Important Anti_Phishing Information

Dave Yost, Willabay Design LLC - 2/13/2013

Almost everyone has had a bad experience where they clicked on an email, just to find that they have been tricked into opening an advertisement, or something much worse.

As a result of some experiences I had recently, I thought it would be helpful if I explained how to avoid getting into deep trouble (attacked by a virus or other malware, tricked into releasing personal information, etc).

Here is a typical fraudulent email, supposedly coming from Lifelock, the company that protects against Identity theft.

> From: Lifelock Subject: Just Detecting an ID theft problem isn't enough

The above email looks at first like it is from Lifelock but the detailed message has a link that is really from a domain called leaap.org. Similar emails come from all kinds of temporary domains that incredibly are opened the day the email is sent and don't stick around. They are often in some strange country.

I use PC based client email programs such as Microsoft Live Email which was similar to Outlook Express on Windows XP. There are many other client based email applications for PCs that let you capture your emails on your PCs. You can also automatically delete your received email on your email provider's account.

Using a client email application or in some cases using your ISP email account, you can open the raw details of an email to get the IP address of the sender. You can find something like this:

> Received from leaap.org ([104.129.21.183]) Note that the 104… is the IP address of the sender.

If you do a whois search on the leap.org domain, you get a new domain set up in Panama. If you do an IP address check on the 104… you get an ISP in Los Angeles. The fact these are different suggests that one better not open this email.

The bad guys who are doing this may be simple spammers, or may be somebody out to get you personally. I get hit with this stuff regularly because I write newspaper columns that some folks do not like.

I also use Webroot Secure Anywhere anti-virus on all of my PCs and my phone. Norton or other NAMED BRAND anti-virus products are also very good. DO NOT search for a free anti-virus. You are going to get bit.

Now, the bad news… If you get your email on a phone or tablet using an Android app or Apple's apps, you may not be able to see the phony details on a message until it is too late. That is how many of us are getting hit with scams these days.

Now; what do you do if you get an obvious phishing email that looks bad….

There is hope out there and our government in the form of the FTC is trying to help. There is also an organization called Antitphishing.org that supports ISP vendors and law enforcement. After verifying that the emails I received are not getting blocked, I sent the details off to these guys.

Go to http://www.consumer.ftc.gov/articles/0003-phishing for a lot of good information on this subject and how to report problems. This has the antiphishing.org reporting information as well.

Hope this story helps.

Dave