

RAGGIRI DIGITALI: COME FUNZIONANO LE TRUFFE SU WHATSAPP, TELEGRAM E SUI SOCIAL

26 Ottobre 2025



Anche le truffe evolvono man mano che le tecnologie migliorano. Oggi i raggiri non sono più come quelli di dieci anni fa, sono più subdoli e inaspettati. Vediamo dov'è che si corre di più il rischio, quali sono le tecniche più usate e a chi bisogna rivolgersi in caso di problemi.

Le piattaforme cambiano e, di conseguenza, anche le truffe si spostano. Dalle app di messaggistica ai marketplace fino ai siti per i pagamenti. In un rapporto del 26 agosto 2025 della [Banca d'Italia](#) si legge che c'è una crescita netta delle frodi:

0,017% per le carte

0,021% per le monete elettroniche

0,002% sui bonifici ordinari

0,057% sui bonifici istantanei

Dal 9 ottobre 2025 è diventata obbligatoria la verifica in tempo reale dell'IBAN e del beneficiario prima di autorizzare un bonifico, proprio per evitare i raggiri. Per quanto riguarda le campagne malevole, in Italia ci sono circa 90-100 campagne fra phishing e malware a settimana.

Dove ci sono più truffe: WhatsApp, Telegram, Marketplace

#1 WhatsApp

A fine luglio 2025 la Consob ha bloccato due app (CapFirst e CapOne) collegate a proposte d'investimento veicolate su WhatsApp con promesse di "fino al 300%". Allo stesso tempo ha chiesto a Google e ad Apple di rimuoverle dagli store e ha

diffuso un'avvertenza sul canale WhatsApp come vettore di proposte abusive. Non è un caso isolato, oggi i raggiri provano a creare un rapporto diretto e rapido via chat.

Tra le tecniche nuove circola anche il trucco del "codice a 8 cifre" legato alla funzione "Dispositivi collegati" di WhatsApp. Non ti chiedono il tuo codice, te ne inviano uno per spingerti a completare un'operazione che di fatto consegna l'account.

#2 Telegram

Ci sono veri e propri gruppi esca, cioè dei canali che convincono la vittima con testimonianze e grafici fasulli prima di indirizzarla su piattaforme di trading o di crypto inesistenti (il cosiddetto pig-butchering). Telegram è una delle piattaforme più usate per questi format. Se ti imbatti in canali che promettono bonus, guadagni sicuri o piattaforme parallele, fermati e incrocia le info. Cerca fonti autorevoli e verifica sempre le recensioni. Telegram è anche un luogo sicuro e affidabile, ma bisogna sapere dove cercare. Anche alcuni casinò online scelgono di appoggiarsi a Telegram per rispettare la privacy dei propri giocatori e per fornire un canale diretto per il login. Se vuoi saperne di più, [scopri i migliori Telegram casino](#) usando siti sicuri e affidabili. Ci sono piattaforme che si occupano di selezionare operatori seri e che ti danno consigli su come trovare quello più adatto alle tue esigenze. Con l'accesso tramite Telegram puoi risparmiare tempo e puoi mantenere l'anonimato se hai bisogno di sentirti più al sicuro.

#3 Marketplace (soprattutto Facebook)

I marketplace sono comodi, ma vari governi e autorità li osservano da vicino perché spesso sono l'anello debole nelle vendite tra privati. Singapore, a settembre 2025, ha ordinato a Meta di rafforzare le misure anti-scam, ha rilevato che Facebook è la piattaforma più sfruttata dai truffatori e Facebook Marketplace è la più debole fra sei piattaforme valutate per gli sforzi anti-truffa.

Phishing PagoPA, manipolazione del pagatore, deepfake

Quali sono le tecniche più usate oggi?

Phishing istituzionale 2.0: Le [campagne italiane che imitano PagoPA](#) mescolano i loghi, i domini molto simili agli originali e i reindirizzamenti legittimi per superare i filtri e per superare i controlli automatici. Un clic porta a delle pagine clone dove inserisci i dati e autorizzi un addebito.

Manipolazione del pagatore: Fa leva sulle urgenze con finti operatori o finti fornitori. Tu autorizzi davvero un bonifico o una ricarica e, proprio perché l'hai autorizzata, il rimborso non è automatico come nelle frodi non autorizzate. Queste frodi sono aumentate, soprattutto sui bonifici e sulle carte.

AI per convincere di più: Oggi vengono anche usati testi e voci generati dall'AI per creare dei messaggi più credibili, in più lingue, e per automatizzare le fasi di adescamento.

Segnali pratici per riconoscere un raggiro

Pressione + scorciatoie: Ti chiedono di fare in fretta e, insieme, ti propongono il canale veloce come un bonifico istantaneo, una ricarica o un link diretto al pagamento.

Promesse fuori scala: "Guadagni garantiti", "rendimenti 300%", "offerta solo oggi" sono numeri e formule che non stanno in piedi nel mondo reale.

Verifica sempre l'IBAN quando paghi un nuovo beneficiario (dal 9 ottobre 2025 le banche ti avvisano se il nome non torna) e ispeziona il link (dominio strano, errori, richieste di credenziali dove non servirebbero).

Chi contattare se qualcosa è andato storto

Se ti accorgi di aver eseguito un pagamento verso un [truffatore](#), ecco cosa devi fare:

Contatta l'istituto di pagamento e segui l'iter previsto per le contestazioni. I presidi PSD2 e le procedure di recall possono aiutare, soprattutto se agisci in tempi strettissimi. I tassi di frode complessivi sono bassi, ma ogni caso va gestito in modo puntuale.

Segnala il phishing e le campagne malevole al CERT-AGID (che monitora l'ecosistema italiano e pubblica gli indicatori di compromissione) o consulta i loro bollettini settimanali per riconoscere i temi del momento.

Presenta denuncia alla Polizia Postale e consulta il portale per le indicazioni operative, e l'autorità che tratta i reati informatici.

Segnala le pratiche commerciali scorrette (per es. pubblicità ingannevoli online) all'AGCM tramite il form ufficiale. Se si tratta di offerte finanziarie abusive, trovi aggiornati anche gli avvisi e i comunicati della Consob.