SIGNATURE BANK®

# INFORMATION SECURITY NEWS BULLETIN

Autumn / Winter 2017

**IN THIS ISSUE:**

- Strong Passwords
- Ransomware
- Online Banking Safety
- Adding Cyber Security Software to Protect Your Accounts Even More

## Strong Passwords Are Your First Line of Defense.

Strong Passwords are unique, formed as long phrases that mix CAPITAL and lowercase letters, numbers and/or symbols, with a minimum of 10 Characters, such as:

mYp@SSW0rd1s$tr0NG

- Use a unique password for every online account that you maintain – at home, at your Bank, with retailers, clubs and trade associations, etc.
- Change your passwords regularly and with discipline - at least every 90 days.
- Never share your passwords, even with people that you trust – accidents happen!


## Beware of Ransomware.

Ransomware is a type of malware that locks your computer screen and prevents you from accessing files until you pay a ransom to the hacker. If your computer becomes infected by ransomeware all of your personal and company information will be compromised and your files will be inaccessible. And ransomware doesn't just encrypt hard drives—it can also affect backup, flash, and cloud storage.

### To avoid becoming infected with ransomware:

- Never open or download attachments from unknown sources. If in doubt, forward the email to your company's Information Security team.
- Never click any links from unknown senders.
- Never enable macros on Microsoft Office documents sent by parties that you do not recognize.
- Install software updates frequently.
- Back up your files regularly on a physical storage device whenever possible.
- Secure your backup in a safe place and disconnect the device from your computer when you aren't using it.

## Add Another Tool to Help Secure Your Accounts.

Install IBM® Security Trusteer Rapport® to maximize your Signature Internet Banking accounts' protection against cybercriminals and fraud. It's effective, easy to use and won't slow down your computer or impact other business applications. You'll find a link at the bottom of each page of Signature Internet Banking as well as on the Privacy & Security page of SignatureNY.com.

Download Trusteer Now

**For more information regarding Information Security and the steps that you can take to protect your data, please contact your Private Client Group.**

## Your Online Banking Security Starts with You.

The convenience of online banking has transformed the way the world does business, but nothing is completely foolproof when it comes to the internet. There are steps that everyone can take to make online banking safer and more secure.

- When accessing a financial website, always look for a domain address that starts with "https:"
  - The "s" indicates it is a secure site.
- Create a strong password for the site. If you have multiple banks or financial institutions, use different passwords for each of them.
- Make sure your operating system is up-to-date with the latest updates or patches.
- Take advantage of the additional security that an internet security software provider such as IBM's Trusteer Rapport can provide. You should do this for both PCs and Macs - Apple systems are not immune to becoming infected by viruses.
- If you are suspicious about an email from your bank, call the bank directly using the number on the back of your bankcard or from the official website to verify the email's authenticity. (For Signature Bank, call 1-866-SIGLINE)
- Never respond to an email that asks you to click on the link and fill in information via a pop up. Most banks are not going to ask you for your information via an email prompt. It is best to open your browser, type in your institution's URL, and enter your information as instructed.
- Avoid using a public computer to access your bank accounts.
- Avoid banking from your laptop or smart phone while on a public Wi-Fi system.
- Monitor your credit and debit card activity frequently and identify each transaction. If you see a transaction that is suspicious, call the credit card company and report it. If the transaction is fraudulent, you can request that it be reversed. You can also freeze the entire account and have a new card and number issued.

Taking these steps will make your information much safer and will allow you to take advantage of the convenience that online banking offers.

## **In the Next Issue:** The Multi-Billion-Dollar Scam of Business E-Mail Compromise

Business E-mail Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. To learn more about BEC now, visit SignatureNY.com and go to About Us > Privacy & Security > Cyber Security > Business Email Compromise and download the FBI's recent Public Service Announcement or, you can access the PSA directly by clicking the link below.

https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise