# TTP Detail – T1598.004

## TTP Information

Name: Spearphishing Voice

Description: Adversaries may use voice communications 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: [Impersonation](https://attack.mitre.org/techniques/T1656)) and/or creating a sense of urgency or alarm for the recipient.

All forms of phishing are electronically delivered social engineering. In this scenario, adversaries use phone calls to elicit sensitive information from victims. Known as voice phishing (or "vishing"), these communications can be manually executed by adversaries, hired call centers, or even automated via robocalls. Voice phishers may spoof their phone number while also posing as a trusted entity, such as a business partner or technical support staff.(Citation: BOA Telephone Scams)

Victims may also receive phishing messages that direct them to call a phone number ("callback phishing") where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing)

Adversaries may also use information from previous reconnaissance efforts (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Victim-Owned Websites](https://attack.mitre.org/techniques/T1594)) to tailor pretexts to be even more persuasive and believable for the victim.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## APTs (Intrusion Sets)

* LAPSUS$
* Scattered Spider