

Phishing

Identity theft is a growing concern in this Internet age. I have written an article in the past concerning this subject however after listening to a retired police officer who is now employed in the fraud division of a local bank I quickly realized that I needed to give my readers an update on this subject. The ex-officer told me of countless stories where individuals were conned out of their money. He told me that one method, phishing, seemed to be more common and very cunning.

Phishing is pronounced just like the popular sport, “fishing” but is not nearly as innocent as the sport. According to Webopedia, phishing is defined as, “The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.” In other words, phishing takes place when a computer user receives an e-mail requesting personal information. The trick however, is that the e-mail looks like it might have come from your trusted bank.

According to an independent journalist, Andy Sullivan, these phishing tactics have duped over 57 million Americans. What an incredible number, why would so many people allow themselves to be tricked so easily. The answer is very obvious once you see the e-mails. I have seen samples of many of these e-mails and understand why computer users can be so easily tricked. The e-mails look and read just like a normal every day e-mail you might receive from your financial institution or online store. The e-mails contain the institutions logos and even incorporate normal looking links like, www.yourbank.com that will function just like you would expect them to.

While researching this topic I discovered important information that you need to know. First, never under any circumstances should you ever send any personal information at the request of an e-mail. Many of you probably already knew this but I just wanted to be sure we were clear. Secondly, never click on any web address listed in a questionable e-mail. Even if you know that the address of your bank is www.yourbank.com do not click on the link. Phishing scammers are able to use HTML code hidden in the message to redirect you to a look alike site. The site might look like the exact same site you use your user name and password to logon with to check your balance or transfer some cash to another account. The problem is, when you insert your user name and password into this site a scammer just stole the keys to your money.

As if this isn't bad enough, it is estimated that about half of these phishing e-mails contain virus and worms that could open your computer and your identity to any hacker on the Internet. This is just one of the many reasons that it is important to have an up to date virus protection software on your computer. We recommend that anyone connecting to the Internet install Panda Antivirus software on their computer. Sure there are plenty of other big name virus software companies out there but Panda is the only one I will use on my personal and work computers.

So what do you do with a suspicious e-mail asking for your personal information? Forward it to your banks fraud department so that they can catch these thieves. If you have any questions concerning the security of your computer call Thomas, Roger or Aaron at Computer Depot, 947-0749.