Computer Security

An Introduction: Computer Security

- **Computer security** is the process of detecting and preventing any unauthorized use of your laptop/computer. It involves the process of safeguarding against trespassers from using your personal or office based computer resources with malicious intent or for their own gains, or even for gaining any access to them accidentally.

- In this lesson, we will cover the basics of computer security and how to deal with its various components and sub-components.

Why Do We Need Computer Security?

- Let us now see why do we need computer security. It is required for the following major reasons −
- To prevent damage of the hardware.
- To prevent theft or damage of the installed software.
- To prevent theft or damage of stored data and information.
- To prevent the disruption of service.
- Likewise, security system keeps the computer system safe by protecting the installed software and the stored data (information).

What do we need to Secure?

Now let's go directly to the point of what all to secure in a computer environment −

- First of all, is to check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment itself.
- People having access to computer systems should have their own user id with password protection.
- Monitors should be screen saver protected to hide the information from being displayed when the user is away or inactive.
- Secure your network especially wireless, passwords should be used.
- Internet equipment as routers to be protected with password.
- Data that you use to store information which can be financial, or non-financial by encryption.
- Information should be protected in all types of its representation in transmission by encrypting it.

Protection of Data and Information

- Following Are The Important Steps To Protect Data –
- Make Backup Of All Your Important Files.
- Keep Your System Virus By Using Anti-virus Software.
- Keep Updating Your Computer System.
- Run Disk Defragmenter And Disk Cleanup On Certain Interval Of Time.
- Use A Firewall.
- Use Anti-spyware Software.

- Further, if you use internet, then you need to take greater precaution. Consider the following points to understand the precautions that need to be taken –

1. Do not click on any link that you don’t know (as it may be dangerous for your computer - virus attack).
2. Do not open unauthorized an unlawful website (it may damage your computer system).
3. Do not download unsolicited data from unknown website.

Potential Losses due to Security Attacks

- The potential loses in this cyberspace are many even if you are using a single computer in your room. Here, I will be listing some examples that have a direct impact on you and on others –

1. **Losing you data** – If your computer has been hacked or infected, there is a big chance that all your stored data might be taken by the attacker.
2. **Bad usage of your computer resources** – This means that your network or computer can go in overload so you cannot access your genuine services or in a worst case scenario, it can be used by the hacker to attack another machine or network.

3. Reputation loss – Just think if your Facebook account or business email has been owned by a social engineering attack and it sends fake information to your friends, business partners. You will need time to gain back your reputation.

4. Identity theft – This is a case where your identity is stolen (photo, name surname, address, and credit card) and can be used for a crime like making false identity documents.

Security Breaches - Terminology

- Exposure
  - a form of possible loss or harm
- Vulnerability
  - a weakness in the system
- Attack
- Threats
  - Human attacks, natural disasters, errors
- Control – a protective measure
- Assets – hardware, software, data

Types of Security Breaches

- **Disclosure**: unauthorized access to info
  - Snooping
- **Deception**: acceptance of false data
  - Modification, spoofing, repudiation of origin, denial of receipt
- **Disruption**: prevention of correct operation
  - Modification, man-in-the-middle attack
- **Usurpation**: unauthorized control of some part of the system (*usurp*: take by force or without right)
  - Modification, spoofing, delay, denial of service

Security Components

- **Confidentiality**: The assets are accessible only by authorized parties.
  - Keeping data and resources hidden
- **Integrity**: The assets are modified only by authorized parties, and only in authorized ways.
  - **Data integrity** (integrity)
  - **Origin integrity** (authentication)
- **Availability**: Assets are accessible to authorized parties.
  - Enabling access to data and resources

Computing System Vulnerabilities

- Hardware vulnerabilities
- Software vulnerabilities
- Data vulnerabilities
- Human vulnerabilities ?

Software Vulnerabilities

- Destroyed (deleted) software
- Stolen (pirated) software
- Altered (but still run) software
  - Logic bomb
  - Trojan horse
  - Virus
  - Trapdoor
  - Information leaks

Data Security

- The *principle of adequate protection*
- Storage of encryption keys
- Software versus hardware methods

Other Exposed Assets

- **Storage media**
- **Networks**
- **Access**
- **Key people**

People Involved in Computer Crimes

- Amateurs
- Crackers
- Career Criminals

Methods of Defense

- Encryption
- Software controls
- Hardware controls
- Policies
- Physical controls

Encryption

- at the heart of all security methods
- Confidentiality of data
- Some protocols rely on encryption to ensure availability of resources.
- Encryption does not solve all computer security problems.

Software controls

- Internal program controls
- OS controls
- Development controls
- Software controls are usually the 1st aspects of computer security that come to mind.

Policies and Mechanisms

- Policy says what is, and is not, allowed
  - This defines “security” for the site/system/*etc*.
- Mechanisms enforce policies
- Mechanisms can be simple but effective
  - Example: frequent changes of passwords
- Composition of policies
  - If policies conflict, discrepancies may create security vulnerabilities
- Legal and ethical controls
  - Gradually evolving and maturing

Goals of Security

- Prevention
  - Prevent attackers from violating security policy
- Detection
  - Detect attackers' violation of security policy
- Recovery
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack succeeds

Basic Computer Security Checklist

- There are some basic things that everyone of us in every operating system need to do –

1. Check if the user is password protected.
2. Check if the operating system is being updated. In my case, I did a screenshot of my laptop which is a Windows 7.
3. Check if the antivirus or antimalware is installed and updated. In my case, I have a Kaspersky antivirus being updated.
4. Check for the unusual services running that consumes resources.

5. Check if your monitor is using a screen saver.
6. Check if the computer firewall is on or not.
7. Check if you are doing backups regularly.
8. Check if there are shares that are not useful.
9. Check if your account has full rights or is restricted.
10. Update other third party software’s.

Class Exercise

1. In your own understanding, what is computer security? [2]
2. Identify and list four risks to computer systems? [4]
3. What four loses can one suffer from the risks you have identified above? [4]
4. What are the four ways to protect your personal computer? [4]

Computer Crime

- Stealing and using or selling of data:
- Company data
- Personal information in company files

Computer Crime

Employees and individuals need to recognize the possible danger from computer systems and protect their assets.

Computer Crime
Security and Privacy

Data communications capabilities provides new challenges

Keep data secure

- Destruction
- Accidental damage
- Theft
- Espionage

Keep data private

- Salaries
- Medical information
- Social security numbers
- Bank balances

Data, [illegible] Computer Crime

Ways to secure data

- Locked servers
- Removable hard drives that are locked when not in use
- Hard disk drives requiring special tools for detachment
- Physical cages around computers that prohibit access
- Passwording files

Computer Crime

- Supplies for the Hacker
  - PC
  - Communications network
- Why hack?
  - Harass
  - Show-off
  - Gain access to computer services without paying
  - Obtain information to sell

Hackers are individuals who attempt to gain access to computer systems illegally

White

Computer Crime
Hackers for Hire

- Computer professionals hired to illicitly gain entry into a system
  - Reveal weak points
  - Protect the points
  - May not alert its own employees of the testing
- Tiger teams
- Intrusion tester
- White hat hackers

Computer Crime
What Systems Have Been Invaded?

- Corporate networks
  - Over half largest corporations were invaded
  - Competitors?
- Government networks
  - Dept of Defense attacked more than 200,000 times per year
  - Computer attack abilities of other nations?
- Web sites

Computer Crime

How Can Systems be Easily Compromised?

- Social engineering
  - Con artist – persuade others to give away their passwords over the phone
- Electronic pickpockets
  - Use computers to transfer or change assets to their advantage

Computer Crime
Frequently Reported Crimes

- Credit-card fraud
  - Numbers captured and used fraudulently
- Data communications fraud
  - Piggyback on someone else's network
  - Office network for personal purposes
  - Computer-directed diversion of funds
- Unauthorized access to computer files
  - Accessing confidential employee records
  - Theft of trade secrets and product pricing
- Unlawful copying of copyrighted software
  - Casual sharing of copyrighted software
  - Assembly-line copying

Computer Crimes

- Bomb
  - Program to trigger damage
  - Scheduled to run at a later date
  - May be found in software for general public, especially shareware
- Data diddling
  - Changing data before or as it enters the system
- Denial of service attack (DOS)
  - Hackers bombard a site with more request for service than it can possible handle
  - Prevents legitimate users from accessing the site
  - Appearance of requests coming from many different sites simultaneously

Computer Crimes

- Piggybacking
  - Original user does not sign off properly
  - Intruder gains accesses to files via the original user id
- Salami technique
  - Embezzlement
- Scavenging
  - Search garbage and recycling bins for personal information

Computer Crimes

- Trapdoor
  - Illicit program left within a completed legitimate program
  - Permits unauthorized and unknown entry to the program
- Trojan horse
  - Illegal instructions placed inside a legitimate program
  - Program does something useful and destructive at the same time
- Zapping
  - Software to bypass security systems

Computer Crimes

- Discovery
  - Difficult
  - Accidental
  - 85% of computer crimes are never reported
- Prosecution
  - Legal representatives lack technical knowledge to understand the crime

Computer Crime
Discovery and Prosecution

Computer Fraud and Abuse Act – 1986

- Computer criminals subject to
  - Fines
  - Jail time
  - Confiscation of hardware
- Supplemented by state statutes

Computer Crime
Discovery and Prosecution

Computer Forensics

Uncovering computer-stored information suitable for legal use

Security

System of safeguards designed to protect a computer system and data from deliberate or accidental damage

- Natural disasters
- Fire
- Accidents
- Vandalism
- Theft
- Theft or destruction of data
- Industrial espionage
- Hackers

Security
Identification and Access

- Provide access to authorized individuals only
- Uses one of more of the following systems
  - What you have
  - What you know
  - What you do
  - What you are

Security
Identification and Access

What You Have

- Key
- Badge
- Token
- Plastic card – magnetized strip
- Active badge – signals wearer's location using infrared signals

Security
Identification and Access

What You Know

- Password
- Identification number
- Combination

Security
Identification and Access

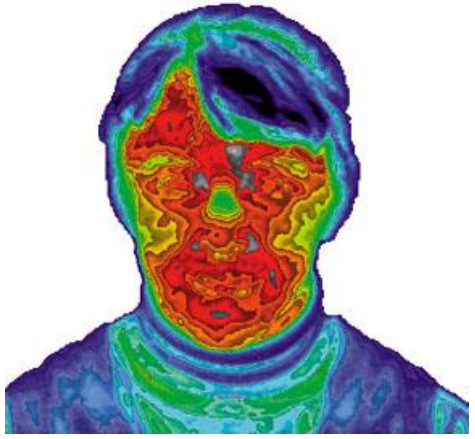
What You Do

- Verify signature – software verifies scanned and online signatures

Security
Identification and Access

What You Are

- Biometrics – science of measuring individual body characteristics
- Fingerprints
- Voice pattern
- Retina of the eye
- Entire face



Security
Identification and Access

- Internal controls
  - Transaction log
- Auditor checks
  - Who has accessed data during periods when that data is not usually used?
  - Off-the-shelf software to access the validity and accuracy of the system's operations and output

Security
Identification and Access

- Secured waste
  - Shredders
  - Locked trash barrels
- Applicant screening
  - Verify the facts on a resume
  - Background checks
- Built-in software protection
  - Record unauthorized access attempts
  - User profile

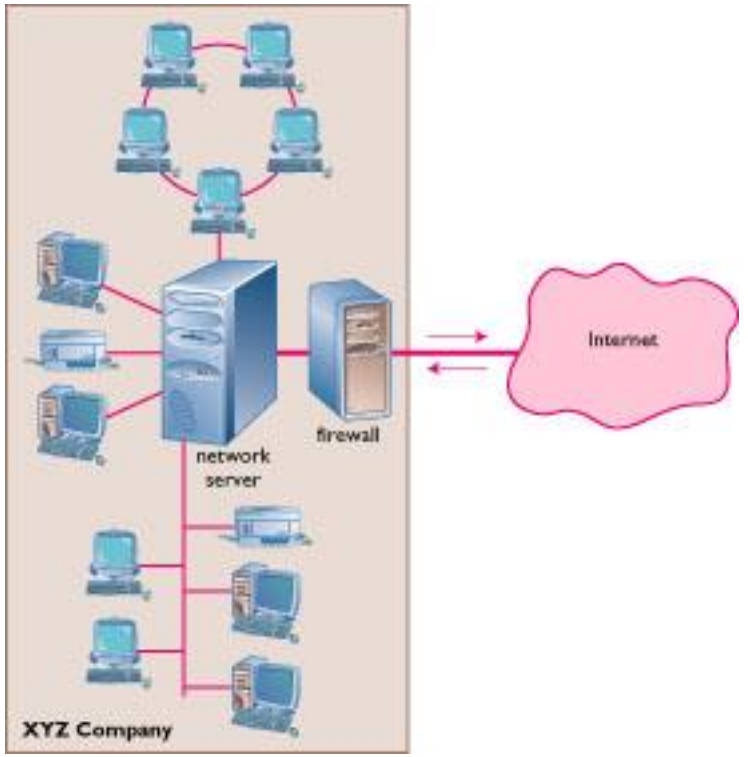
Security
Software Security

Ownership

- Company if programmer is employee
- Contractual agreement if the programmer is not an employee
- Software can be copyrighted

Security
The Internet

- Firewall
  - Dedicated computer that governs interaction between internal network and the Internet
- Encryption
  - Data Encryption Standard (DES)



Security
Personal Computers

- Physical security with locks and cables
- Surge protector
- Uninterruptible power supply (UPS)
- Backup files regularly and systematically

Disaster Recovery

Hardware loss

- Can be replaced
- Temporarily diminished processing ability

Software loss

- Industry standard – make backups of program files

Disaster Recovery

Data loss

- Reassemble records
  - Customer information
  - Accounting data
  - Design information
- Major costs and time

Disaster Recovery Plan

Restoring computer processing operations and data files if operations are halted or files are damaged by major destruction

Disaster Recovery Plan
Approaches

- Manual services temporarily
- Purchase time from a service bureau
- Mutual aid pack
  - Two or more companies will lend each other computer power
  - Problem if regional disaster

Disaster Recovery Plan
Approaches

- Consortium
  - Joint venture
  - Complete computer system
  - Routinely tested
  - Used only if disaster
  - Sites
    - Hot site – fully equipped and environmentally controlled computer center
    - Cold site – environmentally suitable empty shell

Disaster Recovery Plan
Advance Arrangements

Everything except hardware safely stored in geographically distant locations

- Program and data files
- Program listings
- Program and operating systems documentation
- Hardware inventory lists
- Output forms
- Copy of the disaster plan manual

Disaster Recovery Plan
Includes

- Priorities for programs
- Plans for notifying employees
- List of needed equipment and where it is located
- Alternative computing facilities
- Procedures for handling input and output data
- Emergency Drills

Backup
Why Backup?

“If you are not backing up your files regularly, you deserve to lose them.”

Average user experiences loss once a year

Backup
What Can Cause Data Loss?

- Incorrect software use
- Input data incorrectly
- Software may harm data
- Hard disk malfunctions
- Accidentally delete files
- Virus infection

Backup

Methods

Full backup

Differential backup

Incremental backup

Media

Diskette
Tape
Zip disk
CD-R / CR-RW
DVD-RAM
Mirrored hard drive

Pests

Invade the computer system and cause something unexpected to occur

May interfere with function of PC

Worms

- Rare
- Transfers over a network
- Plants as a separate file on the target’s computer

Viruses

- Illicit instructions that pass themselves on to other programs
  - Benign
  - Damaging to computer
- Digital vandalism

Viruses

Vaccine or antivirus

- Stops the spread of and eradicates the virus
- Install software
- Download signature files regularly

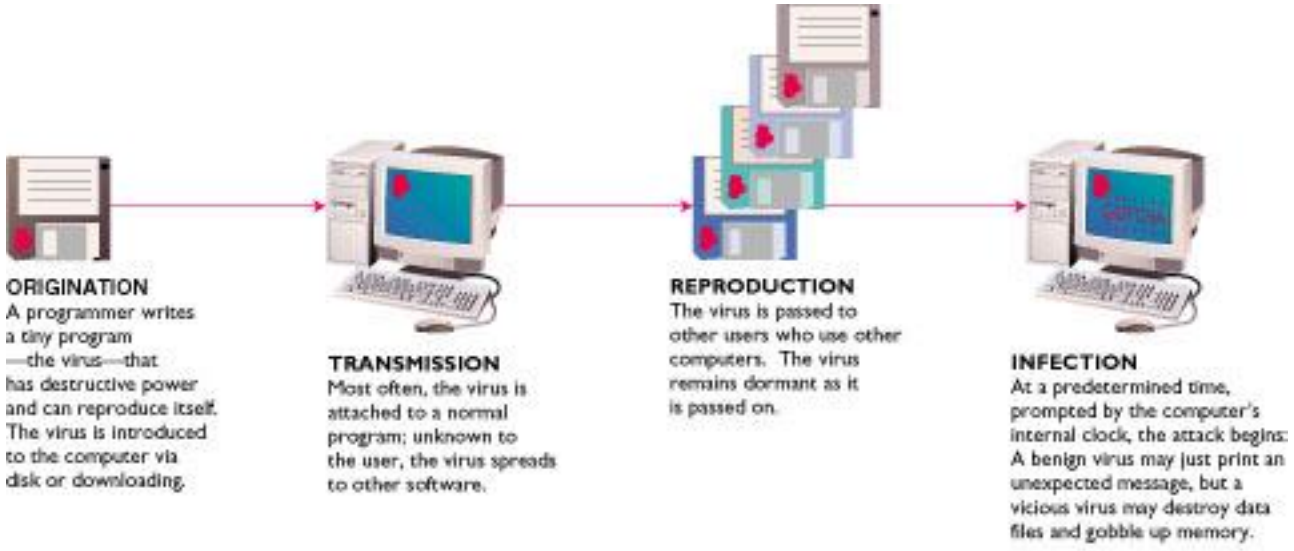
Viruses

- Retrovirus
  - Fights the vaccine and may delete the antivirus software
- Costs
  - Billions of dollars a year
  - Aggravation to individual users

Virus Transmission

Networks

Diskettes



Virus
Getting Infected

- Executing the virus program
- Booting from a diskette containing an infected boot sector including accidentally leaving a “non-system disk” in the floppy drive
- Downloading an infected file and executing it
- Opening an infected e-mail attachment
- By viewing e-mail in some versions of Microsoft Outlook

Virus
Precautions

- Be wary of free software from the Internet or friends
- Only install programs from diskettes in sealed packages
- Use virus-scanning software to check any file or document before loading it onto your hard disk

Privacy

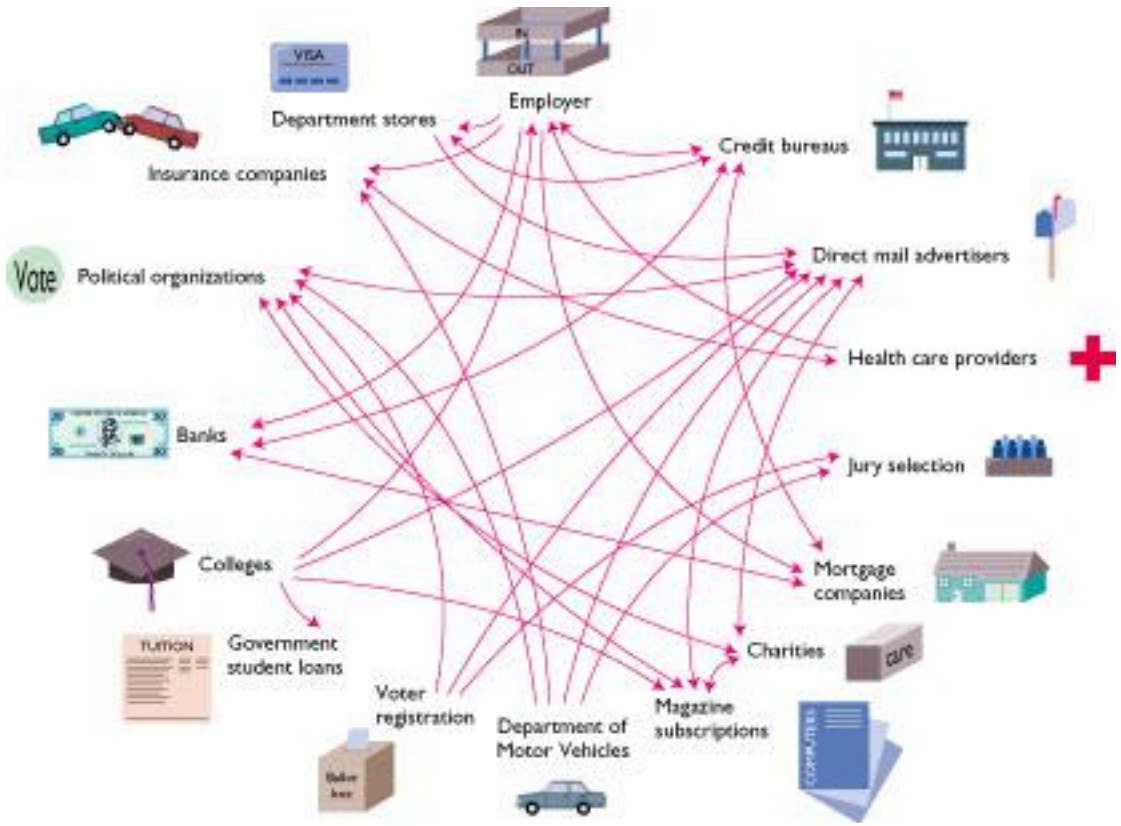
- Where is my data?
- How is it used?
- Who sees it?
- Is anything private anymore?

Everything about you is in at least one computer file

Privacy
How Did They Get My Data?

- Loans
- Charge accounts
- Orders via mail
- Magazine subscriptions
- Tax forms
- Applications for schools, jobs, clubs
- Insurance claim
- Hospital stay
- Sending checks
- Fund-raisers
- Advertisers
- Warranties
- Military draft registration
- Court petition

Privacy
How Did They Get My Data?



Privacy Legislation

- Fair Credit Reporting Act – 1970
- Freedom of Information Act – 1970
- Federal Privacy Act – 1974
- Video Privacy Protection act – 1988
- Computer Matching and Privacy Protections Act – 1988

Privacy
Your Boss is Spying on You!

Monitoring software

- Screens
- E-mail
- Keystrokes per minute
- Length of breaks
- What computer files are used and for how long

Privacy groups want legislation requiring employers to alert employees that they are being monitored.

Privacy
Monitoring by Web Sites

Records:

- City
- Site you just left
- Everything you do while on the site
- Hardware and software you use
- Click stream
  - Series of clicks that link from site to site
  - History of what the user chooses to view

Privacy
Monitoring by Web Sites

Cookie

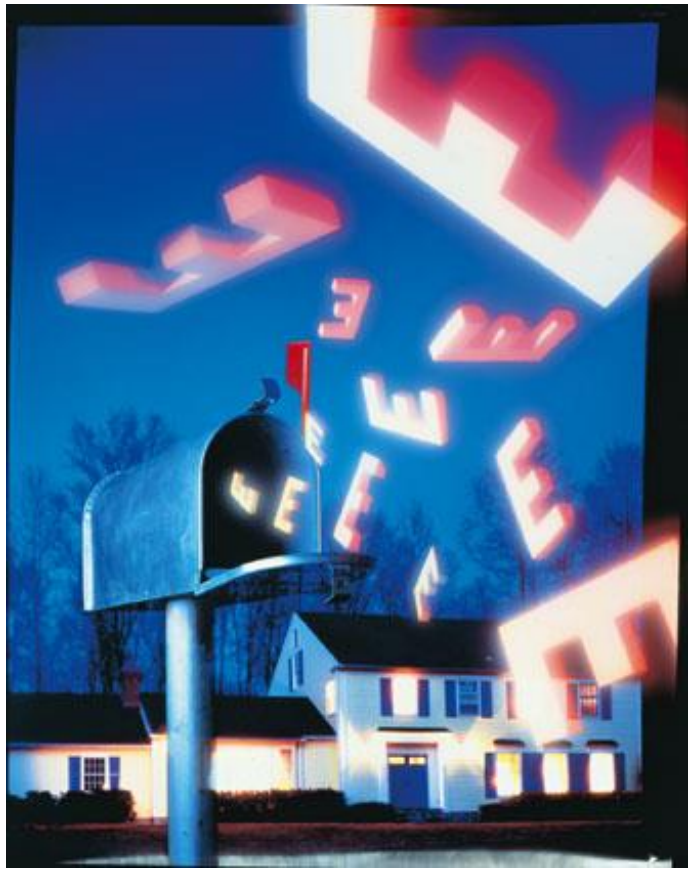
- Stores information about you
- Located on your hard drive
- Beneficial uses
  - Viewing preferences
  - Online shopping
  - Secure sites retain password in cookie
- Controversial use
  - Tracking surfing habits for advertisers
- Can set browser to refuse cookies or warn before storing
- Software available to manage cookies

Privacy

P3P
Platform for Privacy Preference Project

- Standards proposed by the World Wide Web Consortium (W3C)
  - User sets privacy preferences
  - Web server transmits privacy policies
  - Software determines if web site meets users' requirements
- Participation by web site is voluntary

Junk e-mail



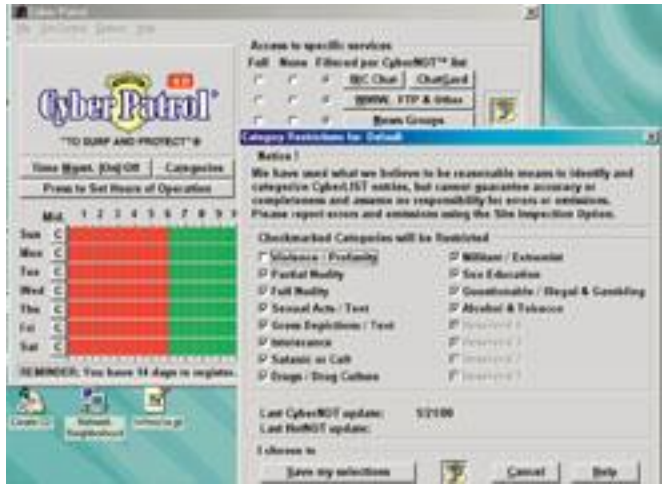
- Cheaper than snail mail
- Spamming
  - Sends e-mail messages to “everyone”
  - Abandons the originating site

Junk e-mail

- Help eliminate junk e-mail
  - Do not complete a member profile with online service
  - Do not fill in registration forms unless the purveyor promises not to sell or exchange your information
  - Never respond to spamming
- Use filter software
- States are beginning to provide laws banning unsolicited junk e-mail

Protecting Children

- Blocking software – high-tech chaperone
- Examine browser history to see what sites are visited
- Locate computer in a semipublic, high-traffic location of your home



Protecting Children

Laws

Communications Decency Act – 1996

Children’s Online Privacy Protection Act (COPPA) – 2000