Badger Bank
Working Together, Achieving Success.

Monthly Security Tips NEWSLETTER

March 2015

Protecting Against Cybercrime

From the Desk of Steve Dehnert, Badger Bank President & CEO

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 include a cybercriminal 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 the 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 cybercriminal groups. The motivations for committing cybercrime 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, U.S. victims lost nearly $180 million through a scam known as the Business Email Compromise. One underground market has more than 14 million U.S. credit cards for sale. The creators of the CryptoLocker ransomware earned approximately $300,000 in profits in its first 100 days.

How Can I Protect Myself?
Cybercrime — whether from malware on a single computer or the recent high-profile hacks against Sony®, Target®, The Home Depot® and others — affects everyone.

Below are some key practices 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's 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're 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," "p@$$word" or "football." Cybercriminals use automated programs that will try

every word in the dictionary within 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 them.
- **Protect Your Personal Information** — Be aware of what financial and sensitive information you give out. Cybercriminals will look at your social networking Web page 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 Should I Do If I Become a Victim?

- If you become a victim of identity theft, notify your financial institution and any other entities with which you have accounts to inform them that someone may be using your accounts 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.
- 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.