THE SAFETY SITE

Monica Palmer, Safety Administrator

***R**ecreational **S**afety takes **R**esponsibility and **C**ontrol*

CYBER SAFETY

Image Courtesy of Kaspersky Lab

The following article is courtesy of Sandy Stocks, RSRC Webmistress, and is greatly appreciated.

Just in time for the online holiday shopping season!

GLOSSARY (***Source: Wikipedia***)

Malware - Malware, short for malicious software, is an umbrella term used to refer to a variety of forms of hostile or intrusive software,[1] including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. It can take the form of executable code, scripts, active content, and other software.[2] Malware is defined by its malicious intent, acting against the requirements of the computer user — and so does not include software that causes unintentional harm due to some deficiency.

Phishing - Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.[1][2] The word is a neologism created as a homophone of fishing due to the similarity of using a bait in an attempt to catch a victim. According to the 2013 Microsoft Computing Safety Index, released in February 2014, the annual worldwide impact of phishing could be as high as US$5 billion.

URL - A Uniform Resource Locator (URL), colloquially termed a web address,[1] is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it. A URL is a specific type of Uniform Resource Identifier (URI),[2] although many people use the two terms interchangeably.[3][a] URLs occur most commonly to reference web pages (http), but are also used for file transfer (ftp), email (mailto), database access (JDBC), and many other applications. Most web browsers display the URL of a web page above the page in an address bar. A typical URL could have the form http://www.example.com/index.html, which indicates a protocol (http), a hostname (www.example.com), and a file name (index.html).

Router - A router is a networking device that forwards data packets between computer networks. The most familiar type of routers are home and small office routers that simply pass IP packets between the home computers and the Internet. An example of a router would be the owner's cable or DSL router, which connects to the Internet through an Internet Service Provider (ISP), i.e., Charter, Cox, Comcast, AT&T, et al.

PERSONAL INFORMATION

Keep your name, address, phone number, school name, and any adult's credit card number to yourself. Never share your Social Security Number with someone that asks for it online, particularly the last 4 digits, which are gold to an online hacker. Safeguard your private information. Lots of websites offer benefits to folks who provide personal information that they turn around and sell to advertisers, marketers and sometimes crooks. Before you fill out that form, make sure you want whatever it is they are offering. The price may be too high.

BEFORE YOU GO ONLINE

Anti-Virus, Anti-Spyware and Anti-Spam Software - Secure your computer before you go online. The minimum you need is strong anti-virus, antispyware and anti-spam security program, along with a strong personal firewall to prevent hackers from sneaking in to your computer. There are a lot of free software programs. It's best to consult with your personal computer technician, or someone at Geek Squad (they see a lot of infected computers, so they know).

FIREWALLS

The Windows Internet Connection Firewall (ICF) exists on many Windows XP computers but is disabled by default. However, when running, ICF can interfere with internet connection sharing and even disconnect you from the internet. You can disable ICF but remember that according to Microsoft, "You should enable ICF on the Internet connection of any computer that is connected directly to the Internet.". Some home routers, however, have built-in firewalls. Plus, there are many third-party firewall programs you can install to replace the firewall provided by Windows.

EMAILS

Set up a free Web-based email address and provide that address to websites whenever you sign up for anything. That way, a lot of the spam will go to that free account instead of your personal inbox.

WATCH WHAT EMAILS YOU OPEN

Don’t open e-mails that are from people you don’t know. Delete them. Also, don’t click on links to sites that you don’t recognize, even if it says “You have Won a Million Dollars! Beware of emails masquerading as a security concern from your bank, Facebook, Amazon, or other eCommerce sites you do not have an account with--that should be a red flag. Call your bank, service provider or institution to verify any emails before you click on any links or fill out any forms--the IRS NEVER emails taxpayers, so anything from the IRS is really a phishing scam. If you suspect the email is a phishing scam, forward it to the company being perpetrated. For example, if an email is made to look like it came from Wells Fargo, but seems to be phishing, hover your mouse over the incoming address and if it is not from the Wells Fargo system, forward it to "reportphish@wellsfargo.com.” Then delete the original and the forwarded copy. Also, if you suspect emails are a hoax, you can check them out before opening them by going to www.snopes.com.

Passwords - Use strong passwords. Use a variety of letters, numbers and special characters--the longer and more complicated, the better. Use different passwords for each account. If an account supports it, use two-factor authentication. Of course, it can get complicated to manage all these passwords, so consider the use of a password manager application. This type of app often acts as a browser plug-in that it monitors password entry and saves your credentials for each account. All you have to actually memorize is the single password for the manager program. If you choose not to use a password manager application, make sure you change ALL your passwords at least once a month and DO NOT use the same password for all accounts—that’s easy access for a hacker to get into all your personal accounts.

Security - Keep your security up to date. Cyber crooks continue to develop new crimeware and other nasty stuff (aka “malware”). Security companies constantly research and update their protection, which you need to make sure your computer – and your family – remain safe from cyber crime.

Use a website rating service to help you avoid the “dark alleys” on the Internet. Several free services rate websites based on whether they offer nasty downloads, drown you with spam or infect your computer merely by visiting the site.

Avoid free screensavers, smiley faces and other free stuff unless you absolutely know the download is safe. It’s the safest way to make sure you don’t infect your computer with crimeware, adware and other nasty stuff that can steal your information and ruin your computer.

Avoid pop-ups (Web browser windows that pop up) like the plague. If you have a newer computer, pop-ups are usually blocked by default. Keep it that way. Above all, never enter personal information in a pop-up window, since it could be a phishing site. Be smart and don’t become another identity theft victim.

ONLINE SHOPPING

Take care when shopping online: Look for indicators that the website is secure, like a small lock icon 🔒 on your browser’s status bar, a trusted seal like those from VeriSign or TRUSTe and a website URL that begins with “https” (that “s” stands for “secure”).

Get a credit report from all three major credit reporting agencies at least once a year. The law says you can get a free annual report, which allows you to review your credit and check to see if someone has opened accounts in your name. If you find anything wrong, contact the credit agencies to report the error.

Review every credit card statement. If a charge looks suspicious, contact your credit provider to have it removed to help avoid future losses.

WIRELESS HOME NETWORK

Lock down your wireless home network. If you don't know how, hire someone to help you or use wireless protection software that makes wireless security easier to manage. Unprotected wireless networks invite cyber crooks to rip you off.

PARENTAL CONTROLS

Turn on or buy parental controls for your computer to manage when your kids can go online, and limit them to approved, safe websites. Some parental controls even limit your children's ability to share or download files, helping to ensure they don't load your system with spyware.

REFERENCES/SOURCES:

1. Wikipedia, https://www.wikipedia.org/

2. National Crime Prevention Council: Mind What You Do Online http://www.ncpc.org/resources/files/pdf/internet-safety/Mind%20What%20You%20Do%20Online%20-%20Adult.pdf

3. "9 Steps to Protect Your Computer From Viruses and Other Malware," by Mary Landsman, Updated January 8, 2017

4. "How to Disable the Windows XP Internet Connection Firewall: Shutdown the Windows XP Firewall If You Can't Access the Internet," by Bradley Mitchel, Updated June 10, 2017