

It's a spoof! The Attorney General's Office is not sending you stock tips

Local News

Posted by: David Haviland

Posted on : March 8, 2013 at 4:35 am

OLYMPIA— It can happen to anyone. Spoofers have targeted two well-respected consumer protection agencies in an attempt to harm the very people those agencies protect.

In mid-January, the Federal Trade Commission warned people that scammers had sent e-mail messages that appeared to be from the FTC to thousands of businesses claiming that people had complained about them. The email included a link or attachment to a document including more information. The goal? Entice frazzled business owners to click on the link or attachment then dump malware on their computer.

Today, the Attorney General's Office learned people are receiving e-mails that appear to be from the AGO Webmaster or other "atg.wa.gov" e-mail addresses with the following subject lines:

- New Pick Coming! But First I need your help, details inside
- Pick Of The Week
- This Stock is another monster week ahead
- DON'T MISS TODAY'S TRADING IDEA
- Your Mind Blowing Monster Pick!
- News Out & Must Read Inside.

Let us assure you. These are spoofs. Scammers know how to make a message appear to be from one e-mail when it's really from someone completely different.

The goals are usually the same: Use a person, agency or business's good name to trick people into parting with their personal information or lure them into clicking on a document or link that will infect their computer with viruses or malware. This is also known as "phishing";

Here are some clues you've received a spoof e-mail:

- It asks you to provide log-in information like your user name or password.
- It contains an attachment or includes a claim a virus is found.
- It appears to be a reply from someone you've never contacted.
- It includes an error message from a system administrator that includes an attachment for you to view or a URL to click.
- The message includes a lot of obvious spelling or grammatical errors.

Sometimes these messages look very professional. Scammers work hard to replicate messages from legitimate sources like government agencies or banks. They'll include a link with text that says, for example, Attorney General's Office but the hyperlink itself goes somewhere else. You can check whether a link is for real by hovering over the text and reading the link that pops up—but be careful not to click on the link while hovering or you could end up on the scammers site!

OnGuardOnline.gov, the federal government's Internet safety Web site, offers the following tips:

- Use trusted security software and schedule regular, automatic updates.
- Never e-mail personal or financial information.
- Only provide personal or financial information through an organization's Web site if you typed in the address yourself and you know the site is secure, including a web address that starts with "https" rather than just "http".
- Review credit card and bank statements as soon as you receive them--- and if you notice you're not receiving your statements as expected, check with your bank or card company right away.

Finally, be very careful about opening attachments or downloading files from e-mails---no matter who sent them. No one is safe from spoofers!