# TTP Detail – T1598.001

## TTP Information

Name: Spearphishing Service

Description: Adversaries may send spearphishing messages via third-party services 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, adversaries send messages through various social media services, personal webmail, and other non-enterprise controlled services.(Citation: ThreatPost Social Media Phishing) These services are more likely to have a less-strict security policy than an enterprise. As with most kinds of spearphishing, the goal is to generate rapport with the target or get the target's interest in some way. Adversaries may create fake social media accounts and message employees for potential job opportunities. Doing so allows a plausible reason for asking about services, policies, and information about their environment. Adversaries may also use information from previous reconnaissance efforts (ex: [Social Media](https://attack.mitre.org/techniques/T1593/001) 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