Customer Security Awareness Program

Dear Warrington Bank Customer, September 2015

We want to help you protect yourself from online crime and fraud. We have put together this list of security tips to help you keep your online credentials safe from identity thieves, fraudsters, and other criminals. Proper individual user security measures are a critical part of keeping your identity and accounts safe in any online transaction ranging from your eBay purchases to checking your account balances on your smart phone or computer to filing your tax returns.

Awareness and Education for Online Banking Security

Cyber criminal attacks on individuals are at an all time high and the perpetrators are becoming more sophisticated all the time so it is important to be aware of the threats and to approach anything on the internet that involves your identity or account numbers with caution. Cyber criminals have done an impressive job of creating fake websites that mimic legitimate sites such as PayPal, the FDIC, and even the IRS in order to steal confidential information. It is an ugly truth that a large amount of identity theft and fraud is committed by family members and friends or acquaintances of victims who, because of these relationships, have relatively easy access to account numbers and passwords saved on computers.

The Warrington Bank employs state of the art security measures to help keep your accounts safe from would-be thieves, but there are a few things you can and should do to help ensure that criminals do not get their hands on your online banking information by compromising your computers or other devices. This information is relevant to all of your online financial and personal information with us and with other banks, businesses, and websites.

Social Networking Risks

Fraudsters have become adept at breaking into password-protected accounts by using information that some individuals readily provide to social networking sites such as favorite books, favorite foods, city of birth, etc. in order to fake their way through password reset processes and secondary verification systems. Think carefully before making any personal information publicly available, as most of it is very useful to an identity thief. Choose challenge questions carefully to avoid using information that could be obtained by identity thieves or readily guessed by a person with a basic knowledge about the target they are attempting to impersonate.

Password Security

It is difficult for online systems to differentiate a legitimate user from a malicious user who has obtained a legitimate user's password. For this reason, it is essential that users keep their passwords private and immediately report any suspected security violations. Below is a list of some common password choices to avoid:

- Your name, or a family member or pet's name
- Social Security, account or telephone numbers
- Any part of your physical address
- Anybody's birth date
- Other information that is easily obtained about the user
- A word in the English or any foreign dictionary, even spelled backwards
- A password used on another site

- Sequences: “12345678”, or “33333333”, “abcdefgh”

Security Practices to Help You Avoid Identity Theft

- Verify use of a secure session (https:// and not http://) when entering passwords on the internet.
- Pay attention to the URL (web address) that you are visiting! Fraudulent websites often create misleading web address like *https://www.somecompany.**com.AnotherWebsite.com**/* to trick users of a *https://www.somecompany.com/* into believing they are visiting a legitimate site where they have an account when they are really at a password harvesting spoof of the legitimate website. **This is a very common trick that scammers use to fool users into divulging passwords to fake copies of real websites!**
- No website or service will ever “lose” a user’s login information and request that the user provide it to the website or company. Requests involving this sort of statement are **always a scam 100% of the time** and usually involve some sort of coercive statement such as threatening the loss of funds if login credentials are not supplied in time.
- Avoid saving passwords to any computer.
- Always use Log Out buttons when you are finished to end your secure sessions. This helps prevent session hijacking attacks where hackers keep sessions open when you think they have been closed.
- Never leave computers unattended when using online banking services.
- Never access sensitive computer systems or websites from public computers at a hotel, library, coffee shop or when using your own devices over any public wireless access point.
- Offers for employment as a mystery shopper, payment processor, etc. where you are required to **use your personal account for someone else’s business purposes are never legitimate.**
- No legitimate business will attempt to move business funds through anyone’s personal account. **This is always a scam 100% of the time.** If you are approached to participate in such schemes, immediately contact local law enforcement, the FBI or the Federal Trade Commission to let them know.

We hope this information is helpful to you. If you have any questions or concerns please feel free to contact us and we would be glad to assist you with questions you may have about cyber security.

Glossary of terms commonly used in discussions of this type of threat:

Adware – The purpose of adware is to display ads. Some adware threats bombard you with so many ads you can hardly use your computer. This can be done to obscure the fact that your computer has been compromised.

Keylogger – A form of spyware, a keylogger captures everything you type including passwords and other sensitive information. Some keyloggers also capture screen shots, log your Internet browsing history, record anything copied to the clipboard, and more.

Phishing – Technique used by fraudsters to acquire username, password and other sensitive information simply by asking. Phishing often takes the form of fake bank emails or fake commercial websites asking for confidential information.

Trojan – A seemingly benign program (such as free games downloaded from the Internet or on a cell phone) that does something criminal in secret such as installing packages of other malicious software or hijacking your computer or phone to make expensive phone calls or even to send Phishing spam to other potential victims.

Malware – The term malware applies to any software whose purpose is malicious, including all other types described here.