Electronic Self Defense

Tips for Staying Safe on the 'Net

Computer & Telecommunication Services

Stockton University

The 411 on 419s

The Internet is full of scams and scammers. One type is the "Nigerian" or 419 scam. In this scam you receive an email message allegedly from a wealthy foreign business person or government authority who is seeking your help in moving large sums of money out of the country but cannot set up a US account. You are promised a large cut just for providing access to a bank account. Hit delete. This is a scam. *Factoid*: The number "419" refers to the article of the Nigerian Criminal Code dealing with fraud.

Think Before you Post

Social networking sites like Facebook and MySpace are great places to meet new people and make new friends. They are also great places for identity thieves or potential employers to search for information. If your page is open to public view, ask yourself a few questions: Could this information be used to steal my identity? Would a potential employer think twice about hiring me based on my postings?

Portable=Stealable

Laptops and flash drives are wonderful devices. They store all our files and easily travel with us. This portability also makes them easy targets for theft. Be sure to keep them secure at all times.

Update, Update, Update

Keep your computer's operating system up to date. Security holes in Windows, OSX, or Linux can provide an opening for hackers.

Resist the Urge to Click

Many unsolicited email messages, especially "phishing" messages that seek personal information, include web links. The message urges the recipient to click on the link to take some action. Delete the message. Do not click on any links.

Before You Checkout…

Online shopping is incredibly convenient. It is also potentially dangerous to your credit rating. Before giving your credit card number to an online vendor, make sure that your transaction is taking place on a secure server. There are two things to look for: The page address will begin with https:// and the browser will display a padlock icon to the right of the address.

Just Say No

If a website insists on downloading software to your computer before allowing you to access the site, be wary. You could be downloading spyware. Reputable sites will always ask permission and will describe the nature and purpose of the download.

Not Another Password!!

Most websites will require you to set up a username and password in order to access content on the site. As a result, we all have dozens of usernames and passwords. It is tempting to use the same password everywhere. Resist this temptation. If one site is compromised, all of your online accounts could be affected. You can simplify password problems by adding something site specific to the password. For example, your favorite password might be "GoFish". For your Facebook account you could use "GoFishFace".

Too Good to be True

This email scam is hard to resist. The sender asks for your name and address. S/he mails you a money order which you deposit in your bank account. You get to keep a percentage of the money. You are then asked to put the remaining funds into a money order from your bank and mail it to a third party. The original money order is usually forged. Chances are the original forger will not be caught, but you may end up jail. Delete any message like this.

Are You Protected?

Protect your computer from infections like viruses, worms, trojans, spyware and root kits by installing antivirus/ antispyware and keeping it up to date. Do not assume that you are protected by the software that came with your computer. Unless you are paying for a yearly subscription, your software is probably out of date.

About Us…

This tip sheet is brought to you by the Office of Computer & Telecommunications Services. Please visit us on the web at http://compserv.stockton.edu

Online Resources

Electronic Self Defense
http://loki.stockton.edu/intech/edefense.htm

In the Spotlight: Online Shopping
http://loki.stockton.edu/intech/spotlight-online-shopping.htm

In the Spotlight: Internet Safety
http://loki.stockton.edu/intech/spotlight-safety.htm

In the Spotlight: Unsolicited Email (aka 'spam')
http://loki.stockton.edu/intech/spotlight-spam.htm

Federal Trade Commission Identity Theft Site
http://www.ftc.gov/bcp/edu/microsites/idtheft

Phishing IQ Test
http://www.mailfrontier.com/forms/msft_iq_test.html

National Fraud Information Center
http://www.fraud.org/

Consumer Reports Web Watch
http://www.consumerwebwatch.org/