GTG.Online

Zero Touch. Zero Trust. Zero Guessing.

Executive Impersonation

The cost of not knowing who really sent an email.

Who's Who In Your Zoo?

Executive Impersonation by phishing attacks involves the malicious actor posing as a high-ranking executive within a company (such as a CEO or CFO) to deceive employees, customers, or partners, typically with the intention of obtaining sensitive information, financial gain, or unauthorized access to systems.

Types of Executive Impersonation Phishing

CEO Fraud/Whaling Attacks
Targets high-level executives to solicit sensitive information or conduct unauthorized financial transactions.

Spear Phishing
Highly targeted phishing emails sent to specific individuals or companies.

Business Email Compromise (BEC)
Exploits a compromise of legitimate business email accounts to conduct unauthorized activities.

Characteristics of Impersonation Emails

Urgent Request
Impersonated executive urgently requesting sensitive information or a fund transfer.

Lack of Detail
Emails are usually vague and lack specific details about the requested action.

Unusual Transaction
Requests for non-routine transactions or activities.

Stop Impersonation

In minutes, GTG Enterprise can begin validating messages.

No more wondering if a trusted executive sent that disparaging note or request for funds, our unique non-repudiation solution verifies that the message you received is identical to the message that was composed and sent internally, neutralizing the threat.