

Computers Are Your Future

Chapter 9

Privacy, Crime, and Security

1

What You Will Learn About

- How technical developments are eroding privacy and anonymity
- Types of computer crime and cybercrime
- Types of computer criminals
- Security risks
- How to protect computer system and yourself
- How encryption makes online information secure

2

Privacy in Cyberspace

- Privacy - an individual's ability to restrict the collection, use, and sale of confidential personal information.
- The Internet is eroding privacy through the selling of information collected through registration forms on Web sites.
- Few laws regulate selling personal information.

3

Technology and Anonymity

- **Anonymity** - the ability to convey a message without disclosing one's identity.
- It can be abused because it frees people from accountability.
- Computers and the Internet enable others to collect information in ways that are hidden from the user's view.

4

Cookies

- **Cookies** are small files that are written to an individual's hard drive whenever they visit a Web site.
- Legitimate purposes of cookies:
 - recording information for future use
 - retail sites using "shopping carts."
 - saving preferences or login information
 - remembering previous orders or searches

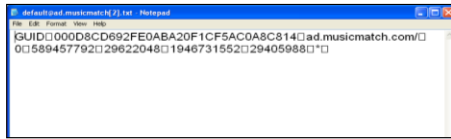
5

Cookies

- Problems with cookies:
 - Ad companies can track a user's browsing actions.
 - Cookies are not encrypted.
 - Hackers can steal cookies. This is a problem on numerous blogging sites.

6

Global Unique Identifiers (GUIDs)



- A **GUID** is a unique identification number generated by hardware or a program.
- It is used to send user information back to the site that created it.

7

Global Unique Identifiers (GUIDs)

Example of GUIDs

- Intel Corporation placed a GUID in its Pentium III processors
- RealNetworks' RealJukeBox player sent information back to the company.
- Microsoft Word 97 and Excel 97 embedded GUID information in every document.

8

Protecting Your Privacy Online

- Browse anonymously by using Web sites such as www.anonymizer.com or www.the-cloak.com.
- Disable cookies on your Web browser.
- Use free e-mail addresses for information placed on Web sites.
- Make sure registration forms have a privacy policy statement.

9

Protecting Your Privacy At Home

Cell phones have GPS capability.

- Parents or EMS can find people.
- Capability is intrusive if an employer tracks an employee.



10

Computer Crime and Cybercrime

- Computer crimes occur when intruders gain unauthorized access to computer systems.
- **Cybercrime** is crime carried out over the Internet.
- **Cyberlaw** tracks and combats computer-related crime.



11

Computer Crime and Cybercrime

Types of Computer Crime

- Identity Theft
- Computer Viruses
- More Rogue Programs
- Fraud and Theft
- Forgery
- Blackmail



12

Identity Theft

- **Identity theft** is one of the fastest growing crimes in the United States and Canada.
- Identity theft occurs when enough information about an individual is obtained to open a credit card account in his or her name and charge items to that account.
- Examples of information needed are name, address, social security number, and other personal information.

13

Computer Viruses

- **Computer viruses** are malicious programs that infect a computer system causing various problems with its use.
- Viruses replicate and attach themselves to programs in the system.
- There are more than 20,000 different computer viruses with the number growing daily.

14

How Virus Infections Spread

Viruses spread by:

- Inserting a disk / USB drive / memory card with an infected program and then starting the program
- Downloading an infected program from the Internet
- Being on a network with an infected computer
- Opening an infected e-mail attachment

15

Types of Viruses

File Infectors

- Attach themselves to program files
- Spread to other programs on the hard drive
- Are the most common type of virus

Boot Sector Viruses

- Attach themselves to the boot sector of a hard drive
- Execute each time the computer is started
- May lead to the destruction of all data

16

Types of Viruses

Macro Viruses

- Infect the automatic command capabilities of productivity software
- Attach themselves to the files in word processing, spreadsheet, and database programs
- Spread when the files are exchanged between users

17

More Rogue Programs

Time Bombs

- Also called **logic bombs**
- Harmless until a certain event or circumstance activates the program



Worms

- Resemble a virus
- Spread from one computer to another
- Control infected computers
- Attack other networked computers

18

More Rogue Programs

Trojan Horses

- Disguise themselves as useful programs
- Contain hidden instructions
- May erase data or cause other damage



19

Meet the Attackers

➤ Hackers

- Computer hobbyists
- Find weaknesses and loopholes in computer systems
- Adhere to the hacker's code of ethics

20

Meet the Attackers

➤ Crackers

- Also called black hats
- Obsessed with entering secure computer systems
- Rarely destructive
- Leave calling cards on the systems they enter

➤ Cyber Gangs

- Bring crackers together by way of the Internet and meetings

21

Protecting Your Computer System

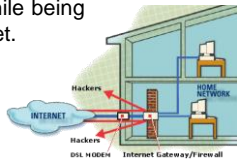
To protect a computer from power-related problems you should:

- Use programs that have an auto save/auto recovery function.
- Use a surge protected power strip
- Or... better yet... equip the system with an uninterruptible power supply, UPS

22

Using Firewalls

- **Firewalls** are programs that are designed to prohibit outside sources from accessing the computer system.
- A **personal firewall** is designed to protect home computers from unauthorized access while being connected to the Internet.



23

Avoiding Scams

- Only conduct business with established companies.
- Read the fine print.
- Don't provide financial or personal information to anyone.
- Be skeptical about information received in chat rooms.

24

Protecting Yourself Against Cyberstalkers

- Don't share personal information in chat rooms.
- Be extremely cautious about meeting anyone you've contacted online.
- Contact the police if a situation occurs that makes you feel afraid while online.

25

Encryption Basics

- A readable message is called **plaintext**.
`I LOVE YOU`
- An **encryption key** is a formula used to make plaintext unreadable.
`V YBIR LBH`
- The coded message is called **ciphertext**.
- An encryption technique called **rot-13** is used in chat rooms and Usenet discussions.

26

Encryption Basics

- **Symmetric key encryption techniques** are encryption techniques that use the same key to encrypt and decrypt a message.
- **Strong encryption** refers to encryption methods that are used by banks and military agencies and are nearly impossible to break.

27

Encryption and Public Security Issues

- Encryption can be used for illegal as well as legitimate means.
- Law enforcement agencies are asking for laws enabling them to eavesdrop on encrypted messages.
- Homeland Security looks for terrorist activity by screening email and internet actions

28
