Security and Privacy

Chapter 10
Computers and the Internet

Data Security
Decentralized networks lend data vulnerable to intentional destruction, alteration, theft, and espionage.

The Network Criminal
The people who attack the vulnerability of data systems possess significant computer expertise and/or have access to sensitive data.

Hackers
Most computer system intruders are not teenagers. Instead, most hackers are competitors who steal proprietary or sensitive government information.

Hackers' Prey
Hackers begin by persuading unsuspecting people to give away their passwords over the phone. Employees should be alerted to such scams.

Employee Passwords
Employees use passwords to work on computer systems. Employers expect these passwords to be kept secret from others.
Employee Secrets

The next five slides offer helpful suggestions and guidelines to keep employee secrets, secret.

1. Avoid Common Names

Common names associated with you are naturally easy for you to remember, but they are easily cracked. Pet names are an example.

2. Mix-n-Match Characters

Make your password a mix of:
- letters and numbers
- upper and lower case
- alphabetic and non-alphabetic characters

not2hard
JUST4u
Han$on

3. Store Passwords Wisely

Keep your password in your head or in a safe, not in an obvious location.

4. Change Password Often

Changing your password should become a habit so that you lessen the chance of it becoming known to intruders.

5. Avoid Hacker Scams

In these scams, the hacker poses as a person to whom you can confide your password. Regardless of the ruse, the wise user will not give their password to anyone.
Computer Crime

Computer crime includes:
- Credit card fraud
- Data communications fraud
- Unauthorized access
- Unlawful copying

Credit Card Fraud

Credit card customer numbers pass between public and private networks. Sometimes these numbers are captured by computer criminals and used to commit fraud.

Data Communications Fraud

This form of fraud involves the interception of network passwords or packets of data passing through networks.

Unauthorized Access

Hackers try to gain access to confidential employee records, company trade secrets and product pricing structures, and much more.

Unlawful Copying

This category of computer crime results in major losses for computer vendors.

Compromising Security

Without realizing it, employers and employees can compromise the security of their computer system. The following slides present some examples of how a system could be compromised.
Some Bad Guy Tricks

- Bomb
- Data diddling
- Piggybacking
- Salami Technique
- Scavenging
- Trapdoor
- Trojan Horse
- Zapping

Bomb

- A “bomb” causes a program to trigger damage under certain conditions in the future

Data Diddling

- Data diddling refers to changing data before or as it enters the system

Piggybacking

- An illicit user “rides” into the system on the back of another user

Salami Technique

- Small “slices” of money are squirreled away to a secret account

Scavenging

- Passwords and other account information may be found in trash cans or recycling bins
**Trapdoor**

- The original programmer may leave an unauthorized point of entry to a program.

---

**Trojan Horse**

- Illegal instructions are hidden in the middle of the program.
- These Trojan Horse instructions cause something destructive in addition to the intended function of the program.

---

**Zapping**

- Zapping encompasses a variety of software which bypass all security systems.

---

**White Hat Hackers**

- Many companies hire professionals to uncover security problems by trying to break into the system.

---

**Detecting Computer Crime**

Most cases are discovered by accident—by actions having nothing to do with computers. The **Computer Fraud and Abuse Act of 1986** has improved awareness of computer-related crimes.

---

**Prosecuting Computer Crime**

- Eighty-five percent of detected computer crime is not reported.
- Prosecution is further hampered by law enforcement officers, attorneys, and judges who do not fully understand the nature of the violation.
Security
A system of safeguards is needed to protect a computer system and data from deliberate or accidental damage or access by unauthorized persons.

Authorized Access
To assure that only the right person is accessing the right computer system, various means have been developed based on:
- What you have
- What you do
- What you know
- What you are

What You Have
This means of authentication is based on your having a physical thing. It might be a key, badge, token, or plastic card.

What You Know
Many systems verify authorized access based on what you know. This might be a password, identification number, or the correct combination of numbers on locks.

What You Do
This mode of authorized access is based on something you do that is unique such as your signature.

What You Are
This security system uses biometrics—the science of measuring individual body characteristics. Fingerprints, retinal scans, and hand characteristics are examples of what you are.
Compromised Systems

When a computer system has been compromised by a natural or man-made disaster, the resulting problems might include:
- Loss of hardware
- Loss of software
- Loss of data

Disaster Recovery Plan

- Spells out a method for restoring computer processing operations and data files
- Companies should perform emergency recovery drills

Recovery From Loss of Hardware

There are various approaches to restoring computer processing operations:
- revert to manual services.
- temporarily use a service bureau.
- mutual aid from another company.
- pre-planned consortium facilities.

Software Security

Software security has been an industry concern for years.
At risk here is who owns custom-made software.

Company Ownership of Software

If the programmer was employed by the company for whom the software was written, then the company owns the software.

Programmer Ownership of Custom Software

If the programmer was hired as a consultant, then ownership should have been addressed in the contract between the company and the programmer.
To prevent theft or alteration of data, security techniques can include:

- Secured waste
- Internal controls
- Auditor checks
- Applicant screening
- Passwords
- Built-in software protection
- Backup systems
- Secured waste
- Internal controls
- Auditor checks
- Applicant screening
- Passwords
- Built-in software protection
- Backup systems

Discarded printouts, printer ribbons, and the like can be sources of data leaks to unauthorized persons. Paper shredders and locked trash barrels can secure these waste products.

These are controls that are planned as part of the computer system. The transaction log is an example. This log records all successful or failed attempts to access certain data.

Auditors not only go over the financial books of a company, but also review computer programs and data. Discrepancies are noted and investigated.

The people who will be working with the computer system should be honest employees. Verifying an applicant’s résumé can weed out dishonest employees before they are hired.

A password is a secret word, number, or combination of the two. It should not be divulged nor should it be so simple as to be easily cracked.
Built-in Software Protection

Software can be built into operating systems in ways to restrict access to computer systems. This kind of protection matches an authorized user with only the data that user should access.

Personal Computer Security

- Secure PC hardware with locks and cables
- Use surge protectors

Backup Systems

Backing up files on a regular basis is a wise precaution—not only for big business, but for the consumer as well.

Pest Programs

Not all programmers write useful or beneficial programs. Some programmers write pest programs that can destroy data, or in the least, disrupt computer systems.

Why Write Pest Programs?

Pest programs are written to show off programming prowess, revenge, sabotage, intellectual curiosity, or a desire for notoriety. Pest programs include worms and viruses.

Computer Worms

A worm is a program that transfers itself from computer to computer over a network. At target computers, the worm creates a separate file for itself.
**Computer Virus**

A computer virus is a set of illicit instructions that gets passed on to other programs or documents with which it comes in contact. Viruses can change or delete files, display words, or produce bizarre screen effects.

**Transmission of Viruses**

Viruses can be passed on via:
- diskettes
- a LAN
- e-mail attachments
- a WAN, including the Internet

**Virus Myths**

- You cannot get a virus just by being on-line
- You cannot get a virus from reading email
- You cannot get a virus from data or graphics files

**Virus Vaccines**

Since viruses are programs written by programmers, it takes another programmer to detect and remove the virus. These anti-virus programs are called vaccines.

**Your Personal Data**

**FACT**: Computer data about you is bought, sold, and traded every day.
**FACT**: More often than not, the exchange of data about you occurs without your knowledge.

**Your Personal Privacy**

The front line of defense in protecting your personal privacy begins with you.

All those forms, surveys, credit card transactions, etc. generate a vast amount of data about you.
### Privacy Legislation

- Fair Credit Reporting Act
- Freedom of Information Act
- Federal Privacy Act
- Video Privacy Protection Act
- Computer Matching/Privacy Protection Act

### Network Security

One or more of the following may be needed to keep data within a network secure:
- Firewalls
- Encryption
- Surveillance software
- Anonymity

### Firewalls

This is a simple method to prevent unauthorized access of a network from the outside.

### Encryption

Encryption is scrambling data into secret codes by using elaborate mathematical functions. Intercepting scrambled data is of no use to computer criminals.

### Surveillance Software

In addition to firewalls and encryption methods, employers might use software that monitors the activity of their workers.

### Anonymity

Network security can also include keeping the e-mail address identity of employees anonymous. This measure reduces junk e-mailings and protects the employee's identity.
**Junk Email (SPAM)**
- Newsgroup messages are a prime source of email addresses
- Use of filter software reduces the amount of SPAM received

**Protecting Children**
- Blocking software is used to prevent access to known objectionable web sites
- The Children’s Online Privacy Act requires web sites to obtain parental consent before obtaining information from children under 13

**Ethics and Privacy**
- Suppose you are a programmer for a medical organization, and while working, you see records about a celebrity. Is it ethical to describe the medical treatment to your friends?

**Conclusion**
- Security and privacy are important issues in the Information Age. The computer industry as well as private citizens share responsibility in addressing these issues.