Stay Secure Online

Questions to ask yourself:

Do you use virus protection software?

Do you use anti-phishing software?

Do you have the latest versions of internet browsers, with pop-up blockers and up-to-date patches?

Have you changed your passwords lately?

Do you have all of your data backed up in a safe place?

Social Engineering

Social engineering is an attack aimed at human beings rather than systems. Instead of breaking into computer networks or systems, social engineers use psychological tricks to get access to your personal information. The bad guys exploit your good faith and helpfulness, or perhaps your insecurity or fear; all with the sole purpose of gaining information.

How to protect yourself:

• Share as little personal information about yourself as possible. Specifically, be very economical with PERSONAL information on social media sites such as Facebook, Twitter, Google+, etc.

• Be wary of online surveys that ask personal information, or emails that request clicking a link and giving personal information.

• Remember this always: No reputable financial institution will never ask you for more than the last four digits of your social security number and will NEVER ask you for your password or PIN.

• Never share your passwords with another person. Co-workers, bosses and system administrators should have their own, and won't need yours.

• Be suspicious of emails that ask a lot of questions or don't "feel right." Just because you recognize the address, doesn't mean the email is legitimate. Fraudsters can "spoof" the email addresses of friends or family.

• When in doubt, type in the address of the site in question or use a bookmark, don't casually click on an email link.

• When in doubt, be suspicious. When asked questions about your finances or private information, don't divulge anything, and let us know immediately.

Creating Safe Passwords

Passwords are a key component of securing your online information and are the first defense against online attacks.

Here are some good guidelines:

1. Use different passwords - Using the same password for every account is a bad idea. Always easier said than done, but, there are TWO places where we strongly suggest you make the password unique and extra hard: your primary financial institution and your primary email address.

2. Consider a passphrase - A passphrase is a sequence of words, rather than just characters. A passphrase is harder to crack and can be easy to remember. Don't use common sayings, quotes, or song lyrics, as they have all been added to cracker databases and aren't reliable. As good as they sound, "FourScoreAndSevenYearsAgo," or "IWillSleepWhenIAmDead," are not very secure.

3. MiX uP tHe cAsE - When mixed case is allowed, adding a combination of upper and lower case characters, or even just a few stray case shifts, can improve the strength of your password or passphrase. Just remember which ones you capitalized.

4. Use Speci@l Character$ - Again, if they're allowed, adding in non-traditional characters can improve password quality.

5. Avoid single words or names - Every word in the standard dictionary has been added to the cracker's programming and won't withstand an attack. In going after YOUR account in particular, a criminal will do some investigating and may know the name of your spouse, children, pet, high school mascot, and possibly even your sister's first cousin's brother's name.

6. Use longer passwords - It's true. A ten-character password is going to be harder to crack than a six character one. But if it's easy, it's still easy. Length by itself is not enough—quality is important too. A long AND well-formulated password is the best combination, as long as you can remember it without writing it down.

7. Don't write down passwords - You're probably going to write them down no matter what - how else to remember them? Here are two things you can do to make it just a BIT harder for the criminals. Don't put them in your wallet and don't leave them next to the machine (whether at home or office). If you MUST write them down, hide them very well, or use a software programs that will encrypt your list of passwords and make it hard to get into.