

Technology, Crime, and Security



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
- US government's key recovery plan



Privacy in Cyberspace

- Privacy refers to 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
- Technology is not only making it easier to invade someone's privacy, but it is also providing a means to protect against privacy invasion



Technology and Anonymity

- **Anonymity** is 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
- Information technologies used on the Internet are:
 - Cookies
 - Global Unique Identifiers (GUIDs)

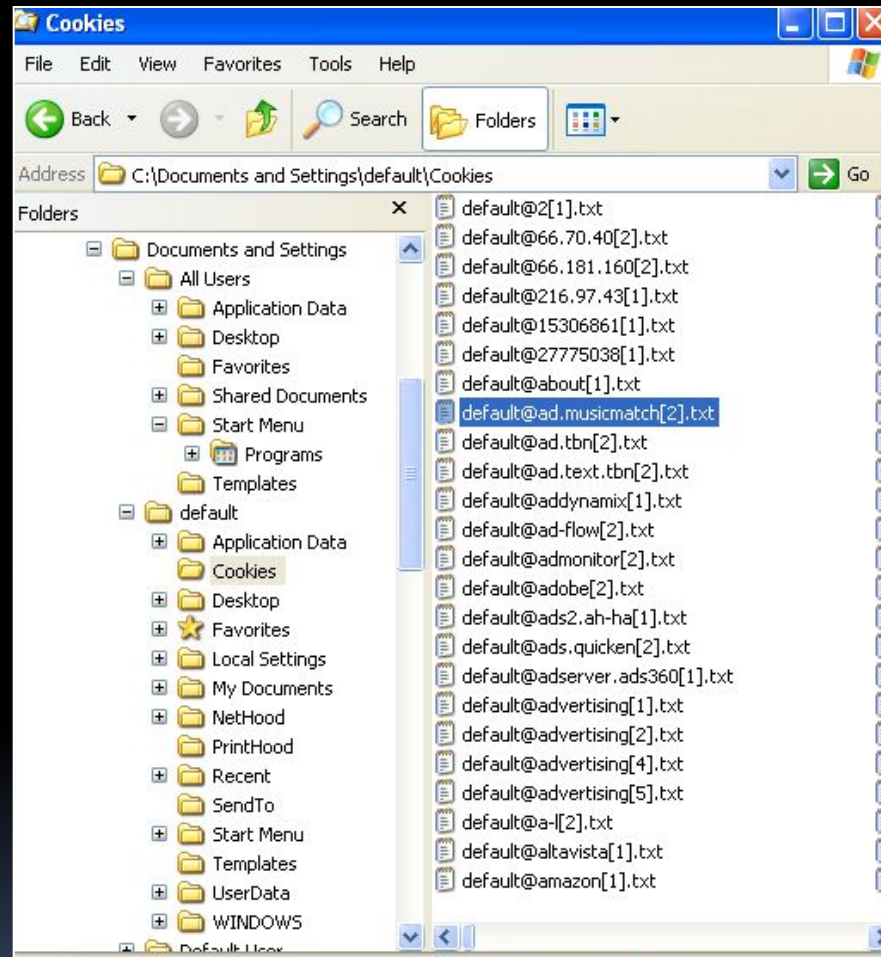


Cookies

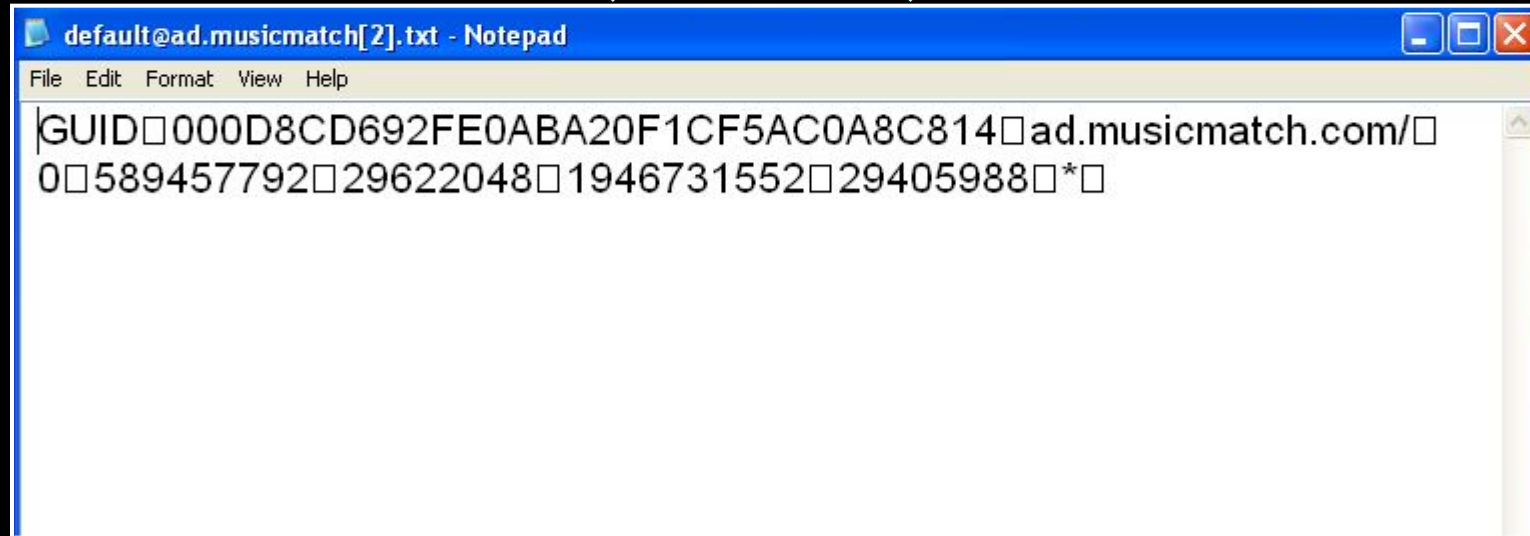
- **Cookies** are small files that are written to an individual's hard drive whenever a Web site is visited
- Legitimate purposes of cookies include recording information for future use; example: retail sites using “shopping carts”
- Questionable practices include banner ad companies tracking a user's browsing actions and placing banner ads on Web sites based on those actions



Example of Cookies



Global Unique Identifiers (GUIDs)



A screenshot of a Notepad window titled "default@ad.musicmatch[2].txt - Notepad". The window contains the following text: "GUID 000D8CD692FE0ABA20F1CF5AC0A8C814 ad.musicmatch.com/058945779229622048194673155229405988*"

- 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



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



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
- Tell children not to divulge personal information to online strangers
- Make sure registration forms have a privacy policy statement



Protecting Your Privacy At Home

- Cell phones have GPS capability
 - Parents, EMS can find people
 - Intrusive if employer tracks employee



Protecting Your Privacy at Work

- Laws do not protect employees from being monitored by their employers
- Companies are concerned about employees:
 - Giving trade secrets to competitors
 - Creating sexual harassment lawsuits by circulating offensive jokes via e-mail
- Three-quarters of large corporations monitor employees' phone calls, e-mail, Web browsing habits, and computer files



Protecting Privacy at Work

- Rules to follow while at work:
 1. Do not use the employer's phone for personal calls
 2. Do not use the employer's e-mail for personal messages
 3. Assume everything you do at work is being monitored



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



Computer Crime and Cybercrime

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



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 their name and charge items to that account
- Examples of information needed are name, address, social security number, and other personal information
- Laws limit liability to \$50 for each fraudulent charge
- An individual's credit report is affected by identity theft

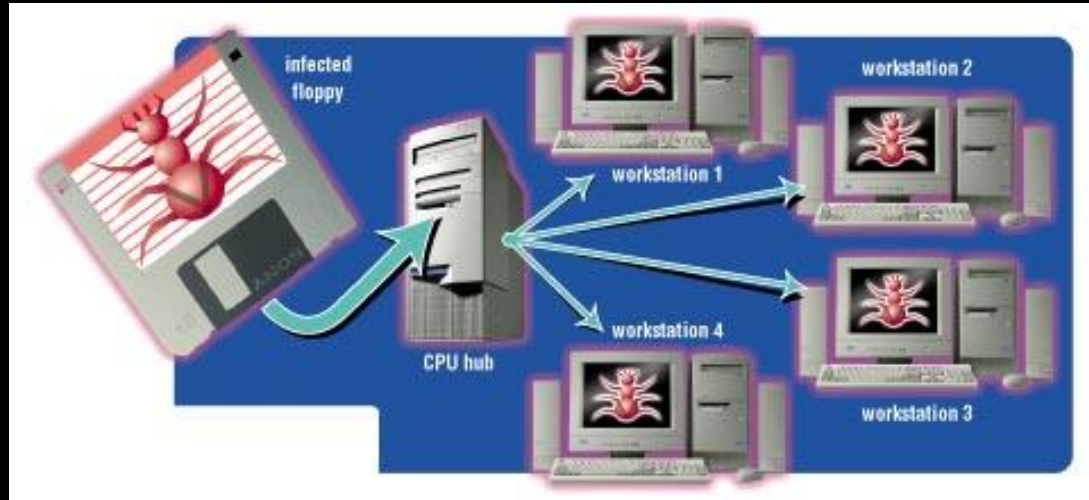


Computer Viruses

- **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



How Virus Infections Spread



- Virus Infections spread by:
 - Inserting a disk 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



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

Types of Viruses

- **Macro Viruses**

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



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



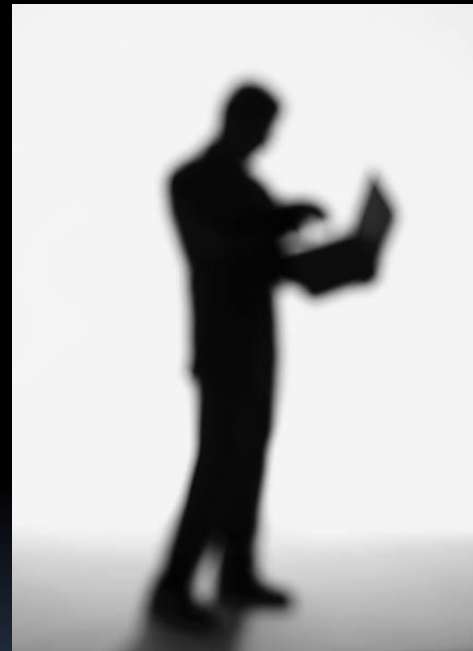
More Rogue Programs

- **Denial of Service Attack (DoS)**
 - Syn flooding
 - Overload an Internet server with a large number of requests
- **Trojan Horses**
 - Disguise themselves as useful programs
 - Contain hidden instructions
 - May erase data or cause other damage



Fraud and Theft

- **Selling social security numbers**
- **Memory shaving – taking RAM chips from computers**
- **Salami Shaving**
 - Programmer alters a program to take a small amount of money out of an account
- **Data Diddling**
 - Data is altered to hide theft



Techniques to Obtain Passwords

- Password guessing
- Shoulder surfing
- Packet sniffing
- Dumpster diving
- Social engineering
- Superuser status



Forgery and Blackmail

- Forgery
 - Internet data can appear to be coming from one source when its really coming from another
 - Forged e-mail and Web pages
- Blackmail
 - Adverse publicity fears

Meet the Attackers

- **Hackers**

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

- **Cyber Gangs**

- Bring crackers together by way of the Internet and meetings

Meet the Attackers

- **Crackers**

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

- **Virus Authors**

- Usually teenage males
- Push the boundaries of antivirus software
- Create viruses that are very damaging

More Attackers

- **Disgruntled Employees**
 - Sabotage their company's computer system
 - Create security holes called trap doors
 - May divulge trade secrets or destroy data
- **Swindlers**
 - Use the Internet to scam money from people
 - Use scams like **rip and tear**, **pumping and dumping**, and **bogus goods**
- **Spies**
 - Participate in corporate espionage
 - Are hackers or former employees
 - Involved in industrial espionage in 125 countries

More Attackers

- **Skills**

- Use Internet auctions
- Secret operatives who bid on a seller's item to drive up the bid

- **Cyberstalkers and Sexual Predators**

- Using the Internet to repeatedly harass or threaten
- Children are at risk from sexual predators



Security Risks

- **Computer security risk** is any event, action, or situation that leads to the loss of computer systems or their data
- **Wireless Networks**
 - Inherently insecure
 - Information sent over airwaves
 - Individual can drive around looking for a signal
- **Corporate Espionage**
 - On the rise
 - Often ex-employees
 - Trap doors



Information Warfare

- **Information warfare** is the use of information technologies to corrupt or destroy an enemy's information and industrial infrastructure
- An enemy attack would include:
 - Electronic warfare
 - Network warfare
 - Structural sabotage
- Information terrorism is a mounting threat



Protecting Your Computer System

- To protect a computer from power-related problems you should:
 - Use programs that have an auto save/auto recovery function
 - Equip the system with an uninterruptible power supply, a battery-powered device that automatically turns on when the power



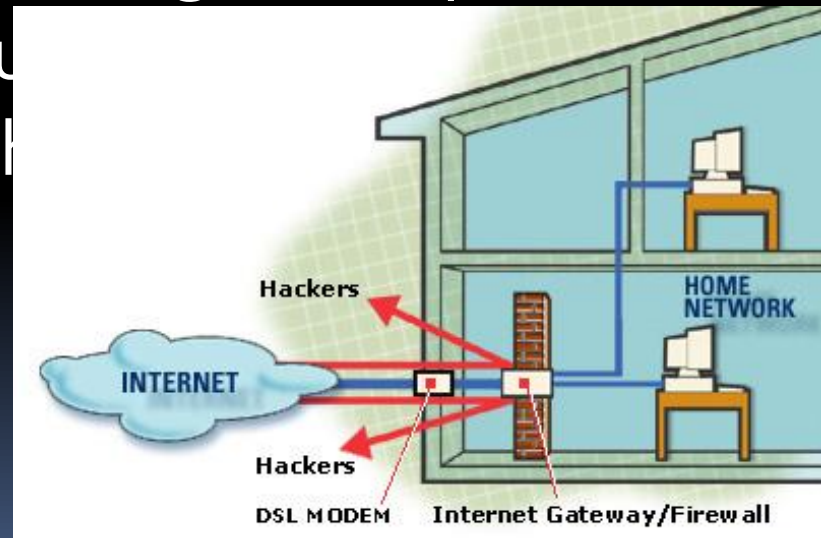
Controlling Access

- To control access to a computer:
 - Use **authentication passwords**
 - Use **callback systems**
 - Use **“know & have” authentication**
 - Tokens – Electronic devices that generate a logon code
 - Smartcards – Credit card-sized devices with internal memory
 - Biometric authentication – Voice recognition, retinal scans, thumbprints, and facial recognition



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 when being connected to the Internet



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



Preventing 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



The Encryption Debate

- **Encryption** is the coding and scrambling process by which a message is made unreadable except by the intended recipient
- Encryption is needed for electronic commerce
- The potential for encryption's misuse troubles law enforcement officials



Encryption Basics

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



Encryption Basics

- **Symmetric key encryption** 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



The Problem of Key Interception

- Rot-13 is not a secure encryption system
- Symmetric key encryption systems are vulnerable to **key interception**, or having their key stolen



Public Key Encryption

- **Public key encryption** uses two different keys
 - Public key is the encryption key
 - Private key is the decryption key
- They are used in e-commerce transactions
- A secure channel for information is provided when the keys are used



Digital Signatures and Certificates

- **Digital signatures** are a technique used to guarantee that a message has not been tampered with
- **Digital certificates** are a technique used to validate one's identity
- **Secure Electronic Transactions (SET)** are online shopping security standards used to protect merchants and customers from credit card fraud



Public Key Infrastructure (PKI)

- A **public key infrastructure** is a uniform set of encryption standards that specify how public key encryption, digital signatures, and digital certificates should be implemented



Encryption and Public Security Issues

- Encryption can be used for illegal as well as legitimate means
- Encryption will devastate law enforcement's ability to fight crime
- Law enforcement agencies are asking for laws enabling them to eavesdrop on encrypted messages
 - **Clipper Chip**
 - **Key escrow plan**
 - **Key recovery**



Summary

- Many websites collect and store information about Web users
- Cookies and GUIDs are used to collect data
- Computer crime and cybercrime
 - Identity theft
 - Computer viruses
 - Rogue programs
 - Forgery
 - Blackmail



Summary continued

- Computer criminals
 - Crackers
 - Cybergangs
 - Virus authors
 - Swindlers
 - Shills
 - Cyberstalkers
 - Sexual predators
- A computer security risk is any event, action, or situation that could lead to a loss or destruction of a computer or data



Summary continued

- Prevent security problems
 - Use an uninterruptible power supply to combat power-related problems
 - Use good passwords
 - Avoid scams and prevent cyberstalking
- Encryption refers to coding or scrambling data
- US government's key recovery plan is a new system that allows investigators to decrypt messages