cybernews

Home » Secure Email » What is email spoofing?

What is email spoofing?

Justinas Mazūra 10 November 2020 No Comments

Email spoofing is the act of sending emails with **a forged sender address**. It tricks the recipient into thinking that someone they know or trust sent them the email. Usually, it's a tool of a phishing attack, designed to take over your online accounts, send malware, or steal funds.

Spoofed email messages are easy to make and easy to detect. However, more malicious and targeted varieties can cause significant problems and pose a huge security threat.

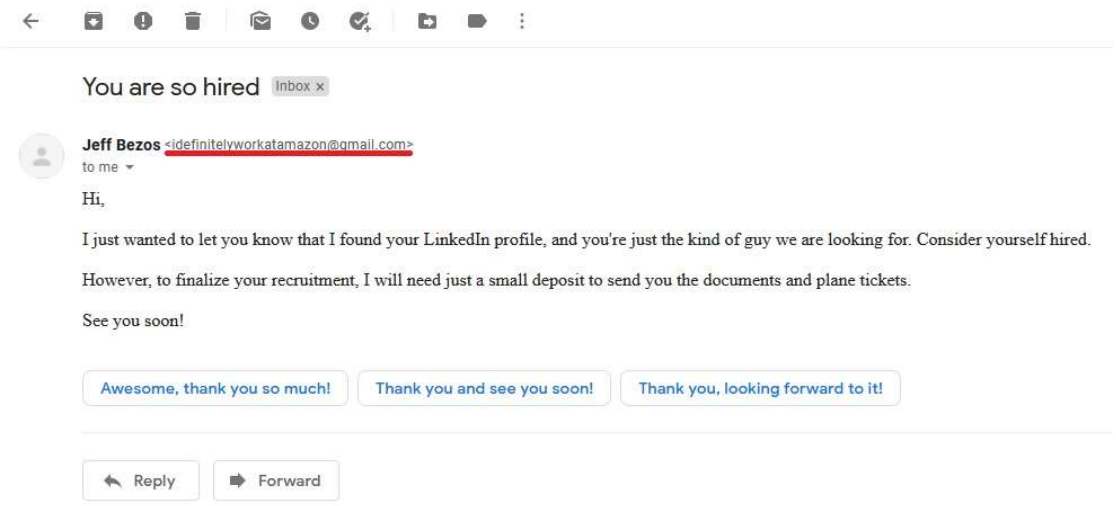
How does email spoofing work?

Email spoofing is possible by **forging email syntax** in several methods of varying complexity. They

Here's what variation you could encounter when surfing the web.

Spoofing via display name

Display name spoofing is a type of email spoofing, in which **only the email sender's display name is forged**. Somebody can do this by registering a new Gmail account with the same name as the contact you want to impersonate. Mind you, the *mailto:* will display a different email address. If you've ever received an email from Jeff Bezos asking you to loan some money – you've encountered an example of spoofing via display name.



This type of email will also bypass all spoofing security countermeasures. It won't get filtered out as spam, because it's a legitimate email address. This exploits user interfaces built with ease of use in mind – most modern email client apps don't show metadata. Hence, display name spoofing is very effective due to the prevalence of smartphone email apps. Often, they only have space for a display name.

Spoofing via legitimate domains

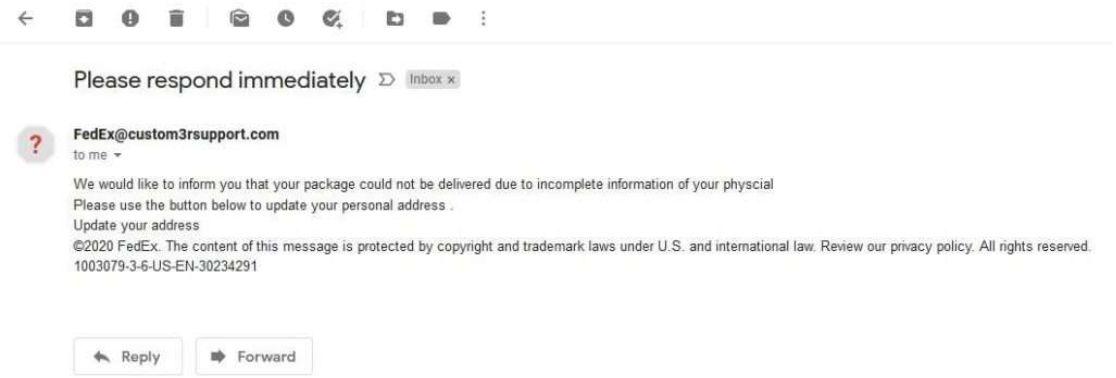
Suppose the attacker is aiming at higher believability. In that case, he may also use a trusted email address in the **From** header, such as "Customer Support Specialist" <noreply@trustedbank.com>. This means both the **display name** and **email address** will show misleading information.

This attack doesn't need to hijack the account or penetrate the targeted company's internal network. It only uses compromised Simple Mail Transfer Protocol (SMTP) servers that permit connections without authentication and allow you to manually specify the "**To**" and "**From**" addresses. Using

The situation is dire because many enterprise email domains aren't using any countermeasures for verification. Still, there are some techniques that you could use to protect your domain – more on that later.

Spoofing via lookalike domains

Suppose a domain is protected, and domain spoofing isn't possible. In that case, the attacker is most likely going to set up a lookalike domain. In this type of attack, the fraudster registers and uses **a domain that is similar to the impersonated domain**, e.g."@doma1n.co" instead of"@domain.co". This change could be minimal enough not to be noticed by an inattentive reader. It's effective because when exactly was the last time you bothered to read an email header?



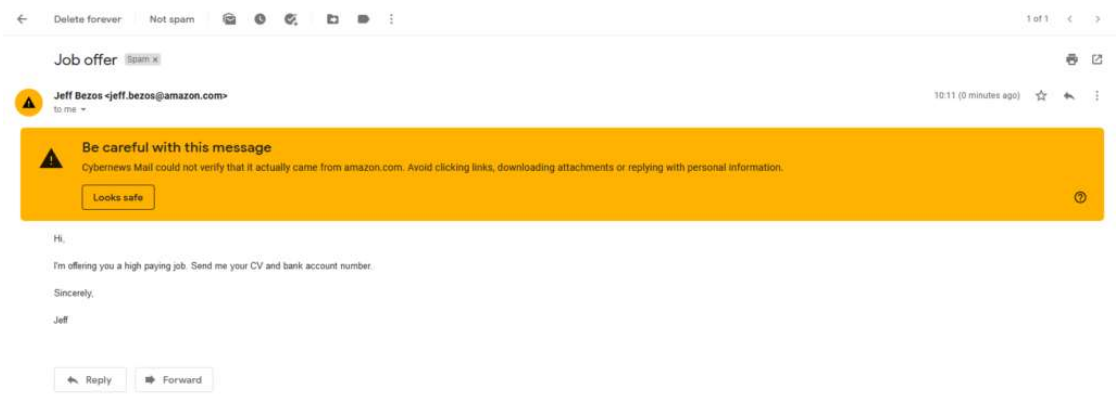
Using a very similar domain, which also bypasses spam checks due to being a legitimate mailbox, the attacker creates a sense of authority. It might be just enough to convince its victim to reveal their password, transfer money, or send some files. In all cases, email metadata investigation is the only way to confirm whether the message is genuine. However, it's sometimes plain impossible to do on the go, especially with smaller smartphone screens.

Spoofing detection: ways to identify email spoofing

Incidentally, it's incredibly easy to identify email spoofing. Aside from the obvious red flags, you only need to look at the **full email header**. It contains all the critical components of every email: **From**, **To**, **Date** and **Subject**. Also, there will be metadata on how the email was routed to you and where it came from. Most likely, it will also contain the verification results your internet service provider used to check if the sender's server had the proper authorization to send emails using that domain.

How you check this data heavily depends on the service you're using and will only work on a desktop.

Here's an example of a spoofed email that I sent to myself pretending to be a billionaire. In this case, the email filter caught it labeling it as spam, so it didn't appear in my primary mailbox. I had to find it in the spam folder. Big yellow warning aside, you've got to admit, it looks pretty realistic.



Suppose I would have picked a lower-profile domain of a lesser-known company with fewer methods to verify. Well, there is still a lot that you can check. If you go to "**Show Original**", you can see that **SPF** is indicated as **SOFTFAIL**, and **DMARC** is indicated as **FAIL**. This is enough to call out the email as spoofed. Some poorly maintained domains do not keep their **SPF** records up to date, failing validation.

Original message

Message ID	<20200819071152.A0133270C7@localhost>
Created on:	19 August 2020 at 10:11 (Delivered after 1 second)
From:	Jeff Bezos <jeff.bezos@amazon.com>
To:	justinas.mazura@cybernews.com
Subject:	Job offer
SPF:	SOFTFAIL with [redacted] Learn more
DMARC:	'FAIL' Learn more

If you want to go deeper down the rabbit hole, at the code level, you'll see that *Received: from,* and *Received-SPF* domains do not match, as well as the IP addresses. This is a clear example of email spoofing. Remember, if IP addresses don't match and SPF validation fails, this isn't a genuine email. It doesn't also hurt to check whether the *Return-Path* is the same as the sender's email address.

How to stop email spoofing?

of the technology. There are some additional countermeasures developed to counter email spoofing. Still, the success rate will depend entirely on whether your email service provider implemented them.

Most trusted email providers use a Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), Domain-based Message Authentication, Reporting & Conformance (DMARC), and Secure/Multipurpose Internet Mail Extensions (S/MIME). They function as additional checks. These tools work automatically, and when used effectively, they immediately disregard spoofed messages as spam. That is why you've seen that yellow bar under our spoofed Jeff Bezos email.

As an ordinary user, you can stop email spoofing by choosing a secure email provider and practicing good cybersecurity hygiene:

- **Use throwaway accounts when registering in sites**. That way, your private email address won't appear in shady lists used for sending spoofed email messages in bulk.
- **Make sure that your email password is strong and is complex enough**. That way, it will be harder for cybercriminals to get into your account and send misleading messages to your contacts.
- **Inspect the email headers, especially when someone asks to click on a link**. Spoofed emails made by talented attackers can be identical to the genuine ones. They can seem indistinguishable even if you're a long-time user.

Why is email spoofing dangerous?

Email spoofing is incredibly dangerous and damaging because it **doesn't need to compromise any account** by bypassing security measures that most email providers now implement by default. It exploits the human factor, especially the fact that no person double-checks the header of every email that they receive. Besides, it's incredibly easy for attackers and **requires almost no technical know-how** to do it on a basic level. Not to mention the fact that every mail server can be reconfigured to be identical or almost identical to slip by.

What to do if your email has been spoofed?

If you got an email from yourself with ransom threats, the first step is to stop and collect yourself. We've already touched on how easy it is to spoof an email. Panicking is playing into the attacker's hands. What you'll need to do then is to **investigate the email header** and check for the IP addresses, SPF, DMARC, DKIM validations. This will clear out whether the email came from your own account. If

Real-world examples of email spoofing

Several years ago, all Seagate employees received emails impersonating their CEO requesting their W-2 forms. Most employees believed that it was a genuine internal business email and, unbeknownst to them, leaked their annual wages.

Multimedia messaging giant Snapchat was also hit by email spoofing when their worker leaked his colleague's payroll information. An unidentified worker received a letter from the CEO. Since the used email seemed legitimate enough, the person complied with the request.

The difference between hacked and spoofed account

A hacked email account means that **the attacker managed to gain full access to your email account**. The emails that the hacker sends will genuinely come from your mailbox. This also means that they probably have access to more than just your email, but all the registered accounts. On the receiver's end, spoofing can look almost identical to a hacked account. Still, the difference is that **your mailbox is, in fact, untouched**. The email only appears to be originating from you, but it's actually from a completely separate account. The hacker doesn't need to take over your account, to spoof your email.

Reasons for Email Spoofing

Almost universally, email spoofing is a gateway for phishing. Pretending to be someone the recipient knows is a tactic to get the person to click on malicious links or provide sensitive information. Also, sending emails in someone's name is useful when gathering more data on the victim (e.g. by asking for confidential information from financial or medical institutions).

Related articles:

Tutanota vs. ProtonMail: which is the better secure email service?
22 October 2020