

INSURANCE

Email and phone pretexts, chained into an account takeover path

Email and voice social engineering · fixed price, agreed in writing

200

EMAIL TARGETS

19

CREDENTIAL ENTRIES

2-channel

ATTACK SIMULATED

THE CHALLENGE

A specialty insurance carrier wanted to test employee resilience against a coordinated, multi-channel social-engineering attack, not email alone.

01

Scope

Targets, pretexts, channels and rules of engagement agreed in writing with the security team, with a fixed price before launch.

02

Build the pretext

Realistic lures written for this organization, with harmless look-alike pages that record who clicked and who submitted credentials.

03

Run and measure

The campaign ran live while we tracked clicks, credential submissions and reports to the security team.

04

Report

Results by group and role, the attack path a real adversary would have taken, and a prioritized plan to reduce the risk.

WHAT WE FOUND

HIGH

A targeted credential-phishing email impersonating the company SSO password-reset flow led 19 employees to submit their credentials.

HIGH

A follow-on voice-phishing (vishing) campaign impersonating the IT help desk reinforced the email pretext; a subset of staff complied fully, including an executive assistant.

IMPACT

The email-plus-phone chain showed a credible path from initial lure to account takeover.

THE OUTCOME

Gave the security team a realistic multi-channel picture of susceptibility and a roadmap for help-desk identity-verification procedures and targeted training for high-exposure roles.

A SIMILAR ENGAGEMENT TODAY

Phishing and social engineering, Medium

A larger campaign across several hundred employees, or two channels such as email and voice. Fixed in writing before work begins.

FROM

\$5,500

PUBLISHED PRICE · USD

Get a fixed-price quote

Scope in one short form. Proposal within one business day.

invadel.com/scope

info@invadel.com · +1 (929) 591-9013