The
Pasadena
Citizen

01-31-2012

Even with holiday shopping over LPPD encourages Internet awareness

Internet safety has become a priority for most households. While children are certainly susceptible to predators, adults are equally as likely to fall victim to a different kind of Internet crime known as “spoofing.” Therefore La Porte Police Department encourages computer users, or anyone interacting with alternate media sources, to use a great deal of care and monitoring during their own interactions as well as those made by children.

E-mail “spoofing” is a term used to describe e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail, phishing, or other fraudulent intentions to hide the origin of an e-mail message. The LPPD is warning residents to be aware that by changing certain properties of the e-mail, such as the “From”, “Return-Path” and “Reply-To” fields, ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the “From” field, it actually comes from another source.

Through these means, an immoral spoofer may pose as a family member, friend, other relative or business requesting money or personal identifying information. If you do not verify such a request over the phone or in person, you could be handing your money or personal information over to a criminal. Therefore, in more sensitive matters or highly-important transactions, La Porte Police suggest taking a few moments to verify who may be contacting you.

In addition, computer security plays a vital role in protecting your assets. There are many forms of computer malware. One of the most malignant forms of computer malware is known as a “Trojan Horse.” Trojan horses are designed to allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, it is possible for a hacker to access it remotely and perform various operations. Usually, the hacker’s objective is to gain access to stored credit card information, passwords, and log a user’s keystrokes.

Listed below are a few tips to prevent electronic communication crime/scams:

Ensure that you are utilizing the most up-to-date patches for your Antivirus software. Antivirus software is created to detect and prevent Trojan horses (and other malware) from ever being installed.

Do not click on suspected e-mail spam. They often contain installers for Trojan horses and other computer viruses/worms.

Ensure websites are secure prior to submitting your credit card number.

Be cautious of scams requiring you to provide your personal information.

Be suspicious of any unsolicited email requesting personal information. Verify over the phone with the friend/family member or business that the request is genuine.

Avoid filling out forms in email messages that ask for personal information.

Always compare the link in the email to the link that you are actually directed to.

Log on to the official website, instead of "linking" to it from an unsolicited email.

In addition to Internet crimes, be aware of simple things you can do prevent yourself from becoming a victim of fraud/identity theft:

Never throw away credit card or bank statements in usable form.

Contact the Better Business Bureau to determine the legitimacy of a company.

Utilize locked mailboxes.

Be cautious if you receive a telephone call stating you are a contest or lottery winner.

Promptly reconcile credit card statements to avoid unauthorized charges.

If you have any questions regarding any of these matters, contact the La Porte Police Department’s Criminal Investigation Division at 281-471-2141 or log onto the Federal Internet Crime Complaint Center website at www.ic3.gov