On-Line Security Tips

Online Safety Tips

What should you be aware of when it comes to online safety? First, follow these guidelines:

- Don't share your UserID or password with anyone, and don't write it down. If you share your password with a third party, you assume responsibility for their actions. Be extremely cautious about using aggregation services, as you're sharing your UserID and password with a third party.
- Avoid accessing your account from public computers in Internet cafes, libraries, hotels, etc.—they can be accessed by malicious users who may have installed software in them to record your keystrokes. If you must use a public computer, make sure it is from a reputable provider.
- When you are finished accessing your account, always log off and close your browser.

Avoid Email Fraud

Email can be a source of danger. Many Internet scams today involve email messages that appear to come from a trusted source but are not trustworthy. Additionally, email attachments can be harmful because they can contain viruses.

The below can be indications that an email is fake:

- The email claims to be from a legitimate company requesting that you change your password by clicking on a link. It may even threaten to suspend your account if you do not do this.
- The email claims to be from a person in authority requesting a copy of a password file, UserID, Social Security number, or banking information.
- The email asks you to verify your account information by clicking on a link and filling in a form.
- Right click on the link in the email and select properties. If the section under URL Address contains an '@' symbol, then it is likely fraudulent. Here are some ways to protect yourself from email fraud:

Here are some ways to protect yourself from email fraud:

- Do not reply to any email asking for personal information.
- Use antivirus software and keep it updated. Scan all attachments with an anti-virus software program before downloading.
- Do not visit links sent by email as these can lead to phishing sites—sites made to look legitimate and designed to collect your personal information. One way to avoid this is to enter the URL into your browser instead of clicking the link.
- Do not open or reply to spam email which can prompt more spam to be sent to your inbox.

- Turn off the "preview pane," as this allows some viruses to be executed even if you never actually open the email.
- Report suspicious email to TD Ameritrade.

To find out more about email fraud and phishing, go to How to spot phishing, under Know the threats.

Beware of Stock Spam

Online investors should be aware of stock spam, part of a common Internet fraud involving a "pump and dump" scheme. In other words, a company might be promoted and recommended as the latest hot stock in chat rooms, supposedly unbiased newsletters, or even in its own press releases. Unwitting investors purchase the stock, creating high demand and inflating its price. Then those who are behind the scheme sell their shares at the peak, stop the hype, and the stock price plummets—causing regular investors to lose money.

To protect yourself, always do your research before you invest:

- **Consider the source.** Be skeptical. People touting a stock may well be individuals who stand to profit
- **Verify information.** Making grand claims is easy for a company to do. Before you invest, be sure to independently verify those claims. When you see an offer in an email or on the Internet, assume it's a scam unless your own research proves it's legitimate.
- **Know where the stock trades.** Many of the smallest and most thinly traded stocks trade in the over-the-counter market (OTC Bulletin Board or Pink Sheets). This is because they don't meet the listing requirements of NASDAQ or NYSE. They're the most susceptible to manipulation, and therefore the most likely to be the focus of a spam scam.

If you receive a stock spam email you can file a complaint with the Securities and Exchange Commission at http://www.sec.gov/complaint.shtml. You probably only receive an auto-reply from them, but they do take complaints seriously and may be acting on yours behind the scenes.

Create Secure Passwords

Choosing your password well and keeping it a secret can be key steps to safeguarding all of your online transactions. To create a password that is more difficult to guess, use a combination of letters and numbers for passwords you create (i.e. 4funcallC3po, Il9vemyd1g). Certain passwords are easier to compromise, so try to avoid common pitfalls by creating secure passwords:

- Don't base your password on personal information—such as the name of your pet or your company.
- Don't use a word found in the dictionary as your password.
- Avoid substituting numbers for letters, for example: using a zero for the letter "o" or a one for the letter "i." These substitutions are well known and predictable.
- Don't use your UserID as your password.
- Don't use simple number sequences like "12345" or a series of duplicate numbers like "11111."
- Change your password frequently, and don't "recycle" a password you've used somewhere else.

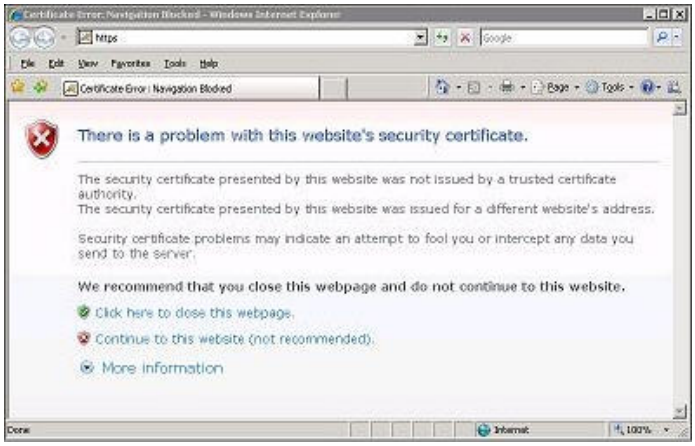
TD Ameritrade does not permit the use of special characters (e.g. #, *, ^, etc.) in passwords.

Check a Site's Security Setting

Make sure you only access personal information through Web sites that use Secure Sockets Layers (SSL). A Secure Socket Layer (SSL) is an additional layer of security that many sites use. You can check whether the site you are on has an SSL in effect by checking for two things:

1. Look at the Web site address. If you are on a secure site, the address will include https:// instead of http://. The extra "s" stands for secure.
2. Look at the bottom of your browser or at the top (after the address bar) for a lock or key icon. This indicates a secure connection. Each secure site comes with a digital certificate, establishing its legitimacy. To view the certificate, double click on the lock or key.

If you get a pop-up message indicating a problem with a site's Security Certificate, do not proceed. The Web site should be secured with a digital certificate, which verifies you're at a legitimate website and not a "spoofed" site. If your browser displays a message box like the one below, you're not guaranteed a secure connection.



Protect your Computer and Network

Protect your computer against new viruses or other attacks with anti-virus and anti-spyware software and configure all software for automatic updates. The anti-virus and anti-spyware software included in operating systems require frequent updates to keep pace with new risks. Security software included with new computers generally require a subscription for protection to continue.

Use the latest version of your web browser. Strong encryption protects your information as it travels over the Internet. Older web browsers may not support the highest strength 128-bit encryption.

Do not allow software to be loaded on your computer if you're not completely familiar with it. If you share your PC with anyone, including your children, make sure they know the rules for downloading and installing software.

Install a hardware- or software-based firewall. A firewall controls how information moves between a computer and a network to help ensure that only legitimate traffic takes place, and hides the presence of computers behind it to make it more difficult for potential intruders to find them.

Protect your Wireless Network

Use of a wireless network presents several security concerns. Wired Equivalent Privacy (WEP) is the standard encryption that wireless devices use. If your wireless network supports WPA or WPA2 you should select that option rather than WEP.

Because this encryption can be breached, make sure you take these steps:

- **Change the administrator password.** After you remove your WiFi router out of the box, you'll be prompted to log into it through a web page using a specified username and password. That username and password is identical for all models of your router—an open invitation to hackers because these common passwords are published by numerous sites. See above for information on creating secure passwords.
- **Change the default Service Set Identifier (SSID).** The manufacturer of your router sets all their routers to the same SSID, for examples "default" or "LinkSys." While the SSID doesn't allow hackers to get it, a default setting often signals them that the owner hasn't taken the proper security precautions. You can change this setting in the setup page of your router.
- **Only access personal information through Web sites that use Secure Sockets Layers (SSL).**
- **Disable file and printer sharing capabilities** when you're connected to a public wireless network.

  If you doubt the security of an open wireless network, don't use it—shut off wireless connectivity or remove the wireless network card. If you leave your computer unattended, disable the wireless mode to prohibit networks that you didn't create from using your wireless software.