TRUFFA DELL'AMMINISTRATORE DELEGATO, PRESIDENTE O CAPO DI AZIENDA

La truffa del CEO si verifica quando un Dirigente e/o un dipendente autorizzato ad effettuare pagamenti viene indotto a pagare una fattura falsa oppure ad effettuare un trasferimento non autorizzato dall'account aziendale.

COME FUNZIONA?

Un frodatore chiama o invia un'email in qualità di figura di alto livello all'interno dell'azienda.

Hanno una buona conoscenza dell'organizzazione.

Richiedono un pagamento urgente.

Utilizzano espressioni come: 'Riservatezza', 'La società si fida di te', 'Non sono al momento disponibile'.

Fanno riferimento ad una situazione delicata (ad es. un controllo fiscale, una fusione, un'acquisizione).

Spesso, la richiesta è per pagamenti internazionali a banche al di fuori dell'Europa.

Il dipendente trasferisce i fondi su un conto controllato dal truffatore.

Le istruzioni su come procedere possono essere fornite in seguito, da una terza persona o via email.

Il dipendente è invitato a non seguire le regolari procedure di autorizzazione.

QUALI SONO I SEGNALI?

- Email/telefonata indesiderata
- Contatto diretto da un alto funzionario con il quale non si è normalmente in contatto
- Richiesta di riservatezza assoluta
- Pressione e senso di urgenza
- Richiesta insolita in contrasto con le procedure interne
- Minacce o adulazioni inusuali/promesse di ricompensa

COSA PUOI FARE?

COME AZIENDA

Sii consapevole dei rischi e assicurati che anche **i tuoi dipendenti siano informati**.

Invita il tuo staff **a trattare le richieste di pagamento con cautela.**

Implementa protocolli interni relativi ai pagamenti.

Implementa una procedura per verificare la legittimità delle richieste di pagamento ricevute via **email.**

Stabilisci un **processo di segnalazione** per la gestione delle frodi.

Rivedi le informazioni pubblicate sul sito web della tua azienda, **limita le informazioni e sii prudente** sui social media.

Incrementa e aggiorna la sicurezza tecnologica.

Contatta sempre la polizia in caso di tentativi di frode, anche se non sei rimasto vittima della truffa.

COME IMPIEGATO

Applica rigorosamente le procedure di sicurezza in vigore per i pagamenti e le forniture. **Non saltare alcun passaggio e non cedere alla pressione.**

Controlla sempre attentamente gli indirizzi email quando si tratta di informazioni sensibili/trasferimenti di denaro.

In caso di dubbio su un ordine di trasferimento, **consulta un collega competente.**

Non aprire mai link sospetti o allegati ricevuti tramite email. Presta particolare attenzione quando controlli la tua email privata sui computer aziendali.

Limita le informazioni e sii prudente sui social media.

Evita di condividere informazioni sulla struttura interna, sulla sicurezza o sulle procedure **dell'azienda.**

Se ricevi un'email o una chiamata sospetta, informa sempre il tuo dipartimento IT.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

TRUFFE DI INVESTIMENTO

I truffatori ti propongono opportunità molto redditizie di guadagno anche in tempi brevi, con investimenti di somme (anche di grossa entità) che generalmente finiscono su conti esteri. Le proposte possono riguardare azioni, obbligazioni, criptovalute, metalli rari, investimenti immobiliari, energie alternative, etc.

QUALI SONO I SEGNALI?

- Ti vengono promessi rendimenti rapidi e ti viene assicurato che l'investimento è sicuro.
- L'offerta è disponibile solo per un tempo limitato.
- Ricevi ripetutamente una telefonata indesiderata.
- L'offerta è disponibile solo per te e ti viene chiesto di non condividerla.

COSA PUOI FARE?

- **Assicurati sempre una consulenza finanziaria imparziale** prima di consegnare denaro o fare un investimento.
- **Rifiuta le vendite telefoniche** relative a tali opportunità.
- **Diffida** delle offerte che promettono un investimento sicuro, rendimenti garantiti e grandi profitti.
- Fai sempre una ricerca online, sul sito e/o sulla società che ti sta offrendo gli investimenti, controlla le opinioni e verifica le eventuali esperienze di altre persone.
- **Attenzione alle truffe future.** Se hai già investito in una truffa, è probabile che i truffatori ti prendano di mira nuovamente o vendano i tuoi dati ad altri criminali.
- **Contatta la polizia** se sospetti qualcosa.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

TRUFFA DELLA FATTURA (SOSTITUZIONE E FALSIFICAZIONE)

COME FUNZIONA?

- Un'azienda viene avvicinata da qualcuno che finge di rappresentare un fornitore/un prestatore di servizi/ un creditore.
- Possono essere utilizzati vari approcci in combinazione tra loro: telefono, lettera, email, etc.
- Il truffatori possono anche intromettersi nello scambio di email fra due aziende (o anche fra un privato ed un'azienda) e dirottando i pagamenti verso IBAN gestiti da loro.
- Il truffatore richiede che vengano modificate le coordinate bancarie per il pagamento delle fatture future (ad esempio i dettagli del beneficiario del conto bancario). Il nuovo account suggerito è controllato dal truffatore.

COSA PUOI FARE?

COME AZIENDA

Assicurati che i dipendenti siano **consapevoli ed informati su questo tipo di frode** e su come evitarla.

Istruisci il personale responsabile del pagamento delle fatture **per verificare sempre eventuali irregolarità**.

Implementa una **procedura per verificare la legittimità** delle richieste di pagamento.

Rivedi le informazioni pubblicate sul sito web della tua azienda, in particolare contratti e fornitori. Assicurati che il tuo personale limiti ciò che condivide sulla società attraverso i propri social media.

COME IMPIEGATO

Verifica tutte le richieste che sostengono di provenire dai tuoi creditori, soprattutto se ti chiedono di modificare i loro dati bancari per le fatture future.

Per i pagamenti superiori ad una determinata soglia, **imposta una procedura per confermare** il conto bancario e il destinatario corretti (ad esempio un incontro con la società).

Non utilizzare i dettagli di contatto indicati sulla lettera/ fax/email che richiede la modifica. Utilizza invece quelli della **corrispondenza precedente**.

Quando paghi una fattura, **invia un'email per informare il destinatario**. Includi il nome della banca del beneficiario e le ultime quattro cifre dell'account designato, impostato per garantire la sicurezza.

Definisci **appositi Singoli Punti di Contatto** con le società verso cui effettui pagamenti regolari.

Limita le informazioni relative al tuo datore di lavoro che condividi sui social media

Contatta sempre la polizia in caso di tentativi di frode, anche se non sei rimasto vittima della truffa.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

TRUFFE SUGLI ACQUISTI ONLINE

Gli acquisti online rappresentano spesso un buon affare, ma devi stare attento alle truffe.

COSA PUOI FARE?

- Quando possibile, **utilizza i siti di vendita nazionali** – sarà più facile risolvere eventuali problemi.
- **Fai le tue ricerche** – controlla le recensioni prima di acquistare.
- **Usa la carta di credito** – hai più possibilità di riavere i tuoi soldi indietro.

- **Paga solo attraverso servizi di pagamento sicuri** – Ti richiedono un servizio di trasferimento di denaro o un bonifico bancario? Pensaci due volte!
- **Paga solo attraverso una connessione Internet sicura** – evita di utilizzare il wifi pubblico gratuito o aperto.
- **Paga solo attraverso un dispositivo sicuro** – Tieni aggiornati il sistema operativo e il software di sicurezza.
- Attenzione agli annunci di affari spropositati o prodotti miracolosi – **Se ti sembra troppo bello per essere vero, probabilmente lo è!**
- Un annuncio pop-up dice che hai vinto un premio? **Pensaci due volte,** l'unica cosa che potresti aver vinto potrebbe essere un malware.
- Se il prodotto non arriva, contatta il venditore. Se non ricevi nessuna risposta, **contatta la tua banca.**

Segnala sempre alla polizia qualsiasi tentativo sospetto di frode, anche se non sei caduto vittima della truffa.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

EMAIL DI PHISHING BANCARIO

Il phishing si riferisce a email fraudolente che ingannano i destinatari nella condivisione delle proprie informazioni personali, finanziarie o di sicurezza.

COME FUNZIONA?

Queste email:

possono sembrare identiche ai tipi di corrispondenza che le vere banche inviano.

replicano i loghi, il layout e il tono delle vere email.

chiedono di scaricare un documento in allegato o fare clic su un link.

usano un linguaggio che trasmette senso di urgenza.

COSA PUOI FARE?

- **Tieni il tuo software aggiornato,** inclusi browser, antivirus e sistema operativo.
- Presta particolare **attenzione** se un'email 'bancaria' ti richiede informazioni sensibili (ad esempio, la password del tuo conto bancario online).
- **Studia l'email**: confronta l'indirizzo del mittente con le altre email ricevute dalla tua banca. Controlla grammatica e ortografia.
- **Non rispondere ad un'email sospetta,** ma inoltrala alla tua banca digitando tu stesso l'indirizzo.
- **Non cliccare sul link o non scaricare l'allegato,** ma digita l'indirizzo nel tuo browser.
- In caso di dubbio, **ricontrolla** il sito web della tua banca o telefona alla banca.

I criminali informatici fanno affidamento sul fatto che le persone sono indaffarate; a colpo d'occhio, queste email contraffatte sembrano autentiche.

#CyberScams

Fai attenzione quando usi un dispositivo mobile. Potrebbe essere più difficile individuare un tentativo di phishing dal tuo telefono o tablet.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | CERTFin CERT Finanziario Italiano | INTESA SANPAOLO

TRUFFA SENTIMENTALE

I truffatori prendono di mira le vittime sui siti di incontri online, ma possono utilizzare anche i social media o le email per prendere contatto.

QUALI SONO I SEGNALI?

Qualcuno che hai recentemente incontrato online dichiara di provare forti sentimenti per te, e ti chiede di chattare in privato.

I loro messaggi sono spesso vaghi e scritti male.

Il loro profilo online non è coerente con ciò che raccontano.

Potrebbero chiederti di inviare foto o video personali.

Prima ottengono la tua fiducia. Poi ti chiedono denaro, regali oppure i dettagli della tua carta di credito/del tuo conto bancario.

Se non invii il denaro, possono provare a ricattarti. Se lo invii, te ne chiederanno di più.

SEI UNA VITTIMA?

Non sentirti in imbarazzo!

Interrompi tutti i contatti immediatamente.

Se possibile, conserva tutte le comunicazioni, come i messaggi delle chat.

Presenta una denuncia alla polizia.

Segnalalo al sito attraverso il quale il truffatore ti ha contattato per la prima volta.

Se hai fornito i dettagli del tuo conto, contatta la tua banca.

COSA PUOI FARE?

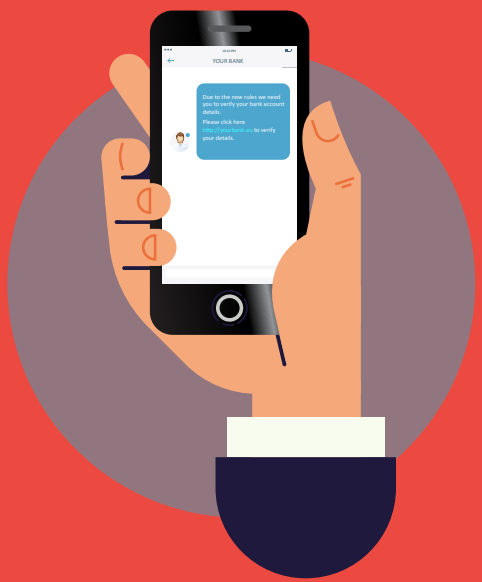
- **Fai molta attenzione** alle informazioni personali che condividi sui social network e sui siti di appuntamenti.
- **Considera sempre i rischi.** I truffatori sono presenti sui siti più affidabili.
- **Sii cauto** e fai delle domande.
- **Fai ricerche** sulla foto e sul profilo della persona per vedere se il materiale è stato usato altrove.
- **Fai attenzione** ad errori di ortografia e grammatica, ad incongruenze nelle loro storie e a scuse quali la fotocamera che non funziona.
- **Non condividere** materiale compromettente che possa essere usato per ricattarti.
- Se accetti un incontro di persona, **informa parenti e amici** su dove stai andando.
- **Attenzione alle richieste di denaro.** Non inviare mai denaro oppure i dettagli della carta di credito, del tuo account online o copie di documenti personali.
- **Evita di inviare pagamenti anticipati.**
- **Non trasferire denaro** per conto di qualcun altro: il riciclaggio di denaro è un reato penale.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO

#CyberScams

SMS DI PHISHING BANCARIO

Lo smishing (dalla combinazione delle parole SMS e Phishing) è il tentativo da parte dei truffatori di acquisire informazioni personali, finanziarie o di sicurezza tramite SMS.



COME FUNZIONA?

L'SMS ti chiederà in genere di fare clic su un link o di chiamare un numero di telefono per 'verificare', 'aggiornare' o 'riattivare' il tuo account. Ma... il link porta ad un sito web fasullo e il numero di telefono porta ad un truffatore che finge di essere la società legittima.

COSA PUOI FARE?

- **Non cliccare su link, allegati o immagini** che ricevi da SMS indesiderati, senza prima verificare il mittente.
- **Non essere frettoloso**. Prenditi il tuo tempo e fai dei controlli appropriati prima di rispondere.
- **Non rispondere mai ad un SMS** che richiede il tuo PIN o la password del tuo conto online o qualsiasi altra credenziale di sicurezza.
- Se pensi che potresti aver risposto ad un testo smishing fornendo i tuoi dati bancari, **contatta immediatamente la tua banca**.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

SITI WEB BANCARI CONTRAFFATTI

Le email di phishing bancario di solito includono link che ti condurranno ad un sito web bancario contraffatto, dove ti sarà richiesto di divulgare le tue informazioni finanziarie e personali.

QUALI SONO I SEGNALI?

I siti web bancari contraffatti sembrano quasi identici ai siti ufficiali delle banche. Questi siti spesso dispongono di una finestra popup che ti chiede di inserire le tue credenziali bancarie. Le vere banche non usano tali finestre.

Questi siti di solito presentano:

Urgente: non troverai mai tali messaggi sui veri siti web.

Finestre pop-up: sono comunemente utilizzate per raccogliere informazioni sensibili. Non cliccarci sopra ed evita di inserire dati personali su tali finestre.

Design scadente: sii cauto con i siti web che presentano difetti di design o errori di ortografia e grammatica.

COSA PUOI FARE?

Non cliccare mai sui link all'interno delle email che conducono al sito web della tua banca.

Digita sempre il link manualmente o utilizza un collegamento esistente dal tuo elenco dei 'preferiti'.

Utilizza un browser che consente di **bloccare le finestre popup.**

Se qualcosa di importante richiede davvero la tua attenzione, sarai avvisato dalla tua banca **quando accederai al tuo account online.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO · #CyberScams

TELEFONATE DI VISHING BANCARIO

Il Vishing (dalla combinazione delle parole Voice e Phishing) è una truffa telefonica in cui i truffatori cercano di indurre la vittima a divulgare informazioni personali, finanziarie o di sicurezza o a trasferire loro del denaro.

COSA PUOI FARE?

- **Fai attenzione** alle chiamate telefoniche indesiderate.
- **Segnati il numero del chiamante** e avvisalo che lo richiamerai.
- Per verificare la loro identità, **cerca il numero di telefono dell'organizzazione** e contattali direttamente.
- **Non dare credito al truffatore utilizzando il numero di telefono che ti ha fornito** (potrebbe trattarsi di un numero falso o contraffatto).
- I truffatori possono trovare le tue informazioni di base online (ad es. attraverso i social media). **Non presumere che chi chiama sia autentico** solo perché possiede questi dati.
- **Non condividere** il numero PIN della tua carta di credito o di debito oppure la password del tuo online banking. La tua banca non ti chiederà mai tali dettagli.
- **Non trasferire denaro** su un altro account a richiesta. La tua banca non ti chiederà mai di farlo.
- Se pensi che sia una finta chiamata, **segnalalo alla tua banca**.

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · CERTFin CERT Finanziario Italiano · INTESA SANPAOLO

#CyberScams