

WARNING

TIPI DI TRUFFE AI DANNI DEI CITTADINI



(+378) 0549 981011



info@aif.sm



www.aif.sm

INFORMAZIONI

Dall'anno 2023, l'Agenzia di Informazione Finanziaria, nell'ambito delle analisi eseguite, soprattutto a supporto delle investigazioni delle Forze di Polizia, ha rilevato una sempre più frequente diffusione di schemi di truffa ai danni di cittadini/residenti e imprese sammarinesi, che hanno comportato rilevanti perdite finanziarie (stimate in circa 900.000 euro) ai danni delle vittime del raggio.

Gli schemi fraudolenti maggiormente analizzati riguardano casi di:

Investment Fraud



INVESTMENT FRAUD CRYPTO DREAM FRAUD

Truffa sugli investimenti

raggiro in cui finti broker promettono rendimenti elevati e sicuri su investimenti inesistenti, come trading online, criptovalute o azioni, spesso tramite piattaforme fasulle.

Romance Scam

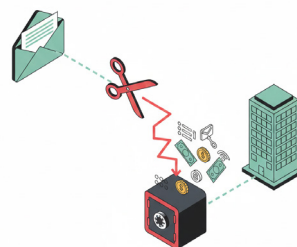


ROMANCE SCAM

Truffa romantica

inganno online in cui truffatori creano false identità su siti di incontri o social media e instaurano finte relazioni affettive allo scopo di estorcere denaro.

Payment Diversion Fraud



PAYMENT DIVERSION FRAUD

Truffa nel dirottamento dei pagamenti

truffa informatica in cui i malfattori si fingono fornitori, partner commerciali o dipendenti senior per indurre un'azienda o un individuo a inviare pagamenti su conti bancari diversi, deviando il denaro in modo illecito.

WARNING

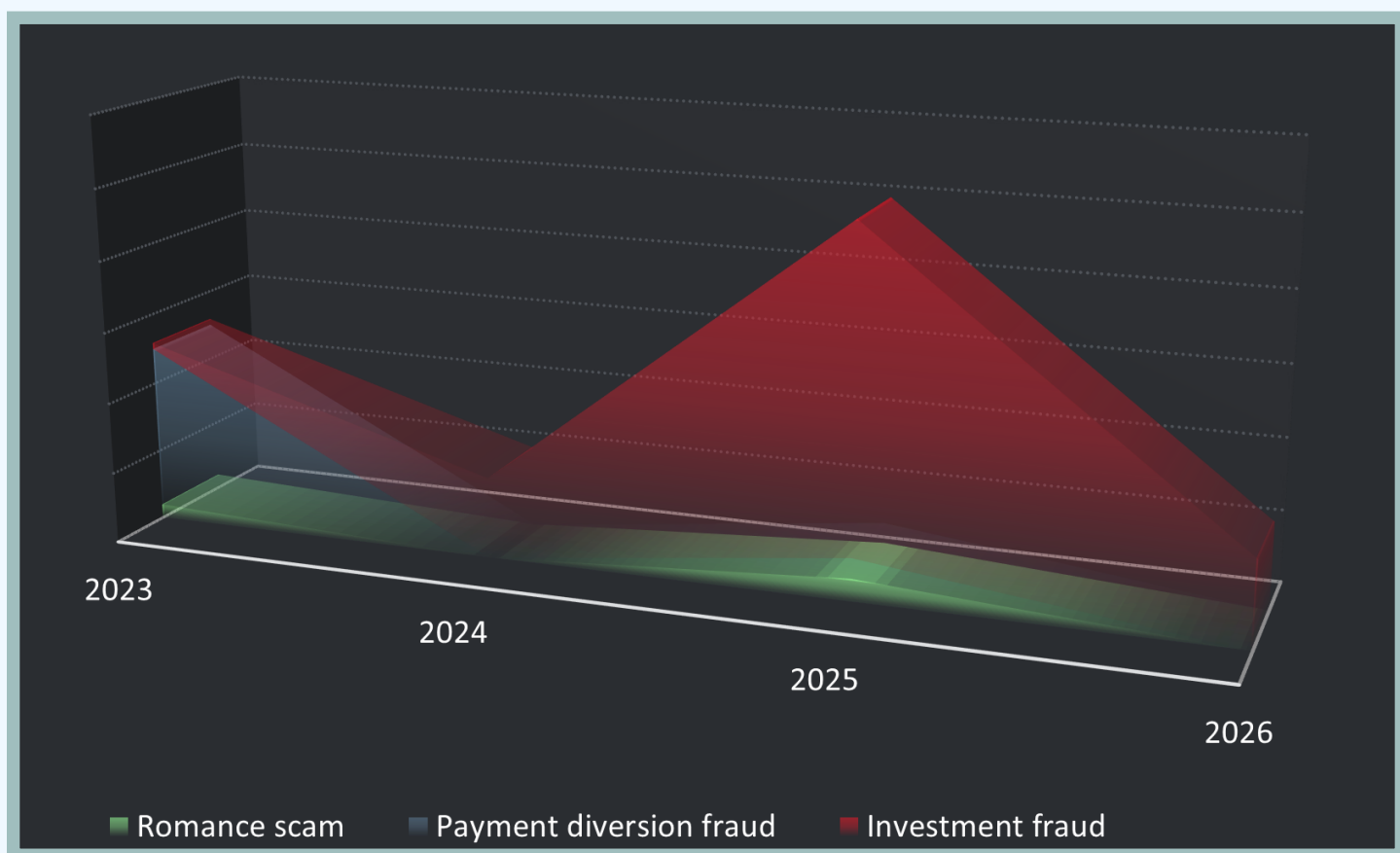
DATI STATISTICI



Impatto finanziario: circa 900.000 euro di cui 600.000 euro sottratti tramite falsi investimenti, cioè la tipologia di truffa più rilevante.

Trend: casi in forte aumento dal 2025 (soprattutto con riferimento a Investment Fraud), senza segnali di flessione nel 2026.

Metodo: Il contatto iniziale può sfruttare il legame emotivo (Romance Scam) come esca per la proposta finanziaria.



WARNING

INVESTMENT FRAUD - CRYPTO DREAM FRAUD



Raggiri nell'ambito di proposte di investimento in criptovalute o in moneta tradizionale, anche mediante l'utilizzo di piattaforme di trading.

Come avviene la truffa

IL PRIMO CONTATTO

L'ESCA

L'EPILOGO

La tipologia operativa qui descritta riguarda raggiri ai danni di persone fisiche contattate telefonicamente (anche da utenze estere, con numerazione diversa da +39) oppure tramite Social Media o mediante attività di passaparola eseguite, in buona fede, da conoscenti/amici/parenti, anch'essi vittime inconsapevoli del raggio.

Di norma, i truffatori si presentano quali promotori finanziari di piattaforme d'investimento o quali rappresentanti/addetti/operatori di società finanziarie estere (con denominazioni riportanti, ad esempio, le parole trading, portfolio/asset management, evocative della gestione/amministrazione finanziaria di fondi); gli stessi si offrono di aiutare la vittima del raggio nell'attività di investimento (sia in criptovalute che in moneta tradizionale) e di recupero degli ingenti guadagni da queste derivanti.

I contatti si fanno via via meno formali, passando a canali di comunicazione criptati (quali WhatsApp e Telegram); i messaggi volti all'avvio dell'attività di trading diventano più pressanti ingenerando nella vittima l'urgenza dell'investimento con la promessa di facili (irreali) guadagni, conseguiti in tempi rapidi, anche intragiornalieri.

L'investimento viene eseguito sulla base di un "rapporto di fiducia", senza la preventiva consegna dei prospetti informativi dell'offerta o con la sottoscrizione di contratti/ordini privi dei dati identificativi della controparte (o comunque con informazioni non adeguatamente dettagliate sull'offerta).

A seguito dell'asserita buona riuscita dell'investimento iniziale di poche centinaia di euro (di norma, inferiore a 500 euro), le vittime del raggio sono persuase a investire ulteriori fondi (di importi singolarmente pari o superiori a 5.000/10.000 euro) e viene richiesto loro di disporre operazioni di "bonifico urgente" a favore o del promotore gli investimenti (a causa di asserite problematiche collegate alla territorialità di San Marino) o a favore di conti esteri (le cui coordinate bancarie iban non iniziano con SM), talvolta (falsamente) indicati come intestati alla vittima della truffa.

Quando la vittima, in luce degli apparenti guadagni conseguiti (indicati come dell'ordine di migliaia di euro), decide di uscire dall'investimento, il promotore – o una figura diversa (talvolta indicata come atta al recupero dei crediti vantati) – chiede il pagamento di commissioni e di tasse per lo sblocco dei fondi; di norma, la vittima è indotta a disporre i citati pagamenti inserendo causali relative alla dazione di prestiti personali e regalie, il tutto al fine di mantenere il massimo riserbo sulla (falsa) attività di recupero delle somme investite.

Investment Fraud



WARNING

ROMANCE FRAUD



Raggiri finanziari nell'ambito di rapporti d'amicizia e sentimentali instaurati online.

Come avviene la truffa

IL PRIMO CONTATTO

L'ESCA

L'EPILOGO

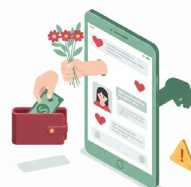
La Tipologia Operativa qui descritta riguarda raggiri ai danni di persone fisiche, di norma persone sole (senza legami sentimentali o con relazioni da poco terminate) contattate tramite Phishing e-mails, Social Media e App di incontri.

I truffatori, facendo leva sul bisogno di affettività delle vittime prescelte, mirano a instaurare con queste un rapporto di fiducia, volto ad ottenere somme di denaro, spesso giustificate con emergenze personali, viaggi o necessità economiche, talvolta riferibili allo sblocco di pacchi (contenenti regalie) alle dogane.

I contatti possono durare mesi, anche utilizzando canali di comunicazione criptati (quali WhatsApp e Telegram), scambiando messaggi personali (da utenze estere, con numerazione diversa da +39) corredati di (false) fotografie.

Una volta consolidato il legame affettivo, le vittime sono indotte ad anticipare fondi per sopperire ad asserite urgenze personali dei truffatori; i medesimi richiedono l'invio di importi variabili (inizialmente dell'ordine di 2.000/3.000 euro fino ad arrivare a 15.000/20.000 euro per singola operazione) – a pagamento di prestiti personali e "codici" di sblocco pacchi – a favore di conti esteri (le cui coordinate bancarie iban non iniziano con SM) indicati come intestati a vari soggetti fisici esteri; in taluni casi, alle vittime viene richiesto l'invio di danaro in contanti tramite il servizio postale.

Romance Scam





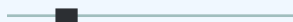
WARNING

PAYMENT DIVERSION FRAUD

Raggiri nell'ambito di pagamenti commerciali verso proprie controparti (fornitori).

Come avviene la truffa

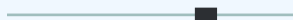
IL PRIMO CONTATTO



L'ESCA



L'EPILOGO

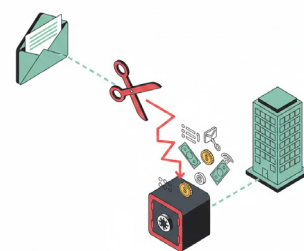


La Tipologia Operativa qui descritta riguarda raggiri ai danni di società e attività intraprese in forma d'impresa, le quali vengono indotte a disporre bonifici, per pagamenti dovuti a propri fornitori, in favore di rapporti di conto diversi da quelli di norma utilizzati.

I truffatori, utilizzando indirizzi e-mail dai domini molto simili o del tutto identici a quelli delle controparti commerciali delle vittime del raggio, richiedono a queste l'invio urgente del pagamento dovuto a proprio favore; il conto destinatario del pagamento risulta, pertanto, "nuovo" rispetto ai conti verso cui sono abitualmente indirizzati i trasferimenti dei fondi.

Il pagamento viene disposto in favore di un conto nelle disponibilità del truffatore e il denaro - se non immediatamente richiamato tramite la propria banca - viene disperso definitivamente tramite prelevamenti di contante o trasferimenti verso una molteplicità di altri rapporti.

Payment Diversion Fraud



WARNING

COSA FARE



Non avere fretta, non condividere informazioni o cliccare sui link; i truffatori creano deliberatamente un senso di urgenza. In caso di dubbi, anche minimi, non agire né investire, ma verificare attentamente la fonte e prestare attenzione a quanto segue.



CAUTELA INVESTIMENTI

Porre particolare attenzione a coloro che propongono investimenti in criptovalute (o in valuta tradizionale) promettendo facili o irrealistici guadagni a mezzo di Social Media e al contenuto e al lessico dei messaggi promozionali (gli stessi potrebbero essere stati generati con strumenti di Intelligenza Artificiale).



VERIFICA INDIPENDENTE

Verificare, in maniera indipendente (anche con ricerche Google) e/o chiedendo l'assistenza di intermediari autorizzati, l'affidabilità del promotore, della società da egli rappresentata e/o della piattaforma di trading.



PROMOTORI NON REGISTRATI

Evitare di avvalersi di promotori finanziari non registrati che utilizzano propri portafogli per acquistare virtual asset per conto di terzi e di pagare a questi soggetti (asserite) commissioni, tasse o altre dazioni di danaro (a titolo di prestito o regalia) utili a rientrare degli investimenti effettuati.



ANALISI PROSPETTI

Richiedere sempre e valutare con attenzione i prospetti informativi delle offerte d'investimento, i contratti sottoscritti e la rispondenza dei destinatari dei fondi alle citate controparti e/o ai termini contrattuali.



CANALI CRIPTATI

Diffidare da coloro che, dopo i primi approcci, passano a canali criptati di comunicazione (quali WhatsApp e Telegram) e che propongono opportunità d'investimento "esclusive" da cogliere con urgenza.



URGENZA / NECESSITÀ

Porre particolare attenzione alle richieste di denaro provenienti da soggetti conosciuti online in riferimento ad una pluralità di sopravvenute emergenze/ necessità.



VERIFICA IBAN

Porre particolare attenzione alle variazioni nelle coordinate bancarie iban delle proprie controparti commerciali, soprattutto quando comunicate via e-mail (possibile Payment Diversion Fraud).



DIVERSO CANALE

Richiedere alla controparte, avvalendosi di un diverso canale di comunicazione, la conferma dell'avvenuta variazione del conto destinatario dei pagamenti (in caso di sospetto di Payment Diversion Fraud).



SEGNALAZIONE AUTORITÀ

Sporgere denuncia alle competenti autorità (in particolare, alle Forze di Polizia) qualora si ritenga di aver subito una truffa.