FS-ISAC

JTNB
Jim Thorpe Neighborhood Bank

Security Tips Newsletter

January 2024 | Issue No. 6

Security is Everyone's Responsibility

Starting Your Year Off Right

Summary

Do you work hard for the money you earn? We feel you do. We work diligently behind the scenes to protect your information and money from fraudsters, but security is a shared responsibility between us. That's why [INSERT YOUR INSTITUTION NAME] wants to ensure you start 2024 on the right track.

Prevention Tips

Improve password security. Passwords are one of the most vulnerable cyber defenses. Improve your password security by doing the following:

- **Create a strong password.** Use a strong password that is unique for each device or account. Longer passwords are more secure. An option to help you create a long password is using a passphrase - four or more random words grouped and used as a password. To create strong passwords, the National Institute of Standards and Technology (NIST) suggests using simple, long, and memorable passwords or passphrases. (See Choosing and Protecting Passwords)
- **Consider using a password manager.** Password manager applications manage different accounts and passwords while having added benefits, including identifying weak or repeated passwords. There are many different options, so start by looking for an application that has a large install base (e.g., 1 million plus) and an overall positive review. Properly using one of these password managers may help improve your overall password security.
- **Use multifactor authentication, if available.** Multifactor authentication (MFA) is a more secure method of authorizing access. It requires two out of the following three types of credentials: something you know (e.g., a password or personal identification number [PIN]), something you have (e.g., a token or ID card), and something you are (e.g., a biometric fingerprint). Because one of the required credentials requires physical presence, this step makes it more difficult for a threat actor to compromise your device. (See Supplementing Passwords)
- **Use security questions properly.** For accounts that ask you to set up one or more password reset questions, use private information about yourself that only you would know. Answers that can be found on your social media or facts everyone knows about you can make it easier for someone to guess your password.
- **Create unique accounts for each user per device.** Set up individual accounts that allow only the access and permissions needed by each user. When you need to grant daily use accounts administrative permissions, do so only temporarily. This precaution reduces the impact of poor choices, such as clicking on phishing emails or visiting malicious websites.
- **Choose secure networks.** Use internet connections you trust, such as your home service or Long-Term Evolution connection through your wireless carrier. Public networks are not very secure, which makes it easy for others to intercept your data. If you choose to connect to open networks, consider using antivirus and firewall software on your device or using a Virtual Private Network (VPN) service, which allows you to connect to the internet securely by keeping your exchanges private. When setting up your home wireless network, use Wi-Fi Protected Accessed 3 (WPA3) encryption. All other wireless encryption methods are outdated and more vulnerable to exploitation. (See Securing Wireless Networks)

- **Keep all of your personal electronic device software current.** Manufacturers issue updates as they discover vulnerabilities in their products. Automatic updates make this easier for many devices—including computers, phones, tablets, and other smart devices but you may need to manually update other devices. Only apply updates from manufacturer websites and built-in application stores, third-party sites and applications are unreliable and can result in an infected device. When shopping for new connected devices, consider the brand's consistency in providing regular support updates.
- **Be suspicious of unexpected emails.** Phishing emails are currently one of the most prevalent risks to the average user. The goal of a phishing email is to gain information about you, steal money from you, or install malware on your device. Be suspicious of all unexpected emails. (See Avoiding Social Engineering and Phishing Attacks)

If you realize you clicked or responded to a phishing email involving your FS-ISAC account, contact us immediately. You will need to change your passphrase. Additionally, you can report the incident to the FTC at ReportFraud.ftc.gov or the Internet Crime Center at www.ic3.gov. Please remember, that *security is everyone's responsibility*.