U.S. Capital Advisors

CYBER FRAUD EMAIL SECURITY

All financial services firms are seeing increased incidents of cyber fraud involving clients whose email accounts have been compromised. Many people believe that this could only occur if they download malware to their computer and further assume they have little to worry about as long as they use proper antivirus software. As you will find below, email hacking is much simpler and scarier than this.

- Fraudsters can readily buy "phishing kits" which are packages that use a well-known brand such as Prudential, ReMax or Google to send emails that direct the user to what appears to be a legitimate branded website. The site prompts you to create a log in using your email address for an ID and then it asks for a password. Out of habit and/or trusting the brand and the innocuous nature of the site many users will use the same password they use for their email log in. Once this is done, the fraudster has captured the user's email log in and has full access to the user's email account.
- Another recent example is to hack an email account and then send their contact list an email asking them to review an attached Google document. They are then required to enter their email address and password to open the document. Once these are entered, the user is redirected to the real Google Docs page, where there is no attachment waiting; however, the fraudster now has access to their email account.
- Once fraudsters gain access to an email account they will search for communications to financial institutions in order to impersonate the account holder to try to direct funds from their accounts. Their success typically depends on how much information is stored in the email account. In some cases they find saved tax returns and similar detailed documents, along with signatures they can copy and paste onto letters of authorization.

We all know that email is a huge convenience in servicing clients, but it is critically important that we maintain the security of our email accounts by protecting the confidentiality of IDs and passwords and taking other precautions. It is for this reason that we make the following suggestions:

- do not share your IDs or passwords and never use the same password for any other site or for any other purpose;
- change your passwords regularly, and whenever possible, use a 2-step verification (Google offers this features for Gmail accounts, see below for more information);
- avoid clicking on links in email messages, particularly one prompting you update personal information by entering your ID and password, even though the email may appear to come from a trusted source; and
- do not store confidential information including passwords and sensitive account information in your email account, and delete from your email account all emails and documents that reflect your financial and key personal information.

Please understand that we have to employ various security procedures designed to help protect your accounts, many of which have been created in response to these specific threats. We apologize if you are inconvenienced by some of these procedures and ask that you work with us as we take steps to verify your instructions and your identity.

For more information on email hijacking see these alerts:
http://www.finra.org/Investors/ProtectYourself/InvestorAlerts/FraudsAndScams/P125460
http://www.ic3.gov/media/2012/EmailFraudWireTransferAlert.pdf

For more information regarding Google's 2-Step Verification:
http://www.google.com/intl/en/landing/2step/#tab=why-you-need-it