Safety First!

Whether you have a web site or just connect to the web to find information and services, you need to be aware of a few hazards. It's not that the web is particularly dangerous, but like any location in the real world you need to know how to stay safe.

First, be aware that as soon as you connect to the internet, it's like leaving your front door open. If you are connected and can go to other sites, other sites and individuals can come into your computer. Most of these visitors are harmless or helpful. For example, many sites drop little files called cookies into your web browser so that the next time you go to that site, it loads faster. But there are also villains out there who will put bad files into your computer, and you need to know how to avoid these.

Defend Your Computer

Your computer probably has some built-in defenses, such as a firewall. Use it! Also install some kind of anti-virus software to get rid of any pests that sneak past the firewall. A good free anti-virus program for Windows is Avast. You must register for this free application, and you'll see other more advanced versions of Avast for sale on this site. Download the free version at http://www.avast.com/free-antivirus-download .

Careful What You Click

Be careful what sites you go to, and look at the URL once the page loads to make sure you are in the right place. One sneaky practice is hijacking you and taking you to a spoof site disguised as a legitimate site. Be cautious about clicking ads, even on sites you know. I've seen bogus ads sneaked onto such respectable sites as Scientific American®! Clicking on any of

Want more free activities, tips, and graphics? Look in the Attic!

these nasties could put a virus onto your computer. For more on phishing sites, see the No Phishing post on Annie's Resource Attic. I've put links to various educational tools, including some designed to teach upper elementary students about web safety.

Monitor Your Mail
Beside hacking into your computer, the bad guys may try to get in the door via your email. If you have a spam or junk filter setting, be sure it's active. It may occasionally catch good stuff, so check what's in the junk bin before you delete. BUT… never open anything you don't recognize, particularly if it has an attachment!!!

Site Security
You also want to protect your web site. Some site software, including Google Sites®, lets you make your site entirely private, only open to people on a list you specify. That may not be a good choice if you need to have the site open to all, but could be helpful for an online class, for example. Google sites has a way for you to have the best of both situations. You can specify a list of people who as collaborators can upload files and make comments. Everyone else can just look at the site.

Also, be careful about putting your contact email on your web site. Robots look for and harvest email addresses, and then you get a ton of junk email. One good way to get around that is to do a graphic of your email address. Use a graphics app like PhotoShop Elements© to make a picture of your email address. You can even decorate it or add a pretty background, then save it as a JPEG file. Upload it just like any other photo or other graphic.

Control Comments On Your Site
Beware of allowing comments. Many blogs have this built-in, and comments are be a great way to have online discussions. But spammers definitely target the comments spaces on your site. Check to see if there is a way to set up comments so that you **approve every comment before it appears**. Google Sites deals with this problem by restricting comments to your list of

collaborators. Presumably, people you know aren't likely to leave spam comments.

Also, if there is a spam filter for comments, or you can get an add-on spam filter, use it! In the two years I've had my site, my comments filter has removed several thousand bogus comments, many full of links, and none of them having anything to do with what is on my site.

Know The Jargon

Keeping up on web safety issues is much easier if you know what the jargon means. The following is a glossary of terms relating to cybercrime. It appeared as the sidebar in an article entitled "In Computers We Trust" by Lee Clippard. You can read the rest of the article at:

http://web5.cns.utexas.edu/news/2010/02/focus-winter-2010/

Cyber Jargon Glossary by Lee Clippard

Bot   A computer that has been infected such that it can be controlled remotely. Large networks of bots, called **botnets**, are responsible for attacks such as spam, phishing, and password cracking. Srizbi and Storm are two recent examples of botnets that resulted in the infection of millions of computers.

Keylogging The practice of logging a series of keys struck on a keyboard, such as passwords and usernames. Keylogging trojans (see definition below) can be installed using a virus or worm.

Malware Short name for malicious software designed to infiltrate a computer without consent. Includes computer viruses, worms, and trojans.

Phishing The process of trying to acquire sensitive information such as usernames, passwords, and credit card numbers by masquerading as a trustworthy entity. Example: A web site set up to mimic a trusted site.

Scriptkiddie   Generally used to describe juveniles who use programs or scripts developed by other programmers to attack computer networks.

Spam Unsolicited e-mails sent to address lists.   Addresses are generally acquired illegally, and spam e-mails are a major source of viruses.

Trojan Malware that attacks the data on your computer and is disguised as or is inside of an otherwise harmless program.

Typosquatting Relies on typographical errors made by Internet users when inputting a Web address into a Web browser.   Users are led to an alternative Web site owned by a "cybersquatter".

Worm A virus that eventually takes over all of a computer's resources until the computer does nothing else but run the virus program.

Zombie   A computer infected by a program that causes spam to be sent without the computer owner's knowledge.