PAY ATTENTION TO THE ADDRESSES OF THE WEBSITES YOU VISIT

When you go onto the internet, your internet browser gives you important information. The address bar, located near the top of your screen, can help you find out whether you are visiting a legitimate website or looking at a scam.

Examining what appears between the "http://" or "https://" and the first "/" in the address bar can tell you what website you are visiting. For example, if you went on Secretary Galvin's Securities Division's webpage your address bar would read: http://www.sec.state.ma.us/sct

If you look between the "http://" and the first "/", you see you are visiting "sec.state.ma.us." This is the address for the Secretary's website.

But let's say an email claims to be from "Your Neighborhood Bank, Inc." and asks you to click on a link in the email to confirm your personal account information. The address of the website you are sent to is: http://giveusyourinformation.com/yourneighborhoodbank

If you look between the "http://" and the first "/", you see you are visiting the site for "Give Us Your Information" not "Your Neighborhood Bank, Inc."

The most important part of the address is just before the first "/". This is called the site name, and it can help you tell which company's website you are visiting. For example, let's say you do business with a company called "My Financial Advisor," but the address bar displays http://www.myfinancialadvisor.phishing.com/.

Looking at the part of the address right before the first "/", you see the site name is actually "phishing.com" and you can tell you are not visiting the website for "My Financial Advisor."

For information on investor education presentations in your area and access to your free annual credit report, please visit the Secretary's website at www.sec.state.ma.us/sct.

Published by:

William Francis Galvin
Secretary of the Commonwealth
Securities Division
One Ashburton Place, Room 1701
Boston, MA 02108
1-800-269-5428
www.sec.state.ma.us/sct

updated 10/07

Don't Take the Bait

Eight Tips to Avoid Phishing Scams

William Francis Galvin
Secretary of the Commonwealth
Securities Division

"Phishing" means sending widespread e-mails to gather personal data for identity theft and other criminal efforts. While e-mails of this sort can look like legitimate communications from a reputable brokerage, bank, insurance company or advisory firm, they really come from con artists or criminals "phishing" for personal information. Often the "phisher" will send an email that links the user to a "spoofed" website.

"Spoofing" means duplicating a legitimate website, by including familiar logos and by using a nearly identical website address or domain name, to solicit the user to submit personal information. While the website address may appear similar to that of a legitimate company, it was actually created by a copycat. Criminals often lure customers to "spoofed" websites using "phishing" type emails.

RAISE YOUR E-MAIL AWARENESS

1 Legitimate companies will not use email to ask for account information, passwords, verification of security questions or other sensitive information.

2 Even if the email you receive has a ".com address" of a company you do business with, if it seems suspicious, you should call the company directly. Instead of responding to the email, call the customer service number on your account statement – customer reports and complaints can help combat fraud.

3 Watch out for emails claiming to alert investors to a breach of security and asking you to submit personal information – this is another version of a phishing scam!

4 When in doubt about only suspicious, unsolicited e-mails, just hit the "delete" key.

DON'T TAKE THE BAIT!
Watch Out for the Warning Signs

5 **Beware of an unfamiliar or misspelled company name.**

If the address that comes up in your browser does not match the name of the company you are used to, beware. Similarly, if you want to visit a company called "My Broker" but the address in your browser says http://www.mybrokker.com, chances are it is not a legitimate website.

6 **Beware of all numbers before the site name.**

For example, if you look in the address bar and see http://1248395.www.legitimatecompany.com, chances are it is a scam and not the website of "Legitimate Company."

7 **Beware of keywords like "verify," "account process" or "update" in the site name.**

For example, if the address bar says http://accountverify.net/legitimatecompany.com, do not be fooled. Companies frequently use their brand or entity name in their website address, but not words like "account" or "verify."

8 **When in doubt, test it out.**

Put the legitimate company's name into an internet search engine to see if the website listed in your results has the same address as the company soliciting you via email. If not, the solicitation may be a fraud!