August 2014
Volume 9, Issue 8

Secure Online Banking

Enterprise Information Security Program

From the Desk of Paul Federighi, Chief Information Security Officer

Virtually every financial institution is using the Internet to communicate and allow customers to conduct transactions online. Customers today expect this convenience, and if done securely, these transactions can be as safe as those conducted in person.

Start with the Basics

Ask yourself the following four questions below. If your answer to all three each is a yes, your chances of being impacted by a cyber incident are low. If any of your answers are no, then your chance of being impacted by a cyber incident are high. Understand these risks and take the recommended actions.

1. Is My Computer as Secure as Possible?

Using an unsecured computer is like leaving the door of your house wide open: you are making it easy for someone with malicious intent to access your property. An unprotected machine can become infected with malware in a matter of moments, leaving you vulnerable to identity theft or other crimes.

Having up-to-date security software protection isn't an option; it's a requirement and should become as automatic as locking your doors when you leave your house. Be sure your computer is current with all operating system and application software updates. Anti-virus and anti-spyware software should be installed, running, and receiving automatic updates.

In addition to taking precautions when using your own computer, practice vigilance when using someone else's. Don't use public computers or public networks for financial or other sensitive transactions. You have no control over the security of a public computer or public wireless network.

2. Is My Connection to the Internet as Secure as Possible?

Simply connecting to the Internet makes you vulnerable to a potential attack. Using a firewall helps minimize risks by blocking malicious traffic to your computer. Make sure you have a firewall, that it is turned on, and kept updated. New computers may be shipped with it on by default, but double-check.

When entering sensitive information into a website, look for the "https://" and check that the lock icon is present in the URL bar. This indicates that your communications are encrypted. Also pay attention to the browser you use to connect to the Internet. Keep it updated and patched, and set to auto update. If you are using a wireless network to connect to the Internet, make sure encryption is enabled and change the default network name and password that come with the wireless router.

3. Is My Password as Secure as Possible?

Strong passwords don't have to be hard to remember, just hard to guess. A good password is at least ten characters and uses a mix of upper case, lower case, and numeric or special characters. Each of your online accounts, especially financial ones, should have its own strong password so that if one is compromised, the attacker does not have automatic access to your other accounts.

4. Do I Know How to Recognize a Scam?

Keeping your computer secure is only part of the equation when conducting online banking. You need to be alert for scams and the things you can do to protect yourself.

Phishing is one of the most common scams attackers use. A phishing scam typically consists of an email, trying to entice the recipient into clicking a link or downloading an attachment. A phishing scam targeting your financial accounts will consist of an email message notifying you of a "problem" with your account and ask you to click on a link to your "bank's" site and submit sensitive information. This site however is a very convincing fake version of the legitimate site. This website may then prompt you to provide personal information such as Social Security, bank account or credit card numbers, and/or it may download malicious software onto your computer.

Instead of clicking on the link to your bank's website embedded in an email, navigate to the financial institution's website on your own by typing the address directly into your browser. Beware of attached files, as they may contain malware. Open attachments only from trusted sources, and if you are in doubt, don't open it at all. You may also consider using anti-phishing software to help block many phishing-related emails.

Remember, no legitimate financial institution will ever ask you to provide sensitive information in an email.

For More Information

FDIC: Safe Internet Banking https://www.fdic.gov/bank/individual/online/safe.html

CIS Newsletter: Cyber Crime and How it Affects You
https://msisac.cisecurity.org/newsletters/2012-12.cfm

CIS Newsletter: Creating a Secure Password:
https://msisac.cisecurity.org/newsletters/2012-04.cfm

CIS Newsletter: Using Wi-Fi: Connect With Care:
https://msisac.cisecurity.org/newsletters/2013-07.cfm

Provided By:

CENTER FOR INTERNET SECURITY

STOP | THINK | CONNECT

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.