Computer Security

Any computer connected to the Internet or another computer is at risk Think of a compute like your home. You wouldn't leave the door unlocked with a sign announcing all of the valuables inside. That would be silly. To have a computer without a security system is like an open house. You need to know what the risks are, and how to protect yourself.

RISKS...

Virus: A virus is a program or code that is loaded onto your computer without your knowledge. They can send copies of themselves to other computers through networks, file sharing, and email. Viruses use up your memory, and may harm your computers.

Worm: A worm is a virus that does a lot of damage. It can “worm” its way through a network and infect all of the computers inside.

Hackers: Hackers are people who are trying to get information off of your computer. They seek out gaps in your security to find your passwords, your accounts, or other information.

Bugs: Bugs are errors in programs. Some bugs cause security risks by making it easier for hackers or their programs to get through.

Backdoor: These are also called trapdoors. Some programs have security holes built in. Programmers often write secret openings into programs so they can access them. These can create security risks.

Spyware: Spyware is a type of virus that spies on the user. It is a program that records passwords and accounts. The spyware will transmit the information to a hacker or company that will use your information.

Malware: Malware is any program that can do harm. Spyware, viruses, back doors and other programs are all considered malware.

SECURING YOUR COMPUTER...

Firewall: In a building, the designer will put extra walls in to prevent the spread of fire. These firewalls are for safety. In a computer, a firewall is an extra level of security. It could be hardware, software, or both. It prevents an unauthorized user from entering your system and getting your information.

Anti-virus software: There are many programs that can search your computer for viruses and malware. They are designed to find the programs and get rid of them. Many of these programs can work in real time, so that when you open up a program or file they can spot it right away. They can also search your entire system for older infections.

Secured Sites: Whenever you need to enter data into a *trusted* site, you should make sure it is secured. There are two things to look for. First, instead of http:// at the beginning of the web address, it will have https://. The extra "s" stands for secure.

Another thing to look for is a little symbol of a lock at the bottom of the page. This also means that you are on a secured site. Secured sites will **encrypt,** or code, the data, so that if a hacker was viewing your system, they couldn't steal it as easily. By only putting credit card info, personal data, and bank info into encrypted, secure sites, you are better protected from thieves.

Patches: Some computer programs have errors. When the company that made the computer finds the error, they will make a "patch." A patch is a little bit of code that will fix a bug in a program. If you get notice that your software needs an update, install the patch. It will keep your computer more secure.

Backups: Even with the best software available, hackers are constantly writing new viruses. You can never consider your computer perfectly secure. You should make a backup of your programs and data every so often. Backups help you restore your information back to a safe point.

Email: Email provides a very specific risk. By using specialized programs, thieves and crooks often will use email to get information. One way is by putting a virus as an attachment to an email. Never open an attachment from a stranger. In fact, it's a good idea to not open email from people you don't know. When I get mail from someone I don't know, I carefully read the "To", "From", and "Subject" lines. If it sounds fishy, it probably is. In fact, speaking of fishy, the term **phishing** (pronounced fishing) means that someone is sending you an email trying to get you to respond with personal data. Never open, reply to, or look at attachments from an unknown sender.

Some phishing scams are very convincing. They will copy logos and icons from real, honest sites and try to trick you into giving info. They may try to warn you that your account was hacked, and if you click on their link, they'll help you secure it. Don't do it! If you have doubts about your account, go to the trusted site and log in directly. Do not click on an email link to go there. Never give private info to a site you didn't choose to go to, or a number you did not call.

Passwords: Passwords provide a special risk. Even the best passwords can be hacked, if the user is insistent enough. A bad password is short, with letters only, and is predictable, such as the name of your pet. A better password has letters, numbers, capitals, symbols, and is a bit longer. Passwords should be changed frequently. Choose passwords that you do not need to write down, and never, ever share them.

Sources: http://www.cert.org/homeusers/HomeComputerSecurity/