Internal Spearphishing, Technique T1534 - Enterprise

Archived: 2026-04-05 14:37:32 UTC

After they already have access to accounts or systems within the environment, adversaries may use internal spearphishing to gain access to additional information or compromise other users within the same organization. Internal spearphishing is multi-staged campaign where a legitimate account is initially compromised either by controlling the user's device or by compromising the account credentials of the user. Adversaries may then attempt to take advantage of the trusted internal account to increase the likelihood of tricking more victims into falling for phish attempts, often incorporating Impersonation.[1]

For example, adversaries may leverage Spearphishing Attachment or Spearphishing Link as part of internal spearphishing to deliver a payload or redirect to an external site to capture credentials through Input Capture on sites that mimic login interfaces.

Adversaries may also leverage internal chat apps, such as Microsoft Teams, to spread malicious content or engage users in attempts to capture sensitive information and/or credentials.[2]

Source: https://attack.mitre.org/techniques/T1534