Five simple tips for better cybersecurity

October 23 2023, by Kyle Shaner

With news of hacking attempts and data breaches, protecting your information online can seem like a daunting task.

However, some simple steps can reduce your risks of being victimized online, said Hazem Said, head of University of Cincinnati's School of

Information Technology and co-director of the Ohio Cyber Range Institute.

For Cybersecurity Awareness Month in October, Said offered five tips for better cybersecurity.

Use strong passwords and a password manager

While simple passwords are easier to remember, they're also easier to guess or crack. Complex passwords that are longer with uppercase and lowercase letters, numbers and special characters are more secure.

Passwords also shouldn't be reused across multiple accounts to limit the damage if a password would be compromised.

To remember all the complex passwords you have, a password manager can store them securely. Many phones, computers and web browsers have built-in password managers, or third-party options are available as well.

"This is a challenge for people, and with today's world, everyone needs to find a way that works for them, how their mind thinks and their lifestyle," Said said.

Turn on multi-factor authentication

Even if your password is compromised, you can add a layer of security by turning on multi-factor authentication. When you have multi-factor authentication enabled, additional information is required to login, such as a security code sent to your phone or email.

Users can set their preferences to select which multi-factor authentication method works best for them and to skip the step on

trusted devices.

"Our life is now digital. As we lock our homes and cars, we need to put locks on our digital life," Said said. "There are multiple ways to still make it convenient and accessible."

Recognize and report phishing

Phishing is when scammers send emails, phone calls, text messages or other messages in an attempt to trick people into revealing personal information, such as passwords or credit card numbers.

Signs of phishing attempts include urgent or threatening language, requests for sensitive information, things that seem too good to be true, suspicious sender email addresses, unsolicited information, suspicious attachments and spelling and grammatical errors.

As scams continue to get more sophisticated, it's important to slow down, especially when something seems off.

"I try to pause with every email I get and avoid opening messages that I didn't request," Said said. "If in doubt, assume it's phishing. We sometimes say, "Give people the benefit of the doubt." Don't give emails, phone calls or text messages the benefit of the doubt."

Email programs often give users an option to report junk or phishing emails. People also can forward phishing emails to their employer's information security staff or block senders.

Update software

Software and app developers routinely release updates to add new features to their products, fix bugs and improve security. By keeping

your devices up to date, you can reduce the risk of hackers being able to access your personal information.

One of the simplest ways to protect yourself is to set up automatic updates for software and apps. While it's OK to wait to install feature updates, you should install security updates as soon as possible.

"Don't wait, especially if it's a security update," Said said.

Be careful about where you share your information

You should be careful about where you share information, particularly financial and other sensitive information.

By limiting the number of places your information is stored, you can reduce the chances of it being compromised. If you do share personal information, ensure the organization you're sharing it with is reputable.

"We live in a digitally connected world," Said said. "Enjoy it with caution."

Provided by University of Cincinnati