

Guidelines for Information Security and Internet Usage



Information Security

The use of technology and the Internet is a ubiquitous part of how we communicate at work, school and home. With the increasing volume and complexity of cyber security threats, we must understand what these threats are and how we can protect ourselves and the information in our care. This pamphlet provides general guidelines on protecting information and assets, both at work and at home.

1. Use and Regularly Update Firewalls, Anti-virus, and Anti-spyware Programs

One of the most effective ways of protecting your computer is to use a firewall and up-to-date anti-virus and anti-spyware products.

A **firewall** works by examining information coming from and going to your network and/or the Internet. It identifies and rejects information that comes from a location known to be dangerous or contains information that seems suspicious. It can even protect your computer from being discovered by a hacker looking for vulnerable systems.

Anti-virus programs work by identifying specific malicious behaviors and files and stopping them from accessing your system, causing damage and spreading to other systems. Many new viruses, worms, and Trojan horses are created every day, so keeping your anti-virus product's definition file updated at least daily is important regardless of which product you choose.

Anti-spyware programs protect against software that performs behaviors such as pop-up advertising, collecting personal information, installing a new toolbar that you can't get rid of, or changing the configuration of your computer, generally without appropriately obtaining your consent. Anti-spyware products also need to be kept up-to-date in order to detect the newest identified threats.

2. Install and Patch Operating Systems, Browsers, and Other Programs

Software makers routinely create updates for their products, in some cases to provide feature improvements but also as the first line of defense in keeping your computer as secure as possible. Whenever security updates, service packs, or patches become available, it is very important to promptly download them and patch your operating systems and programs. These patches are created to protect systems against potential attacks, and sometimes dangerous attacks already exist by the time updates are released. You also want to make sure you update any software you use on the Internet or for connectivity within your network (browsers, email, web applications, or remote desktop software) because these kinds of attacks are becoming more common and more dangerous.

3. Understand Passwords and Authentication

Passwords and other authentication methods like tokens, keys or biometrics are ways systems verify that you are who you claim to be. If someone else uses your credentials, the system will think it's you. That person can do anything you can do on your computer and the system will log their actions (such as deleting files, sending malicious e-mails, or browsing to inappropriate sites) under your access credentials. It is very important to protect both your access and yourself by using strong passwords or even two-factor authentication schemes. Don't share your passwords and access codes, don't store them in unencrypted files, and don't write them down unless you then place them in a locked, secured location.

Passwords need to be strong and complex so they are not easily guessed or quickly cracked. Default passwords, names and dictionary words, even in different languages, can be easily guessed or cracked so use complex passwords that are at least eight characters long and have numbers, letters, and special characters in them. Passwords aren't much use if you cannot remember them, so use a pass-phrase instead. The phrase "Would you like 3 scoops of ice cream?" can become the strong password "Wul3\$o1c?"

4. Lock Your Workstation and Laptop Whenever You Leave It

One of the fastest ways to compromise a system is to simply walk up to an unattended, unlocked workstation or server and access the system. No passwords to break, no equipment to set up, no permissions to circumvent – just start typing and clicking and everything is accessible by the attacker. E-mail access, project files, confidential records, and personal files can all be easily compromised. In addition, it can take mere seconds for someone to open an anonymous-access service to your machine or install a backdoor into the system. The attacker can then access your folders, files and applications at a later time and at their convenience. If someone does do something malicious via your account, the system will record the event as done by you, not by someone else. Be safe and lock your system when you leave it. In many systems you can lock the system with the <Ctrl><Alt> combination or <Windows Tab><L>.

Also configure your system to automatically lock after a short period of inactivity. It is an easy way to help protect your account and the items you have access to. Lockout after fifteen minutes of inactivity is recommended and shorter periods for critical systems or even laptops when you are traveling.

5. Backup Important Files Regularly

There are many ways you can lose information on a computer – a destructive virus, a power surge, lightning, floods, a big magnet, or sometimes equipment just fails. If you regularly make backup copies of your files and keep them in a separate place, you can get some, or even all, of your information back in the event something happens to the originals on your computer.

6. Be Cautious When Using the Internet

Browsing to unknown sites can increase the risk of becoming infected with spyware, viruses and other malicious code. Download files and install programs only when you are authorized to do so, and only when there is a real need. Know with whom you are dealing on the Internet – anonymous doesn't necessarily mean safe, and many criminals are very good at impersonating real financial organizations like banks and credit card companies. Never share personal or confidential information if you are uncertain of the recipient's identity or if you are uncertain that they need the information in question. Even when you are certain with whom you are dealing, never share sensitive or confidential information over an unencrypted Internet connection.

7. Be Cautious about Messaging Security - E-mail and Instant Messaging (IM)

E-mail and instant messaging are wonderful tools but they can be used or misused in a variety of ways. As a general rule, do not send confidential or sensitive information, like Social Security numbers, account numbers, or secret information through unencrypted e-mail or IM. Do not open a message that is of a questionable nature, such as when it has an unusual attachment or it is from an unknown sender.

Spammers can try to validate targeted e-mail accounts in order to continue spamming them and malicious code is often spread via e-mail or even IM attachments. Remember that e-mail and news are subject to forgery and spoofing so apply common sense before assuming a message is valid.

Phishing is a special type of e-mail or IM attack. A phisher sends out a fake notice like "your credit account has been disabled," a plea for help, or a note about an enticing subject. Your system can be infected with spyware, viruses or a Trojan horse sometimes by just clicking on that link and visiting the malicious site. If you share personal information with others as a result of answering these messages, your identity can also be stolen.

8. Review Your Computer Security

Review your computer's security periodically and apply appropriate repairs, upgrades, and replacements. Maintaining your computer is an important component in your security strategy. Maintaining your computer and its systems will help keep your programs up-to-date and less vulnerable.

9. Know How to Respond to a Cyber Incident

Learn how to recognize cyber attacks and know what to do if things go wrong. Ask if your organization has a cyber security incident response plan and a cyber security incident response team and use it when appropriate. Remember that rapid response can be crucial, so when things do go wrong or you encounter a suspicious security-related event, report it immediately. If you don't know how to report a cyber incident, ask your supervisor, someone in your IT department or your help desk.

10. Remember that Cyber Security is Everyone's Responsibility

By protecting yourself and the systems entrusted to you, you are protecting your co-workers, your entire organization's network and data.

**Cyber Security Is OUR
Shared Responsibility**

Photo by: © 2009 Jupiterimages Corporation

Brought to You By the MS-ISAC:



**Multi-State
Information Sharing and Analysis Center
(MS-ISAC)**

www.msisac.org