# TTP Detail – T1672

## TTP Information

Name: Email Spoofing

Description: Adversaries may fake, or spoof, a sender’s identity by modifying the value of relevant email headers in order to establish contact with victims under false pretenses.(Citation: Proofpoint TA427 April 2024) In addition to actual email content, email headers (such as the FROM header, which contains the email address of the sender) may also be modified. Email clients display these headers when emails appear in a victim's inbox, which may cause modified emails to appear as if they were from the spoofed entity.

This behavior may succeed when the spoofed entity either does not enable or enforce identity authentication tools such as Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and/or Domain-based Message Authentication, Reporting and Conformance (DMARC).(Citation: Cloudflare DMARC, DKIM, and SPF)(Citation: DMARC-overview)(Citation: Proofpoint-DMARC) Even if SPF and DKIM are configured properly, spoofing may still succeed when a domain sets a weak DMARC policy such as `v=DMARC1; p=none; fo=1;`. This means that while DMARC is technically present, email servers are not instructed to take any filtering action when emails fail authentication checks.(Citation: Proofpoint TA427 April 2024)(Citation: ic3-dprk)

Adversaries may abuse absent or weakly configured SPF, SKIM, and/or DMARC policies to conceal social engineering attempts(Citation: ic3-dprk) such as [Phishing](https://attack.mitre.org/techniques/T1566). They may also leverage email spoofing for [Impersonation](https://attack.mitre.org/techniques/T1656) of legitimate external individuals and organizations, such as journalists and academics.(Citation: ic3-dprk)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion