A Cybersecurity Checklist

FDIC Consumer News 2016

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 banking or other communications involving sensitive personal information.** Public Wi-Fi networks and computers at places such as libraries or hotel business centers can be risky if they don't have up-to-date security software.

3. **Get to know standard Internet 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 during transmission).

4. **Ignore unsolicited emails asking you to open an attachment or click on a link if you're not sure it's 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 files or to independently verify that the supposed source actually sent the email to you by making contact using a published email address or telephone number.

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

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

7. **Be discreet when using social networking sites.** Criminals comb those sites looking for information such as someone's place of birth, mother's maiden name or a pet's name, in case 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 device unattended and use a device password or other method to control access if it's 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 information with people they don't know, and make sure the devices they use to connect to the Internet have up-to-date security.

10. **Small business owners should have policies and training for their employees on topics similar to those provided in this checklist 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's network, and additional safety measures, such as requiring confirmation calls with your financial institution before certain electronic transfers are authorized.

Source: https://www.fdic.gov/consumers/consumer/news/cnwin16/checklist.html