FRODI E TRUFFE LEGATE ALLE CRIPTO-ATTIVITÀ

RIMANI VIGILE E DIFENDITI

La rapida crescita delle cripto-attività e le loro caratteristiche specifiche (accessibilità globale, velocità, anonimato e spesso irreversibilità delle transazioni) ti rendono un bersaglio privilegiato per i criminali informatici. I truffatori utilizzano tecniche sofisticate per ingannarti, come "schemi Ponzi", false opportunità di investimento, offerte gratuite sui social media e messaggi ingannevoli. Usano anche truffe romantiche legate agli investimenti o indirizzi falsi per compromettere il tuo portafoglio. Spesso ti contattano tramite social media, app di messaggistica, e-mail e chiamate inaspettate che sembrano autentiche. Potresti affrontare rischi come perdite finanziarie, furto di identità e stress emotivo.

Sii prudente e segui questi consigli per restare al sicuro.

Fai attenzione a possibili frodi e truffe legate alle cripto-attività: scopri di più sui diversi tipi di frodi e truffe (guarda le pagine 5, 6, 7 e 8)

Individua i segnali di pericolo: impara a riconoscere comportamenti, messaggi o offerte sospette (guarda pagina 2)

Proteggi te stesso e i tuoi beni: metti al sicuro le informazioni personali (guarda pagina 3)

Scopri cosa fare se diventi vittima di frodi o truffe (guarda pagina 4)

Segnali di pericolo

Una promessa che sembra troppo bella per essere vera.

Un’offerta non richiesta.

Un rendimento garantito, rapido ed elevato.

Urgenza di agire (ad esempio, offerte a tempo limitato che ti spingono ad agire immediatamente).

Una richiesta di pagamento tramite metodi non tracciabili (ad esempio cripto-attività, carte regalo o carte di debito prepagate).

Un invito a cliccare su un link, eseguire la scansione di un codice QR o scaricare un’app.

Una richiesta di inviare o condividere chiavi private e seed phrase (elenco di parole per accedere e recuperare il tuo portafoglio di cripto-attività).

URL sospetto o errato.

Logo leggermente modificato, un sito web che copia quello di un’azienda reale o sembra professionale ma senza contatti verificati, informazioni sulla registrazione dell’azienda, track record o presenza verificabile.

Piattaforma di scambio sconosciuta.

Un allegato sospetto, in particolare .exe, .scr, .zip o documento Office abilitato per le macro (.docm, .xlsm).

Passi per proteggerti

1 Fermati e rifletti prima di agire

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

2 Controlla attentamente la fonte

- Verifica sempre da dove provengono messaggi, chiamate, e-mail e link, anche se sembrano ufficiali, provengono da un amico, un familiare o un personaggio pubblico. Cerca errori di ortografia, URL strani o indicatori di sicurezza mancanti (ad esempio verifica che il link al sito web includa una "s" in "HTTPS" per assicurarti che sia sicuro e controlla eventuali lettere aggiunte o mancanti nel nome dell'azienda).
- Non aprire link da messaggi non richiesti, installa solo applicazioni ufficiali da store affidabili e non eseguire la scansione di codici QR sconosciuti.
- Anche se una proposta sembra ufficiale, confrontala sempre con il sito dell'azienda o verifica che l'account sui social media sia certificato (ad esempio, con il segno di spunta ufficiale).
- Usa contatti verificati per raggiungere direttamente l'azienda o la persona e non fare mai affidamento sulle informazioni fornite dal presunto truffatore (ad esempio, cerca il nome dell'azienda in modo indipendente, utilizzando elenchi aziendali verificati). I truffatori possono fingere di essere autorizzati o imitare il sito web di un'azienda che opera in conformità alla legge. Puoi verificare se l'emittente di cripto-attività o il prestatore di servizi in cripto-attività è autorizzato nell'UE o ha notificato il white paper relativo alla cripto-attività consultando il registro dell'ESMA ( ). Puoi anche visitare il sito web dell'autorità nazionale competente (per verificare se sono stati emessi avvisi o liste nere), oppure l'elenco IOSCO I-SCAN (iosco.org/i-scan/).

3 Non condividere mai password, chiavi private o seed phrase

Chiunque abbia accesso a questi dati può prendere il controllo dei tuoi beni. Le aziende che operano in conformità alla legge non chiederanno mai le tue password o codici di sicurezza via e-mail, SMS o telefono.

4 Mantieni dispositivi e chiavi private sicuri

Usa password robuste e uniche per ciascun account relativo alle cripto-attività, mantienile segrete ed evita di riutilizzare le stesse credenziali su piattaforme diverse (cfr. alcuni suggerimenti sulle password qui). Abilita l'autenticazione a più fattori quando possibile. Mantieni aggiornati e attivi software e protezioni antivirus.

5 Fai attenzione alle offerte di investimento inaspettate

Diffida degli investimenti che promettono rendimenti molto alti. Se sembra troppo bello per essere vero, probabilmente è una trappola.

6 Rifletti prima di condividere informazioni sui social media

Chat di gruppo, forum, post e foto sui social media possono essere fonti preziose di informazioni per i truffatori. Rivelare troppo su di te o sui tuoi investimenti può renderti un obiettivo facile.

Cosa fare quando si è vittima di una frode o truffa

Interrompi immediatamente le transazioni

Blocca i trasferimenti verso conti sospetti ed evita ulteriori perdite. Smetti di avere contatti con i truffatori: ignora le loro chiamate ed e-mail e blocca il mittente.

Cambia le password su tutti i tuoi dispositivi e app/siti web

I truffatori acquistano online le password rubate e le provano su più account. Cambiare una sola password non basta: assicurati di cambiarle tutte, così i truffatori non potranno riutilizzarle.

Disconnetti e revoca gli accessi

Revoca le autorizzazioni sospette presenti nei contratti digitali che operano automaticamente sulla blockchain (smart contract) per impedire ai truffatori di spendere i tuoi token senza consenso. Molti portafogli e blockchain explorer offrono strumenti per vedere quali smart contract hanno accesso ai tuoi token. Per farlo puoi:

- usare un "permission checker" affidabile, che verifica se un utente o un indirizzo blockchain è autorizzato a eseguire un'operazione;
- rivedere l'elenco delle approvazioni, e
- utilizzare il pulsante "revoca" direttamente dalla piattaforma.

Sposta i tuoi fondi

Se il tuo portafoglio è compromesso, trasferisci immediatamente le risorse rimanenti in un nuovo portafoglio sicuro.

Contatta il tuo fornitore di cripto-attività

Informalo il prima possibile tramite canali ufficiali, per esplorare eventuali opzioni. Anche se nella maggior parte dei casi non sarà possibile annullare la transazione sulla blockchain, il fornitore potrebbe bloccare l'account del truffatore (se si trova sulla sua piattaforma) e inserire nella lista nera l'indirizzo del portafoglio.

Segnala e avvisa

Denuncia l'accaduto alla polizia o all'autorità nazionale competente e informa le persone a te vicine (ad esempio amici e familiari) per aumentare la consapevolezza. Queste azioni sono il modo migliore per proteggere te e gli altri.

Attenzione alle frodi di "recupero fondi" (recovery room)

Il truffatore potrebbe contattarti come vittima di una truffa precedente, fingendo di essere un'autorità pubblica (ad esempio polizia, autorità fiscale o finanziaria, ecc.) e offrendo di recuperare i soldi persi dietro il pagamento di una commissione. Questo è spesso un altro tentativo di truffa. Ricorda: il fatto di essere stato truffato una volta non significa che non possa accadere di nuovo.

Cfr. l'avviso congiunto delle autorità europee di vigilanza per saperne di più sui rischi connessi alle cripto-attività ( ) e la scheda informativa "Le cripto-attività spiegate: Che cosa significa il regolamento MiCA per te come consumatore" ( ).

Autorità bancaria europea, Autorità europea delle assicurazioni e delle pensioni aziendali e professionali, Autorità europea degli strumenti finanziari e dei mercati, 2025

Lussemburgo: Ufficio delle pubblicazioni dell'Unione europea, 2025

PDF ISBN 978-92-9407-213-9 doi:10.2853/0858931 DZ-01-25-101-IT-N

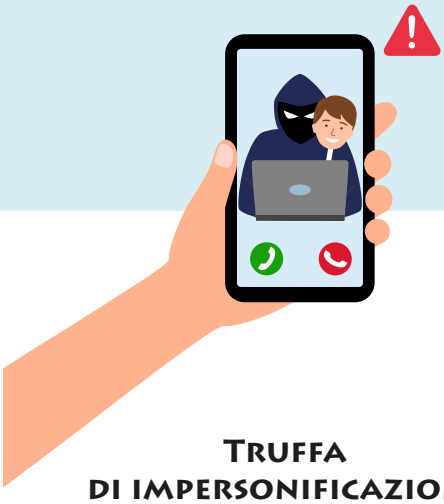
TIPI DI TRUFFE LEGATE ALLE CRIPTO-ATTIVITÀ

Schema "Pump-and-dump" o "rug pull"

Vedi un annuncio sui social media o un sito web che promuove "un'opportunità di investimento a tempo limitato" in cripto-attività, raccomandando di investire in un nuovo token o progetto legato alle cripto-attività. Dopo aver espresso interesse, vieni contattato e indirizzato a una piattaforma di scambio o a un canale di messaggistica (ad esempio Telegram, Viber o WhatsApp). Un contatto apparentemente credibile promette profitti rapidi o rendimenti elevati se investi subito. Sei incoraggiato a investire una piccola somma e poi ti spingono a investire di più.

Cosa potrebbe succedere:

Scopri che il token in cui hai investito è privo di valore e il contatto smette di rispondere. Quando provi a prelevare i tuoi soldi, il sito web non esiste più e l'azienda è irraggiungibile. I truffatori hanno gonfiato artificialmente il valore di una cripto-attività a basso prezzo ("pump") per poi vendere i propri token ("dump"), causando il crollo del valore e lasciando gli investitori con delle perdite. In alternativa, potrebbero chiudere il progetto e scomparire con i fondi ("rug pull").



Truffa di impersonificazione

Dopo aver pubblicato una domanda su una piattaforma di social media o un sito riguardo a un problema con il portafoglio di cripto-attività, ricevi un messaggio diretto (DM) o un'e-mail da qualcuno che finge di essere un contatto affidabile (ad esempio, una piattaforma di scambio, un fornitore di portafogli, un supporto IT o persino un amico). Questa persona ti chiede la tua seed phrase (cioè la sequenza di parole che funge da backup centrale per accedere al tuo portafoglio digitale), password o chiavi private (un codice crittografico generato automaticamente che dimostra la proprietà delle risorse digitali).

Cosa potrebbe succedere:

Una volta condivise seed phrase, password o chiavi private, il truffatore le usa per rubare le tue cripto-attività o altri fondi. Tieni presente che la perdita delle chiavi private comporta la perdita permanente e irreversibile dell'accesso e della proprietà delle tue cripto-attività. A differenza delle transazioni bancarie, nel caso delle cripto-attività, una volta che le attività sono state trasferite, il recupero è quasi impossibile.

Phishing

Ricevi un messaggio inaspettato via e-mail, telefono, pop-up o social media, che sembra provenire da un noto fornitore di cripto-attività. Il messaggio ti invita ad accedere o scaricare una nuova app. Potresti anche ricevere un'e-mail che sembra provenire dall'app del tuo portafoglio di cripto-attività, invitandoti a risolvere un problema di sicurezza cliccando su un link non ufficiale o aggiornando l'app.

Cosa potrebbe succedere:

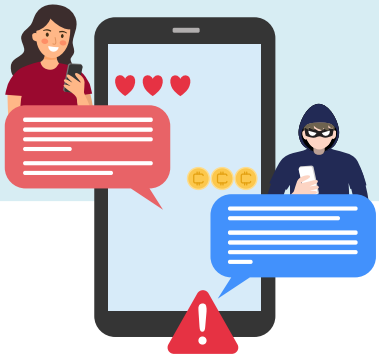
Cliccando sul link, scaricando l'app o scansionando un codice QR, installi un malware che consente al truffatore di accedere alle tue informazioni e rubare cripto-attività o altri tuoi fondi.

Truffa del giveaway

Ti imbatti in un annuncio sui social media che afferma che alcune aziende stanno regalando cripto-attività dopo un piccolo investimento. L'annuncio include un video o un post con foto di celebrità o marchi – di solito falsi o ottenuti senza autorizzazione – che promettono di "raddoppiare le tue cripto-attività" se invii denaro per primo. Logo, layout, testimonianze e linguaggio sembrano professionali e ufficiali, così come il sito a cui si viene reindirizzati.

Cosa potrebbe succedere:

Dopo aver inviato le tue cripto-attività, non ricevi nulla in cambio e hai perso il denaro inviato. Il giveaway era falso e il post o la diretta con celebrità o aziende note era progettata per ingannarti.



Truffa romantica legata agli investimenti

Sei stato contattato su social media, app di incontri o via telefono/SMS da qualcuno che non hai incontrato di persona. Questa persona intrattiene conversazioni frequenti, personali e romantiche, ispirando fiducia con profili falsi. Gradualmente, la conversazione si sposta su opportunità finanziarie, con promesse di grandi profitti da investimenti in cripto-attività e incoraggiandoti a investire con rendimenti elevati e rischi bassi. Ti guida nella creazione di un account e nel versamento di un piccolo importo iniziale per rendere lo schema credibile.

I truffatori creano profili online falsi e utilizzano immagini rubate o generate dall'intelligenza artificiale per avvicinarti.

Cosa potrebbe succedere:

Il truffatore prende più denaro possibile, poi interrompe tutte le comunicazioni e scompare. Il sito o l'app di investimento fraudolento viene disattivato, lasciandoti senza accesso ai presunti investimenti. In alcuni casi, i truffatori usano le informazioni ottenute durante la truffa per colpire amici e familiari o commettere un furto di identità che può avere conseguenze finanziarie o legali per te (ad esempio, il truffatore può verificare i portafogli rubati a tuo nome e potresti essere ritenuto responsabile di debiti o crimini commessi a tuo nome fino a prova contraria).

Schema di Ponzi

Sei invitato a partecipare a un progetto che promette rendimenti elevati e costanti da investimenti in cripto-attività, spesso sostenuti da testimonianze o false storie di successo. Lo schema può essere presentato come un'opportunità di marketing multilivello, in cui si guadagnano premi non solo dal proprio investimento, ma anche reclutando altri. I primi investitori sembrano ricevere pagamenti, incoraggiando più persone a unirsi e promuovere il sistema.

In realtà, non vi è alcuna attività o profitto reale. Il denaro proviene solo dal contributo dei nuovi investitori, usato per pagare i rendimenti agli organizzatori del sistema e ai primi partecipanti.

Cosa potrebbe succedere:

Una volta che i nuovi investimenti rallentano, lo schema crolla e tu, come la maggior parte dei partecipanti, perdi i tuoi soldi. Gli organizzatori scompaiono, lasciandoti senza possibilità di recupero. La struttura multilivello aiuta la truffa a diffondersi rapidamente, poiché le vittime diventano inconsapevolmente promotrici.

Un indirizzo "look-alike" che compromette il tuo portafoglio

Dopo aver effettuato una transazione in cripto-attività, noti un nuovo indirizzo nella cronologia del tuo portafoglio. Questo indirizzo sembra simile a uno con cui hai interagito in precedenza. I truffatori possono far apparire falsi indirizzi nella cronologia delle transazioni inviando al tuo portafoglio una piccola quantità di cripto da un indirizzo simile. Finisci per archiviare nell'attività recente o nei suggerimenti automatici del tuo portafoglio l'indirizzo falso creato dal truffatore. I truffatori creano deliberatamente indirizzi simili cambiando solo pochi caratteri, spesso al centro dell'indirizzo, per evitare di essere scoperti.

Cosa potrebbe succedere:

Quando provi a inviare cripto-attività e copi l'indirizzo errato dalla cronologia del tuo portafoglio, inconsapevolmente invii fondi al portafoglio del truffatore. Poiché queste transazioni sono spesso irreversibili, i tuoi fondi vengono persi in modo permanente nella maggior parte dei casi. Questa truffa si basa sull'inganno visivo e sull'errore dell'utente, sfruttando la distrazione e l'abitudine di copiare e incollare gli indirizzi del portafoglio senza controllarli attentamente.