Cyber Security

Securing Your Mobile and Online Banking Transactions

Center for Internet Security®

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides

© 2014 Center for Internet Security. All rights reserved.

The information in this document is provided by the Center for Internet Security (CIS), for non-commerical informational and educational purposes only. CIS does not warrant the accuracy or completeness of the information or commit to issue updates or corrections to the information. CIS is not responsible for any damages resulting from use of or reliance on the information contained herein.

Introduction

Are you confident when you use mobile and online banking that your transactions are secure? In today's rapidly developing digital world, where depositing a check can be as easy as taking a picture with your smart device or logging into your account from anywhere, protecting your information and devices has never been more critical.

Phishing, Malware, and Identity Theft

While there are many ways that information can be compromised, and the techniques used by online criminals are constantly evolving, the majority of risks that users face fall into just a few categories. Here's a look at several of the most common techniques used by cyber criminals, and some steps you can take to help protect your devices and information.

Phishing

When cyber criminals "go phishing," consumers are the prey and fake websites and fraudulent emails are the bait.

Phishing typically works like this: A user receives an urgent email, allegedly from a trusted party such as a retailer, government agency, law enforcement, email provider, or bank. Such emails generally include links that lead to a website where the recipient is asked to enter sensitive information such as a password, Social Security number, or other privileged information. This information is then captured by the cyber criminals who designed both the email and the website to mimic the trusted third party's actual online presence.

A phishing scam may also try to entice a user into opening a file attached to an email. Malicious code could be embedded in the file and if the user opens it, malware is downloaded to the computer.

How to Protect Yourself from Phishing Scams

Be smart when conducting online transactions.

To avoid being conned by a phishing scam, always verify the legitimacy of any website that asks you for personal information. One way to make sure you're not being sent to a fraudulent website is to type the known and verified address of the website you're being asked to visit into your browser's address bar instead of clicking on a link provided in the email.

Urgent-sounding or enticing communications should raise a red flag. Criminals create these scams to prey on emotions. Use caution any time you receive a text message or email telling you to immediately update your personal information, activate an account, or check on an unexpected delivery. Rather than clicking on a link or calling the number provided in the text or email, verify the request. Type the URL of the organization's website into your browser, or call the its general customer service number to check the validity of the message. Be sure to delete emails coming from addresses or individuals that are unknown to you. Resist the temptation to follow a link or open an attachment from someone unknown to you.

Malware

Computer programs intended to gather information or disrupt a computer's normal functions are known as malicious software or malware. Your computer or device can be infected with malware by visiting compromised or malicious websites or by opening infected email attachments.

How to Protect Yourself from Malware

Keep your computer and devices up to date with the latest security patches.

It's not enough to install an Internet security software package when you first get your computer. You also need to download updates such as virus definitions for the antivirus software so it is equipped to respond to the latest malware threats. You will need to update regularly and there are many applications that let you set up automatic updates as well. Check to make sure your security subscription is current. A computer with antivirus software and an operating system that is regularly updated, combined with a personal firewall, provide a strong foundation for protection from malware and other online threats.

Identity Theft

Once criminals gain access to a user's personal information—whether it's by phishing or malware—they can then use the information to set up new financial accounts. Identity theft is sometimes the result of criminals gaining access to the type of information needed to set up fraudulent accounts such as name, Social Security number, date of birth or other personal information. Social media sites make things easier than ever for criminals, because there is so much personal information online about users, making it very simple to impersonate someone.

How to Protect Yourself from Identity Theft

Be cautious about how much personal information you make available online.

Keeping financial information safe requires more than just secure online banking – it's important to carefully check your privacy settings on social media sites that you can turn on to restrict access to any personal information.

Do not conduct sensitive transactions on public computers, such as those in hotels, libraries or coffee shops. There is no way to know if they are infected with malware or are lacking adequate security protection. Avoid accessing financial accounts or making online purchases on such computers.

Password protection is crucial. Knowing a password makes it much easier for criminals to access an account, even if they have no other information. All too often people use the same password for multiple accounts. This practice makes the cyber criminal's job easier. Once they have your password, it will work for multiple sites.

Mobile Device Considerations

While the steps described above will help secure online banking, it's also important to consider your use of mobile devices.

One simple solution to reduce your risk: Engage your mobile device's keypad lock function when you're not using it.

Users should also be cautious about where they get their mobile applications, or "apps," for their phones. Consumers should obtain apps from well known reputable sites, where listed apps go through various levels of review, and security tests.

The Bottom Line

By staying informed about the latest risks and staying vigilant about using good security practices, you'll minimize the chances of having your information or device compromised.

For additional copies or to download this document, please visit:

http://msisac.cisecurity.org/resources/guides

© 2014 Center for Internet Security. All rights reserved.