1 What Are Computer Security Risks, and What Are the Types of Cybercrime Perpetrators?

A computer security risk is any event or action that could cause a loss of or damage to computer hardware, software, data, information, or processing capability. Any illegal act involving a computer is a computer crime; the term cybercrime refers to online or Internet-based illegal acts. Perpetrators of cybercrime include: hacker, cracker, script kiddie, corporate spy, unethical employee, cyber extortionist, and cyber terrorist.

2 What Are Various Internet and Network Attacks, and How Can Users Safeguard against These Attacks?

A computer virus is a potentially damaging program that affects, or infects, a computer negatively by altering the way the computer works without the user's knowledge or permission. A worm is a program that copies itself repeatedly, using up resources and possibly shutting down the computer or network. A Trojan horse is a program that hides within or looks like a legitimate program. A root kit is a program that hides in a computer and allows someone from a remote location to take full control of the computer. To take precautions against this malware, do not start a computer with removable media in the drives or ports. Never open an e-mail attachment unless you are expecting the attachment and it is from a trusted source. Disable macros in documents that are not from a trusted source. Install an antivirus program and a personal firewall. Stay informed about any new virus alert or virus hoax. To defend against a botnet, a denial of service attack, improper use of a back door, and spoofing, users can install a firewall, install intrusion detection software, and set up a honeypot.

3 What Are Techniques to Prevent Unauthorized Computer Access and Use?

Unauthorized access is the use of a computer or network without permission. Unauthorized use is the use of a computer or its data for unapproved or illegal activities. Organizations can take measures such as implementing a written acceptable use policy (AUP), a firewall, intrusion detection software, an access control, and an audit trail. Access controls include a user name and password or passphrase, a CAPTCHA, a possessed object, and a biometric device.

4 What Are Safeguards against Hardware Theft and Vandalism?

Hardware theft is the act of stealing computer equipment. Hardware vandalism is the act of defacing or destroying computer equipment. The best preventive measures against hardware theft and vandalism are common sense and a constant awareness of the risk. Physical devices and practical security measures, such as locked doors and windows, can help protect equipment. Passwords, possessed objects, and biometrics can reduce the risk of theft or render a computer useless if it is stolen.

5 How Do Software Manufacturers Protect against Software Piracy?

Software piracy is the unauthorized and illegal duplication of copyrighted software. To protect themselves from software piracy, manufacturers issue a license agreement and require product activation.

6 How Does Encryption Work, and Why Is It Necessary?

Encryption prevents information theft and unauthorized access by converting readable data into unreadable characters. To read the data, a recipient must decrypt, or decipher, it into a readable form. An encryption algorithm, or cypher, converts readable plaintext into unreadable cipher text. Encryption is used to protect information on the Internet and networks.

7 What Types of Devices Are Available to Protect Computers from System Failure?

A system failure is the prolonged malfunction of a computer. A common cause of system failure is an electrical power variation such as noise, an undervoltage, or an overvoltage. A surge protector, also called a surge suppressor, uses special electrical components to smooth out minor noise, provide a stable current flow, and keep an overvoltage from reaching the computer and other electronic equipment. An uninterruptible power supply (UPS) contains surge protection circuits and one or more batteries that can provide power during a temporary loss of power.

8 What Are Options for Backing Up Computer Resources?

A backup is a duplicate of a file, program, or disk that can be used to restore the file if the original is lost, damaged, or destroyed. Users can opt for a full backup or a selective backup. Some users implement a three-generation backup policy that preserves three copies of important files: the grandparent, the parent, and the child. Others use RAID or continuous backup. Most operating systems and backup devices include a backup program.

9 What Risks and Safeguards Are Associated with Wireless Communications?

Wireless access poses additional security risks. Intruders connect to other wireless networks to gain free Internet access or an organization's confidential data. Some individuals intercept and monitor communications as they transmit. Others connect to a network through an unsecured wireless access point (WAP), sometimes using the techniques of war driving or war flying. Some safeguards include firewalls, reconfiguring the WAP, and ensuring equipment uses a wireless security standard, such as Wi-Fi Protected Access (WPA) and 802.11i.

10 How Can Health-Related Disorders and Injuries Due to Computer Use Be Prevented?

A computer-related repetitive strain injury (RSI) can include tendonitis and carpal tunnel syndrome (CTS). Another health-related condition is eyestrain associated with computer vision syndrome (CVS). To prevent health-related disorders, take frequent breaks, use precautionary exercises and techniques, and use ergonomics when planning the workplace. Computer addiction occurs when the computer consumes someone's entire social life.

11 What Are Issues Related to Information Accuracy, Intellectual Property Rights, Codes of Conduct, and Green Computing?

Computer ethics govern the use of computers and information systems. Issues in computer ethics include the responsibility for information accuracy and the intellectual property rights to which creators are entitled for their works. An IT (information technology) code of conduct helps determine whether a specific computer action is ethical or unethical. Green computing reduces the electricity and environmental waste while using a computer.

12 What Are Issues Surrounding Information Privacy?

Information privacy is the right of individuals and companies to deny or restrict the collection and use of information about them. Issues surrounding information privacy include the following. An electronic profile combines data about an individual's Web use with data from public sources, which then is sold. A cookie is a file that a Web server stores on a computer to collect data about the user. Spyware is a program placed on a computer that secretly collects information about the user. Adware is a program that displays an online advertisement in a banner or pop-up window. Spam is an unsolicited e-mail message or newsgroup posting sent to many recipients or newsgroups at once. Phishing is a scam in which a perpetrator attempts to obtain personal or financial information. The concern about privacy has led to the enactment of many federal and state laws regarding the disclosure of data. As related to the use of computers, social engineering is defined as gaining unauthorized access or obtaining confidential information by taking advantage of the trusting human nature of some victims and the naivety of others. Employee monitoring uses computers to observe, record, and review an employee's computer use. Content filtering restricts access to certain materials on the Web.