Phishing
AI POWERED PROTECTION

THREAT AWARENESS

CEO Fraud e Whaling: quando l'attacco punta al vertice aziendale

I criminali impersonano dirigenti per sottrarre fondi e dati riservati: come difendersi

A cura del team CENANT di GPI Cyberdefence

30 marzo 2026 www.gpiphishing.com

THREAT AWARENESS

I criminali impersonano dirigenti per sottrarre fondi e dati riservati: come difendersi

01 I “grandi pesci” sono i bersagli più redditizi

Nel vocabolario del social engineering, “whaling” indica gli attacchi mirati ai vertici aziendali: CEO, CFO, direttori HR, responsabili finanziari. La metafora è esplicita — mentre il phishing comune lancia una rete su migliaia di bersagli, il whaling mira a un singolo “pesce grosso” con un attacco altamente personalizzato.

La posta in gioco è proporzionalmente più alta: i dirigenti hanno accesso a dati sensibili, a sistemi critici e, soprattutto, possono autorizzare transazioni finanziarie di importo elevato senza necessità di ulteriori approvazioni.

02 Come funziona la CEO Fraud

Lo schema più comune prevede che un collaboratore in area amministrativa o finanziaria riceva un'e-mail apparentemente inviata dal CEO o da un altro dirigente di vertice. Il messaggio chiede di effettuare un bonifico urgente a un nuovo fornitore estero, invocando massima discrezione e rapidità.

Il mittente ha un aspetto credibile perché l'attaccante ha raccolto in precedenza informazioni sull'organizzazione: struttura, nomi, progetti in corso, stile comunicativo del dirigente impersonato. Spesso l'attacco viene eseguito in momenti in cui il vero CEO è irreperibile: in viaggio, in riunione, fuori orario.

RIFERIMENTI

1 Proofpoint, Voice of the CISO, Report annuale (2024).
2 Twitter Hack 2020, FBI Report.

03 Un caso reale: Twitter, 2020

Nel luglio 2020, Twitter ha subito uno degli attacchi di social engineering più clamorosi della storia recente. Attraverso una campagna di vishing (voice phishing) mirata ai dipendenti, gli hacker hanno convinto alcuni collaboratori a fornire credenziali di accesso a una piattaforma interna. Una volta dentro, hanno compromesso gli account di Barack Obama, Elon Musk, Apple e Jeff Bezos per promuovere una truffa in criptovalute.[2]

L'attacco non ha richiesto vulnerabilità tecniche: ha richiesto solo fiducia mal riposta.

> *Il 72% dei CISO italiani ha identificato l'errore umano come la principale vulnerabilità informatica nelle loro organizzazioni (Proofpoint, Voice of the CISO 2024).*

04 Come proteggere l'organizzazione

Procedure di verifica obbligatorie. Qualsiasi richiesta di bonifico, cambio di coordinate bancarie o accesso a dati riservati deve essere verificata attraverso un secondo canale indipendente, una telefonata diretta, non una risposta all'e-mail stessa.

Doppia autorizzazione per operazioni critiche. Nessuna transazione significativa dovrebbe poter essere autorizzata da un'unica persona, indipendentemente dal suo ruolo.

Formazione specifica per il top management. I dirigenti sono bersagli privilegiati e devono essere formati con simulazioni di attacco realistiche, non solo i dipendenti operativi.

RIFERIMENTI

1 Proofpoint, Voice of the CISO, Report annuale (2024).
2 Twitter Hack 2020, FBI Report.

GPI PHISHING — CYBERSECURITY PLATFORM

Proteggi il vertice aziendale dalla CEO Fraud e dal Whaling

Simulazioni mirate, verifica delle procedure finanziarie e formazione per il top management.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com