CYBER SECURITY newsletter

ADVANCED COMPUTER SECURITY

Problem

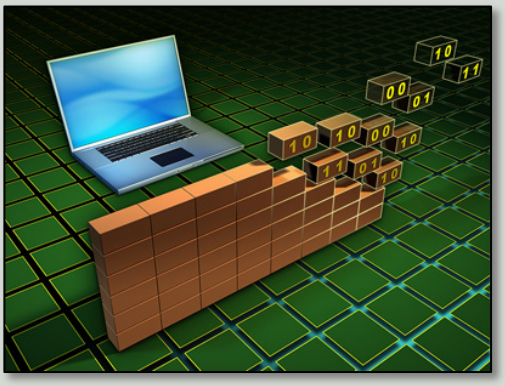
Your computer is one of the primary targets for cyber criminals around the world. Not only does your computer contain a tremendous amount of private and valuable information, but your computer can be used to attack or harm other computers. To protect both yourself and our confidential information, we recommend the following.

Solution

1. Updating: Always be sure your computer has the latest patches installed and you are running the latest versions of your applications, including your browser. Old or outdated software have a tremendous number of security weaknesses which attackers exploit. The simplest way to protect yourself is ensure automatic updating is enabled on both your computer and your most commonly used programs. Also, if you are no longer using a program, remove or uninstall it.

A great way to make sure both your operating system and your applications are up to date is use the free tool Secunia Personal Software Inspector. Simply download and install this tool from http://secunia.com/, then run it to check the update status of your system. We recommend you run this tool at least once a month.

In addition to applications, you also want to ensure your browser plugins or add-ons are current. Every plugin you add to your browser becomes another potential avenue for cyber criminals to attack. A great tool to check your browser's plugins is Browser Check. Simply visit http://browsercheck.qualys.com and it will give you a full report on what plugins you have, which ones are current, and the ability to update any old plugins. Once again, we recommend you check your plugins at least once a month.



Advanced Computer Security

Your computer is a primary target. In addition, outdated programs and browser plugins you use every day can expose you to additional risk. In this newsletter we explain these dangers and what you can do to protect yourself, including tools you can use.

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

OpenDNS

Another way to protect yourself from visiting malicious websites is to use a secure DNS server. DNS is how the Internet converts website names into IP addresses, so your browser knows where to go. One option is the free service OpenDNS. You enable this service by configuring your computer's DNS options (or your wireless Access Point) to use OpenDNS servers. These DNS servers protect you by ensuring that if you attempt to resolve any known malicious websites OpenDNS will stop you before you go there.

In addition OpenDNS has extensive filtering capabilities, such as identifying and blocking unwanted or inappropriate content. This is an excellent solution if you have a family and want to protect your children from accidently visiting harmful websites. To learn more about OpenDNS, including how to set it up on your home computer or customize filtering options, visit their website at http://www.opendns.org.

2. Firewall: In addition to automatic updates, make sure you have a firewall installed and enabled. Firewalls help protect your computer so threats such as worms cannot attack your computer.

3. Anti-virus: Also make sure you are using updated anti-virus software which helps protect your system and data against trojans, viruses, spyware and other forms of malware. Often programs such as firewalls and anti-virus are bundled with security software packages.

Cyber attackers may not be your only concern, you may also want to protect your private information. There are numerous organizations attempting to harvest as much of your information as possible. Here are some options to protect your privacy.

4. **Private Mode**: Consider browsing in private mode. This is a common feature that most browsers support. It does not record online activity such as the websites you visit, does not cache any website content, and usually wipes any cookies stored on your system.

5. Toolbars: Do not install any toolbars in your browser, as many of them are designed to record your online activities.

7. Adobe Flash: You may not realize it, but if you have Adobe Flash installed on your computer (and you most likely do) then Flash is storing an entirely separate set of cookies, cookies that are not erased by your browser. To manage your Flash settings, including cookies, you can visit the Adobe website and change the settings of your Flash player online.

Finally, if you cannot upgrade your browser to the latest version, or if you want additional protection for your browser we highly recommend the low cost utility Sandboxie. This program runs your browser in an isolated space, a sandbox. This sandbox protects your system from most known attacks, and can help privacy by isolating cookies and various cached files. Learn more at http://www.sandboxie.com.

By following these advanced steps, you can help ensure both your computer and our organization remain secure.