GRAPHUS

Executive Spoofing

Feature Guide

How Executive Spoofing Works

Executives here mean individuals (mostly C-level executives or executives from HR, finance, IT etc.) whom hackers may impersonate for malicious purposes.

Graphus creates a trust graph which is unique for an organization. Any sender interacting with the organization will have a trust rating in the graph.

Assuming that admins have added the key executive names in the Settings page in the Graphus portal, the following scenarios are possible:

Scenario 1: Hacker creates a new email address and tries to impersonate an executive by setting the executive name as the sender's name. Since this email address has no trust rating in the trust graph and the executive name matches with the one configured in Graphus, the email will be auto-quarantined.

Scenario 2: The executive is using their personal email address to communicate with the organization. This email address will most likely be present as a trusted entry in the trust graph based on the executive's previous interactions. This email will not be flagged by Graphus.