SEC
Office of Investor Education and Advocacy

Investor Bulletin:
Social Media and Investing – Understanding Your Accounts

The SEC's Office of Investor Education and Advocacy is issuing this Investor Bulletin to provide investors with tips they should consider when establishing an account on a social media website. Investors' use of Facebook, Twitter and other social media websites as an investing tool has increased substantially in recent years. Investors who use social media websites for investing should be mindful of the various features on these websites in order to protect their privacy and help avoid fraud.

Tips investors should consider when using social media websites

Privacy Settings: Investors should be mindful of the default privacy settings when establishing 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. Investors should check default settings and modify them, if appropriate, before posting any information on a social media website.

Biographical Information: Many social media websites require biographical information to open an account. This information may not have to be made available to other social media users once the account is active. Investors should consider customizing their privacy settings to minimize the amount of biographical information that they allow others to view on the website. For example, many users permit "friends" or authorized users to see their birthday month and date, but not the birth year. Or similarly, many users choose not to display their address, hometown, work or other identifying information.

Account Information: Investors should never communicate account information, Social Security numbers, bank information or other sensitive financial information on a social media website. If investors need to speak to their financial professionals regarding their accounts or investments, they should seek a firm-sponsored method of communication, such as telephone, letter, firm e-mail or firm-sponsored website. A financial professional's social media website may not necessarily be a firm-sponsored site and may be that individual's personal site.

Friends/Contacts: Investors should consider whether it is appropriate to accept a "friend" or other membership request from a financial service provider, such as a financial adviser or broker-dealer, given the intended purpose of the social media website. There is no obligation to accept a "friend" request of a service provider or anyone you do not know or do not know well. Denying a request may be appropriate, depending on your comfort level with the person requesting access to your media site. Remember that once a person is your "friend," that person, and possibly that person's friends, can see any posting made on your social media site, unless privacy restrictions are activated.

Site Features: Investors should familiarize themselves with the functionality of the social media website before broadcasting messages on the site. Investors should consider that certain messages may be seen only by specified recipients (direct mail, e-mail or instant messaging functionality) and others may be viewed by all users (for example, posts on the "wall" on Facebook).

On-Line Security Tips: As with all computer and web-based accounts, investors should take precautions to ensure that information contained in their social media accounts remains secure.

Pick a "strong" password, keep it secure, and change it frequently. Investors should select "strong" passwords for their social media accounts. Strong passwords are not easy to detect and generally consist of eight or more characters that are a combination of letters, numbers and symbols. Strong passwords should not be based on common words, phrases, or personal information, such as a name or birthday. Investors should keep their passwords in a safe place and out of plain sight. Investors should never share their social media passwords on the Internet, over e-mail, or on the phone. In addition, investors should change their social media passwords at least every six months.

Use different passwords for different accounts. Investors should not use a single password for different social media accounts. Using a single password for different social media account accounts is the equivalent of using a single key for your car, house, and mail box – if you lose the key, you give away access to everything.

Use caution with public computers or wireless connections. Investors should try to avoid accessing their social media accounts on public or other shared computers. Investors who use a public computer to access their social media account should remember:

- Log out of the account completely by clicking the "log out" button on the social media website to terminate the online session. Closing or minimizing the web browser does not necessarily log out the account.
- Delete the computer's "temporary Internet files" and Internet history.

Investors should also be mindful of accessing their 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. Investors who use a public wireless network to access their social media accounts should remember:

- Do not type any passwords unless the website you are accessing uses a secure connection that scrambles your password. The easiest way to determine whether a website is secure is to look in the address bar. If the page's web address begins with "https" instead of "http," then it is a secure connection.
- Avoid entering sensitive personal information. Investors should avoid accessing or providing any personal financial or investment information such as Social Security numbers, bank or brokerage account numbers, bank or brokerage account passwords, over a public wireless network.
- Turn off file sharing. With some computers, by default all of your hard drive is wide open to any other computer connected to the same network. Make sure this feature is turned off when accessing information over a public wireless network.
- Make sure your computer has current anti-virus software and a firewall.

Be extra careful before clicking on links sent to you, even if by a friend. Investors should always verify that links or messages containing links that are sent to their social media accounts come from legitimate sources.

Clicking on a malicious link could:

- link to a website that tricks you into providing personal information that can be used to steal your money or identity, or
- cause malicious software (e.g., computer viruses, worms, Trojan horses, or spyware) to automatically infect your social media account or your computer.

To guard against dangerous links, investors should remember the following:

- Do not click on a link that appears to be randomly sent by someone you know, especially if there is no explanation for why the link was sent, or if the explanation is out of character for the sender.
- Do not click on a link that was sent to you by a business you do not know. Perform an online search for the business and go directly to the business' website to determine if the link is legitimate.
- Do not click on a link that was sent to you by a business that you have an existing account with. Investors should confirm the legitimacy of the link by either going directly to the business' website or calling up the business with a confirmed telephone number.

Secure your mobile devices. Many mobile devices, such as smartphones or tablets, have software applications that allow users automatic access to their social media accounts. Unauthorized access to these mobile devices could compromise the personal information contained in your social media accounts. Investors who have mobile devices that are linked to their social media accounts should make sure that these devices are password protected in case they are lost or stolen.

Related Information

For additional educational information for investors, see the SEC's Office of Investor Education and Advocacy's homepage and the SEC's Investor.gov website. For additional information relating to social media and privacy issues, also see:

SEC's Investor Alert: "Social Media and Investing: Avoiding Fraud."

Financial Fraud Enforcement Task Force's web page on privacy issues.

U.S. Army: "9 Critical Steps: Protecting Yourself on Facebook."