Help Protect Yourself Against Cybercrime

The financial services industry, along with most other industries, has witnessed an increase in the number of criminals who are using the Internet for illegal purposes. Financial services firms, their advisors and their clients are targets simply because, as the old saying goes, that's where the money is.

Both personal and business related information is extremely valuable to criminals and in order to gain access to that information, they will attempt to steal the information when individuals log into a computer network. The most valuable information to criminals are the account numbers, social security numbers and other personally identifiable information which will help facilitate their attempts to gain access to your personal accounts via fraudulent withdrawals or other attempts at identity theft.

How do the criminals obtain this information?

There are multiple ways in which cyber criminals attempt to gain access to your personal information. On your personal computer, clicking on links, pictures, websites, downloading files, and so on, can all provide a route for a cyber criminal to gain access to your computer. Sometimes these criminals will then download a virus, spyware, or other program to your computer. For example, a keylogger could provide the criminal with a history of all the keystrokes that have made on your computer. By obtaining this information, the criminal potentially could acquire your login, password, account number and other sensitive information.

How can you be attacked in a Cyber Crime?

Simply by connecting to the Internet you are making yourself a potential target of criminals. Every day, criminals use automated tools to scan for unprotected or vulnerable computers. Criminals may target you specifically or you may be the subject of a random attack. Your computer may then be used to steal your personal information. Two examples are trojans and spyware. Trojans are a form of malware masquerading as something the user may want to download or install, that may then perform hidden or unexpected actions, such as allowing external access to the computer. A Trojan may be used to install a keylogger application. Your computer may, without your knowledge, be used to facilitate other crimes and attacks on others. Computers can be hijacked to provide storage of illegal data or it could be used as a platform to launch attacks or commit crimes against others.

The best way to protect yourself from cybercrime is to use common sense, be prepared and take precautions.

- Keep your operating system updated. The recommended and easiest way to get updates is to turn on Windows Updates. Purchase anti-spyware and anti-virus software and configure your software to automatically download and install updates.

- Always log out of any web sessions and close your web browser when you are finished conducting business such as banking or brokerage.

- Do not select any links provided in any unsolicited email by unknown sources. Please delete the email and delete/empty the email from your recycle bin.

- Do not respond to any unsolicited (spam) incoming emails or open any attachments contained within the email.

- Do not respond to an email requesting personal information or that asks you to verify your information" or to confirm your user id and password. Call the institution directly using a number from your credit card or latest statement to confirm the validity of the request. If you need to go to the institutions website then type in the URL (web address) yourself and do not use any links contained within the email.

- Have separate passwords for work related and non-work related accounts.

- Lock your mobile device with a passcode.

- Encrypt your files and folders.

- Utilize software that will allow you to remotely erase sensitive information from a device that is lost or stolen.

- Use a personal firewall to help prevent unauthorized access to your computer while you are online.

- Use caution when accessing public hot spots, particularly public hot spots which do not require you to enter a password in order to access the internet. Additionally, do not perform any sensitive transactions while utilizing these services such as logging into your bank or brokerage accounts.

- Do not share your login or password information with anyone else. Please change your password at least on a quarterly basis and change it immediately if you suspect that your password has become known by someone else.

Report an online security issue.

If you think your identity or online account has been compromised, please call your financial advisor or 1st Global Client Services at 1-877-959-8400.

Resources for more information:

MS-ISAC Tip -- Surf Safe On The Internet
http://msisac.cisecurity.org/daily-tips/Surf-Safe-on-the-Internet.cfm

US-CERT Shopping Safely Online
https://www.us-cert.gov/ncas/tips/ST07-001

National Cyber Security Alliance
http://staysafeonline.org/business-safe-online/

FTC Identity Theft Site
http://www.consumer.ftc.gov/features/feature-0014-identity-theft