TRUFFA DEL CEO/COMPROMISSIONE DELLA MAIL AZIENDALE

La truffa del CEO si verifica quando 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 (ad esempio come CEO o CFO).

Hanno una buona conoscenza dell'organizzazione.

Richiedono un pagamento urgente.

Utilizzano espressioni come ad esempio: '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 e consapevoli.**

Incentiva 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