# TTP Detail – T1598.003

## TTP Information

Name: Spearphishing Link

Description: Adversaries may send spearphishing messages with a malicious link 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](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) 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, the malicious emails contain links generally accompanied by social engineering text to coax the user to actively click or copy and paste a URL into a browser.(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin) The given website may be a clone of a legitimate site (such as an online or corporate login portal) or may closely resemble a legitimate site in appearance and have a URL containing elements from the real site. URLs may also be obfuscated by taking advantage of quirks in the URL schema, such as the acceptance of integer- or hexadecimal-based hostname formats and the automatic discarding of text before an “@” symbol: for example, `hxxp://google.com@1157586937`.(Citation: Mandiant URL Obfuscation 2023)

Adversaries may also embed “tracking pixels”, "web bugs", or "web beacons" within phishing messages to verify the receipt of an email, while also potentially profiling and tracking victim information such as IP address.(Citation: NIST Web Bug) (Citation: Ryte Wiki) These mechanisms often appear as small images (typically one pixel in size) or otherwise obfuscated objects and are typically delivered as HTML code containing a link to a remote server. (Citation: Ryte Wiki)(Citation: IAPP)

Adversaries may also be able to spoof a complete website using what is known as a "browser-in-the-browser" (BitB) attack. By generating a fake browser popup window with an HTML-based address bar that appears to contain a legitimate URL (such as an authentication portal), they may be able to prompt users to enter their credentials while bypassing typical URL verification methods.(Citation: ZScaler BitB 2020)(Citation: Mr. D0x BitB 2022)

Adversaries can use phishing kits such as `EvilProxy` and `Evilginx2` to perform adversary-in-the-middle phishing by proxying the connection between the victim and the legitimate website. On a successful login, the victim is redirected to the legitimate website, while the adversary captures their session cookie (i.e., [Steal Web Session Cookie](https://attack.mitre.org/techniques/T1539)) in addition to their username and password. This may enable the adversary to then bypass MFA via [Web Session Cookie](https://attack.mitre.org/techniques/T1550/004).(Citation: Proofpoint Human Factor)

Adversaries may also send a malicious link in the form of Quick Response (QR) Codes (also known as “quishing”). These links may direct a victim to a credential phishing page.(Citation: QR-campaign-energy-firm) By using a QR code, the URL may not be exposed in the email and may thus go undetected by most automated email security scans.(Citation: qr-phish-agriculture) These QR codes may be scanned by or delivered directly to a user’s mobile device (i.e., [Phishing](https://attack.mitre.org/techniques/T1660)), which may be less secure in several relevant ways.(Citation: qr-phish-agriculture) For example, mobile users may not be able to notice minor differences between genuine and credential harvesting websites due to mobile’s smaller form factor.

From the fake website, information is gathered in web forms and sent to the adversary. 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 craft persuasive and believable lures.

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: reconnaissance

## Malware

* SMOKEDHAM

## Tools

* AADInternals

## APTs (Intrusion Sets)

* APT28
* APT32
* CURIUM
* Dragonfly
* Kimsuky
* Magic Hound
* Moonstone Sleet
* Mustang Panda
* Patchwork
* Sandworm Team
* Sidewinder
* Silent Librarian
* Star Blizzard
* ZIRCONIUM