Protecting Against Cybercrime

FIRST NATIONAL BANK OF DENNISON

What is Cybercrime?
Cybercrime is any violation of federal, state, or local statute, or malicious or suspicious activity, in which a computer, network or device is an integral component of the violation. Examples can include: a malicious cyber criminal breaking into a computer to steal information (computer intrusion) or to change a website (website defacement); malware being placed on a computer without the owner's permission; and that malware using that computer's resources to send spam.

Who Are the Actors and What Do They Want?
Cybercrime actors can generally be classified into several categories: lone hackers, script kiddies, insiders, hacktivists, terrorists, nation-states, and organized cyber criminal groups. The motivations for committing cybercrime will vary and can include a desire for recognition or promotion of an ideology; theft of money or information for industrial espionage; or the creation of widespread disruption. Cybercrime is big business. Between October 1, 2013, and December 31, 2014, for example, U.S. victims lost nearly $180 million through a scam known as the Business Email Compromise.[i] One underground market has more than 14 million U.S. credit cards for sale[ii]. The creators of the CryptoLocker ransomware earned approximately $300,000 profit in its first 100 days.[iii]

How Can You Protect Yourself?
Cybercrime—whether from malware on a single computer or the recent high-profile hacks against Sony, Target, Home Depot and others—impacts everyone. Below are some key practices you can use to help minimize your risk of being a victim:

- **Configure Your Computer Securely**
  Make sure your computer, smartphones, and tablets are safe. Use privacy and security settings in your software, email system and web browsers. New strains of malicious software are appearing all the time, so it is imperative to regularly update your anti-virus software to identify and thwart the newest threats.

- **Keep Software and Operating Systems Updated**
  Be sure to install all software updates as soon as they are offered; using the "auto update" setting is the best way to ensure timely updates. Similarly, make sure you keep your operating system and any third-party plug-ins that you use updated.

- **Use Strong Passwords**
  Never use simple or easy-to-guess passwords like "123456" or "p@$$word" or "football." Cybercriminals use automated programs that will try every word in the dictionary in a few minutes. When creating a password, use at least 10 characters, with a combination of uppercase and lowercase letters, numbers, and symbols.

- **Be Cautious About Links and Attachments**

Be cautious about all communications you receive including those purported to be from friends and family, and be careful when clicking on links in those messages. When in doubt, delete it.

- **Protect Your Personal Information**
  Be aware of financial and sensitive information you give out. Cybercriminals will look at your social networking webpage to find information about you--remember, many of the answers to website and bank security questions can be found online, like the color of your car (remember posting that picture of you standing in front of your car?) and your mother's maiden name. Use privacy settings to limit who can see the details of your social network pages, and be smart about what you decide to share online.

- **Review Your Financial Statements Regularly**
  Cybercriminals find loopholes and your accounts may get hacked through no fault of your own, so review your financial statements regularly. Contact your financial institution immediately if you see any suspicious looking activity.

What to Do If You Are a Victim?

- If you've been a victim of identity theft, notify your bank, and any other entities with which you have accounts, to inform them that someone may be using your account fraudulently. Contact all three major credit bureaus to request a credit report, and have a fraud alert and a credit freeze placed on your account.

Document and Inform

a. Collect and record attack/restoration details
b. Contact IT Dept
c. Contact customers affected by telephone, e-mail or U. S. mail (see attached)
d. Hold a postmortem meeting with CEO, Security Officer, VP Data Services and Internal Auditor.
e. Contact law enforcement agencies (when appropriate) including filing a Suspicious Activity Report (SAR) TDF 90-22.47 (r).
f. Develop a plan of action for future attacks
g. Modify the Information Security Program Risk Assessment Addendum(s) and these Incident Response Procedures to reflect plan changes.

- Internet-related crime, like any other crime, should be reported to appropriate authorities at the local, state, or federal levels, depending on the scope of the crime.

The following resources can help with reporting cyber crime:

- Your local police department
- Your State Attorney General's Office - http://www.naag.org/
- FBI Internet Crime Complaint Center - http://www.ic3.gov/default.aspx

The information provided in the Monthly Security Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.
Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.

---

[i] http://www.ic3.gov/media/2015/150122.aspx
[ii] http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf
[iii] http://threatpost.com/cryptolocker-creators-infected-nearly-250000-systems-earned-30m-since-september/103261