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.

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.

How Email spoofing works and Example

The goal of email 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.

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 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 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.

Spamming is a form of cyber-attack done purposefully to irritate the email service user making his email storage full or done with intention of harming or taking valuable data. Spam messages are unsolicited email messages sent in a bulk amount where the content of the email is not important to the recipient and remains full of unwanted or unrequested information, links or attachments. Some of them may be harmful to you or for your system also.

Types of spam

Spammers use many forms of communication to bulk-send their unwanted messages. Some of these are marketing messages peddling unsolicited goods. Other types of spam messages can spread malware, trick you into divulging personal information, or scare you into thinking you need to pay to get out of trouble.

Email spam filters catch many of these types of messages, and phone carriers often warn you of a "spam risk" from unknown callers. Whether via email, text, phone, or

social media, some spam messages do get through, and you want to be able to recognize them and avoid these threats.

Phishing emails

Phishing emails are a type of spam cybercriminals send to many people, hoping to “hook” a few people. Phishing emails trick victims into giving up sensitive information like website logins or credit card information.

Email spoofing

Spoofed emails mimic, or spoof, an email from a legitimate sender, and ask you to take some sort of action. Well-executed spoofs will contain familiar branding and content, often from a large well-known company such as PayPal or Apple. Common email spoofing spam messages include:

A request for payment of an outstanding invoice

A request to reset your password or verify your account

Verification of purchases you didn’t make

Request for updated billing information

Tech support scams

In a tech support scam, the spam message indicates that you have a technical problem and you should contact tech support by calling the phone number or clicking a link in the message. Like email spoofing, these types of spam often say they are from a large technology company like Microsoft or a cybersecurity company like Malwarebytes.

If you think you have a technical issue or malware on your computer, tablet, or smartphone, you should always go to the official website of the company you want to call for tech support to find the legitimate contact information.

Advance fee scams

This type of spam promises a financial reward if you first provide a cash advance. The sender typically indicates that this cash advance is some sort of processing fee or earnest money to unlock the larger sum, but once you pay, they disappear.

While it may not be possible to avoid spam altogether, there are steps you can take to help protect yourself against falling for a scam or getting phished from a spam message:

All of us can fall victim to phishing attacks. We may be in a rush and click a malicious link without realizing. If a new type of phishing attack comes out, we may not readily recognize it. To protect yourself, learn to check for some key signs that a spam message isn't just annoying—it's a phishing attempt:

Sender's email address: If an email from a company is legitimate, the sender's email address should match the domain for the company they claim to represent. Sometimes these are obvious but other times the changes are less noticeable, like example@paypa1.com instead of paypal.com.

Missing personal information: If you are a customer, the company should have your information and will likely address you by your first name. A missing personal greeting alone isn't enough to spot a phishing email, but it's one thing to look for, especially in messages that say they are from a company with whom you do business. Receiving an email that says your account has been locked or you owe money is cause to worry, and sometimes we rush to click a link in order to fix the problem. If it's phishing, that's exactly what the sender wants, so be careful and check if the email is generic or addressed specifically to you.

Links: Beware of all links, including buttons in an email. If you get a message from a company with whom you have an account, it's wise to log in to your account to see if there is a message there rather than just clicking the link in the message without verifying first. You can contact the company to ask if a suspicious message is legitimate or not. If you have any doubts about a message, don't click any links.

Grammatical errors: We all make them, but a company sending out legitimate messages probably won't have a lot of punctuation errors, poor grammar, and spelling mistakes. These can be another red flag to indicate that the email could be suspect.

Too-good-to-be-true offers: Many phishing messages pretend to be from large, well-known companies, hoping to ensnare readers who happen to do business with the company. Other phishing attempts offer something for free like cash or a desirable prize. The saying is often true that if something sounds too good to be true it probably is, and this can be a warning that a spam message is trying to get something from you, rather than give you something.

Attachments: Unless you are expecting an email with attachments, always be wary before opening or downloading them. Using anti-malware software can help by scanning files that you download for malware.

Report spam

Email providers have gotten pretty good at filtering out spam, but when messages make it through to your inbox, you can report them. This is true for spam calls and

text messages, as many carriers give you the ability to report spam as well. You can also choose to block the sender, often in the same step as reporting the message.

Reporting spam can help your email provider or phone service carrier get better at detecting spam. If legitimate emails get sent to your spam filter, you can report that they should not be marked as spam, and that also provides useful information on what should not be filtered. Another helpful step is to add senders you want to hear from to your contacts list proactively.