Protect Your Social Media Accounts

The Internet has made our lives easier in so many ways. However, you need to know how you can protect your privacy and avoid fraud. Remember, not only can people be defrauded when using the Internet for investing; the fraudsters use information online to send bogus materials, solicit or phish.

Phishing is the attempt to obtain financial or confidential information from Internet users. This phishing expedition usually begins with an email that looks as if it is from a legitimate source, often a financial institution. The email contains a link to a fake website that looks like the real site. Fraudsters want you to provide account and password information, and then they have access to your account.

Here's what you can do to protect yourself when using social media:

Privacy Settings: Always check the default privacy settings when opening an account on a social media website. The default privacy settings on many social media websites are typically broad and may permit sharing of information to a vast online community. Modify the setting, if appropriate, before posting any information on a social media website.

Biographical Information: Many social media websites require biographical information to open an account. You can limit the information made available to other social media users. Consider customizing your privacy settings to minimize the amount of biographical information others can view on the website.

Account Information: Never give account information, Social Security numbers, bank information or other sensitive financial information on a social media website. If you need to speak to a financial professional, use a firm-sponsored method of communication, such as telephone, letter, firm e-mail or firm-sponsored website.

Friends/Contacts: When choosing friends or contacts on a social media site, think about why you use the website. Decide whether it is appropriate to accept a "friend" or other members hip request from a financial service provider, such as a financial adviser or broker-dealer. There is no obligation to accept a "friend" request of a service provider or anyone you do not know or do not know well. Site Features: Familiarize yourself with the functionality of the social media website before broadcasting messages on the site. Who will be able to see your messages - only specified recipients, or all users?

On-Line Security Tips

As with all computer and web-based accounts, take precautions to keep your social media account information secure. Here are some security tips:

- Pick a "strong" password, keep it secure, and change it frequently.
- Use different passwords for different accounts.

- Use caution with public computers or wireless connections. Try to avoid accessing your social media accounts on public or other shared computers. But if you must do so, remember to log out completely by clicking the “log out” button on the social media website to terminate the online session.
- Be mindful of accessing your social media accounts on public wireless connections, such as at a coffee shop or airport. It is very easy to eavesdrop on Internet traffic, including passwords and other sensitive data, on a public wireless network.
- Be extra careful before clicking on links sent to you, even if by a friend.
- Secure your mobile devices. If your mobile devices are linked to your social media accounts, make sure that these devices are password protected in case they are lost or stolen.