FRODI E TRUFFE FINANZIARIE ONLINE NELL'ERA DELL'INTELLIGENZA ARTIFICIALE

RIMANI VIGILE E DIFENDITI

Le frodi e le truffe finanziarie online non sono una novità, ma l'intelligenza artificiale (IA) le ha rese più sofisticate e difficili da individuare. I criminali ora usano messaggi e siti web falsi, profili di celebrità contraffatti e persino voci o video generati dall'intelligenza artificiale che imitano il tuo consulente bancario, i tuoi amici o i tuoi familiari per ingannarti.

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 fondamentali per proteggerti.

Fai attenzione alle frodi e alle truffe finanziarie online alimentate dall'IA,
ad esempio impersonificazione, phishing, truffe di investimento e assicurative e persino frodi e truffe romantiche. Scopri di più sui diversi tipi di frodi e truffe (guarda le pagine 5, 6 e 7).

Per le frodi e le truffe specifiche sulle cripto-attività guarda la relativa scheda informativa ( ).

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

Proteggiti:
metti al sicuro le tue 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.

Una chiamata inaspettata da un numero sconosciuto.

Una richiesta urgente di denaro o informazioni personali, anche da parte di qualcuno che finge di essere un familiare, un amico o persino un personaggio pubblico.

Una richiesta di prendere il controllo del tuo dispositivo, scaricare un'app, scansionare un codice QR o fare clic su un link.

Una richiesta di informazioni personali o dati bancari (ad esempio password, numeri di carta di credito, credenziali di home banking o codici di sicurezza).

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

Un indirizzo e-mail o un link sospetto o errato (ad esempio errori di ortografia nell'URL o indirizzi web insoliti).

Un allegato proveniente da una fonte sconosciuta, in particolare .exe, .scr, .zip o documenti Office abilitati per le macro (.docm, .xlsm).

Grammatica o formattazione insufficiente in un documento dall'aspetto ufficiale, anche se l'IA può aiutare i truffatori a mascherare meglio questi difetti.

Un sito web che sembra professionale ma non riporta contatti verificati o informazioni sulla registrazione dell'azienda.

Un'intonazione innaturale, senza pause e troppo fluida o robotica. Presta attenzione alla "clonazione vocale", anche se le voci generate dall'IA possono sembrare molto naturali.

Un video in cui la voce suona robotica o troppo uniforme, i movimenti delle labbra e le espressioni facciali non sono sincronizzati con il parlato oppure sfondi, luci e ombre sono incoerenti. Spesso si tratta di video generati dall'IA (deepfakes).

Passi per proteggerti

1 Non condividere mai informazioni personali o bancarie

Le aziende che operano in conformità alla legge non ti chiederanno mai PIN, password, credenziali di home banking o codici di sicurezza via e-mail, SMS, social media o telefono.

2 Fermati e rifletti prima di agire

Non avere fretta di inviare denaro, condividere informazioni o cliccare su un link: i truffatori creano deliberatamente un senso di urgenza (ad esempio problemi informatici con la tua banca, chiamate di emergenza che coinvolgono amici e familiari, linguaggio minaccioso ecc.). In caso di dubbi, anche minimi, non agire: termina la chiamata e verifica attentamente la fonte o l'identità.

3 Controlla attentamente la fonte/identità

- Verifica sempre da dove provengono messaggi, chiamate, e-mail e link, anche se sembrano ufficiali o provenire da un amico, un familiare o un personaggio pubblico. Chiama o invia messaggi alla tua famiglia e ai tuoi amici utilizzando un numero noto tramite un canale sicuro; cerca errori di ortografia, URL strani o indicatori di sicurezza mancanti (ad esempio verifica che il collegamento al sito web includa una "s" in "HTTPS" per assicurarti che sia sicuro e verifica eventuali lettere aggiunte o mancanti nel nome dell'azienda).

- Non aprire link da messaggi non richiesti, installa solo applicazioni ufficiali dagli store affidabili e non scansionare codici QR sconosciuti.

- Concorda con la tua famiglia una "parola sicura": una frase segreta da usare per confermare l'identità se qualcuno con una voce familiare ti chiama con una richiesta urgente di denaro e sostiene di essere un parente (ad esempio genitori, sorella/fratello, figli).

- 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, usa elenchi ufficiali e metodi di contatto già confermati). I truffatori possono fingere di essere autorizzati o imitare il sito web di un'azienda che opera in conformità alla legge. Verifica se eventuali avvertenze sono state emesse dall'autorità finanziaria nazionale o incluse nell'elenco IOSCO I-SCAN (iosco.org/i-scan/). Per gli emittenti di cripto-attività o i prestatori di servizi in cripto-attività, controlla se sono autorizzati nell'UE o se hanno pubblicato il relativo white paper (ad esempio, consulta il registro dell'ESMA:).

4 Fai attenzione ai possibili inganni basati sull'IA

Con l'avanzare della tecnologia, le truffe diventano sempre più convincenti, nonostante le migliori misure di sicurezza. Se qualcosa ti sembra insolito o noti uno dei segnali di allarme indicati sopra, fermati e rifletti.

5 Non installare software di accesso remoto né condividere lo schermo

Banche e intermediari finanziari non lo richiederanno mai.

6 Mantieni dispositivi e account sicuri

Usa password robuste e uniche, mantienile segrete ed evita di riutilizzare le stesse credenziali su piattaforme diverse. Abilita l'autenticazione a più fattori quando possibile. Trovi alcuni consigli sulle password qui ( ). Mantieni aggiornati e attivi software e protezioni antivirus.

7 Sii prudente con le opportunità di investimento inaspettate e a tempo limitato

Se sembra troppo bello per essere vero, probabilmente è una trappola.

8 Rifletti prima di condividere informazioni sui social media

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

Cosa fare quando si è vittima di una frode o una 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.

Contatta la tua banca o intermediario finanziario

Informa immediatamente la tua banca o intermediario finanziario tramite i canali ufficiali, per valutare le opzioni di blocco o annullamento delle transazioni.

Cambia le password su tutti i 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.

Segnala e avvisa

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

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

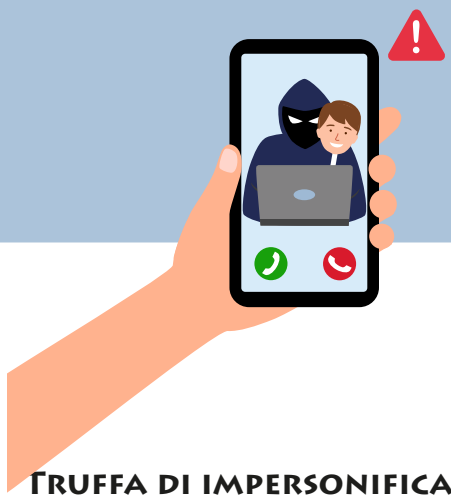
Il truffatore potrebbe contattarti sapendo che sei stato vittima di una truffa precedente, fingendo di essere un'autorità pubblica (ad esempio, polizia, autorità fiscale o finanziaria, ecc.) e offrendo di recuperare i soldi persi dietro pagamento di una commissione. Spesso si tratta di un altro tentativo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

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 978-92-9407-263-4 doi:10.2853/5386132 DZ-01-25-151-IT-N

TIPI DI FRODI E TRUFFE FINANZIARIE ONLINE POTENZIATE DALL'IA



Truffa di impersonificazione e uso di deepfake

Ricevi una chiamata inaspettata da qualcuno che sostiene di essere la tua banca, un'autorità pubblica (ad esempio polizia, autorità fiscale o finanziaria, ecc.), una compagnia di assicurazioni, una società IT o persino un familiare. Il chiamante potrebbe sollecitarti a trasferire fondi per metterli al sicuro, riferendo di attività sospette sul tuo conto o sulla tua polizza assicurativa. Potrebbero anche chiederti di fornire i tuoi dati bancari (ad esempio numero di carta di pagamento, credenziali di home banking o password), cliccare su un link o installare un software, fingendo che possa risolvere rapidamente il problema. Il chiamante potrebbe utilizzare un numero falsificato, che spesso corrisponde al numero di telefono della banca per sembrare legittimo (spoofing).

I truffatori utilizzano l'IA per creare video, immagini o audio falsi che imitano la voce (ad esempio il consulente bancario o un familiare), il volto (ad esempio una celebrità) o i movimenti di qualcuno. **Questo fenomeno è noto come "deepfake".**

Cosa potrebbe succedere:

Menzionando dettagli personali e creando un senso di urgenza, il truffatore ti induce a compiere azioni non volute, come inviare denaro, fare clic su un link malevolo o installare un malware sul tuo dispositivo. Questo può dare al truffatore accesso diretto alle tue credenziali bancarie, permettendogli di cambiare password, accedere al conto bancario e rubare denaro. Ricorda: il fatto che il chiamante conosca i tuoi dati personali non significa che sia affidabile.

Phishing e ingegneria sociale

Ricevi un'e-mail o un messaggio che sembra provenire dalla tua banca o da un intermediario finanziario, avvisandoti di "attività sospette" sul tuo conto. Il logo, il layout e il linguaggio sembrano professionali e il messaggio potrebbe apparire nella stessa chat di altre conversazioni con la banca. Ti viene chiesto di cliccare su un link per verificare il tuo conto o reimpostare la password. Il link porta a un sito web falso identico al tuo home banking. Senza accorgertene, inserisci i tuoi dati in un sito progettato per rubare le tue informazioni personali.

I truffatori utilizzano l'IA per creare messaggi di phishing convincenti analizzando i dati dei social media per identificare le loro vittime e adattare il contenuto a ciascun obiettivo.

Cosa potrebbe succedere:

Il truffatore accede al tuo conto bancario e ruba denaro o crea un profilo falso con i tuoi dati personali per commettere frodi.

Truffa su investimenti o assicurazioni

Vedi un annuncio sui social media o su un sito web che promuove "un'opportunità di investimento a tempo limitato con rischi bassi" o uno "sconto a tempo limitato" su un'assicurazione di una nota compagnia. L'annuncio mostra la foto di una celebrità e raccomandazioni spesso false. Dopo aver cliccato sul link o compilato un modulo, vieni contattato e indirizzato a una piattaforma o canale di messaggistica dove ricevi consigli e documenti dall'aspetto professionale. Sei incoraggiato a investire una piccola somma, seguita da somme maggiori, o a pagare il premio su un conto apparentemente sicuro.

I truffatori utilizzano strumenti di IA per rendere queste proposte o e-mail molto convincenti e difficili da individuare. Usano anche bot sui social media basati sull'intelligenza artificiale per creare account falsi che interagiscono con te, diffondono disinformazione e simulano comportamenti reali per guadagnare fiducia e influenzare le tue decisioni.

Cosa potrebbe succedere:

Dopo aver provato a prelevare i tuoi soldi o fare un reclamo, il contatto smette di rispondere. Scopri che l'azienda non esiste o che il rischio contro cui ti sei assicurato non è coperto. Quindi ti rendi conto di aver inviato denaro direttamente a un truffatore come parte di uno schema fraudolento. Sfortunatamente, non puoi recuperare i tuoi soldi e i tuoi dati personali e finanziari possono essere utilizzati per commettere ulteriori frodi (ad esempio firmare contratti per tuo conto che potrebbero causarti ulteriori perdite).

Frodi e truffe romantiche

Sei stato contattato sui social media, app di incontri o via telefono/SMS da qualcuno che non hai mai incontrato di persona. Questa persona intrattiene conversazioni frequenti, personali e romantiche, ispirando fiducia con profili falsi. Nel corso del tempo, la conversazione si sposta verso denaro o opportunità finanziarie, come investimenti in cripto-attività con promesse di alti rendimenti e bassi rischi. La persona ti chiede di trasferire denaro o ti guida nella creazione di un conto e nel versamento di un piccolo importo iniziale per rendere lo schema credibile, prima di spingerti a investire di più.

I truffatori utilizzano l'IA per generare profili falsi, identificare le loro vittime sui social media/app di incontri usando i dati che hai reso disponibili, o chatbot per generare messaggi.

Cosa potrebbe succedere:

Il truffatore prende più denaro possibile, poi interrompe tutte le comunicazioni e scompare. Il sito web o l'app di investimento fraudolento vengono disattivati, rendendo impossibile l'accesso ai presunti investimenti. Oltre alla perdita economica, le informazioni personali condivise potrebbero essere utilizzate per colpire amici e familiari o per il furto di identità che può avere conseguenze finanziarie o legali (ad esempio, il truffatore potrebbe effettuare acquisti, prendere prestiti o commettere crimini a tuo nome).

Truffa sugli acquisti

Trovi un'offerta allettante su un marketplace online. La società che propone l'offerta richiede un pagamento al di fuori della piattaforma ufficiale, sostenendo di usare un "sistema di pagamento sicuro", e ti invia un link per completare l'acquisto. Il link ti reindirizza a una pagina fraudolenta di autenticazione bancaria che imita il sito ufficiale della banca con il suo logo e il suo design, inducendoti a inserire i tuoi dati bancari per effettuare il pagamento.

I truffatori utilizzano l'IA per creare siti bancari falsi, conferme di ordini e fatture convincenti, imitando tono, branding e stile delle aziende reali. In alcuni casi, usano chatbot IA per rispondere alle domande e rendere l'offerta più credibile.

Cosa potrebbe succedere:

Il pagamento tramite un collegamento esterno aggira le protezioni del marketplace. Il truffatore ottiene le tue credenziali bancarie e accede al tuo conto.