Protect yourself from phishing scams so you don't fall prey to the next Twitter hacker

Humans are still our biggest cybersecurity weakness. Here's how to be smarter when it comes to avoiding scams through email and on your phone.

Don't give cybercriminals access to your accounts by accident.

Angela Lang/CNET

When dozens of celebrity Twitter accounts started promoting a Bitcoin scam one Friday in July, something was clearly going wrong down at Twitter HQ. By the end of the month, Twitter said certain employees had fallen for a scam and unwittingly helped hackers gain access to sensitive login credentials. The hacker, allegedly a teenager in Florida who's now charged with 30 felonies, tapped the usernames and passwords to access an internal system at Twitter and take control of high-profile accounts. The breached accounts included those of Elon Musk, Bill Gates and presumptive Democratic presidential nominee Joe Biden.

Maybe you aren't in control of extremely sensitive passwords that could let someone take over the communications channels of tech luminaries and

presidential hopefuls. But in your work or personal life, chances are you have access to a system or account that hackers would like to breach. The prize could be customer data that would help identity thieves do their work, your company's intellectual property or even your personal income data, which could help someone steal your tax refund or file for unemployment benefits in your name.

That access means you, too, could be the target of spear-phishing, a juiced-up hacking technique that tries to trick you into handing over login credentials or download malicious software. Twitter says the attack targeted employees on their phones, which means the hackers could have used phone calls or text messages to mislead their targets. Spear-phishing attacks also often take place over email. The attacks typically pair an urgent sounding message with credible-sounding information specific to you, like something that could have come from your own tax return. These scams are extra hard to avoid falling for, because they aim to override any red flags you might notice about the email with details that make the sender sound legitimate.

When Twitter employees fell for a spear-phishing trick, Democratic presidential candidate Joe Biden's Twitter account was compromised and pushed a cryptocurrency scam. CNET has blocked out the address that hackers included in the tweet.

Screenshot by Queenie Wong/CNET

Despite corporate training and stern warnings to be careful who you give your password to, people do fall for these tricks. We wouldn't know the reported contents of former Hillary Clinton campaign chair John Podesta's emails, including his technique for making risotto (hint: keep stirring!), if he hadn't entered his personal username and password into a fake form designed by hackers specifically to capture his credentials.

Another consequence of falling for a spear-phishing scam could be downloading malicious software, like ransomware. You could also be convinced to wire money

to a cybercriminal's account. Still, you can avoid falling for these scams by taking these security habits to heart. Here's how to avoid a spear-phishing scam.

Know the basic signs of phishing scams

Phishing emails, texts and phone calls try to trick you into visiting a malicious website, handing over a password or downloading a file. This works in email attacks because people often spend the whole day at work clicking on links and downloading files as part of their jobs. Hackers know this and try to take advantage of your propensity to click without thinking.

So the No. 1 defense against phishing emails is to pause before clicking. First, check for signs the sender is who they claim to be:

- Look at the "from" field. Is the person or business's name spelled correctly, and does the email address actually match the name of the sender? Or are there a bunch of random characters in the email address instead?
- While we're at it, does the email address seem close, but a little off? E.g. Microsft.net, or Microsoft.co.
- Hover your mouse over any links in the email to see the true URLs they will send you to. Do they look legitimate? Remember not to click!
- Check the greeting. Does the sender address you by name? "Customer" or "Sir" would be red flags.
- Read the email closely. Is it generally free from spelling errors or odd grammar?
- Think about the tone of the message. Is it overly urgent or trying to get you to do something you normally wouldn't?

Don't fall for more advanced phishing emails that use these techniques

Even if an email passes the initial smell test outlined above, it could still be a trap. A spear-phishing email might include your name, use more polished language and seem specific to you. It's just plain harder to notice. Then there are targeted phone calls, in which someone calls you and tries to manipulate you into handing over information or visiting a malicious website.

Because spear-phishing scams can be so tricky, there's an extra layer of caution you should apply before acting on a request that comes over email or the phone. The most important of these extra steps: guard your password. Never follow a link from your email to a website and then enter your account password. Never give your password to anyone over the phone.

Banks, email providers and social media platforms often make it policy to never ask for your password in an email or phone call. Instead, you can go to the company's website in your browser and log in there. You can also dial back to the company's call customer service department to see if the request is legit. Most financial institutions, like your bank, will send secure messages through a separate inbox you can access only after you've logged onto the website.

Beat phishing by calling the sender

If someone sends you something "important" to download, asks you to reset your account passwords or requests that you send a money order from company accounts, call the sender of the message -- like your boss, your bank or other financial institution, or the IRS -- and make sure they really sent it to you.

If the request came by phone call, you can still pause and double check. For example, if someone says they're calling from your bank, you can tell the caller you're going to hang up and call back on the company's main customer service line.

A phishing message will often try to make the request seem incredibly urgent, so you might not feel inclined to add an extra step by calling the sender to double-check. For example, an email might say that your account has been compromised and you need to reset your password ASAP, or that your account will expire unless you act by the end of the day.

Don't panic. You're always in the right if you take a few extra minutes to verify a request that could cost you or your company financially, or damage your reputation.

Lock down your personal information

Someone who wants to spear-phish you has to get personal details about you to get started. Sometimes your profile and job title on a company website will be enough to tip off hackers that you're a valuable target for one reason or another.

Other times, hackers can use information they find about you in data breaches. There's not much you can do about either of those things.

But sometimes you're spilling information about yourself that can arm hackers. This is a good reason to set your social media accounts to private and not post every detail of your life on Twitter.

Finally, enable two-factor authentication on your work and personal accounts. It's a service that adds an extra step to the login process, and that means hackers need more than just your password to access sensitive accounts. That way, If you do hand over your credentials in a phishing attack, hackers won't have everything they need to log in and wreak havoc.

Follow these steps and you'll be prepared to avoid the pain of getting spear-phished. These tips are also good for avoiding coronavirus scams as well as tax scams. While you're learning how to stop hackers from making your life harder, you can also avoid getting malware on your Android phone and keep it safe even if it's refurbished.