MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER (MS-ISAC)

Cyber Security Awareness

William F. Pelgrin
Chair

Published by: The Multi-State Information Sharing and Analysis Center (MS-ISAC) — http://www.cscic.state.ny.us/msisac/index.html

Introduction

Information is a critical asset. Therefore, it must be protected from unauthorized modification, destruction and disclosure. This brochure describes information security concepts and defines steps required to properly safeguard information. It is the responsibility of everyone- - each employee and home user—-to become familiar with good security principles and to follow the information protection tips.

Did You Know?

Based on recent statistics:
That the average unprotected computer can be compromised in a matter of minutes.

The majority of individuals who thought their computers were safe… were wrong.

User IDs and Passwords

Your user ID is your identification, and it's what links you to your actions on the system. Your password authenticates your user ID. Protect your ID and password. Remember, generally, you are responsible for actions taken with your ID and password. Follow these best practices:

1. Your password should be changed periodically.
2. Don't reuse your previous passwords.
3. Don't use the same password for each of your accounts.
4. NEVER tell or share your password with ANYONE.
5. When your computer prompts you to save your password, click on "No."
6. Never use a word found in a dictionary (English or foreign.)
7. If you think your password has been compromised, change it immediately. Employees should notify the information security officer or manager at their organization.

Published by: The Multi-State Information Sharing and Analysis Center (MS-ISAC) — http://www.cscic.state.ny.us/msisac/index.html

8. Make your password as long as possible - - eight or more characters. Create a password that's hard to guess but easy for you to remember. When possible, use a mix of numbers and letters, special characters or use only the consonants of a word. If you have difficulty in thinking of a password that you can remember, try using the first letter of each word in a phrase, song, quote or sentence. For example, "The big Red fox jumped over the Fence to get the hen?" becomes TbRfjotF2gth?.

Home Computer Protection

Properly safeguarding your personal computer (PC) is one of the most important ways of protecting your information from corruption or loss.

1. Log off or lock your computer when you are away from your PC. In most cases hitting the "Control-Alt-Delete" keys and then selecting "Lock Computer" will keep others out. You will need your password to sign back in, but doing this several times a day will help you to remember your password.

2. If you have a modem, make sure it does not accept incoming calls (auto-answer should be off).
3. When possible, remove your personal or sensitive information before allowing your workstation equipment to be repaired off-site or replaced by an outside vendor. If your home computer is being used for work purposes, consult your manager on how best to do this.
4. Install firewall and anti-virus software. If you have multiple machines, have this software on all of them.

Protecting your Information

During an emergency or disruption, critical information - - the information necessary to run your organization's systems, record activities or satisfy legal and/or business requirements—- may be damaged. The best way to protect information is to copy it and store it in a secure location.

1. If you are connected to a network, store your files in folders set aside for you. (For employees, check with your LAN administrator for the schedule of backups).
2. If you are not connected to a network, save your files to CDs or floppy disks regularly.
3. Ensure that backups reflect the most current information by copying the data on a regular basis, and after all significant changes. The frequency of the backup cycle should be consistent with the frequency with which you modify the information.
4. Save your original installation CDs/diskettes to use as the backup for your PC software.

Firewalls

Any machine connecting to the Internet should utilize a firewall. There are two types of firewalls. Software firewalls usually run on PCs. Hardware firewalls are separate devices designed to efficiently protect computers. They are usually used by businesses, organizations, schools and governments. All firewall protection creates a barrier between the computers and the Internet. Firewalls should be configured to filter out unauthorized or dangerous information and prevent intruders from scanning and retrieving personal or sensitive information from the computer. Periodically check your firewall manufacturer's web site for product updates and patches.

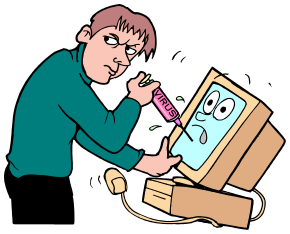
Malicious Code Protection

Malicious code can take forms such as a virus, worm or Trojan. It can hide behind an infected web page or disguise itself in a downloadable game, screen saver or email attachment.

Computer viruses are programs that spread or self-replicate. They usually require interaction from someone to be activated. The virus may arrive in an email message as an attachment or be activated by simply opening a message or visiting a malicious web site. Some viruses consume storage space or simply cause unusual screen displays. Others destroy information. If a virus infects your PC, all the information on your hard drive may be lost and/or compromised. Also, a virus in your PC may easily spread to other machines that share the information you access.

Viruses can exhibit many different symptoms. If your computer behaves erratically, employees are advised to contact their organization computer support representative. At home, disconnect the PC from the Internet and run a full virus scan.

1. Check that your anti-virus software is updated at least every week or set it for automatic updates. New, fast spreading worms and viruses are released every day.
2. Before implementing or using software from any source, check it for viruses with a current virus scanner. Employees, if you do not have a virus scanner installed on your PC, call your organization representative.



3. Store removable media, such as CDs/thumb drives/diskettes as "write protected" whenever possible to help prevent infection by viruses.
4. Do not load free software on your computer from an untrusted source.
5. Consider blocking extensions such as: .bat, .cmd, .exe, .pif, .scr, or .zip through content filtering software.
6. Depending on the extent of the infection, you may need to re-install your operating system.

Published by: The Multi-State Information Sharing and Analysis Center (MS-ISAC) — http://www.cscic.state.ny.us/msisac/index.html

Worms are similar to viruses because they self–replicate, however, they do not require any user interaction to be activated. Worms spread because of vulnerabilities or "holes" in software.

1. Install either a software or hardware firewall. A well configured firewall can help stop propagation of a worm.
2. Anti-virus software will often detect worms. Keep your anti-virus software up-to-date.
3. Know where to find your anti-virus vendor's "rescue" web site for your home computer.
4. Keep your PC and servers "patched."

Trojans (also known as backdoors) are malicious code hidden in a legitimate program that, when executed, performs some unauthorized activity or function. This can range from stealing your password and credit card information to allowing someone to take control of your computer. To prevent installation of Trojans on your machine:

1. Run anti-virus software on your desktop and follow the best practices for using it.
2. Be careful about downloading games, screensavers and other files. Download only from trusted Internet sources.
3. Be careful about file and music sharing services because you can inadvertently share files you did not intend to share. Downloaded files can contain viruses and other malicious code.

A **denial-of-service attack** is an assault upon a network or web site that floods it with so many additional requests that regular services are either slow or completely interrupted. In some instances, a group of remotely controlled, compromised desktops are combined to jointly attack a target system.

Spyware and related "adware," are software sometimes downloaded from a web page, by following a link in an email or are installed with freeware or shareware software without the user's knowledge. Spyware is used to track your Internet activity, redirect your browser to certain web sites or monitor sites you visit. Spyware may also record your passwords and personal information to send to a malicious web site.

1. Read the freeware and shareware license agreement to see if adware or spyware is mentioned before installing the software.
2. Choose to "Close" any pop up windows by clicking on the "X."
3. Do not respond to any dialogue boxes that appear unexpectedly; click on "X". Clicking on "No" or "Cancel" sometimes installs spyware.
4. Beware of visiting web pages which are untrusted.
5. Install software to detect spyware and adware on your PC.

Hoaxes are email messages that resemble chain letters, offer free money, or contain dire warnings and offers that seem to be too good to be true. If you receive a hoax via email, delete it. Sharing hoaxes slows down mail servers and may be a cover for a hidden virus or worm.

Mobile Computing Security

Computers are now accessible via a variety of means. A person can even download data from the Internet to a cell phone. While convenient and fun to use, some good practices will help protect your information.

Laptops, PDAs and Cell Phones are more easily stolen or misplaced because of their size. Remember, if your laptop is gone, your data is too. Small computer devices carry information that must be protected.

Published by: The Multi-State Information Sharing and Analysis Center (MS-ISAC) — http://www.cscic.state.ny.us/msisac/index.html

If you use a laptop, remember the following:

1. Secure it with a cable lock or store it in a locked area or locked drawer.
2. Backup your data.
3. Encrypt confidential information stored on it.
4. Keep it with you during air and vehicle travel until it can be locked up safely. Do not forget to retrieve it after passing through airport security.

Treat all your portable devices in the same careful manner you use with your laptop and keep an eye on them.

Wireless Security

Wireless networks and laptops are very popular for their ease of use and portability. The Internet can be reached via radio waves without having to plug your machine into a network. It is with the same ease of connecting that malicious individuals connect to unprotected networks. Attackers conduct drive-by eavesdropping, called "war driving" to listen in on unsecured devices in homes and businesses. Take the following steps to secure any wireless equipment. Consult your equipment's manual for specific details.

1. Change the default passwords and default SSID, which is an identifier that is sometimes referred to as the "network name". Each wireless device comes with its own default settings, some of which inherently contain security vulnerabilities. Most default passwords are known to hackers.

2. SSIDs should not contain the organization's name or any other identifying information about the organization, the department in which it is located, or its function.

3. Turn off broadcasting the SSID if possible; this will make it more difficult for a hacker to gather your SSID information.

4. Turn on encryption - Encryption settings should be set for the strongest encryption available in the product.

5. Change the default cryptographic key - Many vendors use identical shared keys in their factory settings.

6. Use MAC ACL filtering - Networks use a unique hardware address identifier called a MAC, to help regulate communications between machines on the same network. The MAC Access Control List (ACL) can permit certain MAC addresses access to the network while denying access to other MAC addresses, limiting access to only authorized computers.

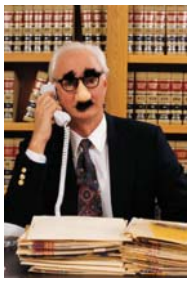
7. Organizations should have a policy regarding use of wireless devices.

Remote Access allows users to access data from outside locations using dial-up equipment and public telephone lines or cellular/wireless phones on the Internet. Because this form of access is designed for off-site use that may extend after normal business hours, extra measures are required to prevent unauthorized access.

1. Keep dial-up numbers confidential.

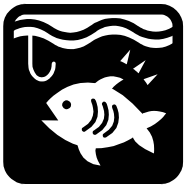
2. Remote access to the office via the Internet should use encryption such as Secure Socket Layer (SSL) or Virtual Private Network (VPN).

Social Engineering is an approach to gain access to information through misrepresentation. It is the conscious manipulation of people to obtain information without their realizing that a security breach is occurring. It may take the form of impersonation via telephone or in person and through email. Some emails entice the recipient into opening an attachment that activates a virus.



1. Before providing information to a telephone caller, check if the individual is authorized to receive that information.

2. Employees should report any suspicious calls to the appropriate individual in your organization.
3. Before opening an email attachment or clicking on a link, verify it is from someone you know, ensure your anti-virus software is current and that the message in the email makes sense for you to receive. If all the parts don't add up, the attachment may contain a virus. Delete it.



Phishing is a scam in which an email message directs the email recipient to click on a link that takes them to a web site where they are prompted for personal information such as a pin number, social security number, bank account number or credit card number. Both the link and web site may closely resemble an authentic web site however, they are not legitimate. If the phishing scam is successful, personal accounts may be accessed. If you receive one of these emails:

1. Do not click on the link. In some cases, doing so may cause malicious software to be downloaded to your computer.
2. Delete the email message.
3. Do not provide any personal information in response to any email if you are not the initiator of the request.

Patching

People are constantly finding security holes (i.e. vulnerabilities) in computer software which could be used to infect your computer with a virus, spyware or worse. When vulnerabilities are discovered, the software vendor typically issues a fix (i.e. patch) to correct the problem. This fix should be applied as soon as possible because the average time for someone to try to exploit this security hole can be as little as a few days.

1. Newer software and operating systems can be set to automatically apply updates. If your software supports this, set up the automatic updates.

2. For older software, the software vendor typically makes the patches available on their web site. Check the web site at least once a month for updates and follow the instructions to apply them. If the vendor provides email notification, subscribe to the notifications and follow the instructions in the email to apply the patch as soon as possible.
3. Many organizations may already have a process for automatically applying patches so check with your help desk before applying patches on your work computer.

Possible Symptoms of a Compromised Computer

Is your machine:

- Slow or non-responsive? Experiencing unexpected behavior?
- Running programs that you weren't expecting?
- Showing signs of high level of activity to the hard drive that is not the result of anything you initiated?
- Displaying messages on your screen that you haven't seen before?
- Running out of disk space unexpectedly?
- Unable to run a program because you don't have enough memory – and this hasn't happened before?
- Program constantly crashing?
- Rejecting a valid and correctly entered password?

Is your organization:

- Finding all of its email refused (bounced back)?
- No longer receiving any email or visitors to your web site?
- Experiencing a number of employees calling the help desk saying their password doesn't work anymore?
- Receiving complaints from the system administrators that their passwords don't work anymore?
- Getting complaints from your users that the network has slow response time?
- Finding there are new processes running on the web server?

Home users may wish to call their ISP and/or anti-virus vendor.

Security Breaches

Security breaches can take several forms. The best defense against security breaches are conscientious and alert users. You are the most important person for early detection and prevention. Examples of breaches include:

- Damage to equipment, facilities or utilities.
- Loss or misplacement of media (e.g. disks, tapes, paper) containing confidential/highly restricted information.
- Inappropriate use of the computing environment.
- Unauthorized access or attempted unauthorized access to information or computing resources.

If you discover a security breach, you should report the breach to your Information Security Officer or manager immediately.

Acknowledgement:

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a collaborative effort for State and Local Governments in strong partnership with the US Department of Homeland Security.

E-Mail: isac@cscic.state.ny.us

Published by: The Multi-State Information Sharing and Analysis Center (MS-ISAC) — http://www.cscic.state.ny.us/msisac/index.html