Help Protect Yourself from Fraud with these Internet Security Tips

With the growing variety of mobile devices, social networking sites and online offers, it's important to help protect yourself and your computer. We've compiled this list of cybersecurity tips you should follow to help keep your information safe.

1. Don't use your full or partial Social Security number as a Personal Identification Number (PIN), user ID or password.

2. Make sure that your password is 8 or more characters and combines letters, numerals and symbols. Don't use the same user ID and password for your financial accounts as you do for other sites.

3. Consider a screen lock on your mobile device. Many mobile phones offer this option, as well as other customizable security settings, that can help keep your phone and information secure.

4. Don't use your mobile device to store sensitive personal information or bank account numbers.

5. Never respond to urgent email claiming to be from a bank or any company that requests your account information or personal details. Forward these emails to abuse(at)csbarkansas.com and please do not include any confidential information about yourself in the email.

6. Limit the amount of personal information you provide on social networking sites. The more information you post, the easier it may be for a criminal to use that information to steal your identity, access your data or commit other crimes.

7. Be cautious about messages you receive on social networking sites that contain links. Even links that look like they come from friends can sometimes be harmful or fraudulent – and in fact may be attempts to gain control of your computer or steal your personal information. If you're suspicious, don't click the link. Contact your friend or the business directly to verify the validity of the email.

8. Keep your computer operating system and browser up to date with the latest software and security downloads. Often called patches or service packs, these should be installed as soon as possible.

9. Don't open attachments or install free software from unknown sources; this may expose your computer and the information on it to unauthorized sources.

10. Install a comprehensive firewall/antivirus/anti-spyware software package on your computer. These software suites help detect and remove viruses and spyware that can steal vital information.

11. Avoid public Wi-Fi networks. Be cautious making purchases from a public computer or Wi-Fi network like a library, airport or coffee shop. If you are making transactions on public Wi-Fi, only do it through encrypted sites, always log out after the transaction and don't use the same password across different websites.

12. Look for https. That little “s” after “http” is a good indicator that the site is probably a safe place to enter your credit card. Make sure you see https on every page you visit, not just the welcome page and especially on the page where you enter financial information.

13. Think twice before shopping from an app. It can be difficult to determine an app’s security because they don’t carry the visual “https” indicator. According to the FTC, researchers have found that many mobile apps don’t encrypt information properly. When in doubt, go to the company’s mobile website (and look for https) rather than shopping through their app.

14. Don’t store card information. If a site asks you to store credit card information, don’t to it, even on a personal computer or your phone. If you do store information, be sure to log out of accounts. If you have credit card information stored on accounts in your phone, you may want to change the settings on your mobile device so it doesn’t automatically connect to nearby Wi-Fi.

15. Don’t email credit card information. Email is not a secure way to send your credit card information over the Internet. It should be transmitted via a secure website (https). Of course, security is not ensured just because a site has you fill out a form and appears to have a legitimate URL. The key here is to be suspicious of any company that requests you email credit card information.

16. Go with the credit card. Credit cards offer more protection than your debit card. Use them for online transactions, especially if it is a site you are not overly familiar with.

17. Monitor activity. No matter what new fraud prevention technology comes our way, you should always do your due diligence. Check credit card activity regularly, review statements line-by-line, and check your credit report annually for any errors or suspicious activity, and report any suspicious activity immediately to your bank.

Community State Bank consumer credit and debit cards are protected with our $0 Liability Guarantee. That means less hassle for our customers since any fraudulent charges that are promptly reported are credited back often as soon as the end of next business day. The $0 Liability Guarantee covers fraudulent purchases and payments made by others using your Community State Bank consumer credit and debit cards. To be covered, report purchases made by others promptly, and don’t share personal or account information with anyone. Access to funds is available the next business day in most cases, pending resolution of claim. Consult customer and account agreements for full details. If you have any questions or concerns, please contact us using any of the contact information provided at the bottom of our home page and please do not include any confidential information about yourself if you choose to email the bank.