Strengthen Your Electronic Defenses

By J.J. Montanaro, a *certified financial planner with USAA*

Comments by Alan B. Power

Consumers reported losing more than S10 billion to fraud in 2023, according to the Federal Trade Commission. That's a staggering number and an indicator that this trend likely won't end soon, as fraudsters' efforts are paying off. *And that number is only what the Federal Trade Commission was aware of.*

Here are five steps you can take in 2025 to avoid falling victim to phishing or smishing scams:

Be deliberate.

Don't get caught up in the emotion the fraudster is trying to fuel. Whether it's excitement at the idea of winning a prize or the fear of a loss, step back and assess. Discuss the communication you received with a friend, family member or colleague. Often, someone else's perspective is all you need to avoid getting caught up in fraud.

This is especially true with Phishing emails asking you to accept big money from a foreign country to give away to the poor, sickly, or disadvantaged – and – oh, by the way – you get to keep part of it. Just delete them and never provide them with any of your information.

Pay attention to detail.

If you receive an email purporting to be from one source and the *email* address does not match, that's probably an indicator something is off. Funky formatting, graphics or grammar are signs, too. Hover over any links to see where they direct you. <u>You are not going to click</u>, because you know better, but that simple action may confirm your suspicions.

Do not respond to suspicious emails. Any time you have a doubt, pick up the phone and call the person or go online separately – not through the links provided in the email. Keep in mind, the really good fraudsters can even mask their email and substitute it with an email that looks like it came from someone you know. If something doesn't look right, don't bite.

Be proactive.

If you aren't certain, reach out directly to the institution or organization that may be - but is probably not - reaching out to you. Use a number you know or search for it on your own. Don't use a number *or a link* provided in the suspicious communication.

Look before you leap. There are so many scams out there now, it is better that you err on the side of caution vice getting caught up in something.

Avoid attachments and links.

Don't open attachments or click on links unless they come from a trusted source, and you are expecting them. This misstep could result in you accidentally sharing information with a fraudster or even unleashing malware on your phone or computer.

Don't click on an attachment or bill or invoice they have sent. Only click on an attachment from a legitimate source. If you have any doubt, call the person who it came from and verify that they sent an attachment. Attachments can have a hidden virus' that could activate when you try to open it – such as a key logger that would monitor all of your keystrokes and report it back to the fraudster. You would never know it was there but the fraudster would be able to obtain all of your keystrokes or possibly have access to all of your files.

Buy a good virus software and keep it updated. Do not depend on "free" virus software. Why? Because there is no guarantee they will stop a potential virus. You are better off paying the money for a good virus software and being safe.

Keep personal info personal.

Legitimate organizations won't reach out to you for your personal information, ever. Someone directly or indirectly, through a text or email - trying to elicit your Social Security number, bank account number or other personal info - is coming at you from the dark side. No matter the supposed urgency of the request, ignore the urge to share.

And if you don't feel comfortable with sharing, tell them. If they persist, something is wrong.

Be smart and don't get scammed. Don't be one of the ones that the fraudsters take advantage of. Many have been trained to do this and sometimes it is very hard to tell. Just be wary if someone asks you to respond (via email) to an email because they are busy and in a meeting and most certainly, if they want you to buy gift cards for someone.

When in doubt, don't do it. Some fraudsters have even created fake websites that look just like the real ones. Do not use the same password for all of your different sites that you access. If it gets compromised, you will have to change them all – very quickly. And even though it is a pain use complex passwords and two-factor authentication. Sure it may take longer but then the crooks can't hack your bank account, investment account or order a new TV for themselves from Amazon.