto in caso di smarrimento o furto.

PRIVACY & CYBER RISK – DIFFUSIONE ILLECITA DI IMMAGINI PRIVATE

È possibile segnalare la diffusione non consensuale di immagini o video al Garante per la protezione dei dati personali.
Per inviare una segnalazione si utilizza il modulo **che può essere compilato anche senza autenticarsi** disponibile sul sito del Garante.
http://servizi.gpdp.it/diritti/s/revenge-porn-scelta-auth
Bisogna indicare:

- Le piattaforme su cui potrebbe avvenire la diffusione (social network, app di messaggistica, ecc.);
- Le motivazioni che giustificano la possibile violazione.

Se la richiesta soddisfa i requisiti previsti dalla normativa, il Garante interverrà notificando un provvedimento alle piattaforme coinvolte per contrastare la diffusione del materiale.

CONCLUSIONI