What Is Email Spoofing? Definition & Examples | Proofpoint US

Published: 2021-02-27 · Archived: 2026-04-05 12:44:15 UTC

Table of Contents

Email Spoofing Definition

Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they know or trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address, which most users take at face value. Users don't realize the sender is forged unless they inspect the header more closely. If it's a name they recognize, they're more likely to trust it. So they'll click malicious links, open malware attachments, send sensitive data, and even wire corporate funds.

Email spoofing is possible due to how email systems are designed. The client application assigns a sender address to outgoing messages, so outgoing email servers cannot identify whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, not every email service has security protocols in place. Still, users can review each message's email header to determine whether the sender address is forged.

A Brief History of Email Spoofing

Email spoofing has been an issue since the 1970s due to how email protocols work. It started with spammers who used it to get around email filters. The issue became more common in the 1990s, then grew into a global cybersecurity issue in the 2000s.

Security protocols were introduced in 2014 to help fight email spoofing and phishing. Since then, many spoofed email messages are now sent to user spamboxes or are rejected and never sent to recipient inboxes.

Spoofing vs. Phishing

Despite sharing some similarities, spoofing and phishing are two distinct cyber threats with several fundamental differences.

- The goal of spoofing is to impersonate someone's identity, while the goal of phishing attacks is to steal information.
- Phishing scams are fraudulent because they involve information theft. However, spoofing is not considered fraud because the victim's email address or phone number is not stolen but rather imitated.

- Phishing often involves the attacker pretending to be from a trusted organization, whereas spoofing involves changing the sender's email address or phone number to impersonate someone else.
- Phishing is commonly executed with fake websites and data collection portals. Spoofing emails can be used to breach system security or steal user information.

How Email Spoofing Works

Email spoofing aims to trick users into believing the email is from someone they know or trust—in most cases, a colleague, vendor, or brand. Exploiting that trust, the attacker asks the recipient to divulge information or take some other action.

A typical email client (such as Microsoft Outlook) automatically enters the sender address when a user sends a new email message. But an attacker can programmatically send messages using basic scripts in any language that configures the sender address to a chosen email address. Email API endpoints allow a sender to specify the sender address regardless of whether the address exists. And outgoing email servers can't determine whether the sender's address is legitimate.

Outgoing email is retrieved and routed using the Simple Mail Transfer Protocol (SMTP). When a user clicks "Send" in an email client, the message is first sent to the outgoing SMTP server configured in the client software. The SMTP server identifies the recipient domain and routes it to the domain's email server. The recipient's email server then routes the message to the right user inbox.

For every "hop" an email message takes as it travels across the internet from server to server, the IP address of each server is logged and included in the email headers. These headers divulge the true route and sender, but many users do not check headers before interacting with an email sender.

The three major components of an email are:

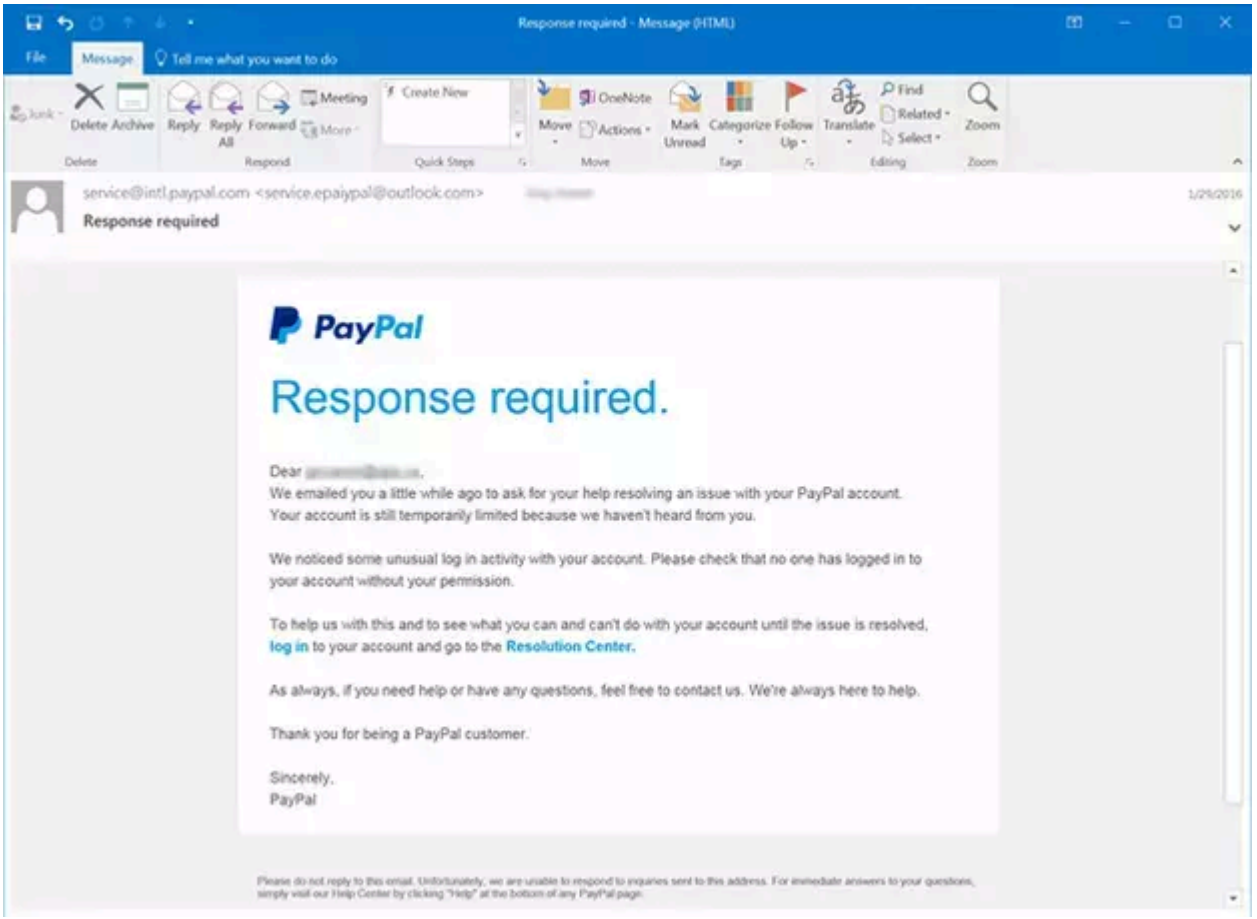
- The sender address
- The recipient address
- The body of the email

Another component often used in phishing is the Reply-To field. The sender can configure this field and use it in a phishing attack. The Reply-To address tells the client email software where to send a reply, which can be different from the sender's address. Again, email servers and the SMTP protocol do not validate whether this email is legitimate or forged. It's up to the user to realize that the reply is going to the wrong recipient.

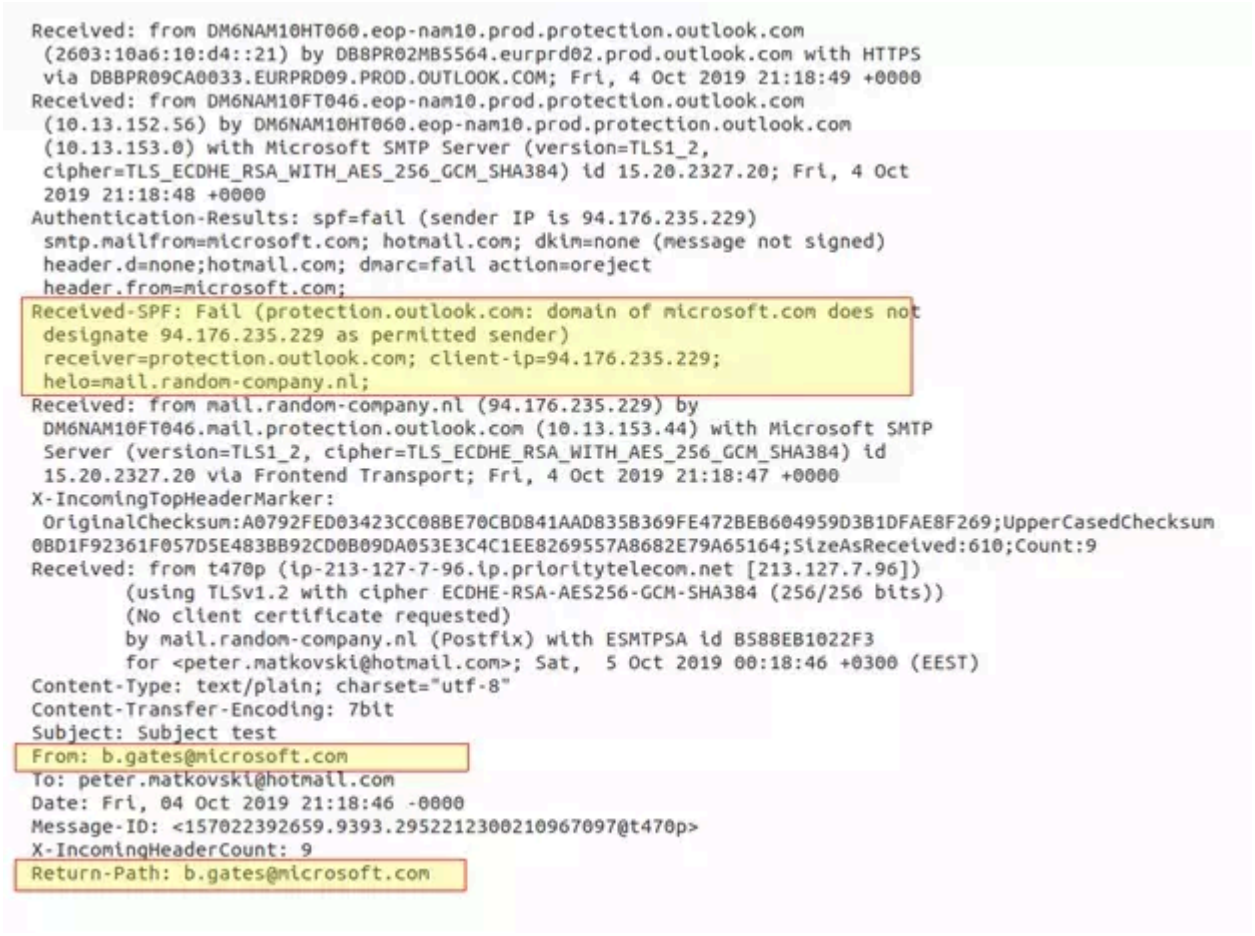
Examples of Email Spoofing

As an example of email spoofing, an attacker might create an email that looks like it comes from PayPal. The message tells the user that their account will be suspended if they don't click a link, authenticate into the site, and change the account's password. If the user is successfully tricked and types in credentials, the attacker can authenticate into the targeted user's PayPal account and steal the user's money.

To the user, a spoofed email message looks legitimate because many attackers use elements from the official website to make the message more believable. Here's an email spoofing example with a PayPal phishing attack:



More complex attacks target financial employees and use social engineering and online reconnaissance to trick a targeted user into sending money to an attacker's bank account. Here's an example of a forged email:



```
Received: from DM6NAM10HT060.eop-nam10.prod.protection.outlook.com
 (2603:10a6:10:d4::21) by DB8PR02MB5564.eurprd02.prod.outlook.com with HTTPS
 via DBBPR09CA0033.EURPRD09.PROD.OUTLOOK.COM; Fri, 4 Oct 2019 21:18:49 +0000
Received: from DM6NAM10FT046.eop-nam10.prod.protection.outlook.com
 (10.13.152.56) by DM6NAM10HT060.eop-nam10.prod.protection.outlook.com
 (10.13.153.0) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.2327.20; Fri, 4 Oct
 2019 21:18:48 +0000
Authentication-Results: spf=fail (sender IP is 94.176.235.229)
 smtp.mailfrom=microsoft.com; hotmail.com; dkim=none (message not signed)
 header.d=none;hotmail.com; dmarc=fail action=oreject
 header.from=microsoft.com;
Received-SPF: Fail (protection.outlook.com: domain of microsoft.com does not
 designate 94.176.235.229 as permitted sender)
 receiver=protection.outlook.com; client-ip=94.176.235.229;
 helo=mail.random-company.nl;
Received: from mail.random-company.nl (94.176.235.229) by
 DM6NAM10FT046.mail.protection.outlook.com (10.13.153.44) with Microsoft SMTP
 Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id
 15.20.2327.20 via Frontend Transport; Fri, 4 Oct 2019 21:18:47 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:A0792FED03423CC08BE70CBD841AAD835B369FE472BEB604959D3B1DFAE8F269;UpperCasedChecksum
0BD1F92361F057D5E483BB92CD0B09DA053E3C4C1EE8269557A8682E79A65164;SizeAsReceived:610;Count:9
Received: from t470p (ip-213-127-7-96.ip.prioritytelecom.net [213.127.7.96])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by mail.random-company.nl (Postfix) with ESMTPSA id B588EB1022F3
        for <peter.matkovski@hotmail.com>; Sat,  5 Oct 2019 00:18:46 +0300 (EEST)
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Subject: Subject test
From: b.gates@microsoft.com
To: peter.matkovski@hotmail.com
Date: Fri, 04 Oct 2019 21:18:46 -0000
Message-ID: <157022392659.9393.2952212300210967097@t470p>
X-IncomingHeaderCount: 9
Return-Path: b.gates@microsoft.com
```

Notice that the email address in the From field is Bill Gates (b.gates@microsoft.com). There are two sections in these email headers to review. The “Received” section shows that the email was originally handled by the email server email.random-company.nl, which is the first clue that this is a case of email spoofing. But the best field to review is the Received-SPF section—notice that the section has a “Fail” status.

How to Identify Spoofing Email

While spoofing scams continue to become increasingly elaborate, particular signs and cues can help you identify a spoofing email.

- **Check the email header:** The email header contains information like the date, subject line, recipient’s and sender’s names, and email address. Check to see if the email address appears from a legitimate source and that the name and other details match up.
- **Look for disconnects between email addresses, display names, etc.:** An email address that doesn’t match the sender’s display name is a telling sign of a spoofed email, especially if the domain of the email address looks suspicious.

- **Assess the email content:** Spoofed emails often contain alarming or aggressive messaging to provoke a sense of urgency and impulsiveness. If the tone of the subject line and email content is tailored to scare you or alarm you, then it likely is a spoofed email.
- **Be watchful for emails requesting personal information:** Spoofed emails are often used in conjunction with phishing scams, where fraudsters impersonate brands or identities to get your personal information.
- **Avoid clicking links or downloading attachments:** If you receive an email that appears suspicious or is from an unknown sender, do not click links or download attachments.
- **Copy and paste the content of an email message into a search engine:** Chances are that text used in a common phishing attack has already been reported and published on the Internet.
- **Look for inconsistencies in the email signature:** If the information in the email signature, such as the telephone number, does not align with what is known about the sender, it may be a spoofed email.

When in doubt, refrain from opening any unknown or suspicious emails. Spoofing email or not, a people-minded, user-focused approach is key to mitigating costly social engineering attacks.

Motivations Behind Email Spoofing

Email spoofing may seem like an unusual tactic, but it can be an effective means of deceiving unaware victims. Some of the primary motivations behind email spoofing include:

- **Acquiring sensitive information:** Attackers may use email spoofing to obtain sensitive information, such as social security numbers, financial details, and other critical information.
- **Taking over online accounts:** Email spoofing can take over online accounts by deceiving users into revealing their login credentials.
- **Distributing malware:** Attackers use email spoofing to deliver malware to the recipient's computer or network.
- **Stealing funds:** Email spoofing is used to steal funds by tricking users into revealing their financial information or transferring money to the attacker's account.
- **Manipulate and influence:** Spoofing email can sway public opinion for special interest groups and parties, whether political, governmental, or environmental.

Email Spoofing Statistics

Email clients configured to use SPF and DMARC will automatically reject emails that fail validation or send them to the user's spam box. Attackers target people and businesses, and just one successfully tricked user can lead to the theft of money, data, and credentials.

It's no wonder that email spoofing has become a commonly exploited avenue for cyber-attackers. Consider the following statistics:

- 3.1 billion domain spoofing emails are sent per day.
- More than 90% of cyber-attacks start with an email message.
- Email spoofing and phishing have had a worldwide impact costing an estimated $26 billion since 2016.
- In 2019, the FBI reported that 467,000 cyber-attacks were successful, and 24% were email-based.

- 91% of bait emails are sent via Gmail, with just 9% coming from other sending domains. (Source: https://blog.barracuda.com/2021/11/10/threat-spotlight-bait-attacks/)
- The average scam tricked users out of $75,000.

A common attack that uses email spoofing is CEO fraud, also known as business email compromise (BEC). In BEC, the attacker spoofs the sender's email address to impersonate an executive or owner of a business. This attack usually targets an employee in the financial, accounting, or accounts payable departments.

Even smart, well-intentioned employees can be tricked into sending money when the request comes from someone they trust—especially an authority figure. Here are just a few high-profile examples of costly spoofing scams:

- The Canadian City Treasure was tricked into transferring $98,000 from taxpayer funds by an attacker claiming to be city manager Steve Kanellakos.
- Mattel was tricked into sending $3 million to an account in China, but it was lucky enough to claw back the money when the defrauded financial executive confirmed that CEO Christopher Sinclair did not send the email message.
- The Crelan bank in Belgium was tricked into sending attackers €70 million.

How to Protect Against Email Spoofing

In addition to having a discerning team with an eye for suspicious emails, specific tools and technologies can help prevent email spoofing from becoming a threat.

- **Secure email gateway:** A secure email gateway can help protect against email spoofing by filtering out suspicious messages and blocking messages from known spoofed email addresses.
- **Implement email authentication protocols:** Implement Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) protocols work together to authenticate emails and prevent email spoofing.
    - Sender Policy Framework (SPF) is a security protocol set as a standard in 2014. It works with DMARC (Domain-based Message Authentication, Reporting and Conformance) to stop malware and phishing attacks.
    - SPF can detect spoofed emails, and it's become common with most email services to combat phishing. But it's the domain holder's responsibility to use SPF. To use SPF, a domain holder must configure a DNS TXT entry specifying all IP addresses authorized to send email on behalf of the domain.
    - With this DNS entry configured, recipient email servers look up the IP address when receiving a message to ensure that it matches the email domain's authorized IP addresses. If there is a match, the Received-SPF field displays a PASS status. If there is no match, the field displays a FAIL status. Recipients should review this status when receiving an email with links, attachments, or written instructions.
- **Use a secure email provider:** Choose a secure email service provider that uses advanced security measures to protect against email spoofing and phishing attacks. For example, ProtonMail is a widely known and free-to-use secure email provider.

- **Use email filters:** Simple email filters limit the number of suspicious emails that get through to users' inboxes. Email filters help detect and filter spoofed messages and block messages from known spoofed email addresses.
- **Educate users:** Train your people to identify and avoid spoofing attacks. Share ways to identify suspicious emails that should be reported before opening.

These are just some of the most common email security solutions that organizations use to better protect themselves from email spoofing and other types of cyber attacks.

Get Ahead of Tomorrow's Threats with Proofpoint

Anticipating the nature of certain cyber threats helps organizations identify where their defenses are weak and which protective measures to prioritize. Most organizations are more resilient through layered strategies that leverage detection and prevention technologies, real-time threat intelligence, and user-focused training programs to reduce the risk of attacks via email and cloud environments. As threats like phishing, BEC, ransomware, and credential theft evolve, it's important to have the right mix of tools and processes to keep your data and your people protected. Take ownership to protect against threats and make strides to improve your cybersecurity effectiveness.

Leverage the capabilities trusted by 83 of the Fortune 100 companies. Contact Proofpoint to learn more.

Related Resources

The latest news and updates from Proofpoint, delivered to your inbox.

Sign up to receive news and other stories from Proofpoint. Your information will be used in accordance with Proofpoint's privacy policy. You may opt out at any time.
