Le strategie di prevenzione e contrasto alle frodi

Giornata Antifrode Europea
«Prevenire la frode informando il pubblico»
Roma, 11 giugno 2025

Primo Dirigente della Polizia di Stato
dott. Luigi BOVIO
Direttore IV Divisione «Financial Cybercrime»
Servizio Polizia Postale e per la Sicurezza Cibernetica

SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Organizzazione

1 DIVISIONE

- Ufficio Analisi, Affari Legali e Pianificazione Strategica
- Amministrazione delle risorse umane e della formazione
- Relazioni internazionali
- Relazioni con gli Uffici del territorio, COSC e SOSC
- Relazioni esterne, Istituzionali e settore scuole
- *CommissariatodiPS* Online

2 DIVISIONE

- **CNCPO** – Centro Nazionale per il contrasto alla Pedopornografia Online
- **UACI** Unità di analisi sul crimine

3 DIVISIONE

- **CNAIPIC** Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
- Cyber-terrorismo
- Pianificazione finanziaria e approvvigionamento di risorse tecnologiche

4 DIVISIONE

- OF2CEN Financial Cybercrime
- Relazione con Poste Italiane S.p.A. and Stakeholder Istituzionali

5 DIVISIONE

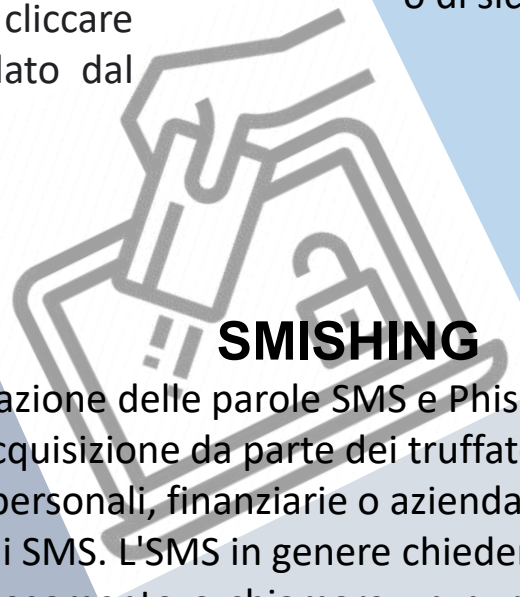
- Unità Sistemi, Reti, Sicurezza e Focal point
- Unità di gestione dei servizi applicativi
- Unità di gestione degli asset tecnologici e di informatica forense

PHISHING

L'attacco viene effettuato inviando messaggi di sollecitazione tramite posta elettronica, che sembra provenire da un'organizzazione attendibile, come una banca o un ufficio postale. Il testo ci avverte che c'è un problema relativo al nostro account, generalmente legato alla sicurezza. Per risolverlo ci invita a cliccare su un link che però ci riporta su un sito fittizio controllato dal cracker

VISHING

(dalla combinazione delle parole Voce e Phishing) è una truffa telefonica in cui i truffatori cercano di indurre la vittima a rivelare informazioni personali, finanziarie o di sicurezza o a trasferirle denaro

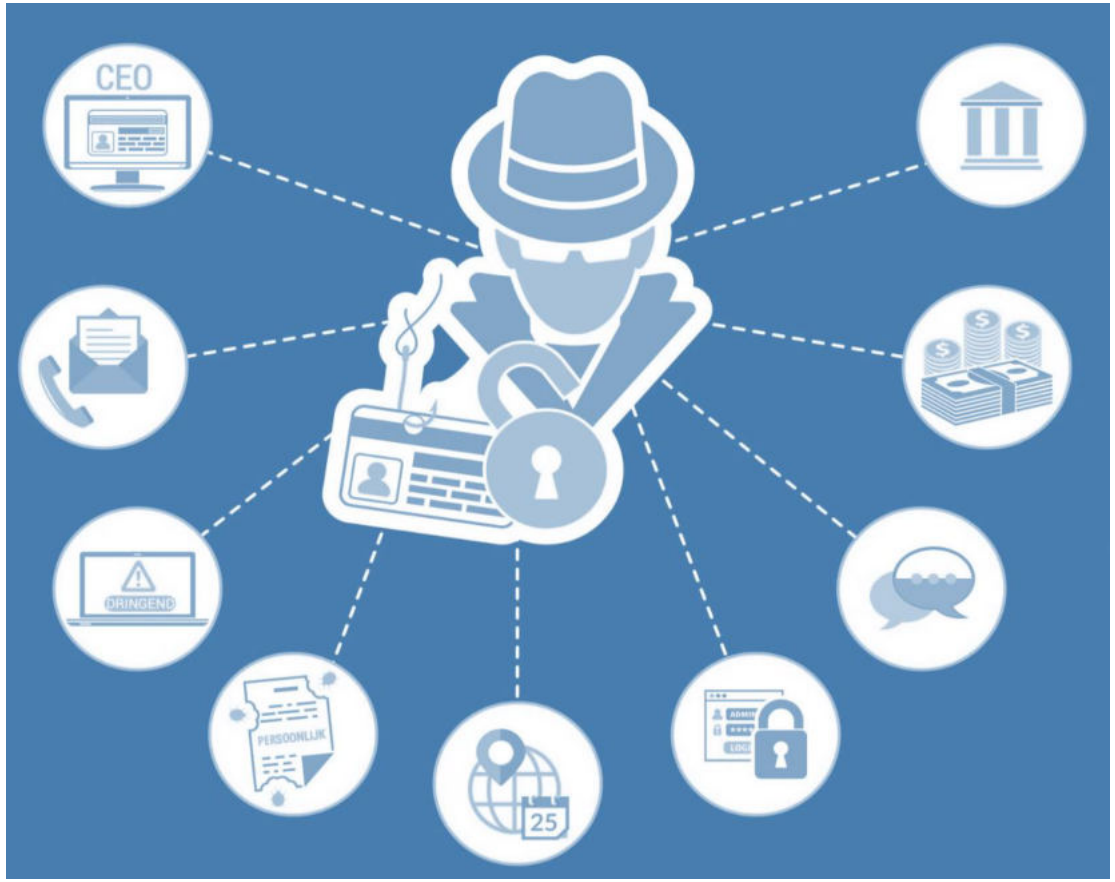


SMISHING

(dalla combinazione delle parole SMS e Phishing) è il tentativo di acquisizione da parte dei truffatori informazioni personali, finanziarie o aziendali Sicurezza degli SMS. L'SMS in genere chiederà di fare clic su un collegamento o chiamare un numero di telefono per "verificare", "aggiornare"o "riattivare" il tuo account. Ma... il collegamento porta a un sito Web e a un numero di telefono fasulli porta a un truffatore che finge di farlo essere la società legittima.

Financial Cybercrime – «Man in the middle» attacks

Gli attacchi basati sul *social engineering* per colpire il mondo dell'impresa sono ricollegabili alle fattispecie del *BEC* e del *CEO Fraud.*



B.E.C. *(Business e-mail compromise)*

Compromettendo una casella di posta elettronica, oppure attraverso tecniche di social engineering o sofisticate tecniche di hacking, l'hacker apprende che tra due soggetti è in corso una corrispondenza elettronica di carattere commerciale. Assumendo l'identità digitale dell'uno o dell'altro, i criminali richiedono pagamenti all'altro verso conti correnti appositamente creati, spesso ubicati all'estero

CEO Fraud

Questa tipologia di frode viene commessa ai danni di dirigenti di alto livello nella gerarchia di un'azienda o di un ente: il falso manager induce un soggetto dell'organigramma aziendale, dotato di poteri di spesa, a disporre trasferimenti di denaro, fingendo di doverlo soddisfare un ordine gerarchico. Anche in questo caso i conti correnti sui quali ricevere i proventi illeciti sono spesso ubicati all'estero.

Un Ransomware agisce utilizzando la sua caratteristica di Cryptovirus: trattasi infatti un malware che cripta i file sul computer infetto e chiede un riscatto per la decifrazione, spesso in valute virtuali. Di solito, la vittima ha poche ore per effettuare un pagamento. Se il denaro non viene trasferito sul conto dei criminali informatici entro questo lasso di tempo la chiave di decriptazione viene rimossa dal computer ed i file rimangono illeggibili.

Il *trading* online è l'attività di acquisto e vendita di strumenti finanziari (come azioni, opzioni, valute, crypto, futures) per mezzo di internet

A) Social *engineering (tecnica di attacco cyber –studio del comportamento delle persone per manipolarle e carpire informazioni confidenziali*

1) chiamata telefonica
2) whatsapp, telegram e instagram
3) Contatti personali (vengono in ufficio per pubblicizzazione prodotto truffaldino

B) Pubblicità sui siti internet e social network

TECNOLOGIA DEEPFAKE ED INTELLIGENZA ARTIFICIALE (AI)

Le minacce più recenti relative ai crimini informatici finanziari riguardano l'uso di deep fake e AI

- CITTADINI: INVESTIMENTI E TRADING ONLINE
- IMPRESE: SOLITAMENTE CEO FRAUD

SPOOFING Che cos'è?

- Il **CLI (Calling Line Identification) SPOOFING** è una tecnica informatica che permette di **falsificare l'identità del chiamante** → **simula** che una comunicazione provenga da una **fonte affidabile** → quando in realtà è **manipolata** da un attaccante.

- Tale fenomeno rappresenta una **grave minaccia** → le **vittime**, basandosi sul **numero visualizzato**, sono convinte di rispondere ad una telefonata di un ente di **fiducia**. → **Ufficio di Polizia o Banca**

SPOOFING NOVITÀ NORMATIVE

L'**AGCOM** con la **delibera n. 106/2025/CONS** del 30.04.2025 ha adottato un **Regolamento** che recepisce le **misure di contrasto al fenomeno del *CLI Spoofing*** proposte dal Servizio Polizia Postale e per la Sicurezza Cibernetica

Le **misure** contenute nel Regolamento rappresentano un **concreto rafforzamento** delle **misure di protezione** degli utenti finali e di **prevenzione** delle frodi informatiche

Tra le azioni previste dal Regolamento, sono state incluse le seguenti misure:

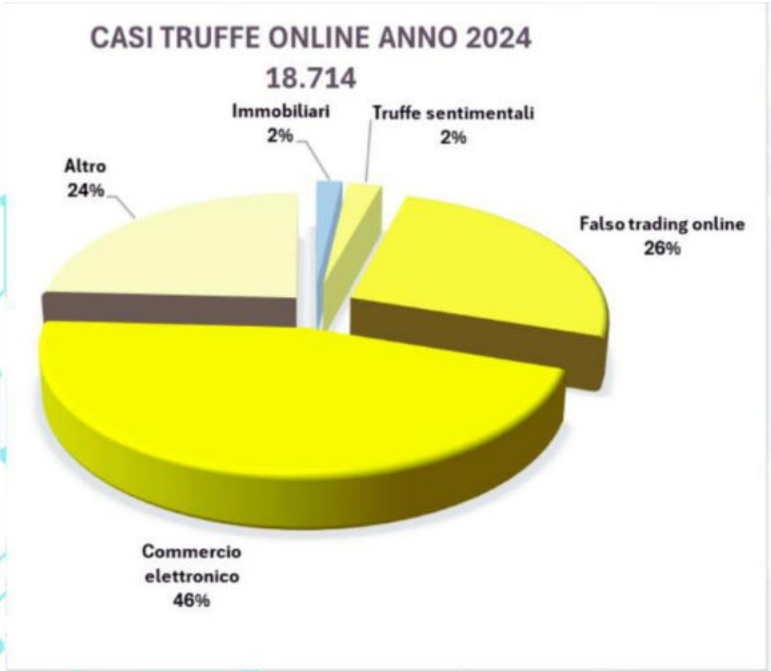
1. **Validazione dell'identità del chiamante** e prevenzione delle falsificazioni dell'ID nelle **comunicazioni VoIP**
2. **Verifica in tempo reale dell'origine** della chiamata e **l'autenticazione** del numero chiamante;
3. Istituzione di ***blacklist* dinamiche** e attività di **monitoraggio del traffico** per identificare **comportamenti anomali** riconducibili a pratiche fraudolente;
4. Implementazione di **blocchi automatici** per le chiamate provenienti da **numerazioni ritenute sospette**

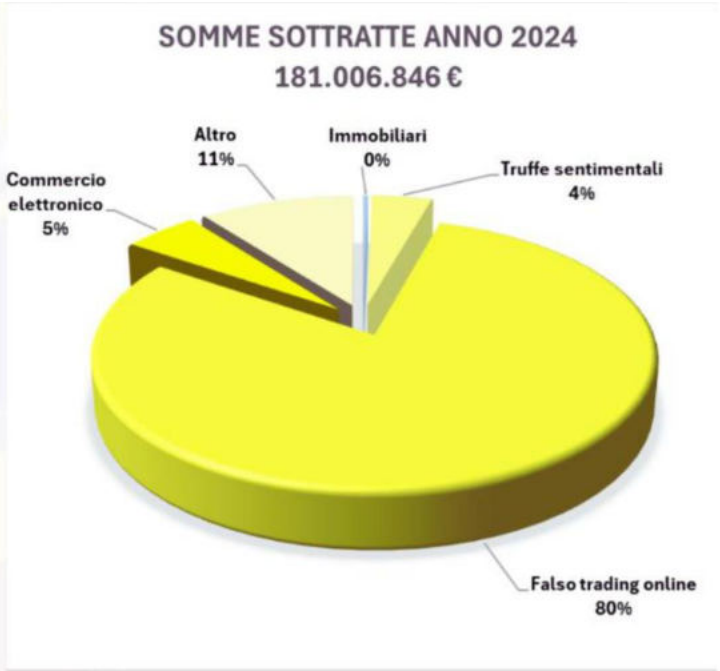
La Sezione Financial Cyber Crime della IV Divisione

Truffe online

	Casi trattati	Persone indagate	Somme sottratte
Anno 2024	18.714	3.581	€ 181.006.846
Anno 2023	16.325	3.571	€ 137.202.592
Var. %	+15%	+0%	+32%

Nel 2024, sono stati trattati 18.714 casi, con un incremento del 15% rispetto ai 16.325 casi del 2023. Il numero di persone indagate è rimasto pressoché invariato, con 3.581 individui nel 2024 rispetto ai 3.571 del 2023. Tuttavia, le somme sottratte hanno subito un notevole aumento del 32%, passando da €137.202.592 nel 2023 a €181.006.846 nel 2024

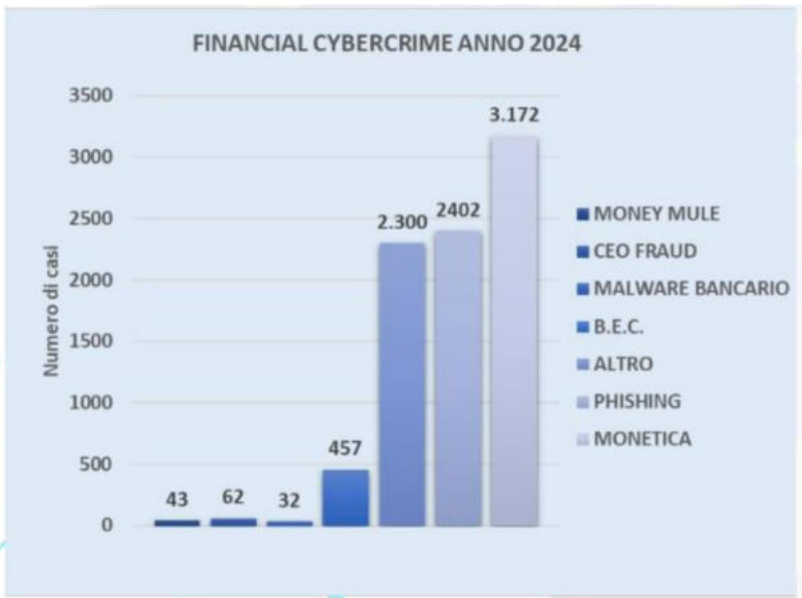




FRODI INFORMATICHE E MONETICA

	Casi trattati	Persone indagate	Somme sottratte
Anno 2024	8.468	919	€ 48.117.336
Anno 2023	10.606	917	€ 40.151.375
Var. %	-20%	+0%	+20%

La tabella illustra i dati relativi ai casi di frodi informatiche e monetica investigati dalla Polizia Postale negli anni 2023 e 2024. Nel 2024, sono stati trattati 8.468 casi con 919 persone indagate e somme sottratte pari a €48.117.336. Rispetto al 2023, i casi trattati sono diminuiti del 20%, rimanendo stabili nel numero di persone indagate. Le somme sottratte sono aumentate del 20%, evidenziando la crescente sofisticazione delle attività fraudolente online



Forme di contrasto alle frodi online

Prevenzione

Repressione

Prevenzione

Le frodi online fraudolento possono essere realizzate **solo con la collaborazione dell'ignara vittima**

La prevenzione è realizzabile mediante una crescente consapevolezza da parte degli utenti dei rischi che possono celarsi in rete: occorre acquisire piena consapevolezza in tal senso riduce sensibilmente la possibilità di cadere nella «trappola».

Numerose sono le campagne si sensibilizzazione sul tema da parte della Polizia Postale:

- sito del Commissariato di PS online
- collaborazioni con stakeolders
- campagne informative destinate a diverse fasce di popolazione

Repressione

- tempestiva comunicazione alle Forze di Polizia
- indagini di polizia giudiziaria tecnico-informatiche e tradizionali
- importanza della cooperazione internazionale

Grazie per l’attenzione