What is Email Spoofing?

Information pulled from: Gartner Report on Email Security pulled from the Garner Market Guide for Email Security
Published 08 September 2020 ID: G00722358

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 either know or can 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. Unless they inspect the header more closely, users see the forged sender in a message. 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 the way email systems are designed. Outgoing messages are assigned a sender address by the client application; outgoing email servers have no way to tell whether the sender address is legitimate or spoofed.

Recipient servers and antimalware software can help detect and filter spoofed messages. Unfortunately, spoofers still get through; however, users can review email headers packaged with every message to determine whether the sender address is forged.

A Brief History of Email Spoofing

Because of the way email protocols work, email spoofing has been an issue since the 1970s. 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, but spammers are always creating new ways to get around these protocols.

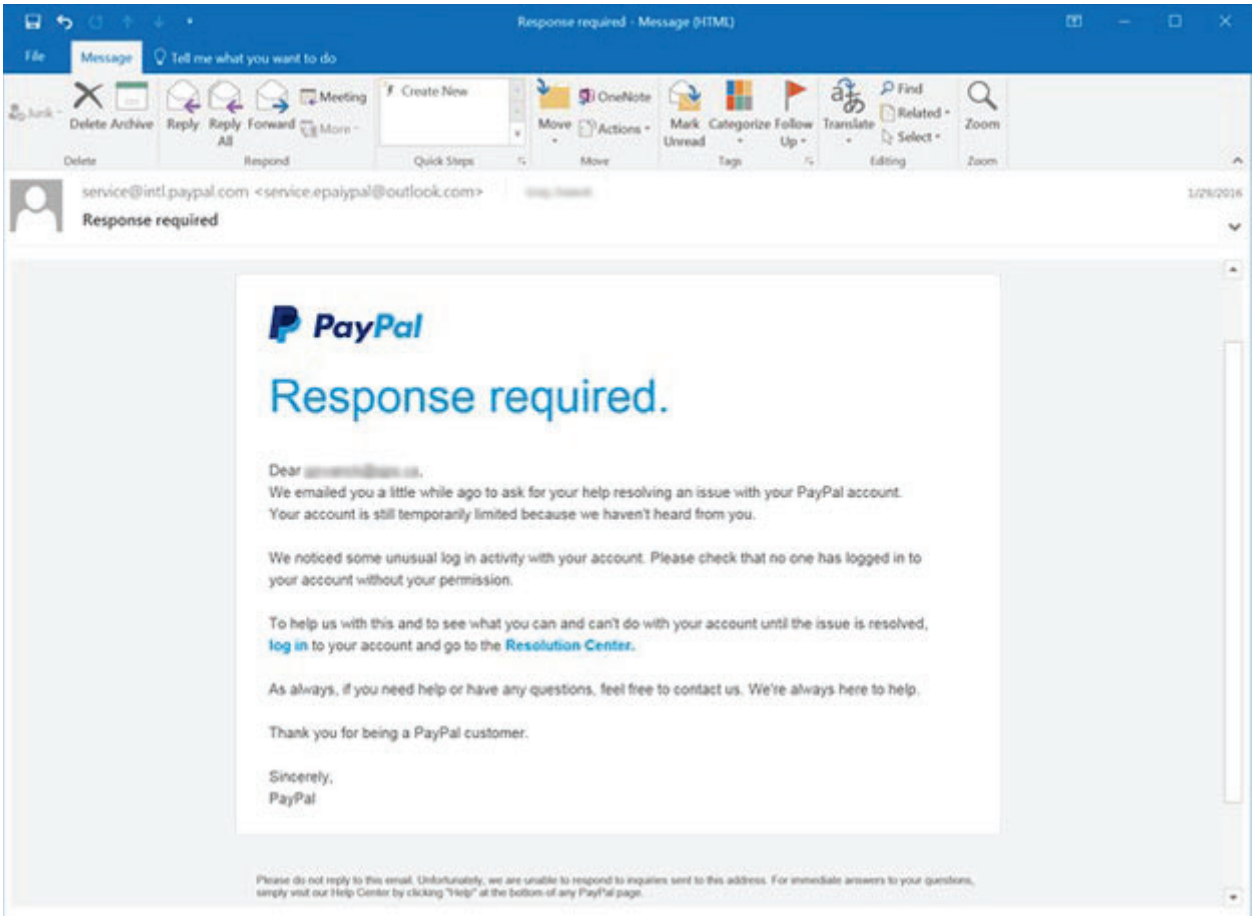
How Email Spoofing Works

The goal of spoofing is to trick users into believing the email is from someone they know or can 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.

For example, 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 now has credentials to authenticate into the targeted user's PayPal account, potentially stealing money from the user.

More complex attacks target financial employees and use social engineering and online reconnaissance to trick a targeted user into sending millions to an attacker's bank account.

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



With a typical email client (such as Microsoft Outlook), the sender address is automatically entered 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 an email address of choice. 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 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.

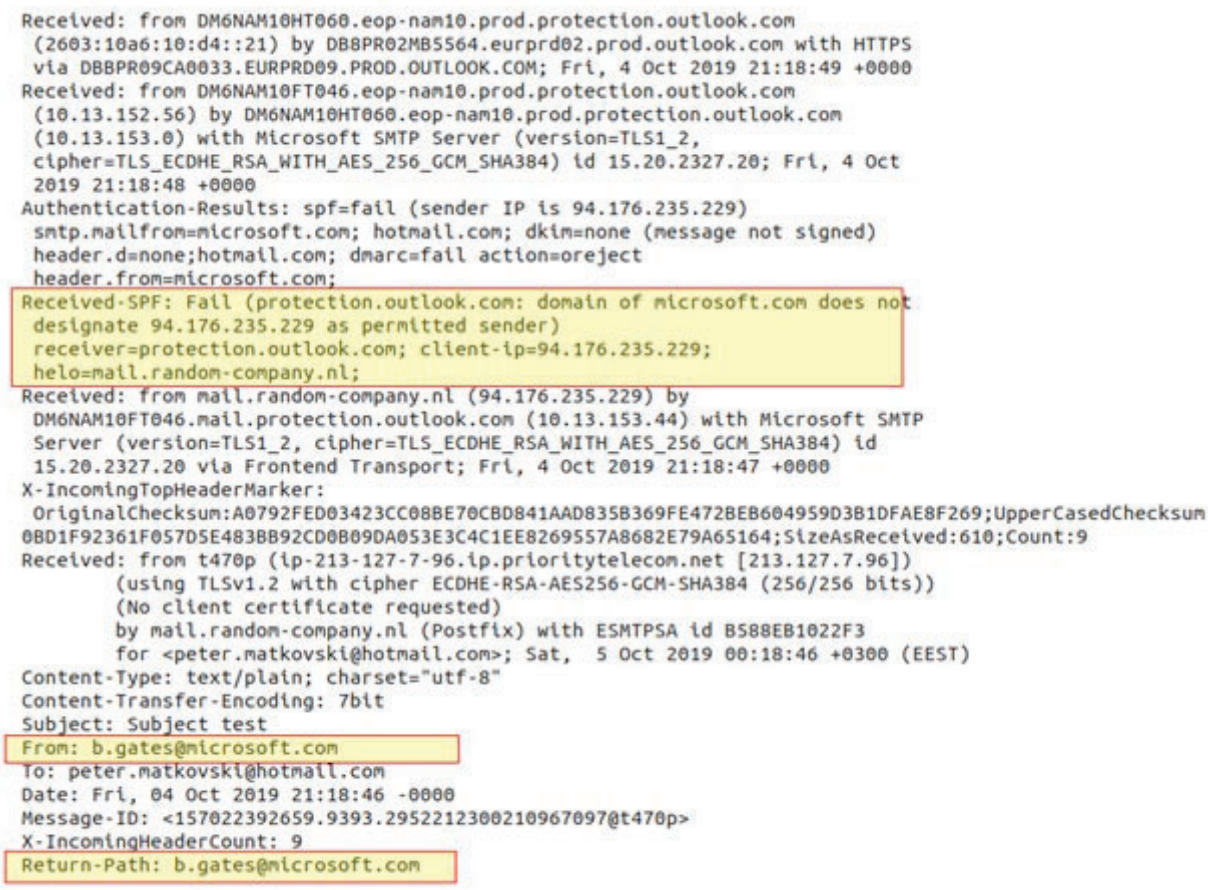
The three major components of an email are:

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

Another component often used in phishing is the Reply-To field. This field is also configurable from the sender and can be used 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.

Here's an example 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 sender field is supposedly from 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 email is forged. But the best field to review is the Received-SPF section—notice that the section has a "Fail" status.

Sender Policy Framework (SPF) is a security protocol set as a standard in 2014. It works in conjunction with DMARC (Domain-based Message Authentication, Reporting and Conformance) to stop malware and phishing attacks.

SPF can detect spoofed email, and it's become common with most email services to combat phishing. But it's the responsibility of the domain holder 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 lookup 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.

Email Spoofing and Phishing Statistics

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

It's no wonder that phishing is one of today's most prominent cyber attacks. 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% of them were email-based.
- 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 phishing 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 was able to confirm that the email message was not sent by the CEO, Christopher Sinclair.
- The Crelan bank in Belgium was tricked into sending attackers €70 million.

How to Protect from Email Spoofing

Even with email security in place, some malicious email messages reach user inboxes. Whether you're an employee responsible for financial decisions or as someone who uses personal email at work, there are several steps you can take to avoid becoming a victim of email fraud:

- Never click links to access a website where you're asked to authenticate. Always type the official domain in your browser and authenticate directly on the site.
- The steps to view email headers are different for each email client, so first look up how to view email headers for your inbox software. Then, open email headers and look for the Received-SPF section of the headers and look for a PASS or FAIL response.
- 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.
- Be suspicious of email supposedly from an official source with bad spelling or grammar.
- Avoid opening attachments from suspicious or unknown senders.
- Emails promising riches—or anything else that's too good to be true—is likely a scam.
- Beware of emails that create a sense of urgency or danger. Phishing and BEC attacks often try to short-circuit recipients' natural skepticism by suggesting that something bad will happen if they don't act quickly. Treat email links with extra caution if the message warns of pending account closures, scheduled payment failures or suspicious activity on one of your financial accounts. Visit the website directly through your browser, not the link in the email.