Phishing for Information: Spearphishing Attachment, Sub-technique T1598.002 - Enterprise

Archived: 2026-04-05 14:20:55 UTC

Adversaries may send spearphishing messages with a malicious attachment to elicit sensitive information that can be used during targeting. Spearphishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Spearphishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: Establish Accounts or Compromise Accounts) and/or sending multiple, seemingly urgent messages.

All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email. In some cases, they may rely upon the recipient populating information, then returning the file.[1][2] The text of the spearphishing email usually tries to give a plausible reason why the file should be filled-in, such as a request for information from a business associate. In other cases, adversaries may leverage techniques such as HTML Smuggling to harvest user credentials via fake login portals.[3]

Adversaries may also use information from previous reconnaissance efforts (ex: Search Open Websites/Domains or Search Victim-Owned Websites) to craft persuasive and believable lures.

Source: https://attack.mitre.org/techniques/T1598/002