ONLINE SECURITY TIPS

The best way to stay ahead of fraud, identity theft, and compromised information is to inform yourself on some safeguard tips and safe practices, especially regarding your internet usage.

- Strong passwords are always a recommended security tip. Avoid using passwords with your birthdate, address, family, etc., as these are more predictable for hackers. The longer a password is, the more secure it is.
- Be sure that you have anti-virus and anti-spyware software on your computer. Make sure that you have them set up to update virus definitions regularly in order to stay protected.
- Browsers should always be closed when you are done using the web. Some browsers can retain information entered in login screens and other places until the browser is exited. Also, use the most current version of the browser available. Be sure to apply any updates to your desktop operating system and browser as often as they are available. Most of these updates are security updates.
- Never log into any online banking, online shopping sites or enter any personal information on a computer or device connected to a Wi-Fi Hotspot. These are not secure and an easy way to get your information compromised.
- It's a good idea to have your security software scan any attachment within e-mails. Every day people's e-mails get hacked/hijacked, and an e-mail from a friend can very well contain a virus or tracking malware without you knowing your computer has been compromised. Likewise, be sure you look at the e-mail addresses of mail you get, not just the name of who it is from. A common phishing scam is to appear to be from a legitimate company, only the e-mail is completely different and the link listed in the e-mail takes you to a clone website where they have you enter personal information. In addition, legitimate companies will never contact you by e-mail and demand that you go to a link to enter personal data, or to give out personal information through e-mail.
- Be aware, another ongoing scam involves sending a text message that your debit card or account has been temporarily blocked. They then have you call a phone number where they request personal information then tell you your account has been reactivated.
- Another scam to be aware of is when selling items on Craig's list or websites of that nature. A common scam is for a scammer to request to buy an item, then they send you a fraudulent cashier check for the item. Many times, they even make the check out for more than the item was sold for, then request you to Western Union them the difference. Many scams can be avoided and if you have any doubt you can call an officer at the bank to get advise on the legitimacy of a sale/check.
- Card skimming is still a prevalent scam used to steal debit/credit card information. A good practice is to either pay cash at restaurants, or only use your card at a register where it never leaves your sight. Also, be careful at gas pumps and ATMs. Skimming devices can be placed on top of the area where the card is swiped and on top of the PIN pad. This will allow your transaction to go through, but at the same time, your information is being stored.
- You should always check your statements regularly. Check into or call us regarding anything that seems irregular. Customers who monitor their accounts online discover problems sooner.
- It's also a good idea to check your credit report at least annually to ensure nothing irregular appears on it. Each year you are entitled to one free credit report from each of

the three major credit bureaus. The site we recommend for a free report is www.annualcreditreport.com

WEBSITES FOR MORE INFORMATION

The Federal Trade Commission (FTC) has a website that contains an abundance of helpful information.

Topics include:

- *Chatting with kids about being online
- *Identity theft
- *Disposing of old cell phones and more

www.FTC.gov (click on consumer information)
www.onguardonline.gov
www.annualcreditreport.com