Phishing
AI POWERED PROTECTION

THREAT AWARENESS

Social Engineering: quando il nemico sfrutta la psicologia, non il codice

Dalle leve emotive al 'cervello rettiliano': perché l'inganno funziona anche sulle persone più preparate

A cura del team CENANT di GPI Cyberdefence

5 gennaio 2026 www.gpiphishing.com

THREAT AWARENESS

Dalle leve emotive al 'cervello rettiliano': perché l'inganno funziona anche sulle persone più preparate

01 Non è un problema tecnico

Il social engineering è una tecnica che sfrutta le debolezze umane per ottenere accesso non autorizzato a informazioni, sistemi o spazi fisici. Diversamente dagli attacchi puramente tecnici, il sociale engineering, non richiede vulnerabilità software, richiede solo un essere umano.

È proprio per questo che è così efficace e così difficile da contrastare con la sola tecnologia. L'attaccante non cerca un bug nel codice: cerca un momento di distrazione, una situazione di stress, un impulso alla cortesia o all'obbedienza.

02 Come funziona il cervello sotto attacco

La neuropsicologia ci offre una spiegazione chiara. In situazioni di stress o urgenza percepita, il nostro cervello attiva strutture evolutivamente antiche, l'amigdala e il sistema limbico, che mettono in secondo piano la corteccia prefrontale, sede del pensiero razionale. È la risposta 'lotta o fuga': istantanea, efficace per i predatori della savana, ma controproducente di fronte a un'e-mail che minaccia la sospensione dell'account.

Gli attaccanti sfruttano esattamente questo meccanismo. Un messaggio che comunica urgenza (“Il tuo account verrà disattivato entro 24 ore”), paura (“Abbiamo rilevato accessi sospetti”) o autorità (“Il CEO richiede un bonifico immediato”) bypassa il ragionamento critico e spinge all'azione impulsiva.

03 Le sei leve psicologiche più usate

> *Il social engineering non scarica un virus: scarica la fiducia. Il rimedio non è solo tecnologico, è educativo.*

03.1
Autorità
un messaggio che sembra provenire da un dirigente, da un ente governativo o da un fornitore fidato viene accettato con meno resistenza;

03.2
Urgenza
scadenze artificiali riducono il tempo disponibile per verificare e riflettere;

03.3
Paura e incertezza
minacce di conseguenze negative spingono ad agire senza analizzare;

03.4
Reciprocità
sfruttare la naturale tendenza umana a ricambiare un favore o una gentilezza;

03.5
Scarsità
la sensazione di stare per perdere un'opportunità irripetibile genera decisioni affrettate;

03.6
Curiosità e avidità
promesse di premi, contenuti esclusivi o informazioni riservate abbassano la guardia.

04 Cosa può fare l'organizzazione

Conoscere questi meccanismi è il primo passo per difendersi. Le simulazioni di attacco, e-mail-trappola, chiamate simulate da un finto helpdesk IT, addestrano i dipendenti a riconoscere questi pattern in contesti realistici, non astratti. La consapevolezza di “come funziona il trucco” riduce significativamente l'efficacia del trucco stesso.

Un'organizzazione resiliente al social engineering è quella in cui ogni dipendente, di fronte a una richiesta insolita, si pone automaticamente la domanda: *perché mi stanno mettendo fretta? Perché chiedono questo a me? Posso verificare su un canale diverso?*

GPI PHISHING — CYBERSECURITY PLATFORM

Difendi la tua azienda dalle tecniche di manipolazione psicologica

Formazione, simulazioni e cultura della sicurezza:
le difese più efficaci contro il social engineering.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com