October is Cybersecurity Awareness Month

Four Simple Steps to Staying Secure

From: Ouch! Newsletter, www.sans.org

Using today's technology safely and securely can seem overwhelming and confusing. However, regardless of what technology you are using or how you are using it, here are four simple steps that will help you stay secure:

YOU are your best defense. Technology alone cannot fully protect you; you are your best defense. Attackers have learned that the easiest way to get what they want is to target you rather than your computer or other devices. If they want your password, credit card, or control of your computer, they'll attempt to trick you into giving it to them, often by creating a sense of urgency. For example, they might call you pretending to be Microsoft tech support and claim that your computer is infected, when in reality they are just cyber criminals who want you to give them access to your computer. Or perhaps they send you an email warning that your package could not be delivered and pressuring you into clicking a link to confirm your mailing address, when in reality they are tricking you into visiting a malicious website that will hack into your computer.

Use strong passphrases and two-step verification. Modern technology has made the old, eight-character password outdated and vulnerable. When a site asks you to create a password, create a strong and unique passphrase instead. A passphrase is a type of password that uses a series of words that is easy to remember, such as bee honey bourbon rain. The longer your passphrase is, the better. Use a different one for each device or online account. This way, if one passphrase is compromised, your other accounts are still safe. Can't remember all those passphrases? Use a password manager, which is a specialized program that securely stores all your passphrases in an encrypted format.

Also, enable two-step verification (also called two-factor or multi-factor authentication). It uses your password but also adds a second step, such as entering a code sent to your smartphone or from an app that generates the code for you. Enabling two-step verification is probably the most important step you can take to protect your online accounts, and it's easier than you may think.

Keep software current. Make sure each of your computers and mobile devices is running the latest version of its software. Cyber attackers are constantly looking for new vulnerabilities in the software your devices use. When they discover vulnerabilities, they use special programs to hack into the devices you are using Meanwhile, the companies that created the software are hard at work fixing the vulnerabilities by releasing updates. By ensuring your devices install these updates promptly, you make it much harder for someone to hack you. To stay current, simply enable automatic updating whenever possible. This rule applies to almost any technology connected to a network, including internet-connected TVs, security cameras, routers, gaming consoles, and even your car.

Plan for backup and recovery. No matter how careful you are, you still may be hacked. If that is the case, often the only way to restore all of your personal information is from backup. Make sure you make regular backups of any important information and verify that you can restore your data from them.

INVESTORS
COMMUNITY BANK

www.InvestorsCommunityBank.com

EQUAL HOUSING OPPORTUNITY

MEMBER **FDIC**