Objective 10

# Government and Financial Online Accounts

GETTING STARTED WITH TECHNOLOGY

## WHAT YOU NEED TO KNOW

**Is online banking safe?**

Financial institutions follow strict security protocols and are dedicated to monitoring threats and suspicious activity. They use varying security measures to keep their customers' information safe, including online. It is wise to contact your individual bank to review their security and protective measures for online banking.

Many of them will include encrypted email messaging, two-factor authentication, electronic signature verification, automatic logout when inactive online, and continuously monitoring activity.

## HOW THIS HELPS YOU

While a bank can monitor and track finances, it is vital for you, the customer, to be diligent as well. Banking technology will typically be able to spot suspicious activity and notify the customer. However, the account holder is just as vital in looking for unauthorized activity on the account. Review your account statements regularly to ensure all charges are correct.

## THINGS TO KEEP IN MIND

Never provide your personal information in response to an unsolicited request. If you believe the contact may be legitimate, contact the financial institution directly, either through the website you know or a phone number. Do not click the link in the email, text or pop up on your computer to visit that site.

Phishing schemes are one of the biggest concerns when looking at security issues and online banking. Phishing occurs when someone receives an email or text message purporting to be a legitimate financial institution. Often these scammers attempt to get critical information from the recipient, which can provide a window into getting inside someone's finances. These phishing scams often ask you to reply with account or social security numbers, birthdates, or even usernames and passwords.

Most banking institutions will not ask you for this information, especially directly through an email message. If you receive a message and are uncertain who it came from, delete it, then contact the bank or financial institution to see if it was a legitimate or phishing message.

## BEST PRACTICES

Taking a few proactive steps can enable you to take advantage of the convenience of online banking and bill pay. Implementing a few security measures at home, combined with the institution's cybersecurity tools will likely keep your banking data safe and secure.

**Use secure networks.** Using a trusted network is important for keeping intruders from using a public Wi-Fi network to spy on your online activity. Disconnect from any network that you don't know what level of security is used, or who is also on the network. Banking from a home network, or turning off Wi-Fi on a smart phone, can reduce the chances of someone breaching your personal information.

**Create strong passwords.** A password that is a combination of two or more words is considered more secure than a short phrase with special characters. But combining a few words and special characters/numbers will make it tougher to access.

**Change passwords regularly.** Many institutions will require you to change your password frequently, because it is a best practice for keeping information secure. Even if it is not required, it is recommended to change your passwords a couple times a year. It is also important to use different passwords for different accounts. If a hacker is able to crack the code between your username and password in one account, they will likely try that combination in other accounts. Be sure to keep unique, strong passwords for your most sensitive data.

**Set up alerts from your bank to notify you of suspicious activities.** In most instances, a bank will allow its customers to choose when they would like to receive notifications. Banks will typically monitor for fraudulent activity, but can also send messages for failed login attempts, deposits and payments, or low account balances.

**Be aware of phishing schemes.** If you are contacted via email or text message by someone claiming to be a bank representative, consider it suspicious. Most banks will not contact customers in a personal manner and will not ask for personal or banking information to be submitted through email or text.

**Choose a bank or credit union that has industry-standard security technology.** Not all banks will employ the same security measures for their banking accounts. Contact a few area institutions to see what security protocols they use to keep data protected.

**What to do if you fall victim to an attack.**
Contact your financial institution immediately. If you have disclosed sensitive personal information in a phishing attack (I.e. a social security number), you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening new accounts in your name.