March 17, 2016

A Bank Customer's Guide to Cybersecurity

CYBERSECURITY, DIGITAL & TECHNOLOGY, FINANCIAL SERVICES
BY SCHNEIDER DOWNS PROFESSIONAL

The Federal Deposit Insurance Corporation (FDIC) recently published a special edition of its quarterly *FDIC Consumer News*, **titled** *"A Bank Customer's Guide to Cybersecurity."* **The piece is packed with great tips and information for consumers as they leverage technology for online shopping, online banking, bill paying and other financial transactions.**

The publication contains several articles directed to online consumers for improving computer and mobile device security, protecting against malicious software ("malware"), avoiding phishing scams, and safely using social networking sites. Listed below is a summary of the key takeaways from the articles.

PROTECT YOUR "CYBER HOME" WITH A SOLID FOUNDATION

This article used a great analogy, comparing cybersecurity to protecting your home. When people go on vacation, they lock the doors and windows, set the alarm, and have someone stop by daily to pick up the mail and switch a few lights on/off. Why? It makes their home less of an attractive target to would-be intruders. Cybersecurity is no different – if a determined "bad guy" really wants to break in and steal information, he will likely get in; but if you follow some fundamental security practices to make your information difficult to steal, you can slow down or deter the attacker's efforts. Some of the key practices include:

- ***Take extra precautions for logging into bank and other financial accounts*** This includes the use of "strong" passwords (including upper-case and lower-case letters, numbers, and symbols), avoiding the use of common words that are easy to guess, and most importantly, using a different password for different accounts – especially bank accounts!
- *Take precautions if you provide financial account information to third parties online.* Many people use "account aggregation" services that provide a single view of all (or many) accounts from different institutions – deposits, investments, insurance, etc. While this is convenient, consumers need to be very careful in selecting the service provider, since it requires them to share account login information with that third party. Make sure that you thoroughly research the provider before divulging your login information to them.
- *Periodically check your bank accounts for signs of fraud.* A good rule of thumb is to check your accounts at least once or twice per week (all bank and credit card accounts) and look for potential fraudulent transactions. Secure online access to accounts makes these reviews very quick and easy to do. If a potential unauthorized transaction is

identified, federal law generally limits your liability for unauthorized use of debit, credit, and (sometimes) prepaid cards; however, there are deadlines for reporting fraudulent transactions, particularly for debit cards. The sooner you detect a problem with your account and report it, the easier it is to fix. A good way to monitor account activity in real time is to receive text or email alerts on your cell phone confirming individual transactions.

- *Basic security tips.* The article also recommends several general computer security tips, such as keeping your software up to date, using anti-virus and personal firewall software, deploying only reputable security products on your computer, and ensuring that the wireless (WiFi) technology utilized is safe. One key activity to avoid is conducting your online banking through public hotspots (e.g., coffee shops and hotel lobbies). These hotspots are often configured with "open" access, which means that they do not enforce passwords or encryption of sensitive data. This allows an intruder to potentially "sniff" your information over the wireless network, opening you to fraud or identity theft.

GOING MOBILE: HOW TO BE SAFER WHEN USING A SMARTPHONE OR TABLET

Mobile devices, particularly smartphones and tablets, have permeated the U.S. consumer market. This article points out several ways to make mobile devices more secure, including:

Avoid apps that may contain malware, by only downloading them from trusted sources. Check with your bank to make sure you are downloading their mobile banking app from the correct location.

- Keep your device's operating system and apps updated
- Consider using mobile security software and apps to protect your device. Most of the major anti-virus brands (e.g., Webroot, McAfee, Norton) have mobile device protection products available.
- Use a password or other security feature to prevent unauthorized access to the device in the event your device is lost or stolen
- Back up data on your smartphone or tablet, by synchronizing to a PC at home or through a reputable cloud service
- Have the ability to remotely remove (i.e., "wipe") data from your device if it is lost or stolen. This can be accomplished through a mobile device security product or through a cloud-based service (e.g., Find My iPhone).

BEWARE OF PHISHING SCAMS: DON'T TAKE THE BAIT

Phishing is one of the most common methods that cybercriminals use to steal information. Through phishing, attackers send email messages that appear legitimate, and may contain names, email addresses and graphics for people or organizations that they trust (e.g., banks, retail stores, government agencies). Phishing messages often contain wording that expresses a sense of urgency, such as *"Your account has been compromised, and your assets have been frozen for your protection. Click here to regain*

access to your funds." The victims get tricked into opening malicious attachments in messages, clicking on links to malicious websites, or simply providing their personally identifying information (PII) or account credentials directly to criminals. A similar deception, known as "pharming," occurs when a hacker hijacks internet traffic and redirects someone from a legitimate website to a malicious (fake) website that looks identical. The FDIC article gives some sound advice on how to avoid becoming a victim of these scams, including:

- Be suspicious if someone contacts you unexpectedly online and asks for your personal information.
- Remember that no financial institution will email you and ask you to include sensitive information such as account numbers and PINs in your response.
- Assume that a request for information from a "bank" where you've never done business is probably a scam.
- Verify the validity of a suspicious-looking email or a pop-up box before providing personal information. A good way to verify links or buttons in emails or websites is to *hover* (don't click!) your mouse pointer over the links, and look at the bottom of your browser to see where the links are *really* pointing.

USING SOCIAL NETWORKING SITES: BE CAREFUL WHAT YOU SHARE

Social media is a very popular way for people to stay in touch with family and friends, meet new people, and interact with businesses like their bank. Of course, social media also provides a treasure trove of information for someone seeking to steal your identity. Identity thieves often create fake profiles on social networks, pretending to be legitimate businesses (including banks), and lure visitors into providing valuable information such as SSNs, bank account numbers, and passwords. Key points mentioned in the article to mitigate the likelihood of someone stealing your identity include:

- Check your security settings on social network sites, and block people who you don't want seeing your page.
- Take precautions when communicating with your bank – never include account information or PII on social media sites.
- Be cautious about giving access to third-party programs or apps, such as sites for games or quizzes, with the ability to use information from your social networking pages (e.g., "Login with Facebook"). These third-parties could be selling your information to people trying to commit fraud.
- Periodically search to see if someone has created a fake account using your name or personal information on social networking sites. It's not narcissistic to "Google" yourself occasionally – it's a good security practice!

Speaking of social media… Do you recall the "house" example earlier? If you're leaving town on vacation, don't announce it to the world through social media. That's an invitation to thieves to visit your unoccupied house and empty it while you're gone.

The special edition of this FDIC newsletter is available for free at www.fdic.gov/consumers/consumer/news/cnwin16. The back of the guide also features an eight-question quiz to test your knowledge of key information, and a checklist with ten simple things bank customers can do to help protect themselves from online criminals. These takeaways are important for everyone, whether a consumer, financial institution or business leader. This information is particularly useful for banks – it's recommended that banks download copies of this publication and consider placing those copies in lobbies and other customer traffic areas to help spread the word.

Schneider Downs has a team of security and banking experts who have the experience to advise you on these and other like matters, and are standing by to assist.

Contact us for more information regarding cybersecurity and visit the Our Thoughts On blog for more articles on related topics.

You've heard our thoughts... We'd like to hear yours

The Schneider Downs Our Thoughts On blog exists to create a dialogue on issues that are important to organizations and individuals. While we enjoy sharing our ideas and insights, we're especially interested in what you may have to say. If you have a question or a comment about this article – or any article from the Our Thoughts On blog – we hope you'll share it with us. After all, a dialogue is an exchange of ideas, and we'd like to hear from you. Email us at contactSD@schneiderdowns.com.