Staying Safe Doesn't Get Any Easier

Last time, we explored the Tech. Support Scam. Just to follow up. While this type of scam has mostly occurred on Microsoft devices, it is now appearing on Apple and Google (Android) devices, including tablets and phones. Remember the mantra. **Don't talk to strangers!**

OK, let's explore **physhing.** Kind of like fishing, only physhing is a tool to reel you in. The bad guys want your personal information, including credit card numbers, passwords and your social security number if you'll let them have it.

Here's how it works. You'll get an email, or maybe a text, saying something like, "Your account is locked, action required" or "Your package cannot be delivered". You'll be asked to click on the *sign in* button in the email to straighten things out. Or sometimes, you'll be asked to call the provided toll free number. Problem is, doing so will not get you to Fedex or your bank but to the criminal enterprise instead. Then, entering your password on a page that *looks like* your bank or Fedex, etc. gives these creeps the keys to your account.

Communicating with these people will get you in trouble. But it is really easy to avoid. Even though the email and the corresponding page looks just like your bank, etc., it is not. SO, **NEVER CLICK A LINK INSIDE AN EMAIL THAT YOU'RE NOT SURE OF!** Call your bank, etc. **BEFORE** you do anything. They will never send you this type of email in the first place.

How did these crooks get your email? Either they used a random email address generator or they got your address from someone they hacked. You can buy email address lists on the dark web as well.

The example shown here is fairly typical of a physhing expedition. How hard is it to generate something like this? The author made this one in 10 minutes.

amazon

Dear Customer:

Your account shows some odd activity.

It's important for you to update your account information so that we can guarantee your security.

Please click HERE so that we may continue to provide you superior service.

Failure to update your information will force us to lock your account, including access to your Prime Video service.

For further information, contact us at security@amzon.com or toll free at 800-323-bogus.

Regards,
Your Friends at Amazon Security

If you were to click the *Here* button, you'd be connected to some criminals in a basement somewhere, likely on the other side of the globe.

A refinement of this scheme is called Spear Physhing. This looks like you're being contacted by someone or some organization that you know well. Somehow, they've gained access to a database with your email address in it. (Those living here in 2008 may remember that a Pulte theft resulted in a data breach involving all then current residents.) And the crooks hope that you'll be more likely to sign in to a counterfeit link, thinking you recognize the sender. The only real defense is not to open any emailed links at all or try this. Hover over the link. The link address will be displayed. If you don't recognize it, don't open it. Best to contact the person or organization you ***think*** is sending it.

Any Comments, clarifications or questions should be directed to the author at jgf6217@gmail.com.
Written by Joe Fitzpatrick