ORDINE DEI PERITI INDUSTRIALI
E DEI PERITI INDUSTRIALI LAUREATI
della Provincia di Vicenza

Via L.L. Zamenhof, 817 - 36100 Vicenza
Codice Fiscale 80017750243
Tel. 0444.327322 | Fax 0444.324270
segreteria@periti-industriali.vi.it
PEC ordinedivicenza@pec.cnpi.it
https://ordine-vicenza.cnpi.eu

Assemblea Ordinaria

Hotel Viest | Vicenza, 30 maggio 2026

Programma di lavoro

Parte istituzionale: Bilancio consuntivo 2025

09:00 **Apertura Assemblea: saluti del Presidente -** *per. ind. Antonio Sofia*
09:10 **Introduzione del Presidente al bilancio consuntivo 2025**
09:30 **Intervento del Tesoriere**
10:00 **Intervento del Revisore dei Conti**
10:05 **Votazione**
10:10 **Premiazione associazione di volontariato Vigili del fuoco di Recoaro Terme (VI)**
10:30 **Attestati neo-iscritti**
10:45 **Coffee break**

Parte pubblica

11:15 **"La Cyber Sicurezza: come possiamo difenderci dai fenomeni di truffe online, phishing, cyber bullismo"**

Corrado Piccione *- Ispettore della Polizia di Stato – Responsabile della Sezione Operativa per la Sicurezza Cibernetica di Vicenza*

12:45 **Saluti finali** *- Presidente per. ind. Antonio Sofia*

Apertura dell’Assemblea

Sofia per. ind. Antonio | Presidente

Come previsto all'articolo 7, comma primo, del Decreto Legislativo Luogotenenziale 23 novembre 1944 n. 382, il Consiglio Direttivo dell'Ordine dei Periti Industriali e Periti Industriali Laureati di Vicenza ha proceduto alla convocazione degli iscritti per proporre l'approvazione del bilancio consuntivo 2025.

La convocazione è avvenuta conformemente a quanto prescritto dall'articolo 3, secondo comma, del Decreto Legislativo Luogotenenziale 23 novembre 1944, n. 382, tramite pubblicazione sul sito web come da art. 32 della Legge 18 giugno 2009, n. 69 e successivo Decreto Legge 30 dicembre 2009, n. 194, convertito con modificazioni dalla Legge 26 febbraio 2010, n. 25.

Gli iscritti sono inoltre stati informati a mezzo e-mail con apposite comunicazioni.

La prima convocazione è stata fissata per il giorno 27 maggio 2026, alle ore 18:00, online.

Poiché la seconda convocazione deve avvenire almeno tre giorni dopo la prima, come previsto all'articolo 3, quarto comma della suddetta norma, questa è stata fissata per oggi **sabato 30 maggio 2026, alle ore 9:00, presso il Centro Congressi dell'Hotel Viest**.

Come da pareri espressi dal Consiglio Nazionale Forense, si applicano le disposizioni dell'articolo 21 del Codice Civile e pertanto:

- alla prima convocazione deve essere presente almeno la metà degli iscritti,
- in seconda convocazione devono essere presenti **almeno due iscritti** oltre ai componenti del Consiglio.

In base all'articolo 21 del Codice Civile, i membri del Consiglio devono astenersi dalla votazione.

La votazione avviene in modo palese per il tramite di alzata di mano.

L'assemblea è presieduta dal presidente dall'Ordine.

A questo punto si procede alla verifica della sussistenza del "quorum deliberativo".

Ordine del giorno

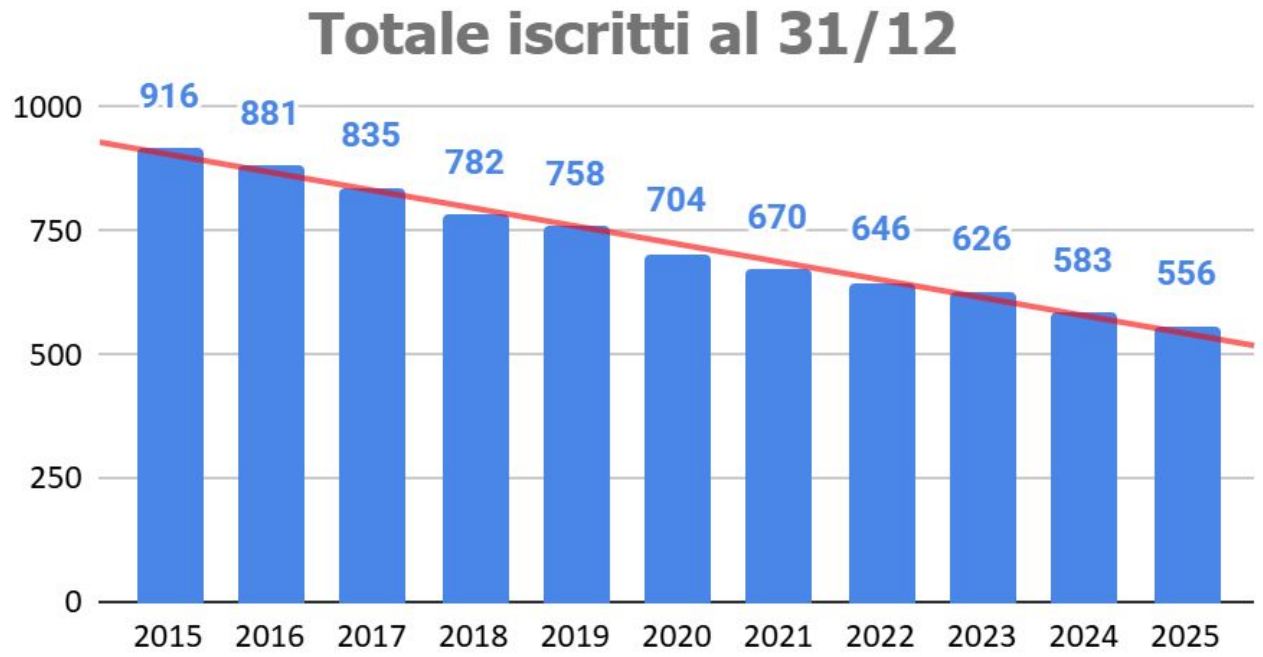
1. **Presentazione e approvazione del Bilancio Consuntivo 01/01/2025 – 31/12/2025**

Intervento del Presidente

Sofia per. ind. Antonio| Presidente

Andamento iscritti dal 2015 al 2025

	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Iscritti al 1 gennaio	958	916	881	835	782	758	704	670	646	626	583
Nuove iscrizioni	10	8	10	5	11	9	10	10	8	7	20
Cancellazioni	52	43	56	58	36	63	44	34	28	50	47
Totale iscritti al 31/12	**916**	**881**	**835**	**782**	**758**	**704**	**670**	**646**	**626**	**583**	**556**



ETÀ MEDIA = 56 anni

In 11 anni abbiamo avuto una **riduzione del 40%** del numero di iscritti. Ciò porta ad una riflessione sulla futura sostenibilità economica dell'Ordine.

Campagna di recupero del credito

Questo è l'**andamento delle quote non pagate**. La situazione che avevamo prima di iniziare la campagna di recupero crediti è confrontata con la situazione dello scorso anno e con la situazione attuale.

Nel 2025 i procedimenti disciplinari per morosità hanno portato a:

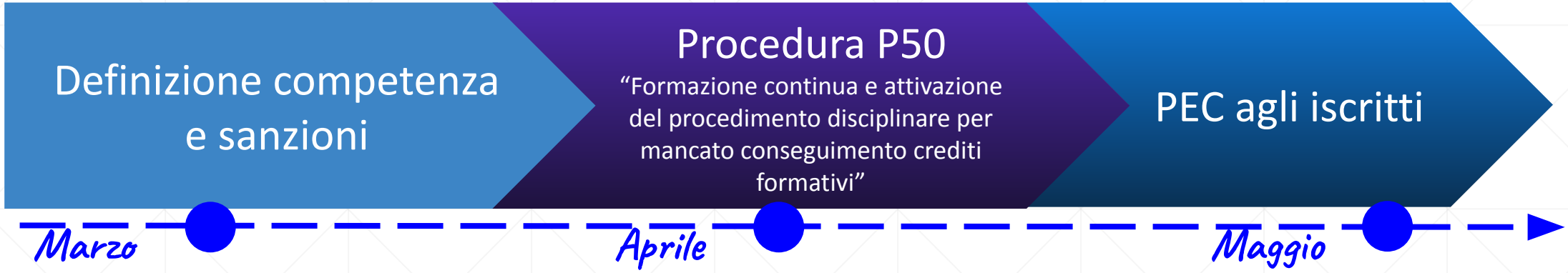
- n. 2 **sospensioni disciplinari**
- n. 4 **cancellazioni disciplinari**

Le quote stralciate a seguito delle cancellazioni NON sono perse: vengono inviate all'Agenzia delle Entrate Riscossione per il recupero coattivo del credito.

I progetti del 2025

Nel corso dell'anno 2025 l'Ordine è stato impegnato in 3 attività progettuali:

1. Gestione formazione continua: risultati progetto



Definizione della **competenza disciplinare** per la formazione continua, in coordinamento con il CNPI, e delle **sanzioni** da irrogare a seconda del numero di CFP mancanti.

La **Procedura interna P50** prevede:

1. Verifica e controllo annuale da parte dell'Ordine sui CFP conseguiti da **tutti gli iscritti**
2. Sollecito, via PEC, agli iscritti che non sono in linea con **24 CFP all'anno**
3. Attivazione dei procedimenti disciplinari nel 2029 (al termine dell'attuale quinquennio formativo) per chi non ha completato l'obbligo formativo

Invio delle **segnalazioni via PEC** agli iscritti per sollecitare l'assolvimento della formazione continua

2. Digitalizzazione archivio: risultati progetto

Aprile	Maggio	Agosto	Settembre	Dicembre
Analisi normativa sulla gestione dell'archivio. **Definizione dei tempi di conservazione** dei documenti, con approvazione della Soprintendenza Archivistica dello Stato. Analisi di mercato e **scouting di fornitori** sulla ***digitalizzazione e conservazione digitale***	Confronto ***internalizzazione / esternalizzazione***	**Svuotamento magazzino:** mobili, stampe, sedie, libri, attrezzature varie	Analisi di mercato e **scouting di fornitori** sulla ***distruzione certificata*** dei documenti cartacei	**Assegnazione contratti** per "digitalizzazione" a COOPERATIVA VERLATA (il 17/09/2025) e "distruzione carta" a DE ZUANI ECOLOGIA (il 17/11/2025). Carta da NON digitalizzare prelevata in data 04/12/2025. FASCICOLI DEGLI ISCRITTI da digitalizzare prelevati in data 02/12/2025. Parte esterna del magazzino svuotata entro il 31/12/2025.

3. Sito internet: risultati progetto

Definizione fornitore per realizzazione sito: **assegnazione incarico alla società Agicom srl nell'ambito del progetto "multi-site" del CNPI**	Implementazione sito: **release del nuovo sito avvenuto in data 26/11/2025** link al sito

Prossimo rinnovo del Consiglio Direttivo

In occasione della prossima **Assemblea Ordinaria**, prevista per la **fine di ottobre 2026**, si procederà al rinnovo delle cariche istituzionali.

Punti chiave dell'appuntamento:

- Presentazione e votazione del bilancio preventivo 2027.
- Scadenza mandato attuale Consiglio Direttivo e presentazione delle candidature per il nuovo quadriennio.
- Votazioni e proclamazione degli eletti.

La vostra partecipazione è fondamentale per il futuro del nostro Ordine.

Anticipazione: Approfondimento Tecnico nella prossima assemblea - Obblighi e Compensi

Durante la prossima Assemblea di **ottobre 2026** verrà dato spazio ad un approfondimento sui seguenti argomenti, fondamentali per la professione:

Obbligo del Preventivo Scritto

Legge 4 agosto 2017, n. 124

- Obbligatorietà della forma scritta o digitale.
- Comunicazione del grado di complessità dell'incarico.
- Indicazione di un “preventivo di massima” e dei dati della polizza assicurativa.

Equo Compenso

Legge 21 aprile 2023, n. 49

- Ambito di applicazione
- Diritto a un compenso proporzionato alla quantità e qualità del lavoro.
- Tutela del decoro e della dignità professionale.
- Parere di congruità con efficacia di titolo esecutivo.

Bilancio consuntivo 2025

Corato per. ind. Giovanni | Tesoriere

Il bilancio consuntivo 2025, finalizzato alla dimostrazione dei risultati di gestione, è costituito dai seguenti documenti:

- Situazione amministrativa con parte vincolata
- Prospetto di concordanza
- Rendiconto finanziario
- Rendiconto dei residui attivi e residui passivi
- Stato patrimoniale e conto economico
- Situazione avanzo di cassa
- Variazioni al preventivo finanziario

Il bilancio è inoltre corredato dai seguenti allegati:

- Relazione del Tesoriere al bilancio consuntivo 2025
- Relazione del Revisore dei Conti 2025
- Pianta e dotazione organica dell'Ordine

Documenti pubblicati online

Bilancio Consuntivo 2025

Documenti pubblicati online

Bilancio consuntivo 2025: la situazione amministrativa

Con la **situazione amministrativa** si calcola l'ammontare dell'avanzo di amministrazione alla fine dell'esercizio:

Avanzo di amministrazione =

= disponibilità liquide + residui attivi - residui passivi

Al 31/12/2025 si evidenzia un **avanzo di amministrazione di € 209.449,15** con una parte vincolata pari a € 33.199,96 e una parte liquida pari a € 176.249,19.

Situazione amministrativa 2025

Consistenza di cassa iniziale	**€ 260.773,22**
+ RISCOSSIONI	+ € 234.968,45
- PAGAMENTI	- € 234.394,88
Consistenza di cassa finale	**€ 261.346,79**
+ RESIDUI ATTIVI	+ € 20.130,04
- RESIDUI PASSIVI	- € 72.027,68
AVANZO DI AMMINISTRAZIONE	**€ 209.449,15**
di cui	
Parte vincolata	***€ 33.199,96***
Fondo svalutazione crediti	€ 13.000,00
Digitalizzazione	€ 12.535,00
Fondo TFR al 31/12/2025	€ 7.664,96
Parte disponibile	***€ 176.249,19***

La situazione amministrativa: rappresentazione “idraulica”

Riscossioni: € 234.968,45

Residui attivi: € 20.130,04

Pagamenti:

€ 234.394,88

Residui passivi: € 72.027,68

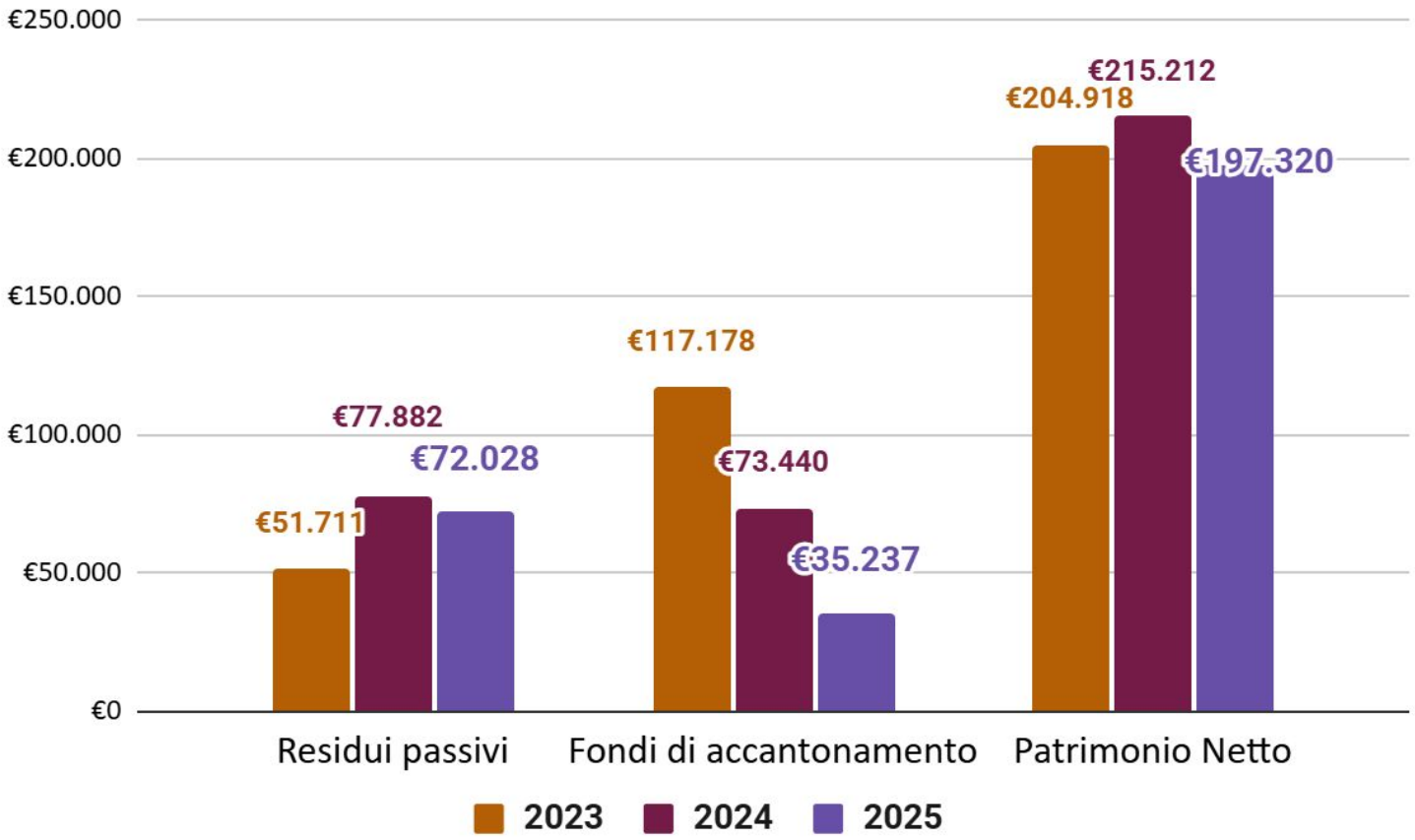
Stato patrimoniale 2025: attivo

Costo magazzino: - 72%

In due anni abbiamo migliorato il patrimonio dell'Ordine:

- la **liquidità** dell'Ente è aumentata del **54%**.
- i **residui attivi** sono diminuiti dell'**86%,** grazie al recupero di **€ 84.660** di quote passate e allo stralcio di circa **€ 39.000**, (inviati all'Agenzia delle Entrate Riscossione per il recupero coattivo del credito).
- Abbiamo svolto un inventario e una valorizzazione delle **immobilizzazioni** dell'Ordine e ne abbiamo quindi ridotto il valore del 68% rispetto al 2023.

Stato patrimoniale 2025: passivo



I **residui passivi** sono in linea con l'esercizio precedente.

Il **patrimonio netto**, che rappresenta la ricchezza dell'Ordine, è diminuito del 3% rispetto al 2023, a causa dei costi economici imputati nel conto economico.

La diminuzione dei **fondi** è legata alla riduzione del fondo ammortamento, che ha in parte assorbito la riduzione delle immobilizzazioni.

Conto Economico 2025

Il Conto Economico aggiunge i costi economici e patrimoniali ai costi finanziari

L'esercizio 2025 è si è chiuso con un disavanzo economico di € 17.891,63, che deriva da:

	2025	2024	2023
Proventi finanziari	197.096,01	213.164,92	238.509,77
Proventi non finanziari	0,00	459,87	10.305,83
Disavanzo economico	17.891,63	-	-
TOTALE PROVENTI	**214.987,64**	**213.624,79**	**248.815,60**
TOTALE A PAREGGIO	**214.987,64**	**213.624,79**	**248.815,60**
Costi finanziari	202.564,92	200.092,30	212.172,76
Componenti non finanziari	8.796,39	0,00	735,33
Ammortamenti	688,35	922,59	625,51
Accantonamento TFR	2.937,98	2.316,43	2.284,24
Avanzo economico	-	10.293,47	32.997,76
TOTALE COSTI	**214.987,64**	**213.624,79**	**248.815,60**
TOTALE A PAREGGIO	**214.987,64**	**213.624,79**	**248.815,60**

I **proventi** iniziano a diminuire a causa del minor numero di iscritti.
I **costi** sostenuti sono in linea con l'esercizio precedente.

Il disavanzo economico è dovuto a:

- *Maggiori costi finanziari* rispetto alle entrate di € 5.468,91.
- *Costi economici*: ammortamenti e accantonamento TFR.
- *Sopravvenienze passive* per € 7.036,44 (derivanti da stralci di crediti).
- *Minusvalenza patrimoniale* di € 1.759,95 (riduzione del valore delle immobilizzazioni al netto della riduzione del fondo ammortamento)

Rappresentazione “idraulica” del conto economico

Totale proventi:
€ 197.096,01

Totale costi vivi € 202.564,92 così suddivisi:
€ 90.184,86 per spese ordinarie
€ 55.757 per il personale
€ 38.540 per organi istituzionali
€ 18.083,06 per interessi, spese bancarie, altre spese

Disavanzo:
€17.891,63 per costi economici, minusvalenze, sopravvenienze passive

Liquidità e gestione finanziaria

Il disavanzo economico NON significa perdita di liquidità, anzi!

Nonostante il disavanzo tecnico, la **liquidità dell'Ordine è in costante crescita: + 54% dal 2023**

Al 31/12/2025 le disponibilità liquide raggiungono i **€ 261.346,79**.

Questa solidità finanziaria è frutto di una gestione attiva che ottimizza le giacenze attraverso strumenti di investimento sicuri.

Liquidità Totale al 31/12/2025

€ 261.347

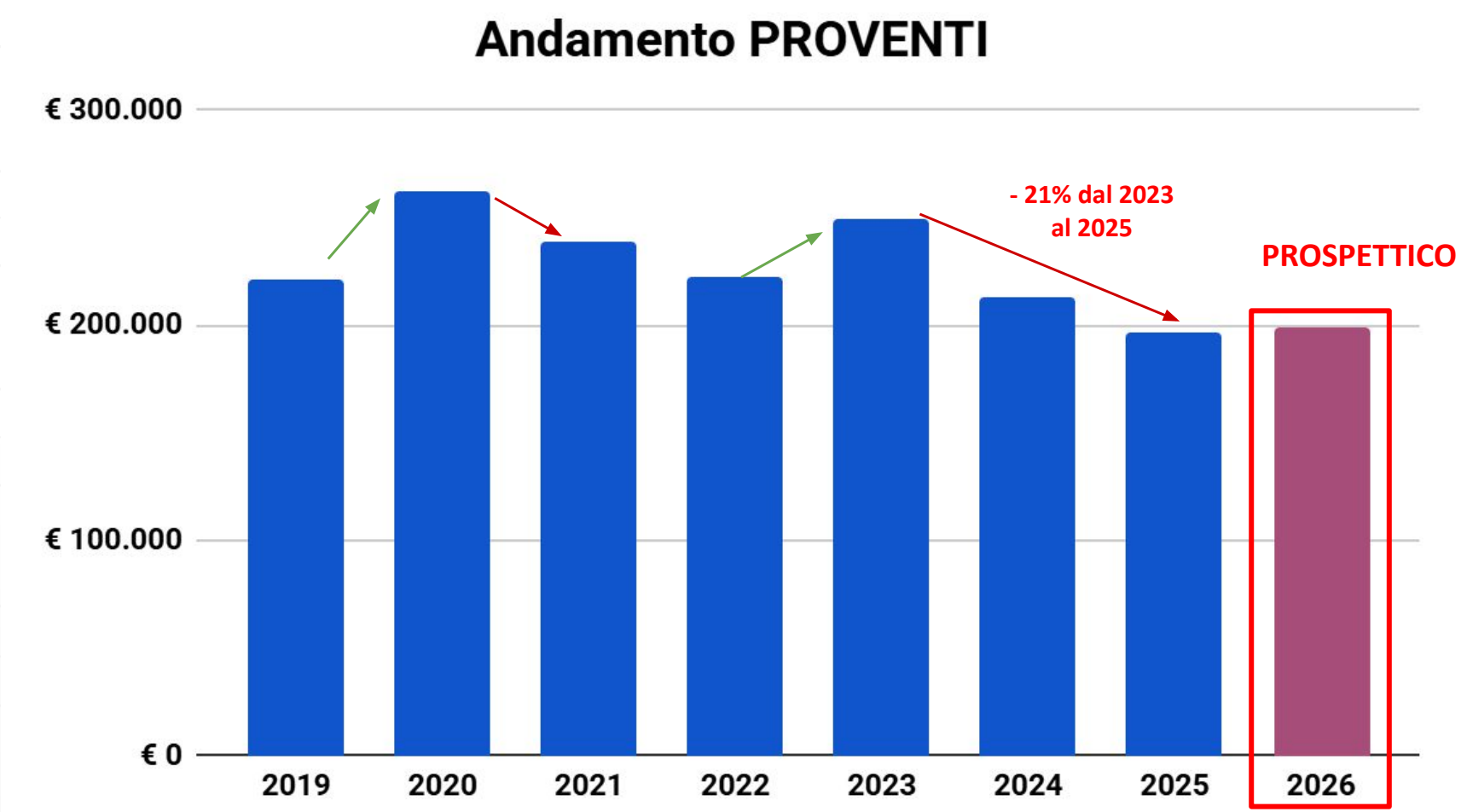
Investimenti Banca Etica

La cassa di € 261.347 include anche **€ 150.000** in Conti Deposito.

Rendimenti vantaggiosi (fino al 1,75% lordo) rispetto al conto corrente ordinario.

Il conto economico: andamento dei proventi

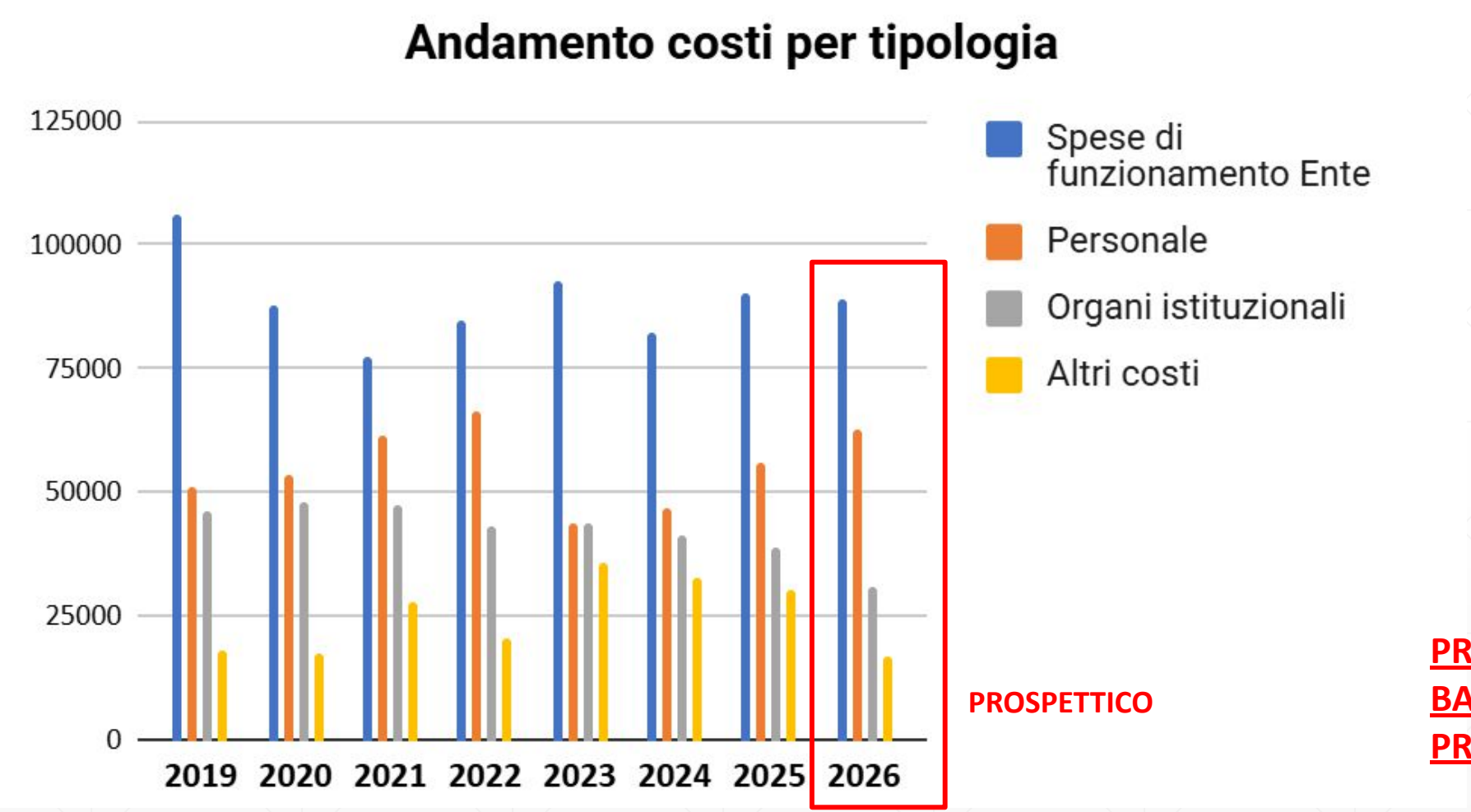
PROVENTI: Iniziamo a vedere una riduzione dei **proventi** a causa del minor numero degli iscritti.



PROSPETTICO: BASATO SULLE PREVISIONI 2026

Il conto economico: andamento dei costi

COSTI: i costi sono in linea con l'esercizio precedente



PROSPETTICO: BASATO SULLE PREVISIONI 2026

Prospetto di concordanza 2025

Situazione iniziale		*Gestione dell'anno 2025*							*Situazione finale*	
Fondo cassa iniziale € 260.773	+	Entrate riscosse € 234.968	-	Uscite pagate € 234.395				=	Fondo cassa finale € 261.347	Gestione di cassa
+		+							+	
Residui attivi iniziali € 41.137	+	Residui attivi anno € 5.965	-	Residui attivi riscossi € 17.863	+	Δ Residui Attivi € - 9.110		=	Residui attivi finali € 20.130	Gestione dei residui attivi
-		-							-	
Residui passivi iniziali € 77.882	+	Residui passivi anno € 38.555	-	Residui passivi pagati € 44.409	+	Δ Residui Passivi 0		=	Residui passivi finali € 72.028	Gestione dei residui passivi
=		=							=	
Risultato di amm.ne iniziale € 224.028	+	Entrate Accertate € 223.071	-	Uscite Impegnate € 228.540	+	Δ Residui Attivi € - 9.110	-	Δ Residui Passivi 0	= Risultato di amm.ne finale € 209.449	Gestione di Competenza

Relazione al Bilancio Consuntivo 2025 del Revisore dei Conti

Santolin dott. Giuseppe Athos | Revisore dei Conti

Il Revisore, nella propria Relazione, esamina il Rendiconto della gestione dell'anno 2025, comprensiva di allegati, ed esprime **parere favorevole** in ordine all'approvazione del bilancio consuntivo 2025.

Relazione del Revisore

Revisore dei Conti

Relazione al Bilancio Consuntivo 2025

Votazione
Bilancio consuntivo 2025

Favorevoli / Contrari / Astenuti

Associazione Nazionale Vigili del Fuoco Volontari - Delegazione di Recoaro Terme (Organizzazione di Volontariato)

Vincitrice del bando emesso dall'Ordine dei periti industriali di Vicenza nel 2025

Il contributo di 1.000 euro è stato utilizzato per contribuire all'acquisto del miscelatore elettronico "DUALFOAM", per potenziare il servizio antincendio reso dal Distaccamento Vigili del Fuoco di Recoaro Terme.

VVF volontari
Delegazione di Recoaro Terme

Alessandro Albiero

Consegna attestati nuovi iscritti

e

Riconoscimenti

La sede dell’Ordine

L’Ordine dei periti industriali di Vicenza ha sede in via Zamenhof 817 a Vicenza, presso Simal Business Center

Si riceve su appuntamento, osservando i seguenti orari di apertura al pubblico:

Martedì e Giovedì: 11.00 - 13.00

Mercoledì: 16.00 - 19.00

Contatti:

Telefono: **0444.327322**

Email: segreteria@periti-industriali.vi.it

Pausa caffè

L’Assemblea ricomincerà tra 30 minuti

Dr. Corrado Piccione

Ispettore della Polizia di Stato – Responsabile della Sezione Operativa per la Sicurezza Cibernetica di Vicenza

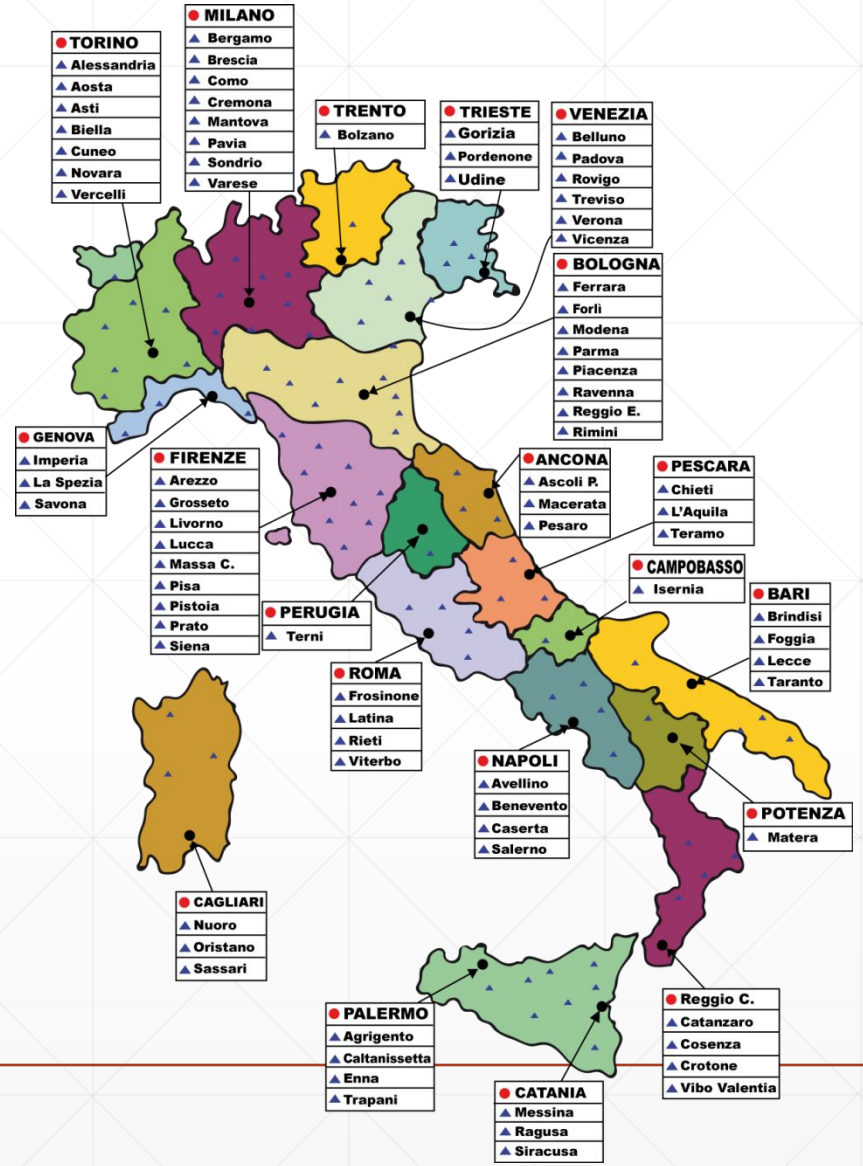
La Cyber Sicurezza: come possiamo difenderci dai fenomeni di truffe online, phishing, cyber bullismo

L’organizzazione della Polizia Postale e delle comunicazioni

Servizio Centrale

20 *Centri Operativi regionali*

80 *Sezioni provinciali*



Centri Operativi Polizia Postale

Sezioni Operative Polizia Postale

Le competenze della Polizia Postale e delle comunicazioni

- *Cyberterrorismo*
- *Computer forensics*
- *Controllo radio frequenze*
- *Crimini informatici*
- *Diritto d'autore*
- *Giochi e scommesse on line (legge 266/'05)*
- *Pedofilia on line*
- *Protezione infrastrutture critiche*
- *Pirateria satellitare*
- *Reati postali e falsi filatelici*
- *Collaborazione operativa con Forze di Polizia straniere (h 24 / 7)*

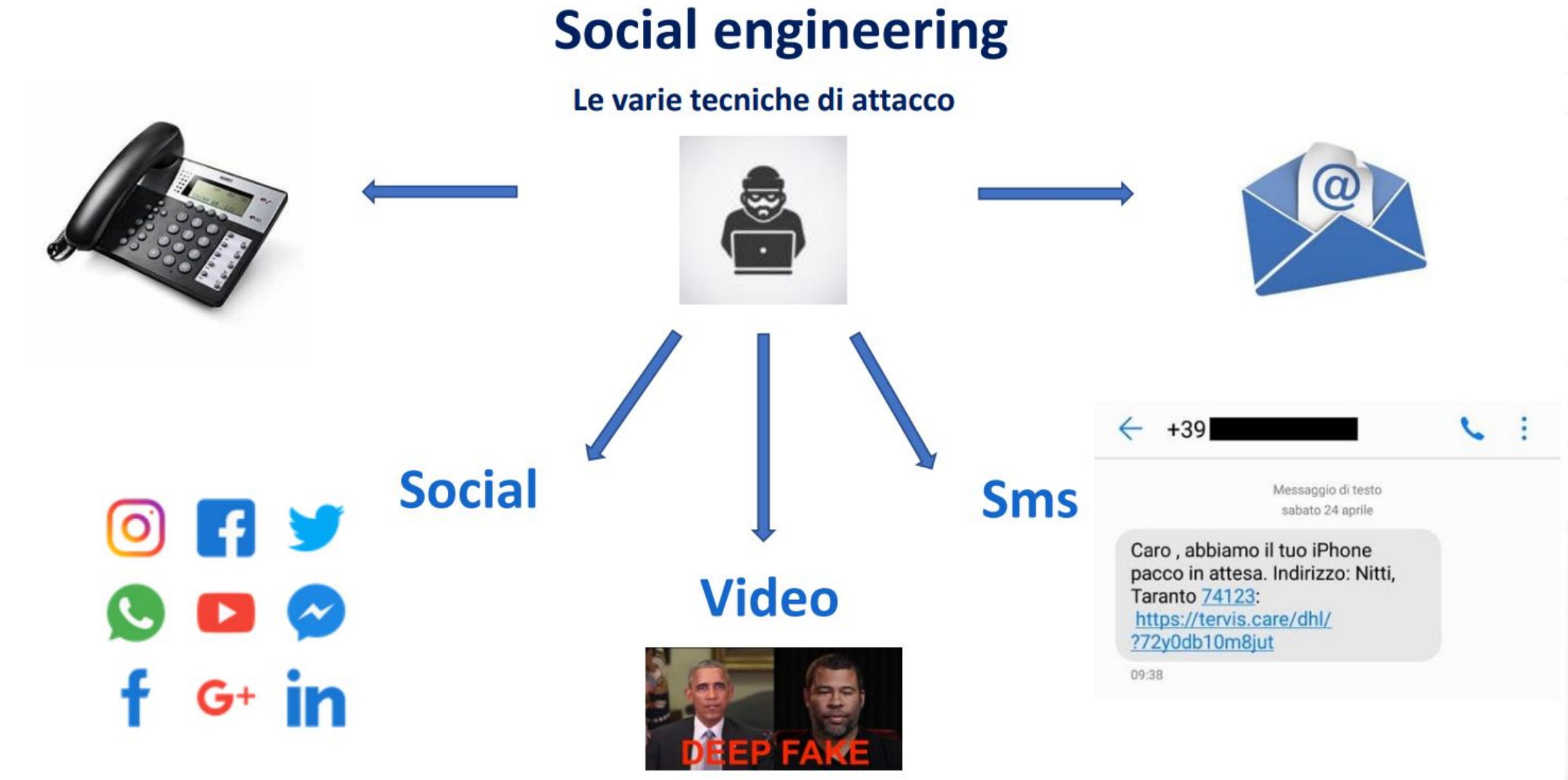
Social engineering

Social engineering

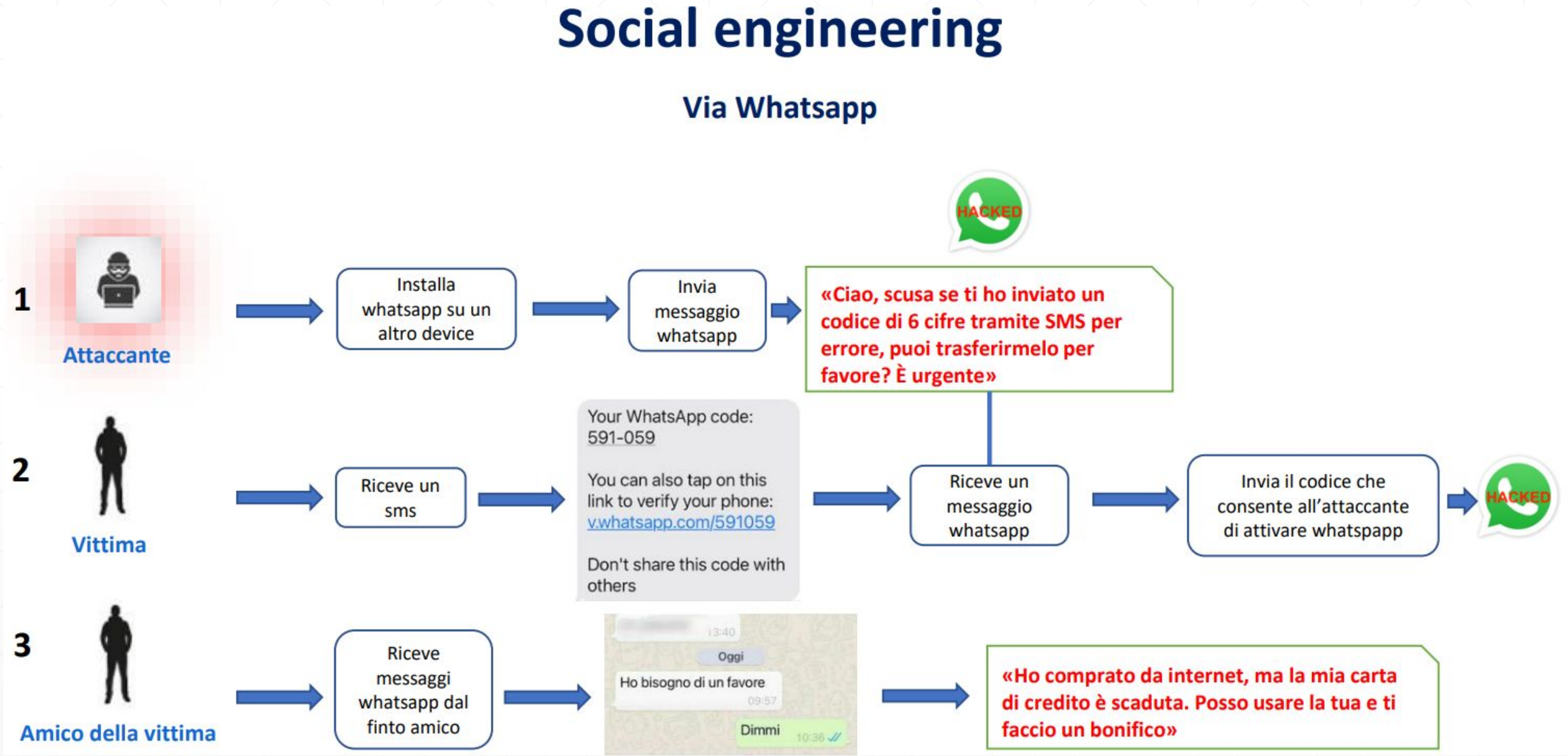
• Il social engineering rappresenta un insieme di tecniche utilizzate dai cybercriminali per attirare gli ignari utenti ad inviare loro i loro dati riservati, infettare i loro computer tramite malware o aprire collegamenti a siti infetti.

• La tecnica più diffusa avviene tramite l'uso della posta elettronica. Le-mail di phishing cercano di convincere gli utenti che esse provengono in realtà da fonti legittime, nella speranza di procurarsi anche pochi dati personali o aziendali

Social engineering



Social engineering



Phishing

Internet e la posta elettronica non sono ambienti privati e sicuri; è come camminare in una grande città; possiamo incontrare molti pericoli:

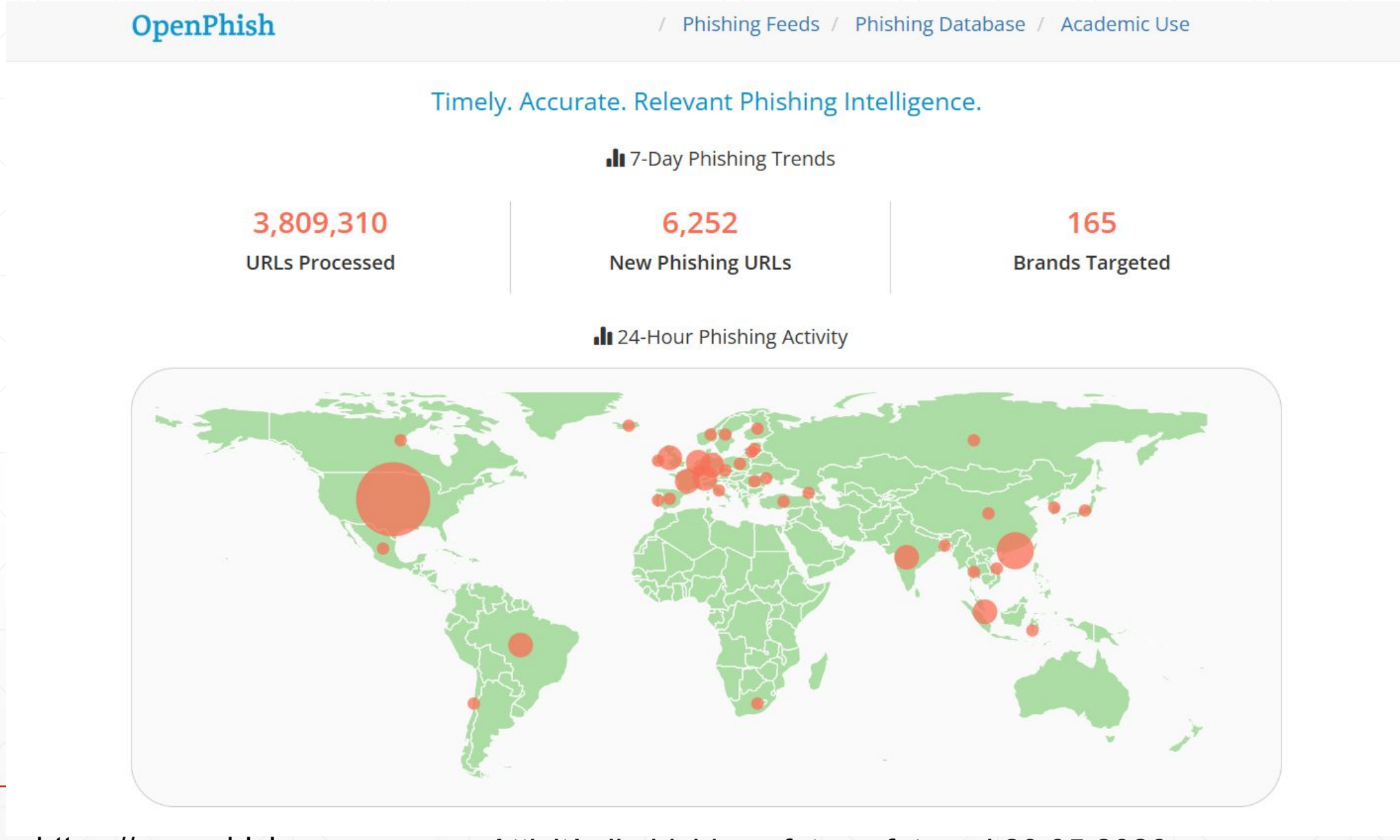
Phishing: messaggi mail fraudolenti che ci inducono a fornire dati personali

- credenziali di accesso
- Password posta elettronica
- Documenti o informazioni aziendali
- Informazioni bancarie

Il 90% delle violazioni di dati inizia con e-mail di phishing.
Spesso basta un solo click per essere compromessi o per esporre dati sensibili.

Nell'86% delle Aziende almeno un utente *abbocca*.

Phishing



Fonte: https://openphish.com

Attività di phishing «fotografata» al 20.05.2026

Phishing

Top 10 Targeted Brands

Bet365	12.4%
Deutsche Telekom	7.8%
Roblox	6.2%
Netflix Inc.	6.0%
DPDgroup	5.5%
Office365	5.1%
Crypto/Wallet	3.9%
Epic Games	3.7%
Adobe Inc.	3.5%
Facebook, Inc.	2.8%

Top 10 Sectors

Online/Cloud Service	20.2%
Gambling	12.6%
Social Networking	11.3%
Gaming	10.6%
Telecommunications	10.6%
Financial	8.9%
Logistics & Couriers	7.6%
Cryptocurrency	6.2%
e-Commerce	3.9%
Government	3.9%

Top 10 ASNs

AS13335 Cloudflare, I...	43.6%
AS16509 Amazon.co...	5.9%
AS54113 Fastly, Inc.	5.1%
AS134548 DXTL Tseu...	2.5%
AS132203 Tencent Bu...	2.0%
AS27647 Weebly, Inc.	1.6%
AS14618 Amazon.co...	1.6%
AS8075 Microsoft Cor...	1.6%
AS31898 Oracle Corp...	1.5%
AS140224 Nebula Glo...	1.4%

Fonte: https://openphish.com

Attività di phishing «fotografata» al 20.05.2026

Phishing

Brand	Che cos'è	Settore
Bet365	piattaforma di scommesse online	Gambling / betting
Deutsche Telekom	grande operatore telefonico tedesco	Telecomunicazioni
Roblox	piattaforma di gioco online/social gaming	Gaming / social
Netflix Inc.	piattaforma streaming	Intrattenimento / cloud service
DPDgroup	corriere e logistica internazionale	Logistica / spedizioni
Office365	servizi Microsoft per email, cloud e produttività	Cloud / servizi aziendali
Crypto/Wallet	wallet e servizi legati a criptovalute	Criptovalute / finanza
Epic Games	piattaforma videogiochi, Fortnite, store digitale	Gaming
Adobe Inc.	software creativi e servizi cloud	Software / cloud
Facebook Inc.	social network Meta/Faceboo	Social networking

CERT di AGID

In questa settimana, il CERT-AGID ha riscontrato ed analizzato, nello scenario italiano di suo riferimento un totale di **104 campagne malevole**, di cui 73 con obiettivi italiani e 31 generiche che hanno comunque interessato l'Italia, mettendo a disposizione dei suoi enti accreditati i relativi **828 indicatori di compromissione (IoC)** individuati.

Computer **E**mergency **R**esponse **T**eam dell'Agenzia per l'Italia Digitale

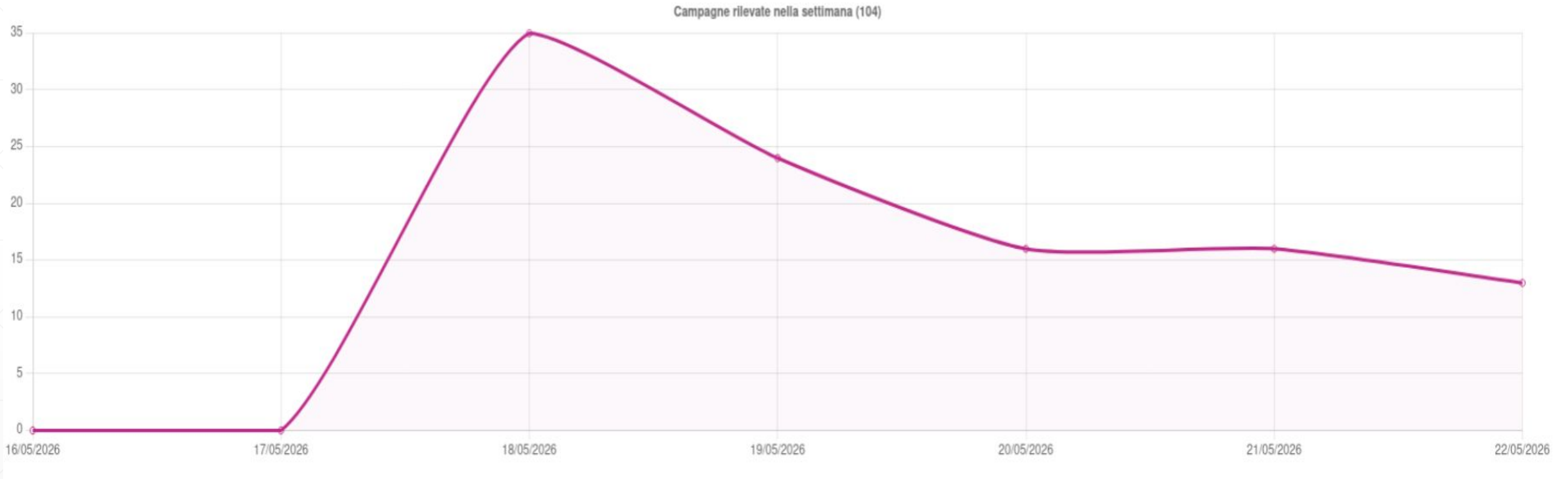
In concreto si occupa, ad esempio, di:

- monitorare campagne malevole, phishing, malware e vulnerabilità;
- pubblicare avvisi, report e analisi tecniche;
- fornire indicatori di compromissione, cioè **IoC**, utili per difendere reti e sistemi;
- supportare le amministrazioni nella prevenzione e gestione degli incidenti informatici.

Il termine **CERT** in generale indica un gruppo di professionisti dedicato alla gestione degli incidenti di sicurezza informatica e al coordinamento degli interventi per contenerne l'impatto.

Quindi, detto semplice: **CERT-AgID è il centro tecnico di AgID che segue la cybersicurezza per la PA, pubblicando anche analisi, allerte e strumenti utili contro minacce informatiche.**

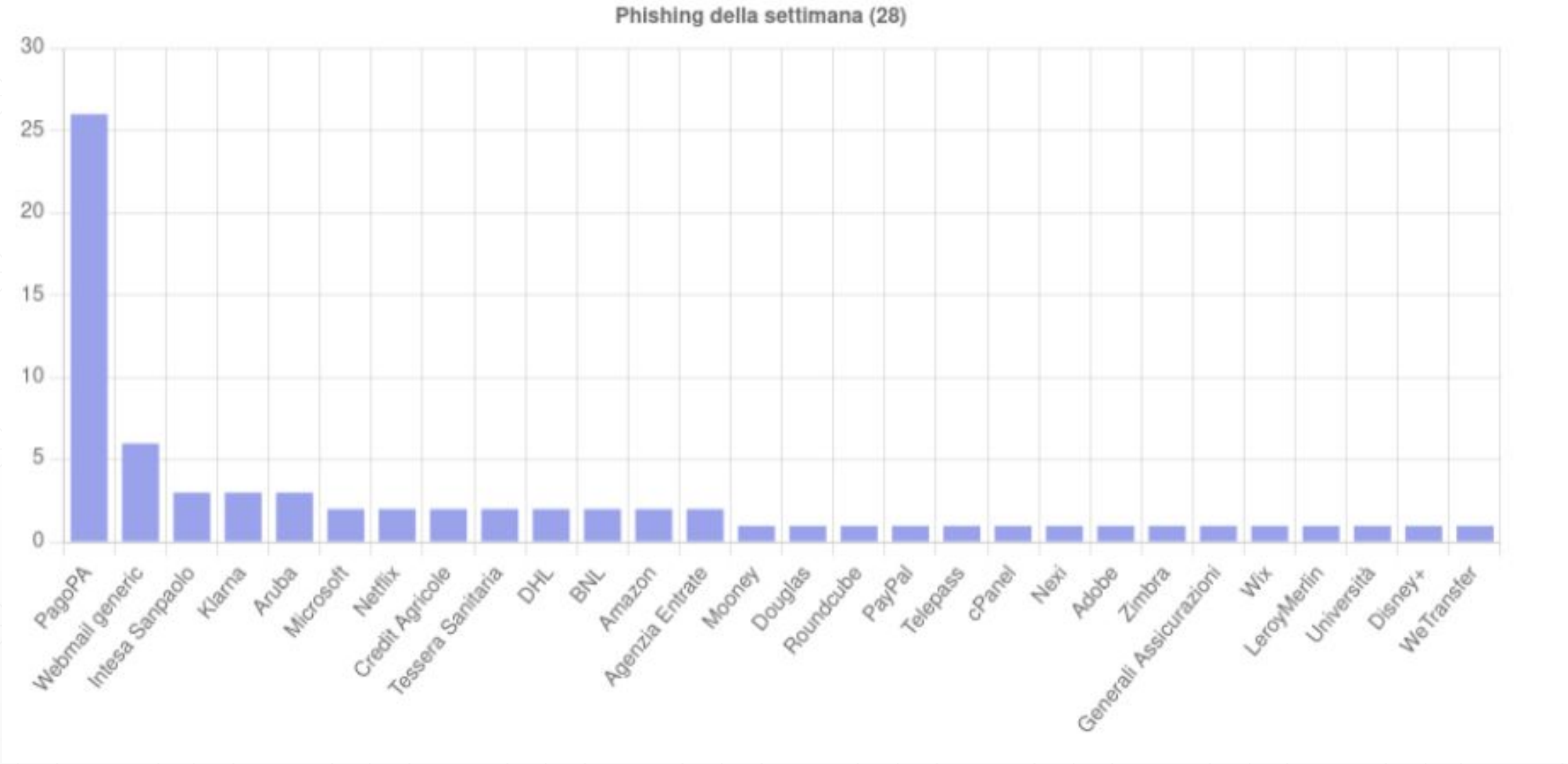
Malware: Campagne malevoli

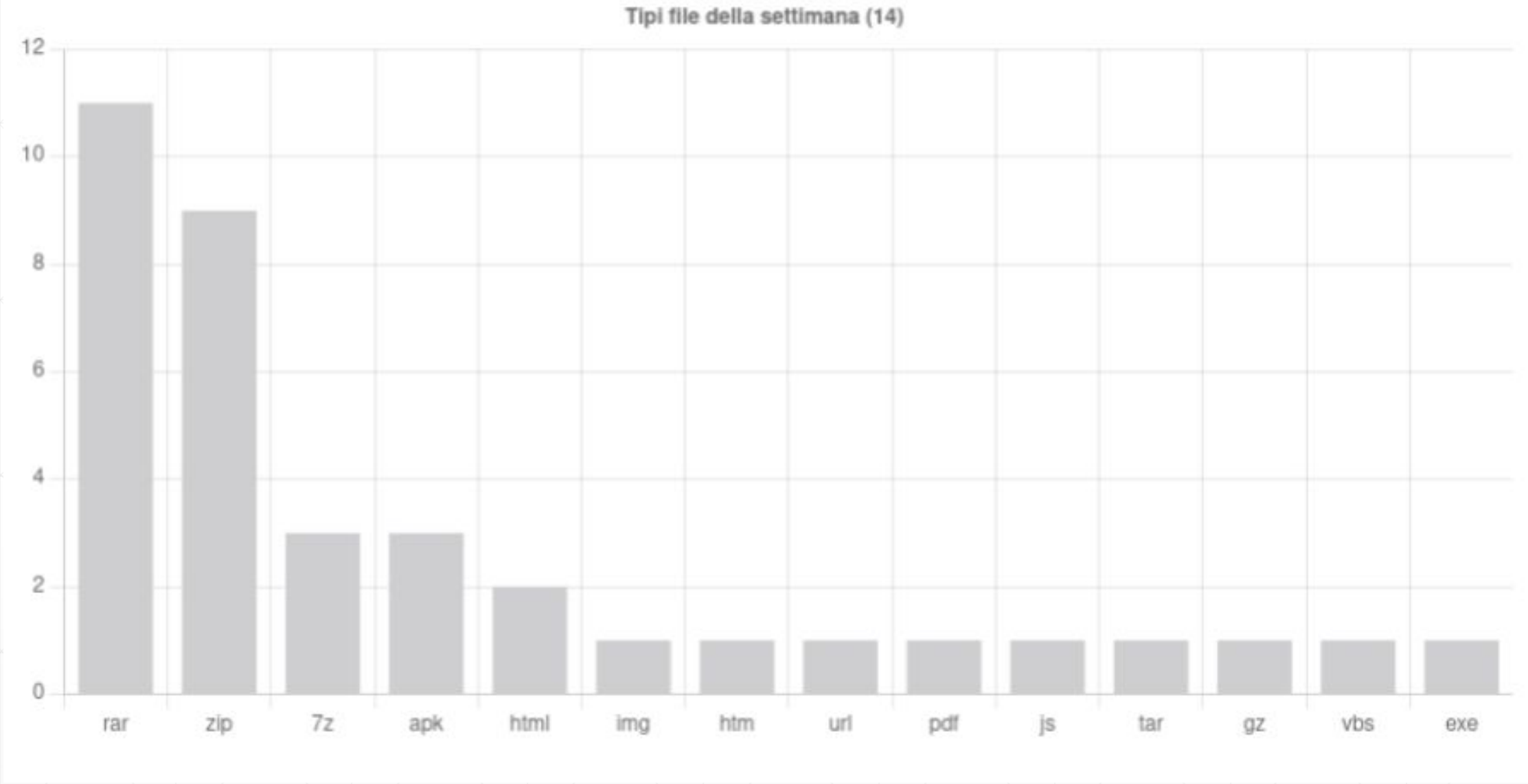


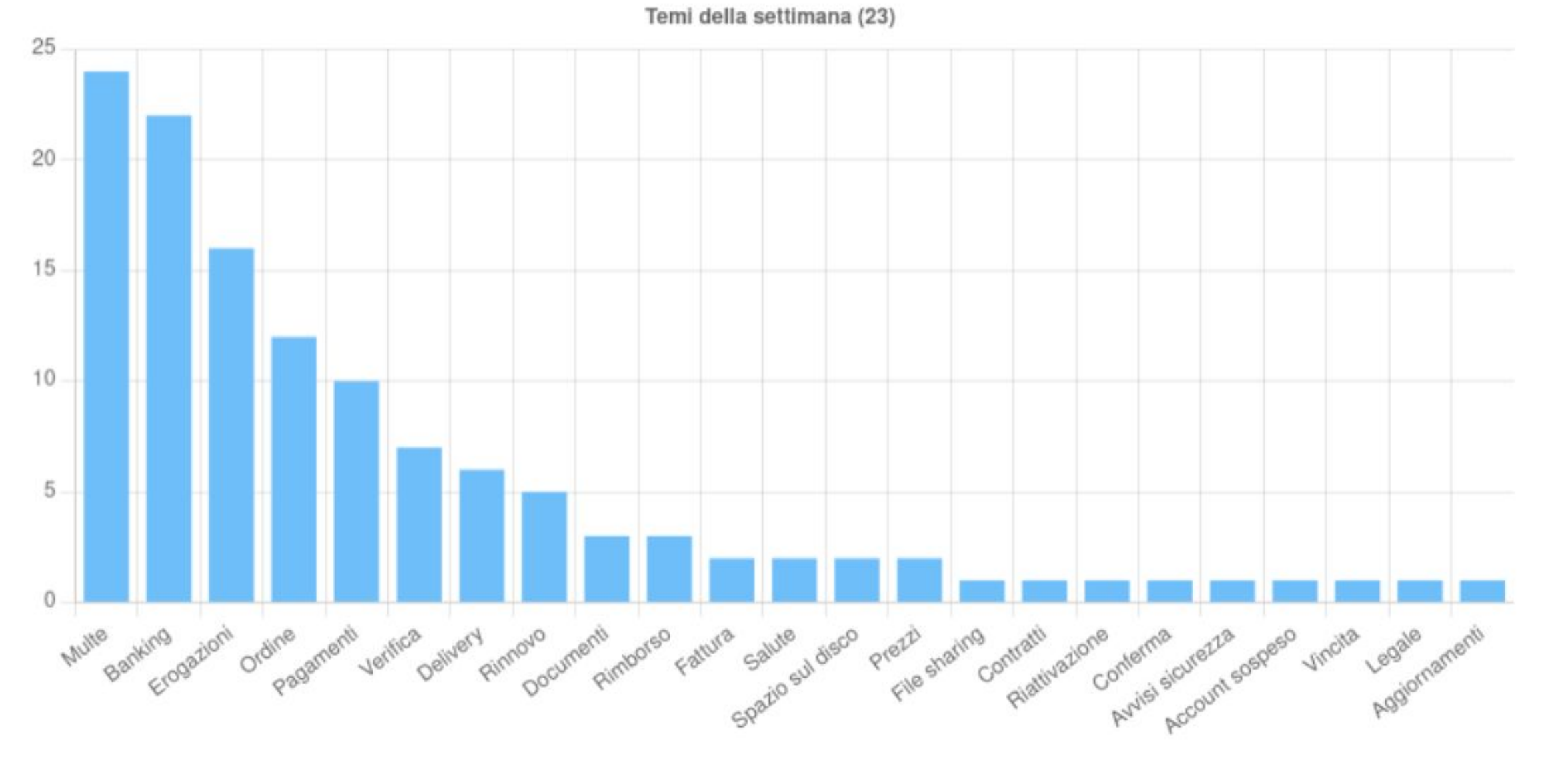
Malware: Campagne malevoli

Sono state individuate, nell'arco della settimana, **12 famiglie di malware** che hanno interessato l'Italia. Nello specifico, di particolare rilievo, troviamo le seguenti campagne:

1. **AgentTesla** – Individuate due campagne italiane a tema *"Ordine"* e otto campagne generiche a tema *"Contratti"*, *"Delivery"*, *"Pagamenti"*, *"Ordine"* distribuite con allegati RAR, ZIP, TAR, GZ e IMG.
2. **Remcos** – Rilevate una campagna italiana ad argomento *"Ordine"* e quattro campagne generiche ad argomento *"Documenti"*, *"Ordine"* e *"Prezzi"* diffuse con allegati 7Z, RAR e ZIP.
3. **XWorm** – Scoperte una campagna italiana a tema *"Ordine"* e tre campagne generiche a tema *"Prezzi"*, *"Preventivo"* e *"Delivery"* veicolate mediante allegati ZIP, RAR e 7Z.
4. **FormBook** – Osservate tre campagne generiche a tema *"Fattura"*, *"Contratti"* e *"Banking"* diffuse tramite email contenenti allegati RAR, ZIP e 7Z.
5. **AsyncRat** – Individuate una campagna italiana a tema *"Fattura"* e una generica a *"Ordine"*, entrambe distribuite tramite link che permette il download di archivio ZIP.
6. Osservate due campagne italiane **Copybara** e **Herodotus** e una campagna generica **RelayNFC** a tema *"Banking"*, veicolate tramite SMS contenenti link per il download di APK malevoli per dispositivi Android.
7. Rilvate infine due campagne italiane **Guloader** e **UpCrypter** e due campagne generiche **MassLogger** e **Purecrypter** che hanno sfruttato gli argomenti *"Documenti"*, *"Ordine"* e *"Pagamenti"* e sono state veicolate con allegati ZIP, RAR o HTML.


Phishing della settimana (28)
30
25
20
15
10
5
0
PagoPA
Webmail generic
Intesa Sanpaolo
Klarna
Aruba
Microsoft
Netflix
Credit Agricole
Tessera Sanitaria
DHL
BNL
Amazon
Agenzia Entrate
Mooney
Douglas
Roundcube
PayPal
Telepass
cPanel
Nexi
Adobe
Zimbra
Generali Assicurazioni
Wix
LeroyMerlin
Università
Disney+
WeTransfer


Tipi file della settimana (14)
12
10
8
6
4
2
0
rar
zip
7z
apk
html
img
htm
url
pdf
js
tar
gz
vbs
exe


Temi della settimana (23)
25
20
15
10
5
0
Multe
Banking
Erogazioni
Ordine
Pagamenti
Verifica
Delivery
Rinnovo
Documenti
Rimborso
Fattura
Salute
Spazio sul disco
Prezzi
File sharing
Contratti
Riattivazione
Conferma
Avvisi sicurezza
Account sospeso
Vincita
Legale
Aggiornamenti

Malware: Campagne malevoli

Sono **23** i temi sfruttati questa settimana per veicolare le campagne malevole sul territorio italiano. In particolare si rileva:

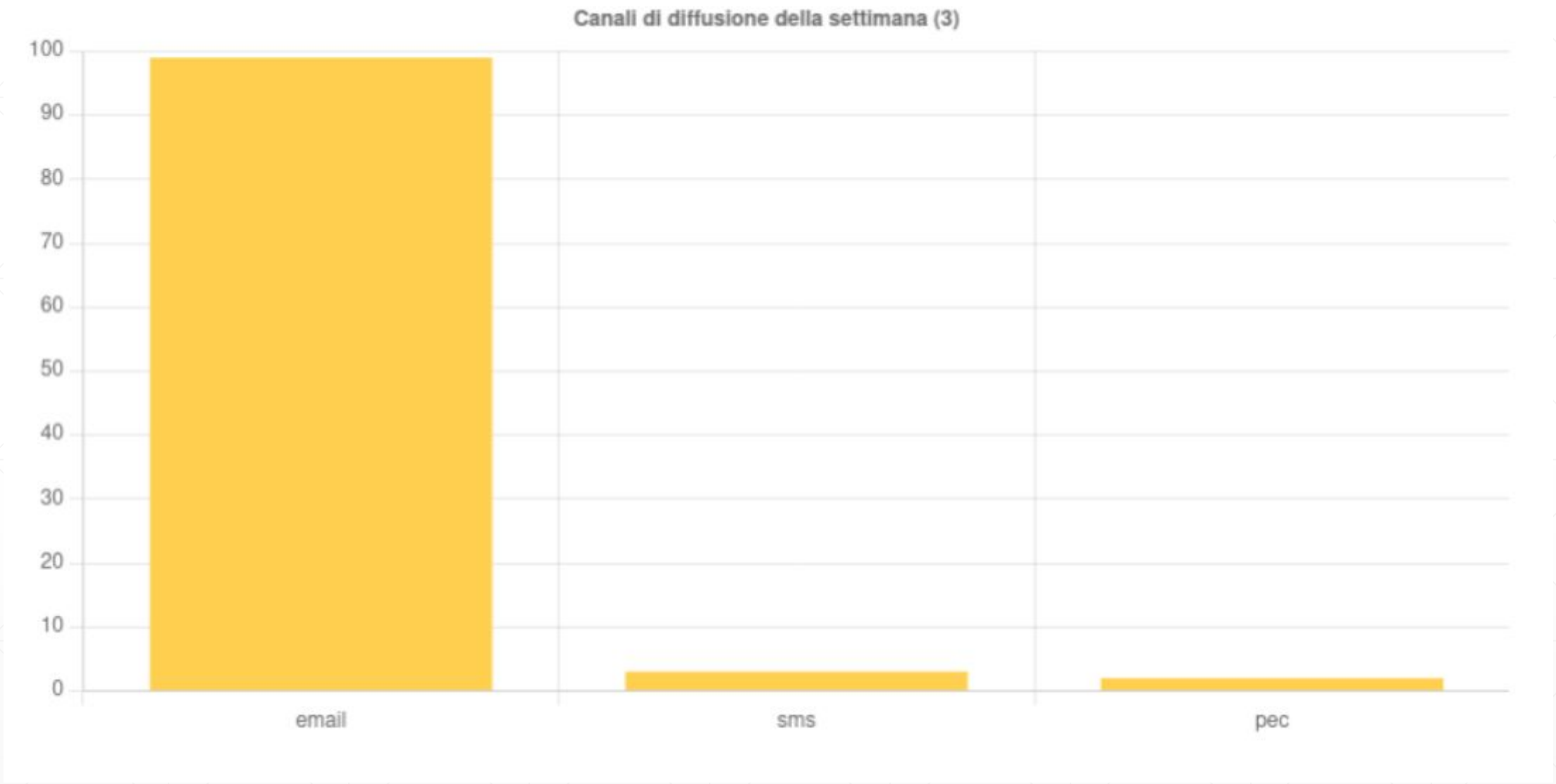
1. **Multe** – Argomento sfruttato in 24 campagne di phishing italiane, tutte veicolate tramite email che si fingono comunicazioni di multe non saldate e abusano del nome di **PagoPA**.
2. **Banking** – Tema utilizzato in 17 campagne di phishing, per lo più italiane, rivolte principalmente a clienti di istituti bancari e di credito, come **Inbank**,**PayPal**, **ING**, **BPM**, **Nexi**, **Intesa Sanpaolo** e **Klarna**. Usato inoltre per veicolare i malware **TrickMo**, **RelayNFC**, **Lokibot** e **AgentTesla**, inviati alle vittime mediante quattro campagne generiche e una italiana.
3. **Erogazioni** – Argomento sfruttato per 17 campagne italiane di smishing ai danni di **INPS**, realizzate sfruttando la piattaforma PHaaS **Darcula**.
4. **Ordine** – Tema utilizzato per veicolare numerosi malware, fra cui **Formbook**, **Remcos**, **AgentTesla**, **PhantomStealer**, **Guloader** e **XWorm**.

Il resto dei temi è stato utilizzato per veicolare campagne di malware e di phishing di vario tipo.

Malware: Campagne malevoli

Eventi di particolare interesse:

1. Individuata una nuova campagna di phishing che abusa del nome e del logo dell'**Agenzia delle Entrate**. La pagina fraudolenta si finge il portale ufficiale di AdE e richiede i dati dell'utente al fine di poter procedere con l'elaborazione di un **presunto rimborso** legato alla **dichiarazione dei redditi del 2025**. Oltre a rubare nome, cognome, codice fiscale, email e numero di telefono, l'obiettivo principale dei criminali è ottenere dati di **carte di credito**.
2. Il CERT-AGID ha rilevato numerose campagne via SMS che abusano del nome di **INPS** per attrarre le vittime con un falso "**bonus carburante**". A differenza dei precedenti phishing, questa volta il flusso è finalizzato al **furto dei dati della carta di pagamento**. Elementi tecnici riconducono alla piattaforma di Phishing-as-a-Service **Darcula**.


Canali di diffusione della settimana (3)
100
90
80
70
60
50
40
30
20
10
0
email
sms
pec

Malware “Ursnif”

Ursnif: che cos’è

Titolo: *Ursnif / Gozi – Il trojan bancario più diffuso*

Contenuti:
- Malware della famiglia **trojan bancari**
- Attivo da oltre 10 anni, continuamente aggiornato
- Obiettivo: **rubare credenziali bancarie e dati sensibili**
- Estremamente diffuso in Europa e in Italia
- Spesso parte di campagne di phishing mirate

Punti chiave:
- Forte capacità di **evitare gli antivirus**
- Vettore iniziale comune: **allegati Word/Excel**, ZIP, link malevoli
- Utilizzato da gruppi cybercriminali organizzati

Malware “Ursnif”

Come funziona Ursnif

Titolo: *Tecniche di attacco*

Meccanismi principali:
- **Keylogging:** registra ciò che l’utente digita
- **Webinject:** intercetta credenziali durante l’accesso ai siti bancari
- **Cookie/session hijacking:** sottrae le sessioni già aperte
- **Reconnaissance:** raccoglie info sul sistema (browser, rete, certificati)
- **C2 communication:** contatta i server criminali

Effetti sulla vittima:
- Accesso illecito ai conti correnti
- Possibile furto di identità
- Installazione di ulteriori malware (dropper)

Malware “Ursnif”

Come difendersi

Titolo: *Prevenzione: cosa fare davvero*

Utenti privati:
- Non aprire allegati imprevisti (soprattutto Word/Excel con macro)
- Diffidare da mail che chiedono di “aggiornare” o “sbloccare” account
- Usare l’autenticazione a 2 fattori (2FA)
- Evitare app modificate e software pirata

Aziende:
- Formazione continua dei dipendenti
- **Filtri mail + sandbox allegati**
- Controllo del traffico e blocco domini sospetti
- Backup frequenti

→ *La prima difesa non è tecnica ma comportamentale.*
La maggior parte delle infezioni parte da un clic sbagliato.

Come difenderci: la Sandbox

— Che cos’è una sandbox per allegati

Titolo: *Sandbox: come blocchiamo i malware prima che arrivino all’utente*

Contenuti:
•Ambiente virtuale isolato che apre e testa gli allegati in modo sicuro
•Analizza il comportamento reale del file
•Blocca malware prima che raggiungano la casella di posta
•Usata contro: AgentTesla, Ursnif, Emotet, IcedID, FormBook, Remcos
•Integrata nei sistemi: Microsoft Defender, Palo Alto, Fortinet, Google Workspace Enterprise

Messaggio chiave:
→ *L’utente non riceve nemmeno l’email infetta*

Come difenderci: la Sandbox

🧪 **Cosa controlla la sandbox?**

Dentro la sandbox il file viene testato per vedere se:

- prova a scaricare malware da Internet
- crea file nascosti nel sistema
- modifica il registro di Windows
- tenta di comunicare con server di comando e controllo (C2)
- esegue macro malevole
- estrae o invia dati

Se il file ha comportamenti sospetti → **viene bloccato e quarantinato**.

Come difenderci: la Sandbox

🏢 Chi usa le sandbox?

Sono molto usate da:
- aziende e pubbliche amministrazioni
- Banche
- infrastrutture critiche
- forze dell'ordine
- provider email professionali

Gmail e Outlook ne hanno versioni avanzate integrate per gli account business

🧩 In pratica
La sandbox è come far aprire l'allegato a una macchina virtuale sacrificabile al posto del tuo computer.
Se l'allegato è pericoloso, infetta la sandbox, non te.

Come difenderci: la Sandbox

ESEMPIO DI REPORT SANDBOX (REALISTICO)
(Formattazione simile a FireEye / Palo Alto WildFire / FortiSandbox)

Sandbox Report – Dynamic Analysis
File analizzato: Fattura_2025.zip
Contenuto: Fattura_2025.exe
Dimensione: 412 KB
SHA256: a4f98c1c7b3e9f...
Risultato: MALWARE – AgentTesla (variant 3.0)
Severità: ⭐⭐⭐⭐⭐ Alta

Come difenderci: la Sandbox

Comportamento osservato
Processi sospetti:
- Fattura_2025.exe → avvia regsvr32.exe
- powershell.exe -enc JABX... (PowerShell offuscato)

Il nome fa pensare a un file mascherato da fattura.
Una volta eseguito, avvia:regsvr32.exe Questo è un programma legittimo di Windows, ma spesso viene abusato dai malware per eseguire codice malevolo in modo meno evidente.

Persistenza:
- Creazione chiave Registro:
  HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater

la persistenza avviene creando una chiave di registro:HKCU\Software\Microsoft\Windows\CurrentVersion\Run\UpdaterQuesta chiave fa sì che il malware venga eseguito automaticamente ogni volta che l'utente accede a Windows.
In sostanza: anche se riavvii il PC, il virus riparte da solo.

Come difenderci: la Sandbox

File creati:

%AppData%\Roaming\SystemData\logins.txt%Temp%\capture_001.png

Questo significa che il malware potrebbe:salvare password o credenziali in logins.txt; catturare schermate del PC in capture_001.png;raccogliere informazioni dall'utente mentre usa il computer.

Esfiltrazione dati:

Connessione SMTP verso:
mail.websecure-ddns.com:587
→ tentativo di inviare credenziali rubate

La porta **587** è usata normalmente per l'invio di email tramite SMTP autenticato.
Quindi il malware tenta probabilmente di **spedire all'esterno le credenziali rubate** , usando un server mail controllato o abusato dagli attaccanti.

Raccolta informazioni:

- Estrazione password da:
  Chrome Firefox Outlook FileZilla
  Keylogging attivo (Hook tastiera installato)

Come difenderci: la Sandbox

In sintesi

Questo malware:
si presenta come una falsa fattura, esegue comandi PowerShell nascosti, si installa in avvio automatico, ruba password da browser/email/FileZilla, registra i tasti premuti, cattura schermate e tenta di inviare tutto verso un server esterno tramite SMTP.

È quindi compatibile con un **infostealer con funzionalità di keylogger e screenshot grabber**.
Gravità

La compromissione è **alta**, perché non si limita a disturbare il PC: punta chiaramente alla **raccolta ed esfiltrazione di credenziali**.

Misure immediate consigliate: isolare la macchina dalla rete, non usare più quel PC per cambiare password, acquisire evidenze/log, poi procedere con bonifica o reinstallazione pulita e cambio credenziali da dispositivo sicuro.

SMS + Phishing = Smishing

Smishing

Da: Noreply Service <cs@solcellskompaniet.se>
Inviato: venerdì 12 gennaio 2024 22:26
A: nome.cognome@azienda.it
Oggetto: Friday, January 12, 2024

Support-Desk

Hi Nome Cognome,
The Password; for nome.cognome@azienda.it needs to be revalidiated today
Time: (Friday, January 12, 2024 1:26 PM!)
Tick the box below, to continue with the same password,
KEEP MY CREDIENTIALS

Da: Service.Desk- <luismontes@latiendacom.com>
Inviato: lunedì 15 gennaio 2024 16:44
A:
Oggetto: Notification Storage LImit

Microsoft

Storage Is Almost Full.

96GB 99GB

Email Storage Quota Exceeded.
You must immediately clear your cache in order to send and receive new mails.

Clear Cache Now

NOTICE: If the cache is not cleared, incoming messages will be rejected.

Microsoft Postmaster Delivery System

MS Corporation, One MS Way, Redmond, WA 98052

Da: Area Clienti e Rinnovi <support@celtempimoderni.it>
Inviato: martedì 28 maggio 2024 06:08
A: [redacted] - Info <info@[redacted]>
Oggetto: comunicazioni@staff.aruba.it

aruba.it

Gentile Cliente

Ciao,
ti informiamo che il dominio a cui risulta collegato questo account di posta, scadrà il giorno ***28/05/2024.***

Desideriamo ricordare che, qualora il dominio non venga rinnovato entro tale data, questi e tutti i servizi associati, comprese le caselle di posta verranno disattivate e no npotranno più essere utilizzate per l'invio e la ricezione.

Fattura N : 123653914
Importo dovuto: 4,37€
Data di scadenza:28/05/2024

Puoi accedere alla tua area clienti per visualizzare e pagare la fattura su

RINNOVA IL DOMINIO

Altre considerazioni:

- Se ricevete mail da fantomatici professionisti verificate i dati (indirizzo mail, indirizzi fisici, nomi) perché, se phishing, sono sempre falsi! -

accesso-anomalo-aggiornamento.com
aggiornamento-anomali-sicurezza.com
appaggiorna.com
app-aggiorna.com
appnormativa.com
app-normativa.com
entradesso.work
evolution-postepay.com
identificazione-sicurezza-app.com
infoprivati.com
modulazione-aggiornamento-gisp.com
normativa-web-app.net
portale-info.com
portale-psd2.com
portaleweb1-Intesasanpaolo.xyz
portaleweb2-Intesasanpaolo.xyz
portaleweb3-Intesasanpaolo.xyz
protocollo-dati2021.com
psd2-italia.com
pt-italiane.com

Alcuni domini phishing italiani del 1 aprile 2025

Malware

Tramite mail fraudolente, i cybercriminali possono indurci ad aprire un allegato o cliccare su un link.
In pochi secondi il nostro PC sarà sotto il controllo dell'attaccante il quale potrà:

• Ricercare le vulnerabilità di tutti i dispositivi della rete e attaccare altri dispositivi interni
• Rubare i dati
• Registrare tutto quello che viene digitato sulla tastiera
• Accedere alla webcam e al microfono
• Recuperare le credenziali salvate sul browser
• Installare ulteriori software «spia» che analizzano la rete interna

Spesso l'attaccante rimane nascosto per lungo tempo prima di passare alle fasi finali dell'attacco:
• Eliminare i backup individuati
• Criptare tutti i dati per chiedere un riscatto

Qualche esempio, malware

Rispondi Rispondi a tutti Inoltra

mercoledì 02/02/2022 10:18

IM

Il Ministro degli Interni <IlMinistrodeglilr

Restrizioni anti-Covid19

A nome.cognome@azienda.it

I collegamenti e altre funzionalità all'interno del messaggio sono stati disabilitati. Per riattivare le funzionalità, spostare il messaggio nella cartella Posta in arrivo.
Outlook ha bloccato l'accesso ai seguenti allegati potenzialmente pericolosi: documento_26.zip.

Gentile Nome Cognome,

Il Ministro degli Interni;
mette a disposizione per le attività presenti sul territorio italiano un file di testo contenente le linee guida per le restrizioni anti-Covid19 in vigore dal 01/02/2022, scaricabile in allegato.
Si ricorda ai gentili cittadini che il mancato rispetto delle nuove restrizioni comporterà delle sanzioni penali , anch'esse elencate in allegato.

password: Covid#19

La presente e-mail è stata generata automaticamente, quindi la preghiamo di non rispondere a questo indirizzo di posta elettronica .

Polizia di Stato

POLIZIA

MINISTERO DELLA DIFESA

REPVBBLICA ITALIANA

EUROPOL

INTERPOL

DIREZIONE CENTRALE DELLA POLIZIABRIGATA DI PROTEZIONE MINORI

GARANZIA DI PROCEDURA LEGALE

Alla tua attenzione:

Io sottoscritto Sig. **Lamberto Giannini**, Capo della Polizia e direttore generale della Pubblica Security in collaborazionecon la Sig.ra Catherine De Bolle, Direttore di Europol e Capo della Brigata Protezione Minori (BPM) visti **gli articoli 20 21-1 e da 75 a 78 del Codice di Procedura Penale**.

Ti inviamo questo mandato poco dopo un sequestro informatico dell'infiltrazione informatica per informarti che seioggetto di diversi procedimenti legali in vigore.

Intraprendiamo azioni legali contro di te per:

- Pornografia Infantile
- Pedofilia
- Esibizionismo
- Cyberpornografia
- Offesa Alla Decenza

Per vostra informazione, **la legge 3901 del codice di procedura penale del marzo 2007** aumenta le pene quandosiano state commesse proposte, aggressioni sessuali o stupri.

Hai commesso il reato dopo essere stato preso di mira su Internet (sito pubblicitario), aver visualizzato un sito di pornografia infantile, foto/video di nudo e i tuoi scambi sono stati registrati dal nostro cyber-gendarme e costituiscono laprova dei tuoi reati.
La corte di giustizia che condanna tutti i tentativi relativi al traffico sessuale non ha potuto trascurare alcuno sforzo sutale vandalismo.

In virtù degli **articoli n. 98-468 del 17 giugno 2007, art. 809 comma 15 cp - Gazzetta Ufficiale 11 giugno 2009**.

Chiunque compia tali atti è passibile di procedimenti giudiziari e di una pena da **5 a 10 anni** di reclusione e **di una multada 5.000 a 76.000 euro.**

Per motivi di riservatezza ti inviamo questa e-mail, sei pregato di farti sentire via e-mail scrivendo le tue giustificazioniaffinché siano esaminate e verificate al fine di valutare le sanzioni; questo entro un termine rigoroso di 72 ore.

Siete pregati di risponderci via e-mail scrivendo le vostre giustificazioni affinché vengano messe all'esame e verificate alfine di valutare le sanzioni che entro un termine rigoroso di 72 ore.

Trascorso questo tempo, saremo obbligati a inviare la nostra denuncia al Pubblico Ministero per stabilire un mandatod'arresto nei vostri confronti e procederemo al vostro immediato arresto.

In questo caso, la tua pratica sarà trasmessa anche alle associazioni per la lotta alla pedofilia e ai media per la pubblicazione in modo che la tua famiglia e i tuoi cari sappiano cosa stai facendo, sarai registrato come molestatoresessuale in tutte le amministrazioni in tutta Europa e nel **Registro Nazionale dei Reati Sessuali (RNDS).**

Stiamo ancora aspettando la tua email di ritorno per dirti come procedere.

Cordiali saluti,
Sig. Lamberto Giannini
Capo della Polizia e direttore generale della Pubblica Security

DIREZIONE CENTRALE DELLA POLIZIABRIGATA DI PROTEZIONE MINORI
Via Portuense, 1680, 00148 Roma RM, Italie

POLIZIA DI STATO

7 SEGNALI SUI QUALI PORRE ATTENZIONE

Il primo segnale è il **dominio del mittente**. Controlla sempre ciò che segue la chiocciola: se trovi @poste-italiane-secure.com o @apple-id2026.com, stai di fronte a un fake.

Il secondo segnale è l'**URL del link**. Passa il mouse (o tieni premuto su mobile) e leggi l'indirizzo che appare in basso: se inizia con bit.ly, tinyurl o contiene caratteri cirillici, chiudi subito la mail.

Il terzo segnale sono i **micro-errori** introdotti dall'AI. L'intelligenza artificiale può sbagliare un accento ("PosteItalià") o inserire un'emoji mai usata dal brand.

Il quarto segnale è la **pressione psicologica**: frasi come "Rispondi entro 3 minuti o il conto si blocca" sono la nuova arma per farti agire senza pensare.
Il quinto segnale riguarda gli **allegati**. Se ricevi un file .html o un QR code che non hai richiesto, non aprirlo. Scannerizzalo solo con l'app ufficiale del tuo provider.

Il sesto segnale è la **firma digitale DKIM**: se nell'intestazione dell'email manca la voce DKIM=pass, il messaggio è sospetto.

Infine, il settimo segnale è il **certificato SSL**: il lucchetto del browser deve essere verde e mostrare il nome dell'ente (es. "Banca Intesa Sanpaolo S.p.A."), non solo la scritta https.

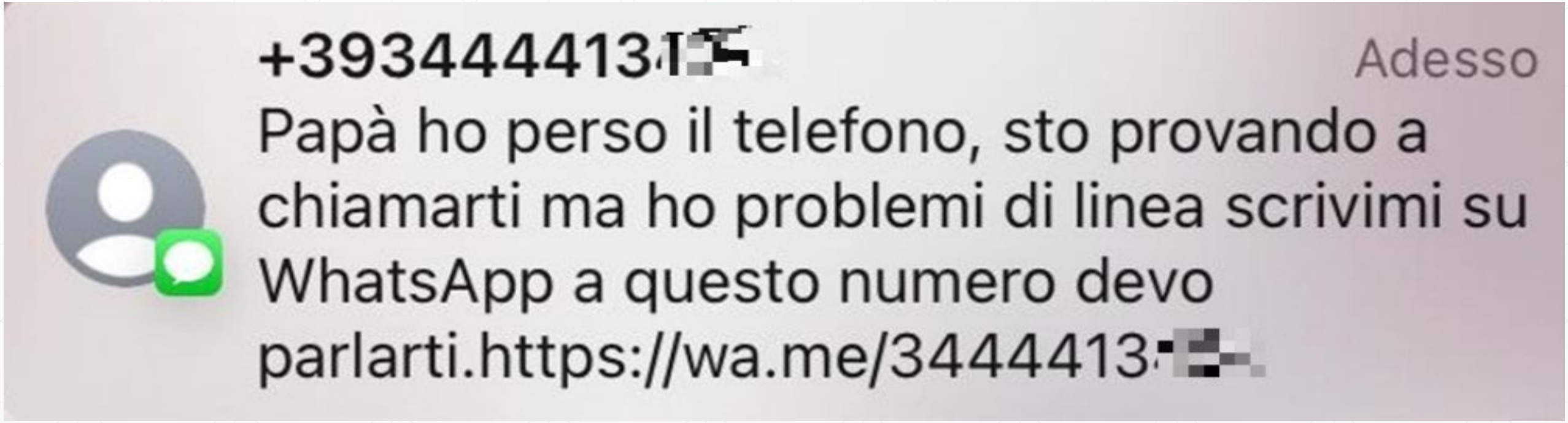
Come difendersi (prima che sia troppo tardi)

Ci sono alcune **regole semplici**, che però vanno interiorizzate:

1. **La banca non vi chiederà mai, via email, SMS o telefono, password, PIN o codici OTP.**
2. Non cliccate su link ricevuti via mail o messaggi per "sbloccare il conto" o "aggiornare l'app".
   Se avete un dubbio, **chiudete tutto** e:
   - entrate nell'app o nel sito **digitando l'indirizzo a mano**,
   - oppure chiamate la banca usando i numeri ufficiali che già conoscete.
3. Scaricate le app **solo dagli store ufficiali** (Google Play, App Store) e mai da link ricevuti in giro.
4. Tenete sempre **aggiornati** sistema operativo e antivirus.
5. Non installate software piratato "craccato": è uno dei veicoli preferiti per i malware.
6. Se qualcosa vi mette ansia, vi fa sentire sotto pressione, vi chiede di agire "subito e senza dirlo a nessuno"…
   fermatevi. Fate una telefonata a qualcuno di cui vi fidate, a un'associazione dei consumatori, alla vostra banca o alle forze dell'ordine. Dieci minuti di prudenza valgono più di mesi di battaglie per recuperare i soldi.

Truffa dell’emergenza familiare 2.0
Ricevete un messaggio o un audio WhatsApp che sembra la voce di vostro figlio, vostra figlia, un parente:
“Ho avuto un incidente… mi servono subito dei soldi… fai un bonifico a questo IBAN… non chiamare nessuno, ti spiego dopo…”.

La voce è identica, il modo di parlare anche. Ma potrebbe essere una voce generata dall’IA, costruita partendo da video, messaggi vocali e contenuti che quella persona ha messo online.



App contenenti malware

Un SMS vi avvisa: “La sua app bancaria è obsoleta. Clicchi qui per scaricare l’aggiornamento”.
La pagina che si apre è identica a quella dello store, ma non è ufficiale.
Installate l’app e in realtà installate un malware che ha pieno accesso al vostro telefono.

Falsa chiamata o SMS dall'"antifrode" della banca

1

Il cliente riceve un **SMS di phishing**, apparentemente proveniente dalla Banca, con un link che rimanda **ad un sito simile** all'Internet Banking della Banca utilizzato dai truffatori per rubare le sue credenziali bancarie e, successivamente, ulteriori dati (es. saldo, movimenti etc.)

2

I truffatori contattano al telefono il cliente e, **fingendosi operatori antifrode della Banca e/o della Polizia Postale** per acquisire la sua fiducia, lo allertano circa **false «operazioni fraudolente momentaneamente bloccate»** sul suo conto corrente.

3

I truffatori convincono il cliente a **recarsi «con urgenza» in filiale** per eseguire, da sportello, operazioni di pagamento (tipicamente bonifici istantanei) verso un nuovo conto corrente appena aperto a suo nome e **al fine di «mettere in sicurezza» i propri fondi.**

4

Una volta in filiale, il cliente viene persuaso ad eseguire un **bonifico** verso un **nuovo IBAN fraudolento** fornito dai frodatori e, convinto di «mettere in sicurezza i proprio risparmi», **li trasferisce verso i frodatori.**

Truffa Trading Online

Truffa Trading Online

LA TRUFFA – «Il primo contatto avviene spesso tramite **social**, app di messaggistica istantanea o contatto telefonico da parte di falsi broker che invitano la vittima a **registrarsi su una piattaforma online**, ovviamente gestita dallo stesso truffatore, e investire piccole somme di denaro, almeno inizialmente. Con la scusa di dover sbloccare il capitale investito o di dover pagare tasse o commissioni, però, i malcapitati vengono **convinti a versare ulteriori somme di denaro**, spesso tramite bonifici istantanei, senza mai riuscire a monetizzare i propri (finti) guadagni.

LA TUTELA – «**Diffidare dalle promesse di guadagni rapidi**, eccessivi e sproporzionati; diffidare da **operatori che contattano dall'estero**; rivolgersi ad operatori del settore qualificati e regolamentati, avendo cura di verificare che si tratti di **società autorizzate**, consultando il sito della Consob e della Banca d'Italia. È importante anche **evitare di comunicare informazioni sensibili** (come credenziali bancarie, password e simili) e non installare mai **software di controllo remoto** suggeriti da sconosciuti».


82% 15:25
Camilla
sta scrivendo...
Ieri
Ciao ciao ciao 10:31
Non sai che mi è appena successo 10:31
Ciao Camilla, sono curioso 😃 10:31
Ho appena chiuso la mia prima transazione, 300€ in più rispetto a quanto avevo investito 10:33
10:35
Grazie, i tuoi consigli sono stati preziosissimi!!!!! 10:35
Quando vuoi, hai il mio numero 😎 10:44
Scrivi un messaggio


42% 14:18
Fabrizio
10 Gennaio
Ciao 👋 scs il disturbo 19:17
Ciao bomber, dimmi tutto 😜 19:19
Ho appena comprato l'auto nuova 19:20
È pazzesko, senza i tuoi consigli non avrei mai potuto guadagnare tanto investendo 19:21
GRAZIE 19:21
Ma ti pare! 😘 tutto merito tuo che ti sei messo in gioco 19:22
Continua così! Tieni d'occhio le aziende hi-tech per quest'anno 19:22
Contaci, quest'anno si svolta 19:30
Scrivi un messaggio

Da: "alessia[redacted]@gmail.com>
A: "poltel.vi.poliziadistato.it" <poltel.vi@poliziadistato.it>
Inviato: Domenica, 9 novembre 2025 16:10:44

Buon giorno sono Alessia[redacted]..Mi sono imbattuta in una piattaforma di trading su telegram,probabilmente fasulla.
Invitata tramite un link..
Ho conseguito dei bonifici tramite banca..dovendo dimostrare il bonifico tramite screenshot del movimento bancario.. ma per avere il mio rimborso di fine lavoro..sono stati chiesti altri soldi..
Chiedo la vostra cortese attenzione...
Contatto:[redacted]

Grazie.Distinti saluti.

Da: "Luca[redacted]<luca[redacted]@gmail.com>
A: "poltel.vi.poliziadistato.it" <poltel.vi@poliziadistato.it>
Inviato: Martedì, 21 ottobre 2025 13:08:42
Oggetto: richiesta informazioni su portale amazon

Buongiorno,
ho depositato molti soldi in un portale gestito da amazon. Ora voglio prelevarli, ma l'assistenza di amazon mi scrive che bisogna prima versare una percentuale del 26% sulla somma presente in quanto la somma è depositata in criptovalute.
Vorrei sapere se sono stato vittima di una truffa.
Vivo a[redacted]
Il mio numero è[redacted].
Saluti,
Luca[redacted]

Da: "[redacted]@gmail.com>
A: "poltel.vi.poliziadistato.it" <poltel.vi@poliziadistato.it>
Cc: [redacted]
Inviato: Domenica, 26 ottobre 2025 17:54:09
Oggetto: Richiesta appuntamento urgente – Denuncia truffa trading online[redacted]

A chi di dovere,

scrivo a nome di mio padre, il Sig. [redacted] (in copia a questa email), per richiedere un appuntamento urgente presso la vostra sede al fine di presentare formalmente una denuncia per grave truffa informatica e finanziaria internazionale.

In sintesi, mio padre è stato contattato da un presunto broker che si presenta con il nome Massimiliano Marchese e indotto a effettuare investimenti nel mercato del Forex e delle criptovalute tramite le piattaforme metaquotes-uk.com e crypto.com. È stato costretto ad aprire conti presso OpenPayd e Simple Europe UAB, fornendo dati personali, copia del documento d'identità e riconoscimento facciale, ed ha eseguito numerosi bonifici bancari per un importo complessivo di circa €274.000, verso conti situati in Malta, Lituania, Francia e Italia.
Oltre al danno economico, mio padre è stato sottoposto a gravi pressioni psicologiche e a una vera e propria violenza emotiva, con continue minacce di blocco dei conti, falsi allarmi di perdita dei fondi e richieste incessanti di ulteriori versamenti.

Alleghiamo alla presente la dichiarazione completa in formato PDF, contenente ulteriori dettagli e IBAN. Ulteriori documenti di supporto (estratti conto bancari, schermate delle comunicazioni, ecc.) sono disponibili e verranno consegnati in formato cartaceo durante l'appuntamento.

Chiediamo cortesemente di poter fissare un appuntamento nel più breve tempo possibile per consegnare la documentazione e formalizzare la denuncia presso la vostra sede.

Da: [redacted]" <[redacted]@gmail.com>

A: "poltel.vi.poliziadistato.it" <poltel.vi@poliziadistato.it>

23 ottobre 2025 16:22

1000051676.png (314 KB) Scarica | Valigetta | Rimuovi
1000051677.png (277,7 KB) Scarica | Valigetta | Rimuovi
1000051679.png (292,5 KB) Scarica | Valigetta | Rimuovi
1000051675.png (265,2 KB) Scarica | Valigetta | Rimuovi
1000051678.png (281,5 KB) Scarica | Valigetta | Rimuovi
1000051681.png (276,5 KB) Scarica | Valigetta | Rimuovi
1000051680.png (276 KB) Scarica | Valigetta | Rimuovi
1000051749.png (237 KB) Scarica | Valigetta | Rimuovi
1000051682.png (248,2 KB) Scarica | Valigetta | Rimuovi

Visualizza tutte le immagini
Scarica tutti gli allegati
Rimuovi tutti gli allegati

Buona sera. mi chiamo A[redacted]
Vivo a[redacted]nel comune[redacted]
Da qualche giorno a questa parte sono soggetto a violenza psicologica ed estorsione da parte di una piattaforma trading di cripto valute. Nei messaggi mi chiedono risarcimenti del più del 50 % del capitale del portafoglio digitale e per ogni giorno che passa mi aumenta del 20%. In fine mi hanno minacciato scrivendomi che rischio 10 anni di carcere.
Questa è la mia prima esperienza nelle cripto valute e non so come comportarmi.
Il mio numero è[redacted]
Hanno anche detto che ci saranno provvedimenti penali a mio carico.
Questi sono solo una parte.

Dati Ordinante

Intestazione	[redacted]
Numero Conto Corrente di Addebito	[redacted]
IBAN Conto Corrente di Addebito	[redacted]

Dati Beneficiario

Intestazione	[redacted]
IBAN o Conto di Accredito	MT22CFTE28004000000000004037385

Dati Operazione

Stato	Eseguito
Importo	12.000,00
Divisa	EUR
Tipologia Spese	SHA - Condivise
Causale Bonifico	ORDINARY TRANSFER
Nome Banca Beneficiario	OPENPAYD FINANCIAL SERVICES MALTA LTD
Nazione Banca Beneficiario	MALTA
BIC/SWIFT	CFTEMTM1XXX
Data Operazione	17/01/2025
Data Valuta Beneficiario	20/01/2025
Data Valuta Ordinante	17/01/2025
ID Transazione/CRO	[redacted]03395ZL1290060530IT
Commissioni Ordinante (EUR)	0,00
Commissioni Beneficiario (EUR)	0,00

Dati Ordinante

Intestazione	[redacted]
Numero Conto Corrente di Addebito	[redacted]
IBAN Conto Corrente di Addebito	[redacted]

Dati Beneficiario

Intestazione	[redacted]
IBAN o Conto di Accredito	MT22CFTE28004000000000004037385

Dati Operazione

Stato	Prenotato
Importo	4.000,00
Divisa	EUR
Tipologia Spese	SHA - Condivise
Causale Bonifico	ORDINARY TRANSFER
Nome Banca Beneficiario	OPENPAYD FINANCIAL SERVICES MALTA LTD
Nazione Banca Beneficiario	MALTA
BIC/SWIFT	CFTEMTM1XXX
Data Operazione	14/01/2025
Data Valuta Beneficiario	16/01/2025
Data Valuta Ordinante	15/01/2025
ID Transazione/CRO	[redacted]0203395
Commissioni Ordinante (EUR)	Informazione disponibile in stato Eseguito
Commissioni Beneficiario (EUR)	Informazione disponibile in stato Eseguito

«Queste truffe hanno conseguenze devastanti per le vittime, non solo per le gravi perdite economiche ma anche per i traumi emotivi che sono costrette a subire non appena si rendono consapevoli di aver subito una manipolazione psicologica che li ha indotti ad agire ingenuamente.
La **prevenzione** rimane, dunque, l'unica arma per contrastare questo fenomeno criminale».

Grazie per l’attenzione

Un ringraziamento a tutti coloro che hanno contribuito a realizzare l’evento, in particolar modo a:

Corrado Piccione	Polizia Postale
Alessandro Albiero	Vigili del Fuoco volontari di Recoaro Terme