CYBER SECURITY newsletter

PROTECTING YOUR COMPUTER

Problem

Your computer has become a critical part of your daily life. You use your computer at home for a variety of activities, such as online shopping, managing your finances, watching movies, reading emails, or perhaps even managing your family photos. In addition, you most likely use a computer at work, regardless of what your job is. Because computers have become such an important part of your daily life, it has also become a primary target for criminals.

Cyber criminals can use your computer for a variety of malicious activities, such as using your computer to send out spam, to host malicious websites, or to launch attacks against other computers. In addition, your computer has a wealth of information that cyber criminals want, including the logins and passwords to your online accounts.

Solution

Fortunately, taking some very simple steps can go a long way in protecting your computer and information. Remember, no single step will protect you and your computer. Always ensure you combine all these steps.

1. Updating/Patching: The number one action you can take to protect yourself is to ensure you are always running the latest version of your operating system and applications. Most attacks launched by cyber criminals today target known weaknesses and vulnerabilities in your computer. By running the latest version of both your operating system and applications, you are secure from most known attacks.

All computers nowadays (regardless of the operating system you choose) support automatic updating. This means as soon as there is a patch or fix for your computer, your computer will automatically download and install it. Be sure this functionality (auto-updating) is always enabled. In addition, always be sure all the applications you are running are updated, such as your browser, Adobe Reader and Microsoft Office. If any of these programs are outdated, there is a good chance they will be hacked.

Protecting Your Computer

Your computer has become a primary target for cyber criminals. The steps described in this newsletter will help protect you, your computer and your information.

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

Securing Your Actions

Technology alone will not help protect your computer. Just as important as technology is how you use and interact with technology. Below are some key things to keep in mind when using your computer on the Internet today.

- *Be careful of which links you click on in emails. One of the most common ways cyber criminals attempt to infect your computer is to have you click on a link that takes you to an infected website. Only click on a link if you were expecting it.*

- *A common attack used to hack into your online accounts (such as your online banking) is to simply guess your passwords. Always use a password that is hard to guess but easy to remember. In addition, never share your password with someone else.*

- *A third type of attack cyber criminals use is creating fake websites that pretend to be selling software, when in reality the software is fake, designed to infect your computer. A very common ploy is to pretend to be selling anti-virus software, the very same programs we tell you to install to protect your computer. Always be sure to purchase or install your anti-virus software from trusted companies. If you are not sure which products are safe, ask the help desk or your security team.*

2. Anti-Virus: Another common method for hacking into your computer is to infect it with viruses, worms or Trojans. These malicious programs (often called malware) are nothing more than programs designed to give cyber criminals total control of your computer. Once these malicious programs infect your computer, cyber criminals can monitor and capture everything you do. They will steal your keystrokes (including your logins and passwords), read your emails, and search your hard drives for sensitive information. In addition, they can use your computer to attack and harm other computers.

Anti-virus is an effective way to help protect your computer against this threat. Anti-virus is a security program you install on your computer. It inspects every file you copy, download, or execute. Anti-virus will then identify, stop, and warn you of any programs it believes are infected. To be effective, always make sure that your anti-virus is updated and current.

Keep in mind, anti-virus is simply another layer of security. While anti-virus is very powerful, it can only detect and protect you against known types of malware. Cyber criminals have become very advanced and are constantly developing new types of malware. It is quite possible that your computer may be attacked by malware never seen before. If that happens, your anti-virus may fail to detect it. This is why it is so important to also follow the other steps described here.

3. Firewall: A third way cyber criminals can hack into your computer is to remotely search for vulnerabilities over the Internet, and when they find a vulnerability they launch an attack against the system.

Like anti-virus, a firewall is a security program designed to protect your computer (in fact, many security programs combine both your anti-virus and your firewall into a single package). A firewall acts like a virtual policeman who decides which computers can and cannot talk to your computer. If there is a vulnerable service on your computer (such as file sharing), and a cyber criminal tries to connect to and exploit that vulnerable service, a firewall will protect you by not allowing the cyber criminal to connect to that service.

Just like automatic updating, almost every operating system now supports a firewall. However, for the firewall to protect you, it must be properly configured and enabled. Ensure that your firewall is by default configured to block any connection to your computer.

4. Password Lock Your Screen. Whenever you leave your computer un-attended make sure you password lock your screen. This protects you from un-authorized people simply walking up to your computer and accessing whatever programs you were last using (such as your email).