COMMUNITYBANK

It's nice to work with people you know!

The Community Bank of Grantsburg-Siren-Cameron continues to work with our customers on keeping financial data safe and secure. Please take a few minutes to learn more about Cybercrime and how to protect yourself and your data.

FDIC Consumer News – Winter 2016 - A Cybersecurity Checklist

Reminders about 10 simple things bank customers can do to help protect their computers and their money from online criminals.

1. **Have computer security programs running and regularly updated to look for the latest threats.** Install anti-virus software to protect against malware (malicious software), that can steal information such as account numbers and passwords: and use a firewall to prevent unauthorized access to your computer.

2. **Be smart about where and how you connect to the Internet for bnaking or other communicatons involving sensitive personal information.** Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they do not have up-to-date security software.

3. **Get to know standard Intenet safety features.** For example when banking or shopping online, look for a padlock symbol on a page (that means it is secure), and https:// at the beginning of the web address (signifying that the website is authentic and encrypts data durinig transmission).

4. **Ignore unsolicited emails asking your to open an attachment or click on a link if you're not sure who truly sent it and why.** Cybercriminals are good at creating fake emails that look legitimate but can install malware. Your best bet is to either ignore unsolicited requests to open attachments or to independently verify that the supposed source actually sent the email to you by making contact using a published email address or phone number.

5. **Be suspicious if someone contacts you unexpectedly online and asks for your personal information.** A safe strategy is to ignore unsolicted requests for information: no matter how legitimate they apear, especially if they ask for information such as a Social Security Number, bank account numbers or passwords.

6. **Use the most secure process you can when logging into financial accounts.** Create "strong" passwords that are hard to guess, change them regularl and try not to use the same passwords or PINs (personal identification numbers), for several accounts.

7. **Be discreet when using social network sites.** Criminals comb these sites looking for information such as someone's place of birth, mothers maiden name or a pets name, in the event those details can help them guess or reset passwords for online accounts.

8. **Be careful when using smartphones and tablets.** Don't leave your mobile devices unattended and use a device password or other method to control access if stolen or lost.

9. **Parents and caregivers should include children in their cybersecurity planning.** Talk with your child about being safe online, including the risks of sharing personal informaton with people they don't know. Make sure the devices they use have up-to-date security.

10. **Small business owners should have policies and trainning for their employees for customers, plus other issues that are specific to the business.** For example: consider requiring more information beyond a password to gain access to your business network: and additional safety measures such as requireing confirmation calls with your financial institution before certain electronic transfers are authorized.