10 Computer Security Tips

Use antivirus and Spyware software

Make sure you have Anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses but with new viruses emerging daily, Anti-virus programs need regular updates to recognize these new viruses. It is important to update your Anti-virus software regularly - the more often you keep it updated, the better - you should consider updating the software at least once a week. If you use your computer and receive a lot of emails, then updates should be made more frequently. You should also consider using software to detect Spyware. Spyware is malicious software (malware) that is downloaded onto your computer (often without your knowledge). It can be used by third parties and criminals to monitor your Internet activities which could compromise the security of your personal information. As with Anti-virus software you should check your system regularly for Spyware at least once a week.

How do I know if my PC is safe?

If you receive a suspicious email, especially from a sender you do not recognize, the best thing to do is to delete the entire message, including any attachment. . If you are determined to open a file from an unknown source, save it first and run your virus checker on that file. If the mail appears to be from someone you know, still treat it with caution if it has a suspicious subject line (e.g. "I loveyou", "Anna Kournikova", or non-sensical phrases such as “we remote hawk year”) or if it otherwise seems suspicious (e.g., it was sent in the middle of the night). Also be wary if you receive multiple copies of the same message from either known or unknown sources. Finally, remember that even friends and family may accidentally send you a virus or the e-mail may have been sent from their machines without their knowledge. This was the case with the "I Love You" virus that spread to millions of people in 2001.

Protect from Internet intruders

You should equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet.

Download security updates from operating systems and other software such as web browsers:

Most major software companies today release updates and patches to close newly discovered vulnerabilities in their software. Sometimes security flaws are discovered in a program that may allow a criminal hacker to attack and or control your computer. Before most of these attacks occur, the software companies or vendors create free patches for you that are posted on websites for download and installation by their customers. It is important to check your software vendors' websites regularly for new security patches or use the automated patching features that some companies offer such as Microsoft and Apple for their respective operating systems.

Password security:

The most secure passwords are those that contain a mix of upper and lower case characters as well as numbers and characters. You should also try and create a password that is around 8 characters long. Ultimately passwords will only keep someone out if they are difficult to guess! As with your PIN number and other private information it is important not to share your password. Try not to use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places.

A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters, symbols and numbers, e.g., K2v$7Ta8.

Change passwords regularly, at least every 90 days.

Do not give out your password to anyone!

Backup your computer regularly

It is important to be prepared for the worst case scenarios, losing your information through a virus attack. Try and back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, consider saving copies of your data on another computer within the network. Many people make weekly backups of all their important data. It's also important to retain and store safely your original software start-up disks. Keep them handy and available in the event your computer system files get damaged.

Limit sharing - don't allow access to strangers

If you or a member of your family downloads files from the Internet via file-sharing networks, such as Kazaa, your computer operating system may allow other computers to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or allow someone to look at the files on your computer if you don't pay close attention. It is advisable therefore, unless you really need this ability, to make sure you turn off file-sharing. Check your operating system and other program help files to learn how to disable file sharing.

Disconnect from the Internet when not in use

Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your Anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet.

Check security settings regularly

The software and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security regularly. You should look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you.

How to adjust Security Settings in Internet Explorer

In the main browser window, select 'Tools' and then 'Internet Options'. When you do this a further pop-up window will open, select the second tab named 'Security', then select 'Custom Level' - from there you can choose an appropriate level to meet your individual needs.

Educate your family and other users of the computer about basic security

It is important that everyone who uses your computer is aware of proper security practices. All users of the same computer should know how to update the virus protection software, how to download and install security patches from software vendors and how to create a proper password. It only takes one user mistake to infect a computer!

This data sheet has been provided as a public service by

Code Electric

Providing central Iowa with quality electrical installations since 1993.
(515) 208-2415
code_electric@msn.com
www.code-elec.com