Living Online Module
Lesson 29 — Security, Privacy, and Ethics Online

Computer Literacy BASICS

Objectives

- Understand methods you can use to prevent data loss.
- Identify types of computer crimes.
- Identify computer viruses.
- Identify various security measures.
- Understand how computer use can impact your privacy.

Objectives (cont.)

- Explore other legal and ethical issues concerning electronic information.
- Identify the responsibilities associated with technology use.
- Explain how to maintain a working environment that is safe and use computer equipment in a way that prevents personal injury.

Vocabulary

- Biometric security measures
- Computer crime
- Computer fraud
- Data diddling
- Hacking
- Identity theft
- Logic bomb
- Software piracy
- Time bomb
- Trojan horse
- Virus
- Worm

Threats to Computer Systems

- Computers are vulnerable to
  - Power failures
  - Power surges
  - Lightning strikes
- Any of these can damage your computer and cause loss of data.
- Basic precautions can minimize these threats to your computer system.

Safeguarding Software and Data

To protect your system and data:

- Secure power cords so that they cannot be kicked and unplugged accidentally.
- Install an uninterruptible power source (UPS).
- Install surge suppressors.
- Save files frequently as you work on them.
- Do regular and frequent backups.

Computer Crime

Computer crime is growing rapidly and includes

- Unauthorized use of a computer.
- Infecting computers with a virus.
- Harassment and stalking via computer.
- Stealing and damaging data or equipment.
- Copyright violations of software.
- Copyright violations of Internet information.

Computer Fraud

Computer fraud is conduct involving the use of a computer to obtain money or property dishonestly or to cause loss, such as

- Stealing money from bank accounts
- Stealing information from other people's computers for gain

Warning Signs of Computer Fraud

Possible signs of computer fraud include

- Low staff morale because unhappy employees may think the company owes them and may take what they think they have coming to them.
- Unusual work patterns, giving employees an opportunity to access computers without supervision.
- Staff members who seem to be living above their income.

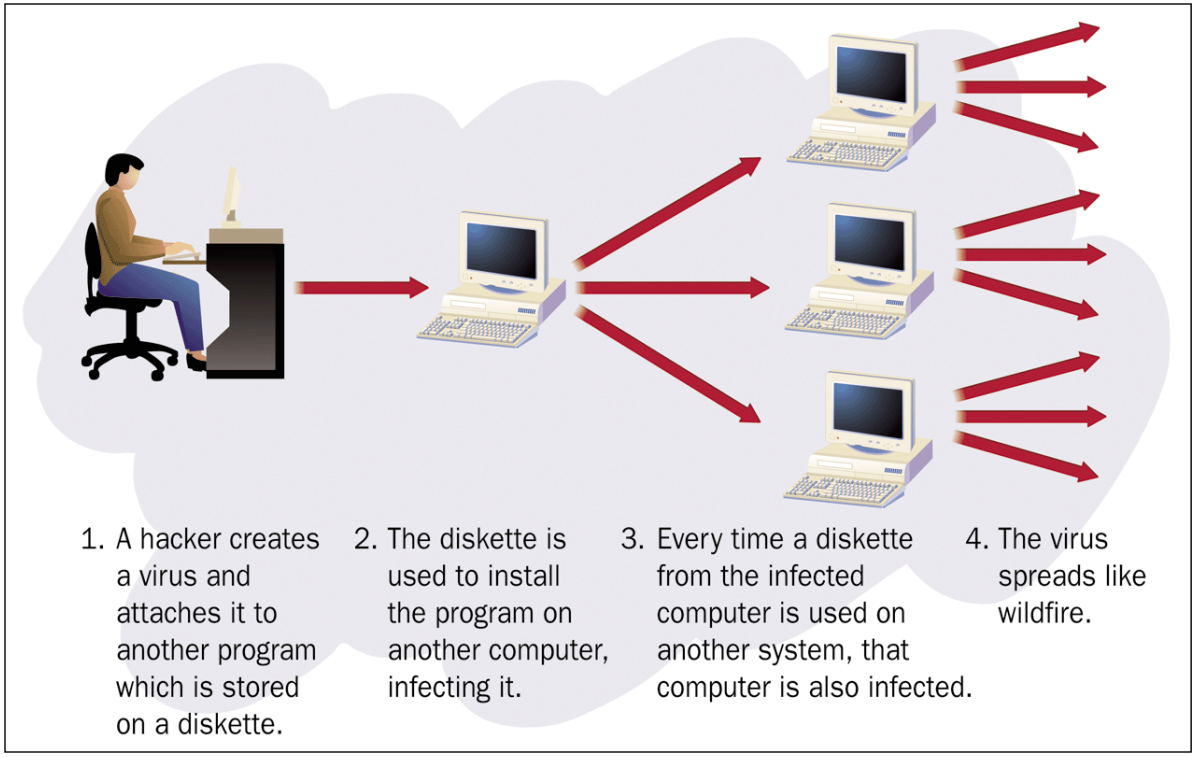
Hacking

- Hacking involves invading someone else's computer without permission.
  - Some people hack for personal satisfaction.
  - Others access computers illegally for personal gain.
- Hackers are usually computer experts who enjoy the power they have to invade someone's privacy.
- Hackers can steal money.
- Hackers also change, damage, or steal data for personal or monetary gain.

Computer Viruses

- A virus is a program, often written by a hacker, that is meant to cause corruption of data.
- Viruses can completely wipe out a hard drive or may just display a harmless message.
- Common virus types include
  - Worms
  - Time bombs
  - Logic bombs
  - Trojan horses

How a Computer Virus Can Spread



Computer Virus Protection

To protect your computer from a virus:

- Obtain antivirus software and update it regularly.
- Be careful when opening e-mail attachments.
  - Viruses are frequently attached to e-mail.
  - Scan messages before opening them.
- Don’t access files on floppy disks or those that were downloaded from the Internet until they are scanned by antivirus software.

Software Piracy

- The illegal copying or use of software programs is called *software piracy*.
- Software piracy costs individuals and businesses money.
- Copying a friend's version instead of buying it is stealing the intellectual property of the creator of the software.

Shareware Is Not Freeware

- Some programs offered on the Internet at no cost are called *freeware.*
- Other programs called *shareware* are offered for free use on a trial basis, but if you want to continue to use the software, you must register it and pay a fee.
  - Downloading and using shareware without paying the author is also software piracy.
- Software piracy is a felony and carries serious consequences if you get caught.

Theft of Computer Time Is a Crime

- When an employee uses a company computer on company time for personal use, this is another form of computer crime.
- Examples of theft of computer time by an employee include
  - Running a small business on the side
  - Maintaining records for an outside organization
  - Keeping personal records

Other Computer Crimes

- Using information you see or find on someone else's computer for personal profit is theft of output.
- Data diddling is the illegal act of changing data before or after it is entered into the computer.
  - Anyone involved in creating, recording, encoding, or checking data can change the data.

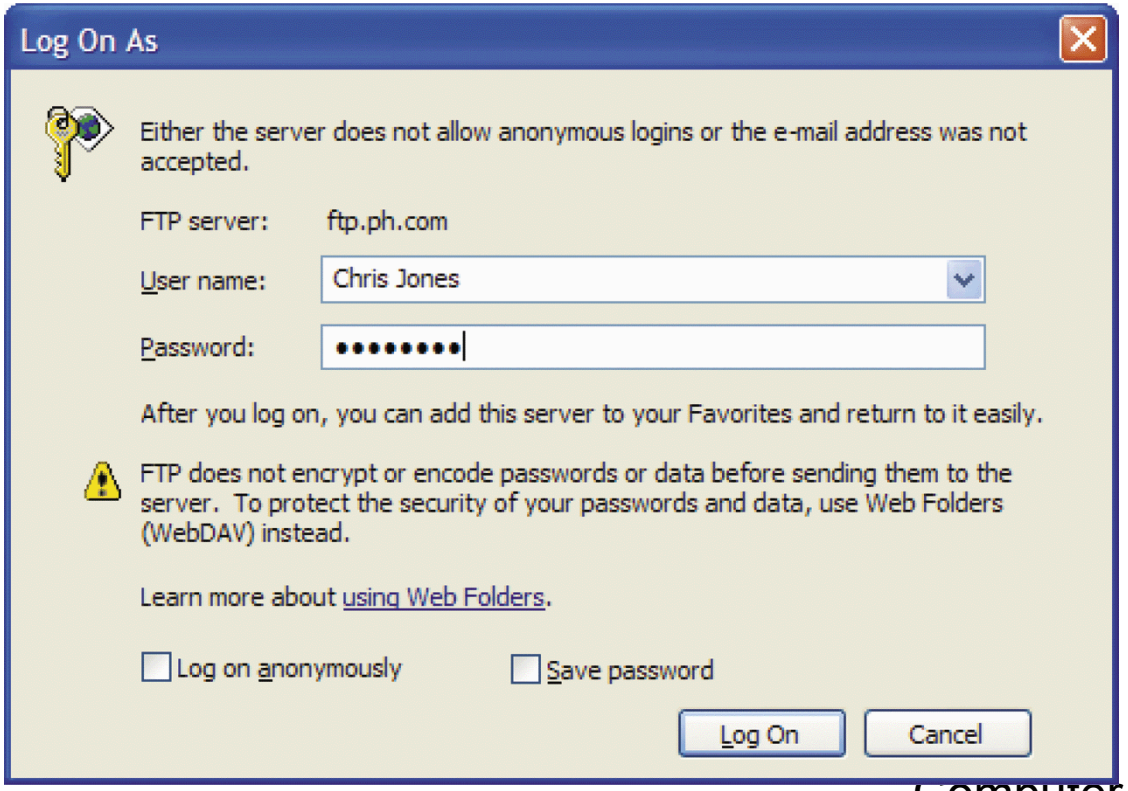
Security Issues

- Computer security is necessary to keep hardware, software, and data safe from harm or destruction.
- Risks to computers and data include
  - Natural causes
  - Accidents
  - Intentional illegal activities
- Safeguards are required for each type of risk.
- It is the responsibility of a company or an individual to protect their data.

Passwords

- The best way to protect data is to restrict access to the system.
- This is usually done by log-in IDs and passwords.
  - Users must protect their passwords so unauthorized users cannot gain access.
  - Passwords should be changed frequently.
  - Notify your supervisor or system administrator if you think someone has stolen your password.

Using a Password to Protect Against Unauthorized Entry



Other Security Measures

- Other methods used to safeguard a computer system and its data include
  - Electronic ID cards to limit access to certain areas
  - Firewalls to block outside attempts to enter the system
  - Antivirus software
  - Screening of potential employees
  - Regular backups of data
  - Biometric security measures

Biometric Security Measures

Internet Security

- The security and privacy of personal information on the Internet is improving all the time.
- But it is still necessary to take precautions to protect both personal and business-related information.
- Many Web sites and online accounts require passwords.

Internet Account Passwords

- Users typically use passwords that are easy to remember to access a restricted Web site or online account.
- This makes them easy to crack for a hacker.
- To protect yourself:
  - Do not use the same password for all online accounts.
  - Change your Internet passwords regularly.

Internet Security: Credit Cards

- Another common security concern on the Internet is credit card information.
- Safeguard your credit card information:
  - Only give credit card numbers to a site that you know and trust.
  - Do not enter card information into an unsecured site.
  - Read a company's privacy policy carefully before giving them personal information.

Internet Security: Personal Information

- Avoid providing your telephone number on Web forms.
- Disclose only what you think is legitimately necessary for the intended purpose.
- Don’t give out personal information to unknown parties.
- Use code names when appropriate to protect your identity and personal security.

Preserving Privacy

When you submit information to a Web site, you have no guarantee how that information will be used or who will see it:

- Information is sold for spam mailing lists.
- Direct marketing companies use the information to create mailing lists.
- Credit history information is sold to marketers and other interested parties.

Cookies

- Cookies are small files that are created when you visit a Web site and are stored on your computer.
- They may make it easier for you to use the site when you return, but also provide the site's owner with information about you and your computer.
- Cookies also take up disk storage space that you might want to use for other data, so it is important to clean up unnecessary cookies regularly with a utility program designed for the purpose.

Spyware

- Spyware can be installed on your computer without your knowledge, usually when you download a file.
- Spyware tracks your Web habits and can even take over control of your computer and direct you to Web sites you have not chosen to visit.
- Spyware can be harmful as well as annoying.
- Firewalls can protect your computer from unauthorized spyware programs.

Private Property—But Not Yours

- When using a company computer e-mail system, all e-mail you send or receive could be viewed by your employer.
- Personal documents you store on a company computer are company property, and you have no right to expect that they will remain private.
- Many companies monitor employee's computer and Internet use.

Legal and Ethical Issues

- Do not copy information from electronic resources, even noncopyrighted material, and claim it as your own.
  - This is illegal and it is called plagiarism.
- Make sure the information you publish is true.
  - If you publish inaccurate information about a person or organization, you could be sued for libel.

Identity Theft

- The flow of information across the Internet makes it easy for criminals to acquire information and prey on unsuspecting victims.
- Identity theft is often used for fraudulent purchases or other economic crimes.
- Credit card numbers, Social Security numbers, and even telephone card numbers are routinely used in crimes that are costly to companies and individuals.

Other Illegal Online Activities

- Using someone's personal data to defraud them or deceive someone else is a serious crime.
- Other significant criminal problems on the Internet include
  - Making sexual advances to minors.
  - Posting anonymous threats.
  - Circulating rumors to manipulate stock prices.
- All are made easier by the Internet, but they are just as illegal and just as wrong.

Unethical Computer Behavior

- Not all improper activities on the Internet are illegal. Activities that may not be against the law but may still harm innocent people include
  - A seemingly harmless or humorous prank that can lead to serious repercussions for people who believe that the information is true
  - Unfair use of free-trial “shareware” software
- The Internet is a powerful tool that must be used ethically and responsibly.

Legal Protection for Technology Issues

- Several laws have been passed to protect computer users, including
  - The Copyright Act of 1976
  - Software Piracy and Counterfeiting Amendment, 1983
  - Electronic Communication Privacy Act, 1986
  - Computer Fraud and Abuse Act, 1986
  - Computer Matching & Privacy Protection Act, 1988
- Many states have laws that pertain to that particular state.

Responsibilities of Technology Users

- Be responsible for your own ethical conduct online.
- Know the computer policies of a company, school, or organization if you use their computers.
- Stay informed about changes and advance-ments in computer technology, including product upgrades and virus threats.

Responsibilities of Technology Users (cont.)

- Recycle computer-related products, such as paper output and used ink cartridges.
- Share your knowledge and experience with your community.

Maintaining a Safe Working Environment

Computer systems pose various potential hazards:

- Check that wires, cables, and power cords are arranged and installed safely.
- Make sure computer equipment is ventilated and cooled to prevent excessive heat buildup.

Avoiding Physical Injuries

- Computer operators need to take precautions to avoid chronic physical maladies such as
  - Repetitive motion injuries
  - Eyestrain
  - Back problems
- Some ways to minimize the risk of injury include
  - Well-designed work areas and ergonomic furniture
  - Good posture
  - Changing position frequently and taking brief breaks

Summary

- Back up data frequently and consistently to avoid losing important information due to a power outage, hardware failure, natural disaster, or computer crime.
- Computer crime has become a major problem, costing companies billions of dollars annually.

Summary (cont.)

- Computer fraud is conduct that involves the manipulation of a computer or computer data for dishonest profit.
- Computer hacking involves invading someone else's computer for personal gain. Sometimes it is done for financial gain and sometimes just as a prank.

Summary (cont.)

- A computer virus is a program that has been written to cause corruption of data on a computer. There are different variations of viruses. These include worms, time bombs, logic bombs, and trojan horses.
- Other computer crimes include theft of computer time, data diddling, and using information from another person's screen or printouts.

Summary (cont.)

- To protect yourself against viruses, install and keep an antivirus program running on your computer. Be sure to update it regularly.
- E-mail attachments can contain viruses. It is a good idea to save any message to disk if you are not familiar with the sender. After saving it to a disk, you can scan it for viruses.

Summary (cont.)

- Computer security is necessary in order to keep hardware, software, and data safe from harm or destruction.
- The best way to protect data is to control access to the data. The most common way to control access to data is to use passwords.
- Companies purchase personal information obtained on the Internet to sell to various companies for marketing purposes.

Summary (cont.)

- Identity theft is a computer crime that involves using another person's identification data to defraud or deceive.
- Laws have been passed in an effort to assist those who have been harmed by computer crimes and offenses, but they are difficult to enforce.

Summary (cont.)

- It is important to know and follow the policies of the organization or company whose computers you use.
- Users of technology are obligated to act responsibly when using computers, dispos-ing of computer parts and materials, and sharing their knowledge.

Summary (cont.)

- Maintaining a safe working environment when using computer equipment involves setting up the equipment properly and taking appropriate precautions to avoid physical injuries caused by computer use.