# TTP Detail – T1566.004

## TTP Information

Name: Spearphishing Voice

Description: Adversaries may use voice communications to ultimately gain access to victim systems. Spearphishing voice is a specific variant of spearphishing. It is different from other forms of spearphishing in that is employs the use of manipulating a user into providing access to systems through a phone call or other forms of voice communications. Spearphishing frequently involves social engineering techniques, such as posing as a trusted source (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 are not directly sending malware to a victim vice relying on [User Execution](https://attack.mitre.org/techniques/T1204) for delivery and execution. For example, victims may receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools ([Remote Access Tools](https://attack.mitre.org/techniques/T1219)) onto their computer.(Citation: Unit42 Luna Moth)

Adversaries may also combine voice phishing with [Multi-Factor Authentication Request Generation](https://attack.mitre.org/techniques/T1621) in order to trick users into divulging MFA credentials or accepting authentication prompts.(Citation: Proofpoint Vishing)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: initial-access

## APTs (Intrusion Sets)

* Storm-1811