Customer Security Awareness Guide

Identity Theft

Identity Theft, (ID Theft) is an ongoing problem for people that use computers and smart phones connected to the internet for communication, entertainment, shopping and banking. It has affected millions of people each year. ID Thieves may open credit card accounts, apply for loans, rent apartments and purchase phone services all in your name. They typically spend your money as quickly as possible, and in many cases, request a change of address so you do not receive bills for their activity. Most victims don't know that their private and personal information has been compromised until they apply for a loan or receive a call from a collection agency. Sewickley Savings Bank takes multiple security measures to ensure that your online banking sessions are secure. The first line of defense is a firewall that is used to protect our online customers. Our system follows a strict set of standards and routinely monitors all activity that passes through the firewall to ensure your data is safe and secure.

Here are some good tips that you can use to protect your Identity when online

- Don't disclose account numbers, social security numbers and credit card numbers over the phone or through email unless you know the person or organization.
- Protect your user name(s), passwords and any additional Personal Identification numbers "PINs". Never use your birthday or Social Security Number as a user ID or password. It is also a good idea to have a different password for every company's website for which you do business. Creating passwords that include letters, numbers and special characters is always best but sometimes difficult to remember. Try creating a master password or **passphrase** containing two or more words and a few numbers that is easy for you to remember. For special characters you could use the @ symbol in place of the letter "a" or some other special character code that only you know and can easily remember.

Once you have your master passphrase, you can customize it for each website you log on to by adding the first and last letter of the company that shows in the address bar. A master passphrase could be something like "dogc@t123" and to log on to Ebay you would use dogc@t123ey.

Sewickley Savings Bank employees will never ask you for your online banking password. If you receive a phone call or email message claiming to be from us asking you for your account information, please call us immediately at **412-741-5000.**

- You should install and run updates to your own firewall, anti-virus and anti-spyware software regularly. Some reliable security software companies include, Symantec, MacAfee, Microsoft, Zone Labs and AGV antivirus. Some vendors may even have a free trial period program downloadable at their website.

Additional precautions to protect your Identity

- Shred old receipts, paid off loan records and bank statements that are no longer needed. Also check for any old medical billing records that are no longer needed since they may contain your social security number.
- Watch your bank and utility account statements as they come in for any unauthorized activity. There will generally be a phone number you can call to report any suspicious transactions and resolve any errors.
- It is also a good idea to keep an eye on your credit report to make sure all of your credit accounts are in good standing with no errors or unauthorized opened accounts. You can request your free annual credit report from **AnualCreditReport.com**. You can also call the free service at **877-322-8228** or send your request by U.S. Postal Service to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Internet Phishing (Scams)

- Protecting yourself from fraudulent emails that come to you is also very important. Many ID Thefts occur when someone clicks on a link they receive in the body of an email message. It is very easy for a would be ID Thief to send you an email having it appear as if it came from a financial institution. They will also embed a link that will navigate your computer or smart phone to a fraudulent website where they hope you will input your private or personal information. This is known as Internet Phishing. Where ID thieves are literally fishing for someone's identify to steal and use to open new accounts and make purchases in your name.
Sewickley Savings Bank will never send you an email asking you to click on a link to their website to update your account information.

- Public WiFi locations are another place that ID Thieves will attempt to steal your personal information when you log on to the network. They may simply watch your communication for user names and passwords but if they have enough time, they could hack their way into your device to obtain private and personal information you may have stored in your device. A recently released report from digital security firm McAfee found that mobile banking applications are becoming a target for malicious software. Even with two-factor authentication, malware creators are finding ways to intercept security-related text messages to gain access to victims' bank accounts. It is always best not to access financial accounts on Public WiFi networks. You should also log off of Public WiFi networks when you do not need internet access.

Protecting your Debit Card

- Being a victim of debit card fraud is not something that any banking customers want to experience, but it happens. As long as there are people out to steal your money, you will have to practice vigilance when it comes to where you use your debit card.

Stand alone ATMs are those not found at bank branches and are prime targets for card skimmers,
which are makeshift devices mounted on card-insertion slots to record card data. Card information is then used to duplicate cards that are used to make unauthorized purchases and cash withdrawals. Fraudsters prefer these ATMs because they are not under the constant watch of bank associates and security cameras. Using ATMs in well lighted and high-traffic areas can reduce the chances of having your debit card skimmed.

ATMs are not the only places through which thieves like to steal debit card information. Payment terminals at gas stations are easy marks for card skimmers too. Especially at self service pumps. As with stand alone ATMs, gas pumps are easily accessible for the installation (and removal) of skimmers. Also, when using a debit card at a restaurant make sure to watch the waiter or waitress charge the card to ensure that there is no debit card fraud occurring.

Using and sharing these precautions is the best way to protect yourself and loved ones from Identity Theft. However if you or someone you know thinks that they are a victim of Identity Theft, you should contact **Sewickley Savings Bank** immediately and then call the fraud department of the three major credit reporting agencies.

Equifax: 800-525-6285 Experian: 888-397-3742 Trans Union: 800-680-7289

You will want to close any other compromised bank accounts and open new accounts to obtain new debit and credit cards. You should also contact the Federal Trade Commission at their Identify Theft Hotline 877-ID-THEFT (877- 438-4338). They will add you to the national consumer fraud database that is shared by local, state and federal law enforcement agencies to help in catching ID Thieves before they can cause additional damage.

VIEW MORE WAYS TO PROTECT YOUR FINANCIAL INFORMATION
AT
www.onguardonline.gov