consumerismo®

THREAT INTELLIGENCE BRIEFING | GIUGNO 2026

Il Nuovo Paradigma delle Truffe in Italia.

Mappa, evoluzione e casi anomali: dalle frodi istituzionali al furto identitario profondo.

A cura dell'Osservatorio di Consumerismo No Profit. Documento di sintesi a uso istituzionale.

L’Emergenza Nazionale: Impatto e Volumi

559,4 Mln €

Importo stimato sottratto nel triennio 2022–2024.

2,8 Milioni

Vittime stimate nel solo 2024.

13.500

Ricorsi ABF per truffe online previsti nel 2025 (56% con esito pro-cliente).

Alert

Modalità Zero: I dati quantitativi su impatti e ricorsi derivano da stime primarie (Banca d’Italia, relazioni FABI e ABF) attualmente in fase di consolidamento formale.

La Matrice delle Minacce: Aree d'Azione

Frodi Digitali

- **Vettore:** SMS, Email, App.
- **Meccanismo:** Smishing bancario, Finti avvisi di multe, Malware Android (APK).
- **Target:** Utenti con home banking ed e-commerce.

Truffe Istituzionali

- **Vettore:** Portali falsificati, Spoofing.
- **Meccanismo:** Falsi pagamenti PagoPA/SEND, Finti rimborsi o bonus INPS / Agenzia delle Entrate, Falsi aggiornamenti SPID.
- **Target:** Cittadini fiduciosi nella PA.

A Domicilio (Fisiche)

- **Vettore:** Contatto fisico diretto.
- **Meccanismo:** Falsi tecnici utenze, Agenti energia predatori, Tecnica dell'Intimidazione (es. l'Arrotino).
- **Target:** Anziani, soggetti isolati o fragili.

L’Escalation di Maggio-Giugno: Il Sorpasso delle “Multe”

Insight Panel

I volumi totali **raddoppiano**. Il baricentro degli attacchi si sposta drasticamente dai **conti correnti** alle **finte contravvenzioni (SEND, PagoPA, ATAC)**, sfruttando l'ansia sanzionatoria per ridurre i tempi di verifica della vittima. **Oltre 1.400 IoC** (Indicatori di Compromissione) rilevati in una sola settimana.

L’Evoluzione Tattica: Dal Phishing al Furto Identitario “Profondo”

Il Vecchio Modello: Phishing Tradizionale (Fino al 2024)

- **Obiettivo:** Rubare Credenziali o codice OTP.
- **Metodo:** “Clicca sul link e accedi”.
- **Impatto:** Danno limitato a una singola transazione non autorizzata.

Il Nuovo Paradigma: Furto Identitario Profondo (2025-2026)

- **Obiettivo:** Rubare Documenti, IBAN e Dati Biometrici.
- **Metodo:** Simulazione di procedure KYC (Know Your Customer) tramite piattaforme PHaaS (es. Darcula).
- **Impatto:** Acquisizione totale dell’identità. Permette ai truffatori di aprire nuovi conti e stipulare futuri contratti a nome della vittima.

Consumerismo avverte: la regola “non cliccare sui link” è obsoleta. **La nuova linea di difesa è la protezione assoluta del riconoscimento video e dei documenti.**

Anatomia di un’Anomalia:
La Trappola del Falso KYC

Anatomy of an Attack

1. L’Esca (Phishing SPID/AgID): Email urgente che richiede "aggiornamento documentale".

2. La Piattaforma (PHaaS): Atterraggio su un portale clone indistinguibile dall'originale.

3. L'Estrazione Dati: Inserimento di generalità, Codice Fiscale, Email, Telefono, IBAN.

4. Il Furto Biometrico (Il punto di non ritorno): Il sistema richiede il caricamento fronte/retro dei documenti d'identità.

5. La Finta Diretta Video: Istruzioni per registrare un video-selfie ("guarda verso la telecamera", "sorridi").

Insight Panel

L'utente crede di completare una verifica di sicurezza; in realtà, sta fornendo il kit completo per la clonazione della propria identità digitale.

Flussi Adattivi: L'Attacco Ibrido 'Phishing + Vishing'

Caso Studio: Agenzia delle Entrate - Cripto-Asset (Rilevazione CERT-AGID, ~19 Giugno 2026).

Step 1: Il Gancio Digitale

SMS con finta urgenza su scadenze imminenti per la "dichiarazione obbligatoria cripto-asset". Abuso totale di loghi e grafiche AdE.

Step 2: L'Analisi della Vittima

La vittima atterra sulla pagina esca. Il sistema analizza il livello di reattività e vulnerabilità.

Pivot Point

Step 3: L'Escalation Umana (Vishing)

Il flusso si adatta dinamicamente. Invece di chiedere un semplice dato, parte una telefonata (spoofed, numero istituzionale) da un finto operatore che guida la vittima in stato di agitazione fino al completamento della frode.

L’Escalation Android:
Da SMS a Controllo del Dispositivo

-23%

Calo dei volumi di Smishing (2024 vs 2025)

Dal 28% al 45%

Aumento della quota di SMS che veicolano Malware

Il Catalogo delle Minacce (APK Bancari)

L’SMS non cerca più solo le credenziali, ma induce l’utente a installare file APK malevoli (Trojan) fuori dagli store ufficiali.

Famiglie attive:

- BingoMod
- Copybara
- MoqHao
- OverlayPhantom
- RelayNFC

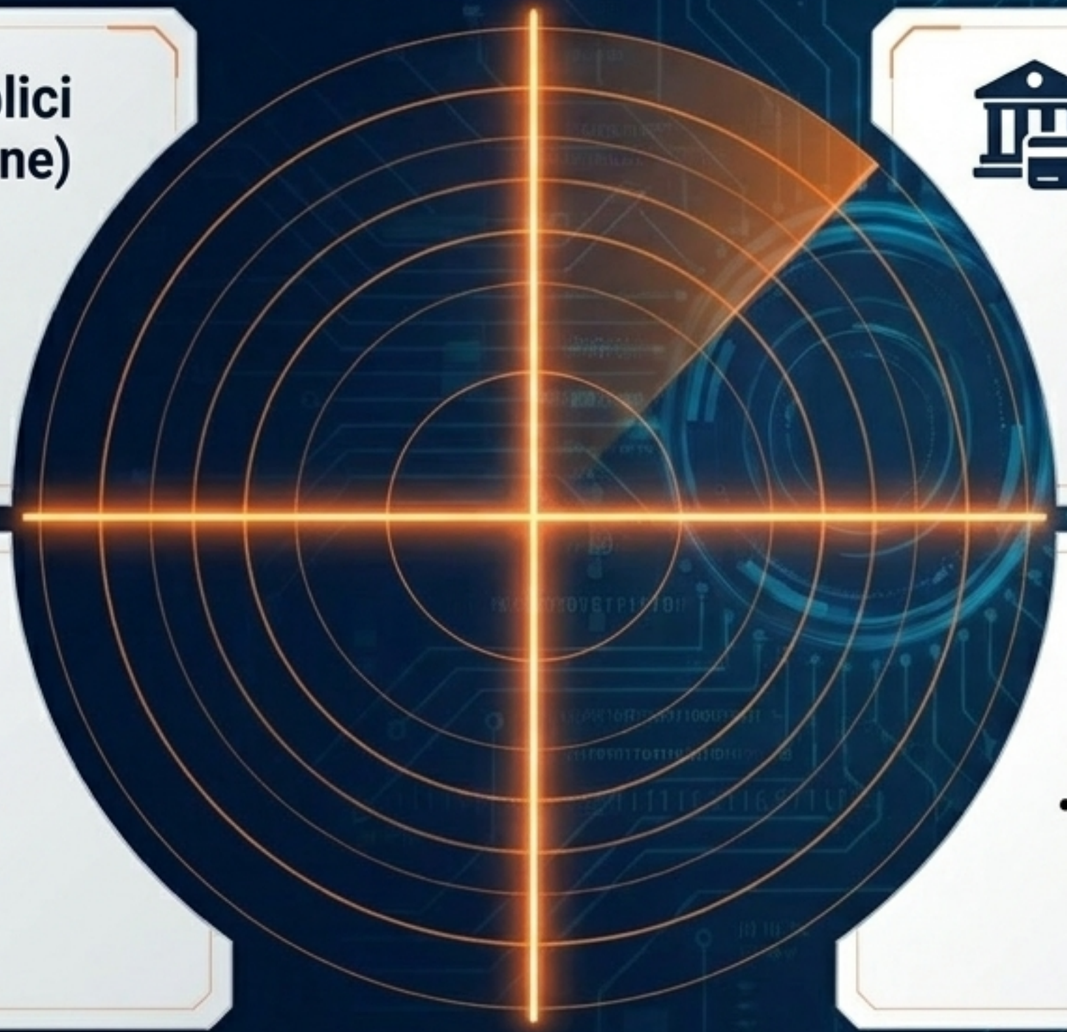
Insight Panel

Il rischio non è più il furto di una password, ma il controllo remoto totale del dispositivo della vittima.

Il Radar dello Sfruttamento dei Brand: **L'Abuso della Fiducia**

The Intelligence Dossier

Nel 2025, **153 marchi** ad alta fiducia pubblica sono stati sfruttati per ingannare i consumatori.



PA e Servizi Pubblici (Altissima Pressione)

- SEND, PagoPA, ATAC, INPS, Agenzia delle Entrate, SPID/AgID, Tessera Sanitaria.

Banche e Pagamenti (Volume Strutturale)

- Intesa Sanpaolo, BPM, BNL, Nexi, Mooney, Klarna, PayPal, ING, Credit Agricole, Inbank.

E-commerce e Infrastrutture (Tema 'Rinnovo')

- Amazon, Adobe, Netflix, Aruba, Hosting/Registrar.

Energia e Utenze (Mercato Libero)

- Finti operatori del mercato libero per carpire bollette e attivare contratti non autorizzati.

Il Fronte Fisico:
L’Equazione della Vulnerabilità Estiva

Le Minacce Attive:

- **Il Ritorno dell’Arrotino:**
  Servizi proposti a pochi euro che, a lavoro concluso, si trasformano in richieste di centinaia di euro sotto minaccia.

- **Falsi Tecnici:**
  Sedicenti incaricati luce/gas/acqua che accedono in casa per sottrarre beni o bollette (per cambi gestore illeciti).

Caso in Evidenza: Olgiate Comasco (Giugno 2026). Un anziano di 91 anni ha subito una richiesta estorsiva di 540 euro per l'affilatura di soli tre coltelli.

Sintesi del Paesaggio: La Biforcazione della Minaccia 2026

Iper-Digitale

Attacchi algoritmici su scala industriale. Sfruttano la fiducia cieca nei sistemi istituzionali (SEND, SPID). Efficaci anche contro utenti ad alta alfabetizzazione digitale tramite tattiche adattive (Vishing).

La Vulnerabilità Umana

Iper-Fisico

Attacchi mirati, basati sulla presenza corporea. Sfruttano l'isolamento sociale e la cortesia/soggezione (Finti Tecnici, Arrotini). Colpiscono spietatamente le fasce demografiche più fragili.

La **sicurezza tecnica** (password, firewall) è ormai aggirata.
Il truffatore del 2026 attacca direttamente **l'identità** dell'individuo o la sua **psiche**, rendendo obsoleta la sola difesa tecnologica.

Playbook di Difesa: Linee Guida per i Consumatori

Regole Auree

- Verificare SEMPRE le sanzioni o cartelle sui canali web/app ufficiali, mai tramite il link fornito.
- Scaricare app esclusivamente dagli store ufficiali (Apple/Google). Mai installare file APK ricevuti via SMS.
- Pretendere sempre preventivi scritti per lavori a domicilio; le utenze non inviano tecnici senza preavviso ufficiale.

Bandiere Rosse
(Fermarsi immediatamente se...)

- Vengono richiesti dati della carta o IBAN via SMS/Email da enti pubblici (INPS, AdE, SEND non lo fanno mai).
- Un processo di "aggiornamento" richiede di caricare documenti d'identità o registrare un video-selfie.
- Il messaggio sfrutta l'urgenza o una "scadenza imminente" per forzare un'azione impulsiva.

Playbook di Sistema: Direttive per Istituzioni e Operatori

Pilastro 1: Aggiornamento Informativo

Le campagne pubbliche devono abbandonare il focus sulle password e focalizzarsi sul pericolo del furto identitario “profondo” (video e documenti).

Pilastro 2: Risposta Rapida

Necessità di un coordinamento accelerato tra telco, banche e istituzioni per la dismissione immediata dei domini malevoli e la diffusione degli IoC.

Pilastro 3: Regolamentazione

Attenzione normativa sull’abuso sistematico dei brand della Pubblica Amministrazione (SEND, INPS) e blocco delle piattaforme criminali Phishing-as-a-Service.

Pilastro 4: Tutela Fisica

Rafforzamento normativo e controlli sulle pratiche commerciali per proteggere le fasce fragili dalle truffe a domicilio e dal porta a porta aggressivo (energia).

Rete di Segnalazione e Supporto Attivo

SPORTELLO NAZIONALE

Hai un problema da segnalare?

CONTATTA:

NUMERO UNICO NAZIONALE
06 94805440

piututela@consumerismo.it

Segnalazioni Tecniche (CERT-AGID)

Per inoltrare email o SMS sospetti e contribuire al rilevamento delle minacce:
malware@cert-agid.gov.it

L'Osservatorio di Consumerismo vigila costantemente per aggiornare la mappa delle minacce a tutela dei cittadini.