Protecting Yourself from Identity Theft

Identity theft is everywhere. In fact, according to a 2013 report by Javelin Research, there is one incident of identity fraud every two seconds. While we cannot prevent all identity theft, there are many steps you can take to reduce your risk of you becoming the next victim of fraud and identity theft.

In an effort to educate our clients, Regent Bank has provided you with the following information and tips about identity theft, fraud, and internet security.

How Does Fraud and Identity Theft Happen?

Identity thieves have become extremely creative on how they can steal your personal information. Here is a list of some of the most common methods of online fraud and identity theft:

Dumpster Diving

Thieves rummage through your trash looking for bills, account statements, or other paperwork with your personal information on it.

Skimming

Skimming happens when a thief takes your credit/debit card numbers by using a storage device when processing your card transaction. Skimmers can be found anywhere credit/debit cards can be ran, including ATM's and self-pumps at gas stations.

Old-Fashioned Stealing

Thieves steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information.

Phishing

Phishing is an attempt to get you to share your personal information with the thief. It usually comes in the form of an email from someone posing as your bank or other official entity. The email is usually instructing you to "verify" your information, which is then used to take over your accounts and identity. If you receive a suspicious email, delete the message immediately.

Smishing

Smishing is very similar to "phishing". However, smishing is when a fraudster sends a SMS text message to a mobile phone. This text message will prompt you to give information, including a name, date of birth, address, phone number, Social Security number, account number, password, etc.

Pharming

Pharming is when a computer hacker redirects a website to a bogus website that mimics the appearance of the original, in order to obtain personal information. These hackers use the information entered on this website to access your back account, steal your identity, or commit other fraud in your name.

Keystroke Logging or Keylogging

Keyloggers are "Trojan" software programs that can detect and copy any files opened on your computer, internet pages visited, information keyed in, and much more. Once the virus is on your computer, fraudsters can record your actual keystrokes and mouse clicks. Passwords and personal information can be stolen by using this method. It is very important to keep your anti-virus and anti-spyware programs up to date to protect your computer from these types of viruses.

How You Can Help Protect Yourself and Your Computer

Regent Bank will do our part to protect your information; however, you play an important role in protecting your accounts. There are a number of steps you can take to ensure that your Regent Bank information remains confidential.

- Keep your user ID and PIN to yourself.
- Do NOT use the save password option on your computer.
- Change your password as often as you wish. (We recommend doing so every 90 days)
- Log out of Online Banking properly prior to visiting other Internet sites.
- Don't use an ID or a PIN that is obvious or easily accessible. Avoid the use of any part of your name, birthdays, children's names, etc.
- Memorize your password! The best password is useless if it can be found written.
- Review your account information often. Report any unusual activity immediately.
- Avoid using public internet access terminals when conducting online banking.
- Never give account information to anyone over the telephone unless you initiated the call.
- Email is not a secure communication device so make sure you do not send any personal information such as account numbers, Social Security number, ID numbers, or PIN numbers by email.
- Never respond to emails asking for any sensitive information.

Keeping Your Computer Safe

- Use a current internet browser with 128 bit encryption that supports secure and private transactions.
- Use the built-in security features that some browsers provide. Choosing certain security settings and options will help protect the privacy of your accounts and personal information.
- The Help Option or Properties on your browser should provide you with the security options available on your system.

- Keep your operating system and Internet browser updated with patches from the vendor's website. For example, use Microsoft's Windows Update feature and install the Critical Updates and Service Packs since these address critical security issues
- Use virus and spyware protection software and update the software regularly in order to detect new threats.
- Use personal firewall software, especially if you connect to the Internet with a broadband (i.e. cable or DSL) connection.
- If your computer is on a wireless network, ensure that the router settings are secure.
- Use caution when downloading files, installing software, or opening email attachments from unverified or unknown sources.
- If anyone else has access to your computer, clear your browser's cache to eliminate copies of web pages that have been stored on your hard drive.

Remember, Regent Bank will **never** send an email, text message, or initiate a phone call asking you for your personal information, such as account numbers, PIN numbers, Social Security numbers, etc. If you receive an unexpected email asking for any personal information, do not click on any links in the email. If you have received an email such as this, please notify us immediately.

Regent Bank takes the security of our customers' confidential information seriously. In relation to our Internet Services, Regent Bank complies with all current banking regulations and utilize the most up to date technology to maintain the integrity of your most sensitive information.

For a detailed description of how we collect, use, and retain our customers' information, please refer to our Privacy Policy.