

COMPUTER CRIME AND SECURITY

COMPUTER CRIME: a criminal act that has been committed where the computer has been the object, subject or instrument of the crime.

Computer crime can take place either through:

1. unauthorized use (use of a computer system without permission)
2. hacking (breaking into computer systems for fun)
3. sabotage and blackmail (breaking into systems for theft or fraud)

Three security measures used to help prevent computer crime:

1. passwords (remembered information)
2. possessed objects ((badges, cards, keys)
3. biometric devices (fingerprint, eye or voice patterns, signature)

TERMINOLOGY:

Piggybacking: tapping into communications lines and riding into a system behind a legitimate user with a password.

Data diddling: entails swapping one piece of data for another.

Scavenging: looking for stray data or "garbage" for clues that might unlock the secrets of a system.

Zapping: penetrating a computer by unlocking the master key to its program and then destroying it by activating its own emergency program.

Worms or Worm Programs: deletion of portions of a computer's memory, thus creating a hole of missing information.

Time Bombs (or logic bombs): the insertion of routines which can be triggered later by the computer's clock or a combination of events.

Virus: a potentially damaging computer program designed to infect other software or files by attaching itself to the software of files with which it comes in contact with. It is an illegal computer code that can do such things as alter programs and/or destroy data.

Host Program: a piece of software that has a virus attached to it. The virus can be spread by way of floppy disks and the Internet.

Antivirus Programs: also called vaccines, have been developed to look for programs that attempt to modify the boot program, operating system or other programs. To protect against viruses, install an antivirus program, scan any floppy disks before using them, and check all downloaded files from the Internet.

Hardware Theft: theft of computer equipment. Portable equipment such as notebook computers has increased the risk of hardware theft. Common sense is the best preventive measure.

Software Theft: can occur in two ways: (1) physically stealing a CD-ROM or floppy disk, or (2) software piracy, which is the unauthorized and illegal copying of copyrighted software. The owner of a software program may make another copy of the program in other two instances: (1) to convert from one computer language to another or from one size disk to another, or (2) to make a backup disk. After you have purchased a software package, you do not have the right to copy, loan, rent or in any way distribute the software to others. Doing so not only is a violation of copyright law, it is also a federal crime!!

Information Theft: deliberately stealing information about a competitor or to get credit card information to be used for purchases.

Encryption: the process of converting readable data to unreadable characters (for the purpose of protecting sensitive data from being stolen and used illegally).

System Failure: caused by fires, floods, storms, or electrical power problems. A surge protector can help smooth out minor voltage errors and provide a stable current flow.

Backup Procedures: a regular plan of copying and storing key data and program files. In case of a system failure, backup copies are used to restore the files. Backup copies should be kept in a fireproof safe or offsite.

Computer Security Plan: the process of identifying all information assets (equipment, software, documentation, procedures, people, data, facilities, and supplies) and the possible risks that could occur. These risks should then be ranked in order of most likely to occur. Then for each risk identify the safeguards that exist to detect, prevent, and recover from a loss should it occur.