
How to Protect Yourself Online

Posted by Mike Wallabe - 2008/01/29 02:34

Here are a few suggestions on ways to keep your personal information and money more secure when you go online:

Beef Up Your Security. Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for those who engage in online financial transactions. Make sure the computer you are using has the latest security patches, and make sure that you access your online brokerage account only on a secure web page using encryption. The website address of a secure website connection starts with "https" instead of just "http" and has a key or closed padlock in the status bar (which typically appears in the lower right-hand corner of your screen).

Security Tip: Even if a web page starts with "https" and contains a key or closed padlock, it's still possible that it may not be secure. Some phishers, for example, make spoofed websites which appear to have padlocks. To double-check, click on the padlock icon on the status bar to see the security certificate for the site. Following the "Issued to" in the pop-up window you should see the name matching the site you think you're on. If the name differs, you are probably on a spoofed site.

Use a Security Token (if available). Using a security token can make it even harder for an identity thief to access your online brokerage account. That's because these small number-generating devices offer a second layer of security - a one-time pass-code that typically changes every 30 or 60 seconds. These unpredictable pass-codes can frustrate identity thieves. While fraudsters can use keystroke logging programs to obtain regular username and password information, they can't use these programs to obtain the security token pass-code. Ask your brokerage firm if you can protect your online account with a security token or similar security device.

Be Careful What You Download. When you download a program or file from an unknown source, you risk loading malicious software programs on your computer. Fraudsters often hide these programs within seemingly benign applications. Think twice before you click on a pop-up advertisement or download a "free" game or gadget.

Use Your Own Computer If You Can. It's generally safer to access your online brokerage account from your own computer than from other computers. If you need to use a computer other than your own, you won't know if it contains viruses or spyware. If you do use another computer, be sure to delete all of the your "Temporary Internet Files" and clear all of your "History" after you log off your account.

Don't Respond to Emails Requesting Personal Information. Legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as email. If you have reason to believe that your financial institution actually does need personal information from you, pick up the phone and call the company yourself - using the number in your rolodex, not the one the email provides!

Security Tip: Even though a web address in an email may look legitimate, fraudsters can mask the true destination. Rather than merely clicking on a link provided in an email, type the web address into your browser yourself (or use a bookmark you previously created).

Be Smart About Your Password. The best passwords are ones that are difficult to guess. Try using a password that consists of a combination of numbers, letters (both upper case and lower case), punctuation, and special characters. You should change your password regularly and use a different password for each of your accounts. Don't share your password with others and never reply to "phishing" emails with your password or other sensitive information. You also shouldn't store your password on your computer. If you need to write down your password, store it in a secure, private place.

Use Extra Caution with Wireless Connections. Wireless networks may not provide as much security as wired Internet connections. In fact, many "hotspots" - wireless networks in public areas like airports, hotels and restaurants - reduce their security so it's easier for individuals to access and use these wireless networks. Unless you use a security token, you may decide that accessing your online brokerage account through a wireless connection isn't worth the security risk. You can learn more about security issues relating to wireless networks on the website of the Wi-Fi Alliance.

Log Out Completely. Closing or minimizing your browser or typing in a new web address when you're done using your online account may not be enough to prevent others from gaining access to your account information. Instead, click on the "log out" button to terminate your online session. In addition, you shouldn't permit your browser to "remember" your username and password information. If this browser feature is active, anyone using your computer will have access to your brokerage account information.

<http://www.sec.gov/investor/pubs/protectyourselfonline.htm>

Post edited by: scotteagle, at: 2008/01/29 01:38

=====

Re:How to Protect Yourself Online

Posted by scotteagle - 2008/01/29 02:37

logo http://www.securityforwomen.com/components/com_fireboard/uploaded/images/bannerTitle.gif

=====