ARE YOU BEING "SPOOFED"?

This Specific Type of SCAM Is Hard To Catch – By Monica Torres

This sneaky, insidious act tricks you into sharing personal information — and it's all too easy to fall for. Here's how to spot it.

Spoofing scams are all too common, and they work because they take advantage of our trust.

Scammers win when they trick you into divulging personal information — and one of the simplest ways they can get you to do this is by impersonating someone you know.

When a bad actor pretends to be someone you trust or a legitimate retailer, this type of scam is known as "spoofing." With spoofing, scammers take advantage of "the fear and the curiosity that we have that this is somebody we know," said Amy Nofziger, the director of victim support for the AARP Fraud Watch Network.

One common tactic in a spoofing scam is to ***make an email address, text message, website or phone number appear like it's the real deal***. But even though it might have a similar or exact same display name, domain address or use the same call-to-action button as a trusted business, politician or boss, it's actually all a deceptive act to convince you into downloading malware or giving up your financial information.

Often, the trickery can only be revealed through minor details. Here are some of the most common ways you will encounter spoofing and what to watch out for:

Phone Spoofing:

Phone spoofing can be hard to spot because there are apps that can replicate caller IDs so that they can carry the display name of people you know, as well as the local area codes that you are familiar with.

Don't trust what you hear, either. In a 2023 "60 Minutes" segment, an ethical hacker used an application to create an AI-generated recording that mimicked the voice of one of the show's correspondents. Through this eerie likeness, the hacker was able to successfully ask a colleague to share that correspondent's passport number in a phone call.

In these cases, "the best thing you could do is say, 'I got to call you right back,' even if it's just one minute," said Cliff Steinhauer, the director of information security and engagement for the National Cybersecurity Alliance.

In the example of the "60 Minutes" colleague who got fooled, "if the [co-worker] had hung up and called her boss back, she would have gotten her boss, not the attacker." To help prevent this kind of spoofing, set up a code word you can ask for as a verifying test, Steinhauer suggested.

Overall, the big telltale sign that the caller is a scammer is not in how legitimate they appear or sound, but in what they are telling you to do. It can be normal to receive a random call that shares information with you like a prescription available for pickup from the pharmacy. But ***you***

should be suspicious if the caller urgently needs you to give up sensitive information in order to continue the conversation.

"If they're saying, 'Your child is hurt and you need to send us an insurance payment right now with prepaid gift cards or cryptocurrency,' they're asking you for something, and that's the biggest red flag," Nofziger said.

Email Spoofing:

Upon first glance, a spoofed email may look reliable. Scammers will often use sender addresses that look like it's coming from a known company or authority figure.

Sometimes, a tiny typo can be the biggest clue that something is amiss, so watch out for emails that have misspellings or unusual syntax. Steinhauer shared an example where an email attacker was using actual vendor's domain name, with the same name and signature, but "the only thing that was different was the spelling of the company's name."

The good news is that email authentication technology that many businesses use can block emails from suspicious senders or confine them to a spam folder. But "if those things aren't set up correctly, then it's possible for attackers to spoof your email addresses," Steinhauer said.

What can be tricky too in these cases is how there can be no obvious typos at all and the email can have the same addresses, logos and branding that you would be familiar with.

So, watch out if the email is supposed to be internal, but you get an alert that it appears like it's coming from an external sender. "Mail being marked as junk or being marked as spam — that could be an indication that somebody has compromised the DNS of the mail service, and they've somehow tricked it into sending an email from another domain," Steinhauer said.

Uniform Resource Locator (URL) Spoofing:

Sometimes, the email or text may be worded correctly, but the attachment or hyperlink you are being asked to click is the suspicious sign.

Many times, scammers will create look-alike URLs that appear legitimate until you look more closely at the punctuation or wording. Drive-google.com is an insecure imitation domain, for example, while drive.google.com is not.

Usually, when you're on a computer, you can hover over the link with your mouse, and you can see the URL that you're going to be taken to. Be wary if the email or website has a link that has been shortened through a service like Bitly so you cannot see where the link will go, Steinhauer said: "It can mask the actual destination of the link." In these cases, it's better to avoid clicking.

Steinhauer gave the example of a random text from a politician that is asking you to donate to their campaign with a link. Instead of clicking a suspicious URL that has been shortened, it's better to just go to that candidate's website directly, he suggested.

Are You Being “Spoofed”?

And if you get an unsolicited email from a business you interact with like an airline, “just go directly to the website that you want to visit,” Nofziger recommended, instead of clicking links within that email.

There are a few steps you can take to protect your information if you believe you've been spoofed.

What To Do If You Get Spoofed:

If you do end up clicking that fraudulent link or you reply to someone you thought was a real authority figure, your next steps depend on where it happened and what you ended up sharing.

Report it:

Immediately let your IT department know you got fooled if it happens at work, Steinhauer suggested.

“If you realize you’ve clicked a link, hopefully you stop there, close out of it, and then send your help desk a ticket,” he said.

If it involves your finances, report what happened to your bank or credit card, too, because they can put a temporary freeze on your accounts. You can also **report the spoof to the FTC.**

Reset passwords and update your computer:

If you believe you may have shared more than you should have with a potential scammer, you need to bolster your online security.

For good cybersecurity, you should continue to install the latest patches and updates on your computer network, authorize multifactor authentication if you have not, and reset your passwords.

If it involves your finances, report what happened to your bank or credit card, too, because they can put a temporary freeze on your accounts. You can also report the spoof to the FTC.

Reset passwords and update your computer:

If you believe you may have shared more than you should have with a potential scammer, you need to bolster your online security.

For good cybersecurity, you should continue to install the latest patches and updates on your computer network, authorize multifactor authentication if you have not, and reset your passwords.

And if you do answer, stay mum if you start getting detailed requests for information.

“Never give out personal information such as account numbers, Social Security numbers, mother’s maiden names, passwords or other identifying information in response to unexpected calls or if you are at all suspicious,” the Federal Communications Commission warns on its website about spoofing.

Avoiding spoofs means treating every email or call with some healthy caution. It can be annoying to seek out extra verification when you feel doubt, but the consequences of dealing with a stolen identity are worse.