FS-ISAC

FIRST COMMUNITY BANK OF MOULTRIE COUNTY

Security Tips Newsletter

October 2023 | Issue No. 3

Security is Everyone's Responsibility

Meeting the Challenge to be Cyber Safe

Key Points

- You are the target of cyber criminals
- Cybersecurity awareness is available to reduce your risk
- There are four key behaviors for improved self-protection

Most consumers are unaware that malicious cyber activity is a criminal enterprise, and like any business, there is a business model based on profit. Within its structure are various teams comprising leadership, marketing, operations, security, business development, and more. *You are their customer/victim target*. The below rewards of good cyber hygiene will help you remain cyber safe!

There are also other considerations such as a person's awareness and the sophistication of the scam. It's important for consumers to consider these factors now, especially as the holiday season nears. October 2023 is Cybersecurity Awareness Month. Since 2004, October has been a dedicated month for the public and private sectors and tribal communities to work together to raise awareness about the importance of cybersecurity. This Cybersecurity Awareness Month will focus on four key behaviors:

- Use strong passwords and a password manager
- Turn on multi-factor authentication
- Recognize and report phishing
- Update software

Risk	Reward
Not using long, unique, and complex passwords. Would you leave all your most precious valuables in a tin box with a plastic zip-tie? Of course not. However, if you're using short, common, and simple passwords for each online account or reusing passwords, that is what you're doing. With compromised passwords, cybercriminals can access banking accounts, take over, wire transfer money, or make online purchases.	First, verify if your email address(es) has been compromised at https://haveibeenpwned.com. If so, there is a strong likelihood that your password has been compromised too. Next, *create a new long, unique, and complex passphrase like "1mnevergonn@BaVictim" for each account or use a password manager that can generate and store all of your passwords, so you only need to remember a single long, unique, and complex passphrase*.
Not enabling or using multi-factor authentication. Using the above illustration, if you had the opportunity to place your most precious valuables in a vault but didn't, your valuables would still be vulnerable. You risk losing them, perhaps never regaining them.	Multi-factor authentication is a cybersecurity measure for an account that requires anyone logging in to prove their identity multiple ways. *Multi-factor authentication makes it extremely hard for hackers to access your online accounts, even if they know your password, thus adding greater security to protect your assets. Implement multi-factor authentication for any account that permits it, especially any account associated with work, school, email, banking, and social media*.
Not uploading and installing software patches timely. Failing to patch the multitude of applications is akin to leaving your keys in the front door and securing your safe with scotch tape.	Every day, software and app developers focus on keeping their users and products secure. *If you install the latest updates for devices, software, and apps, not only are you getting the best security available, but you also ensure that you get access to the latest features and upgrades*.