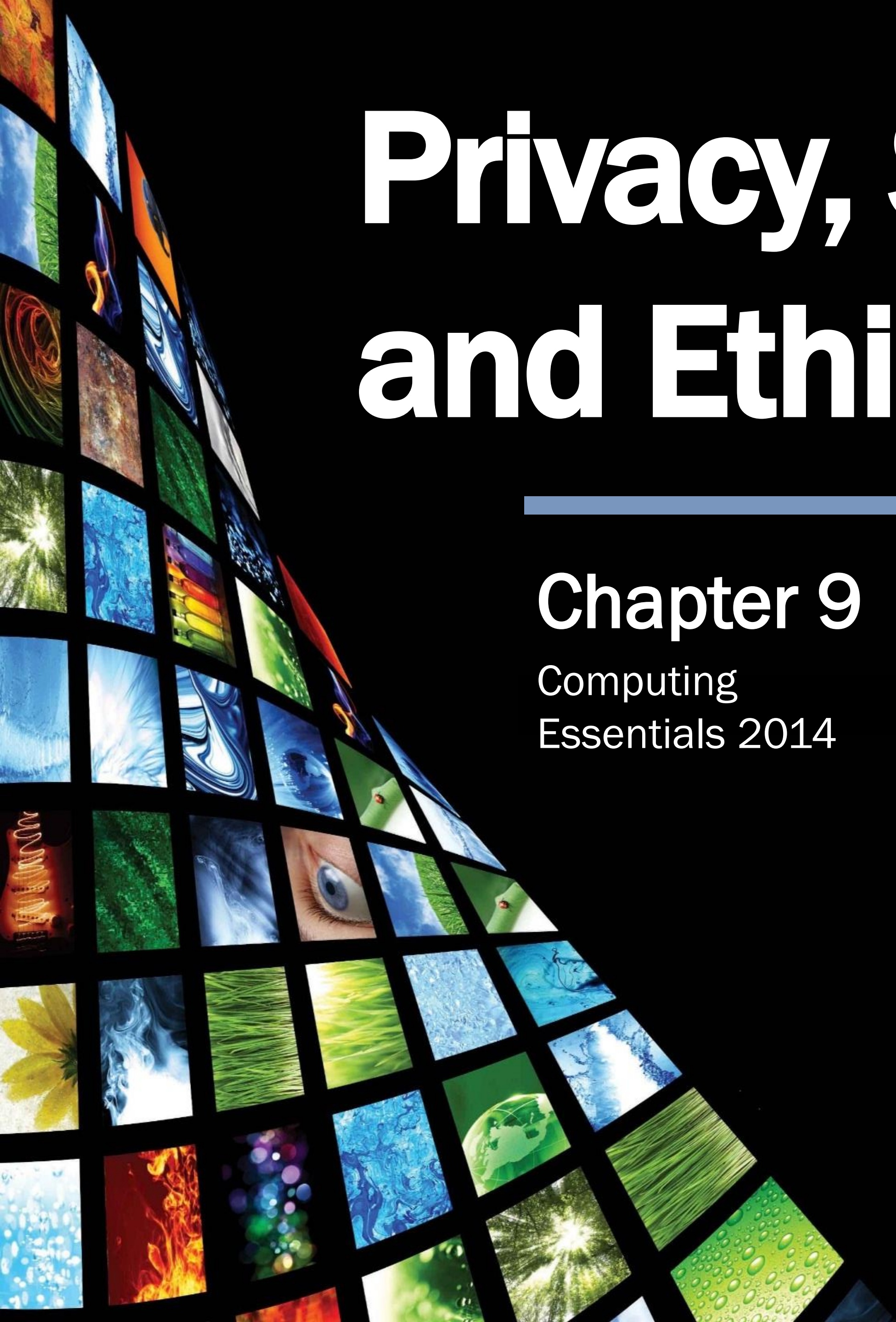


Privacy, Security, and Ethics

Chapter 9

Computing
Essentials 2014

Edited/Modified by Nicole Tobias

Competencies (Page 1 of 3)

- Identify the most significant concerns for effective implementation of computer technology.
- Discuss the primary privacy issues of accuracy, property, and access.
- Describe the impact of large databases, private networks, the Internet, and the Web on privacy.
- Discuss online identity and major laws on privacy.

Competencies (Page 2 of 3)

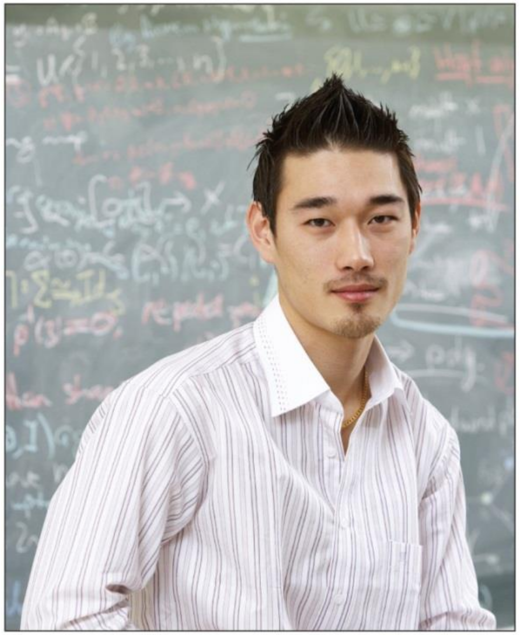
- Discuss cybercrimes including creation of malicious programs such as viruses, worms, Trojan horse, and zombies as well as denial of service attacks, Internet scams, social networking risks, cyberbullying, rogue Wi-Fi hotspots, theft, and data manipulation.
- Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.

Competencies (Page 3 of 3)

- Discuss computer ethics including copyright law, software piracy, digital rights management , the Digital Millennium Copyright Act, as well as plagiarism and ways to identify plagiarism.

Introduction

- The ubiquitous use of computers and technology prompts some very important questions about the use of personal data and our right to privacy.
- This chapter covers issues related to the impact of technology on people and how to protect ourselves on the Web.



Remember Chapter 1?

- What is in an information system?
  - People
  - Procedures
  - Software
  - Hardware
  - Data
  - Connectivity

Effects of Technology

- Positive?

- Negative?

- Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects.

People

- The most significant concerns are
  - Privacy
    - What are the threats to personal privacy and how can we protect ourselves?
  - Security
    - How can access to sensitive information be controlled and how can we secure hardware and software?
  - Ethics
    - How do the actions of individual users and companies affect society?

Privacy

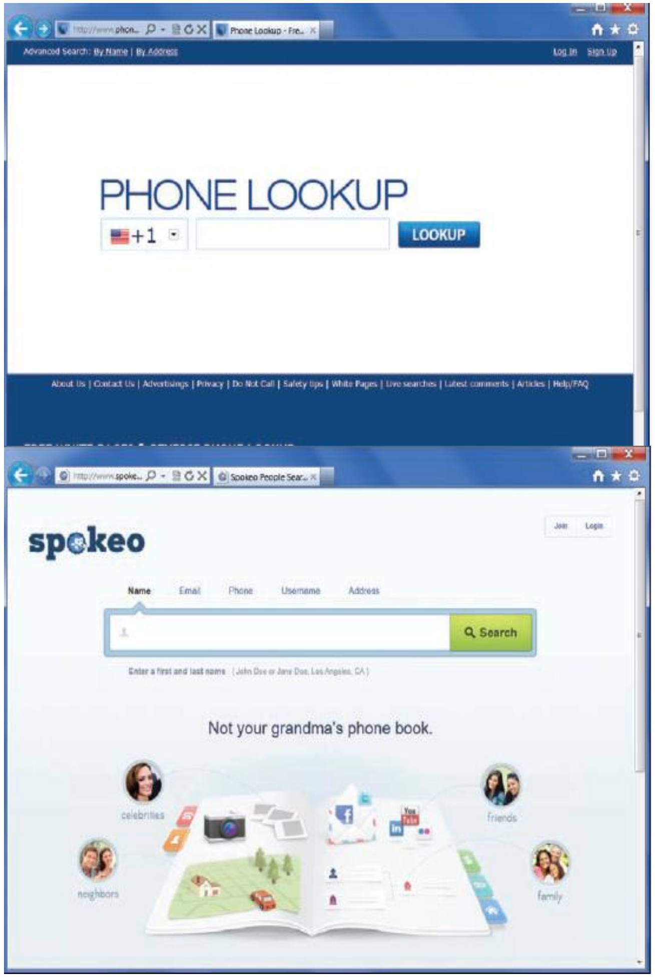
- Privacy – concerns the collection and use of data about individuals
- Three primary privacy issues:
    - Accuracy
    - Property
    - Access

Privacy

- Accuracy
  - relates to the responsibility of those who collect data to ensure that the data is correct
- Property
  - relates to who owns data and rights to software
- Access
  - relates to the responsibility of those who have data to control who is able to use that data

Large Databases (Page 1 of 2)

- Large organizations compile information about us.
- Federal government has over 2,000 databases
- Telephone companies
  - Reverse directory lists of calls we make
- Supermarkets
  - What we buy and when

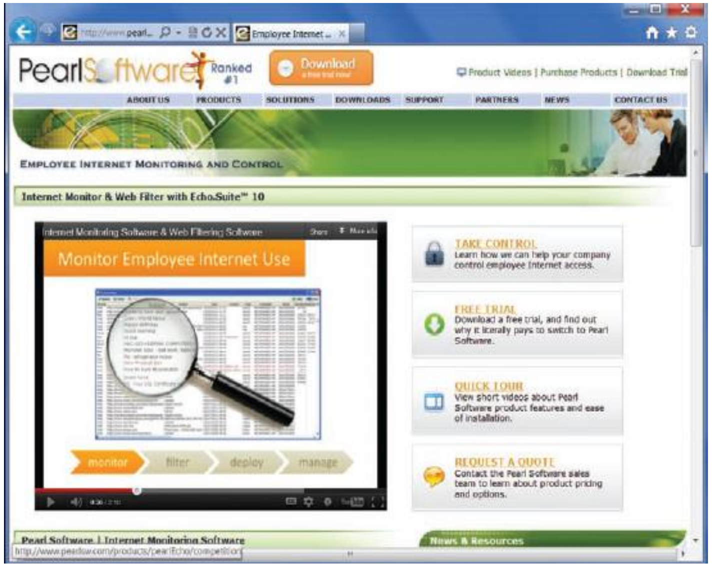

Phone Lookup - Fre...
Advanced Search: By Name | By Address
Log In Sign Up
PHONE LOOKUP
+1
LOOKUP
About Us | Contact Us | Advertisings | Privacy | Do Not Call | Safety tips | White Pages | Live searches | Latest comments | Articles | Help/FAQ
Spokeo People Sear...
spokeo
Join Login
Name Email Phone Username Address
Search
Enter a first and last name (John Doe or Jane Doe, Los Angeles, CA)
Not your grandma's phone book.
celebrities
friends
neighbors
family

Large Databases (Page 2 of 2)

- **Information resellers or information brokers**
  - Collect and sell personal data
  - Electronic profiles easily created
- **Personal information is a marketable commodity, which raises many issues:**
  - Collecting public, but personally identifying information (e.g., Google's Street View)
  - Spreading information without personal consent, leading to identity theft
  - Spreading inaccurate information
    - Mistaken identity
    - Freedom of Information Act

Private Networks

- Employers can monitor e-mail legally
  - 75 percent of all businesses search employees' electronic mail and computer files using snoopware
  - A proposed law could prohibit this type of electronic monitoring or at least require the employer to notify the employee first


http://www.pearl...
Employee Internet ...
PearlSoftware Ranked #1
Download a free trial now!
Product Videos | Purchase Products | Download Trial
ABOUT US
PRODUCTS
SOLUTIONS
DOWNLOADS
SUPPORT
PARTNERS
NEWS
CONTACT US
EMPLOYEE INTERNET MONITORING AND CONTROL
Internet Monitoring Software & Web Filtering Software
Share
More info
monitor
filter
deploy
manage
News & Resources
http://www.pearlsw.com/products/pearlEcho/competition

Internet Monitor & Web Filter with Echo.Suite™ 10

Monitor Employee Internet Use

TAKE CONTROL
Learn how we can help your company control employee Internet access.

FREE TRIAL
Download a free trial, and find out why it literally pays to switch to Pearl Software.

QUICK TOUR
View short videos about Pearl Software product features and ease of installation.

REQUEST A QUOTE
Contact the Pearl Software sales team to learn about product pricing and options.

Pearl Software | Internet Monitoring Software

The Internet and the Web

- Do you think that your emails are private?
  - illusion of anonymity
- IP addresses used for tracing and investigating computer crimes
- Browsing the Web
  - History files
  - Temporary Internet files

Viewing and Blocking Cookies

- Cookies
    - Small pieces of information that are deposited on your hard disk from web sites you have visited
        - First-party cookies
            - Generated by current website
        - Third-party cookies
            - Generated by an advertising company

Web bugs

- Invisible images or HTML code hidden within a web page or e-mail message.
- Used to transmit information without your knowledge back to the source of the bug.

- Example
  - Mass e-mailings from spammers
  - Reason for some e-mail programs blocking emails with Images and HTML

Spyware

- Wide range of programs
- Designed and used to secretly record and report an individual's activities on the Internet.
- Possible changes made to browsers to do so.
- Most invasive and dangerous type
  - Computer Monitoring software
  - A.k.a. keystroke loggers
    - Can be legally used by companies and law enforcement

Online Identity

- The information that people voluntarily post about themselves online
- Archiving and search features of the Web make it available indefinitely
- Major Laws on Privacy
  - Gramm-Leach-Bliley Act
    - Protects financial information
  - Health Insurance Portability and Accountability Act (HIPAA)
    - Protects medical records
  - Family Educational Rights and Privacy Act (FERPA)
    - Restricts disclosure of educational records

Security

- Security involves protecting individuals and organizations from theft and danger

- Hackers
  - Gain unauthorized access
  - *Not all hackers are intent on malicious actions and are not all criminals

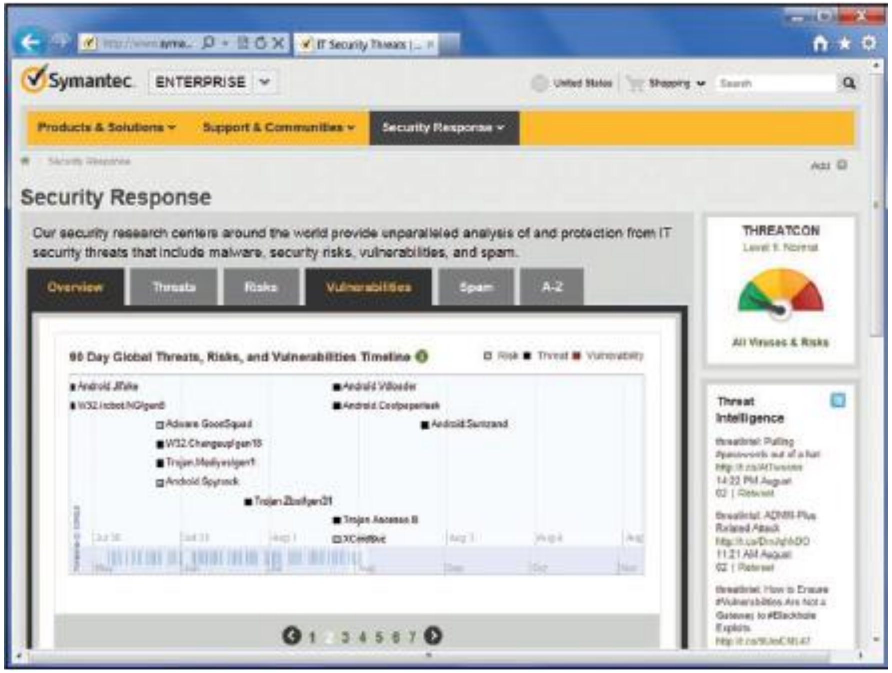
Cybercrime

- Cybercrime or computer crime is any offense that involves a computer and a network
- Recent estimates
  - Affects 400 million people
  - Costs over $400 billion dollars

    (Each Year)
- Malicious programs, denial of service attacks, Internet scams, theft and data manipulation

Computer Crime (Page 1 of 6)

- Malicious Programs - Malware
  - (1) Viruses
  - (2) Worms
  - (3) Trojan horse
- Zombies
  - BotNets



Security Response

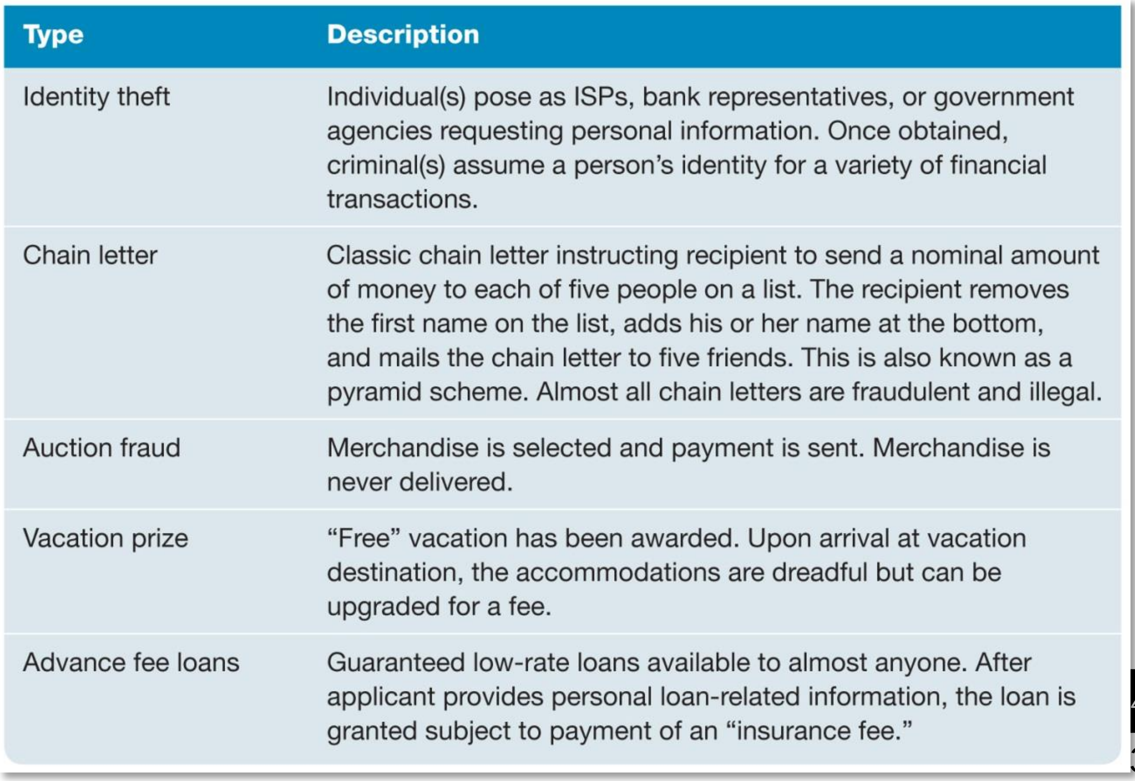
Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam.

Computer Crime (Page 2 of 6)

- **Denial of Service**
  - (DoS) attack
  - Attempts to slow down or stop a computer system by flooding it with requests for info and data.
  - Targets
    - ISP and Websites
  - Once attacked
    - Servers are overwhelmed and unable to respond
    - Effectively the website is shut down

Computer Crime (Page 3 of 6)

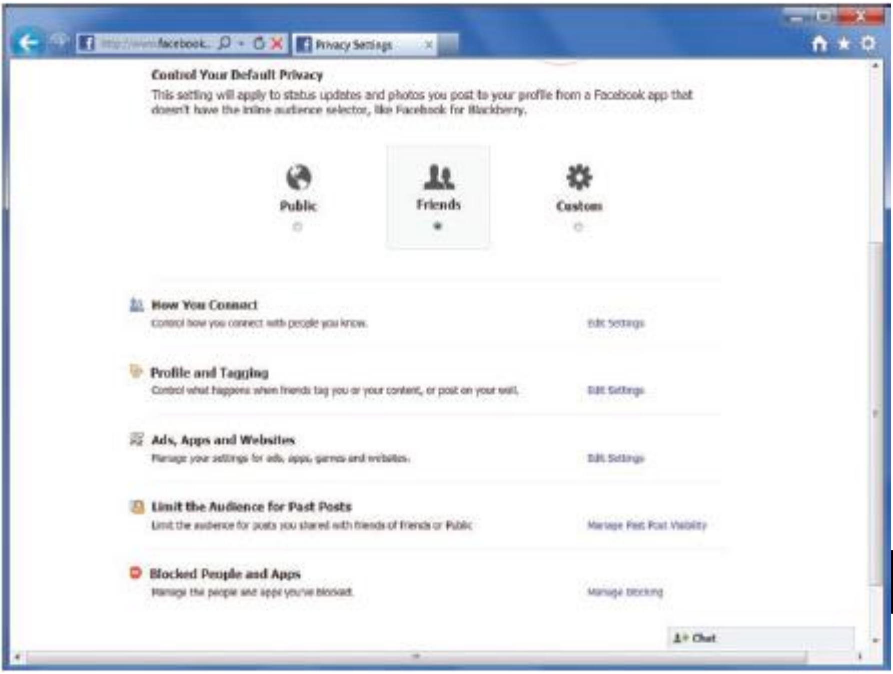
- Internet scams
  - Scam = Fraudulent or deceptive act or operation designed to trick individuals into providing information or wasting time.
  - Phishing



Type	Description
Identity theft	Individual(s) pose as ISPs, bank representatives, or government agencies requesting personal information. Once obtained, criminal(s) assume a person's identity for a variety of financial transactions.
Chain letter	Classic chain letter instructing recipient to send a nominal amount of money to each of five people on a list. The recipient removes the first name on the list, adds his or her name at the bottom, and mails the chain letter to five friends. This is also known as a pyramid scheme. Almost all chain letters are fraudulent and illegal.
Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
Vacation prize	"Free" vacation has been awarded. Upon arrival at vacation destination, the accommodations are dreadful but can be upgraded for a fee.
Advance fee loans	Guaranteed low-rate loans available to almost anyone. After applicant provides personal loan-related information, the loan is granted subject to payment of an "insurance fee."

Computer Crime (Page 4 of 6)

- Social networking risks
  - Open sharing of information among individuals
  - Photos, job loss, stalking



Control Your Default Privacy

This setting will apply to status updates and photos you post to your profile from a Facebook app that doesn't have the inline audience selector, like Facebook for Blackberry.

Public ○ | Friends ● | Custom ○

How You Connect
Control how you connect with people you know. — Edit Settings

Profile and Tagging
Control what happens when friends tag you or your content, or post on your wall. — Edit Settings

Ads, Apps and Websites
Manage your settings for ads, apps, games and websites. — Edit Settings

Limit the Audience for Past Posts
Limit the audience for posts you shared with friends of friends or Public. — Manage Past Post Visibility

Blocked People and Apps
Manage the people and apps you've blocked. — Manage Blocking

Computer Crime (Page 5 of 6)

- **Cyber-bullying**
  - The use of the Internet, cell phones, or other devices to send and post content intended to hurt or embarrass another person
  - Can lead to criminal prosecution
- **Rogue Wi-Fi hotspots**
  - Imitate these free Wi-Fi networks
  - Capture any and all information sent by the user to sites including names and passwords.

Computer Crime (Page 6 of 6)

- **Theft**
  - Steal data, computer time, equipment, and programs.
  - Can include:
    - White collar crimes
    - The use of a company’s computer time by an employee to run another business
- **Data manipulation**
  - Finding entry into someone’s computer network

Computer Fraud and Abuse Act

- Makes it a crime to view copy or damage data using any computer across state lines
- Prohibits unauthorized use of any government computer or a computer used by any federally insured financial institution.
- Up to 20 years in prison and fines up to $100,000.

Measures to Protect Computer Security

- Some of the principle measures to ensure computer security are:
  - Restricting access,
  - encrypting messages,
  - anticipating disasters, and
  - preventing data loss

Restricting Access

- Security experts are constantly using ways to protect computer systems from access by unauthorized persons.
- Methods of doing so include:
  - Posting guards
  - Biometric scanning
  - Assigning passwords

Assigning passwords and tokens

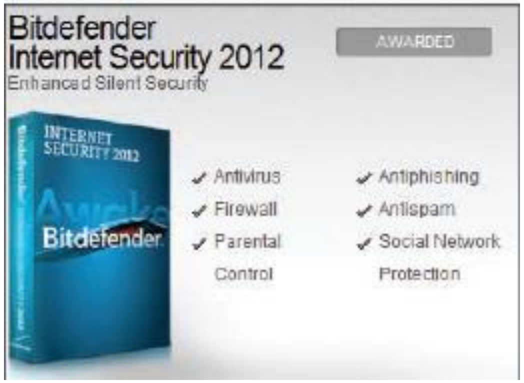
- Passwords are secret words or phrases that must be keyed into a computer system to gain access.
- Password strength is gauged as to how easily it can be guessed
- Dictionary attacks
    - Use software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account.

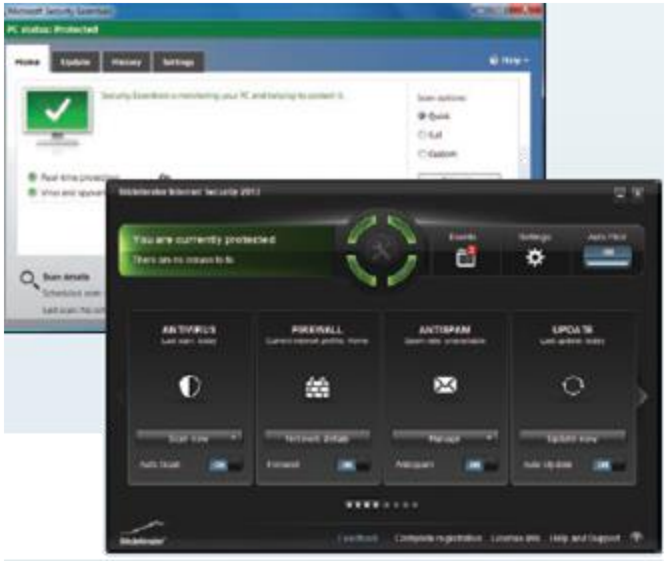
Other Security Measures

- Security suits
    - Provide a collection of programs designed to protect your privacy and security while you are on the web.
- Firewalls
    - Act as a security buffer between a corporation’s private network and all external networks, including the Internet.

Making IT Work for You ~ Security Suites

- Security Suites are software packages that include various utilities that help protect your computer from cybercrime.





Encrypting Data

- Encryption
  - The process of coding information to make it unreadable except to those who have a special piece of information known as an encryption key.
- Common uses:
  - E-mail encryption
  - File encryption
  - Website encryption

Encrypting Data

- **Most common protocol for website encryption is**
  - https
  - HyperText Transfer Protocol Secure
- **VPNs**
- **Wireless network encryption**
  - WPA2 (Wi-Fi Protected Access)

Anticipating Disasters

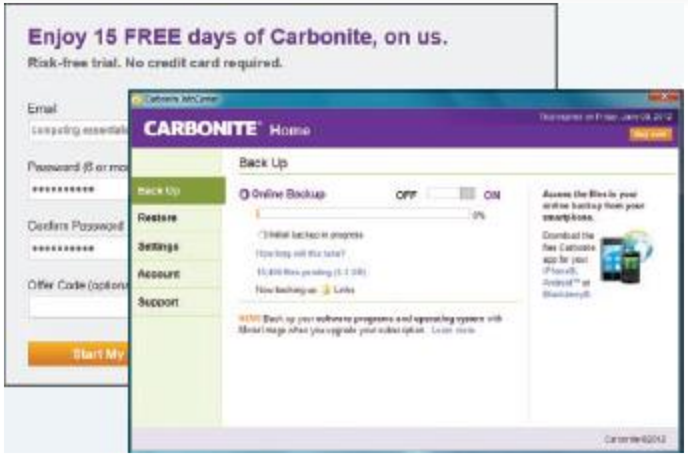
- Always be prepared for disasters.
- Physical security
  - Protecting the hardware form possible human and natural disasters.
- Data security
  - Protecting software and data from unauthorized tampering or damage.
- Most organizations have a *disaster recovery plan*
  - Describes ways to continue operation until things can be restored to prior state.

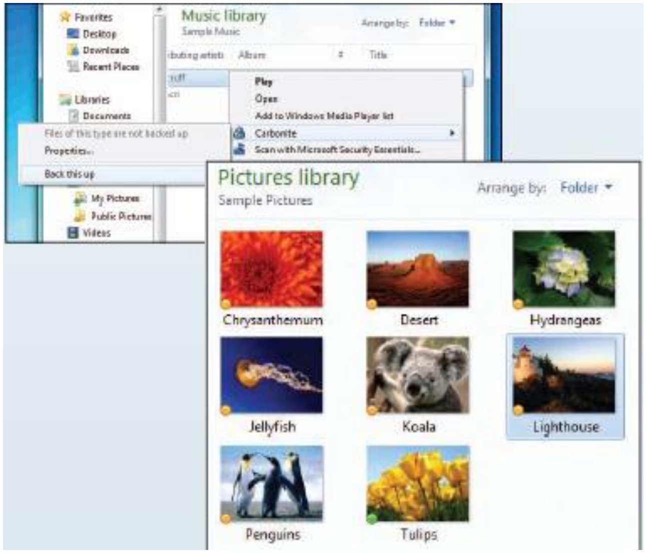
Preventing Data Loss

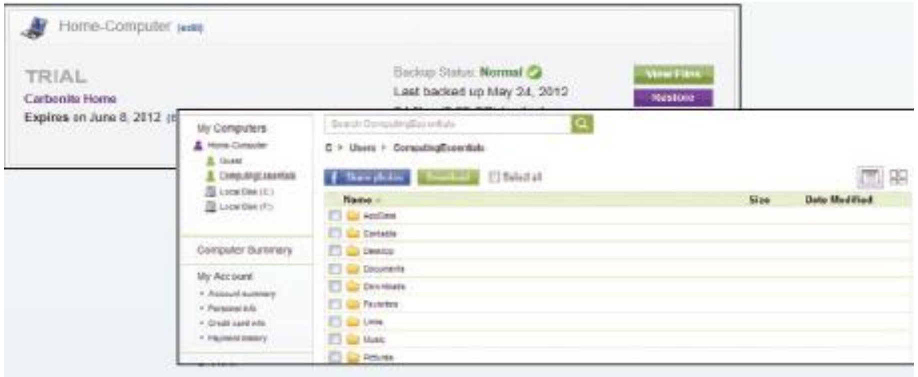
- Equipment is replaceable.
- A company's *data*, may be irreplaceable.
- Redundant storage
  - RAID (Chapter 7)
- Backup Batteries
- Making frequent backups
  - Usually stored offsite
- Incremental backups

Making IT Work for You ~ Cloud-Based Backup

- Cloud-based backup services such as Carbonite provide cloud-based backup services.


Enjoy 15 FREE days of Carbonite, on us.
Risk-free trial. No credit card required.
Email
Password (6 or mo
Confirm Password
Offer Code (option
Start My
CARBONITE Home
Back Up
Restore
Settings
Account
Support
Online Backup
OFF
ON
0%
Initial backup in progress
Access the files in your online backup from your smartphone.





Ethics

- What are ethics?
  - Standards of moral conduct
- Technology is moving so fast that it is difficult for our legal system to control how computers are used.
- Computer ethics are guidelines for the morally acceptable use of computers in our society.

Ethics

- **Copyright and Digital Rights Management**
  - Copyrights
    - Gives content creators the right to control the use and distribution of their work
  - Paintings, books, music, films, video games
  - Copyright violations include making unauthorized copies of digital media that is copyrighted.

Ethics

- **Software piracy**
  - Unauthorized copying and distribution of software
  - Costs the software industry $30+ billion annually
  - Digital rights management (DRM)
    - Technologies that control access to digital media
    - Used to:
      1. Control the number of devices that can access a file
      2. Limit the kinds of devices that can access a file

Ethics

- **Software piracy (cont.)**
  - Digital rights management (DRM)
    - Some companies feel that they have to use this to protect their rights.
    - Some users feel they should have the right to use the media they buy as they choose.

Ethics

- **Software piracy (cont.)**
  - Digital Millennium Copyright Act
    - Makes it illegal to deactivate or otherwise disable any antipiracy technologies.
    - Copies of commercial programs cannot be legally resold or given away
    - Regardless of whether you do it or not… The law is clear:

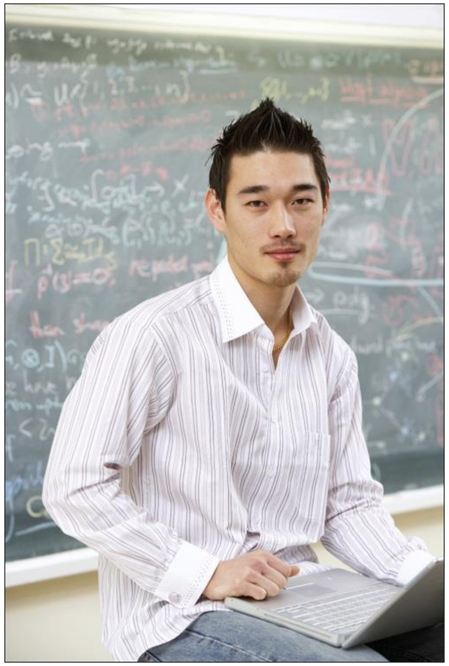
It is illegal to copy or download copyright-protected music or videos from the Internet without appropriate authorization

Ethics

- Plagiarism
  - Representing some other person’s work and/or ideas as your own without giving credit to the original source.
  - Computers have made this easier.
  - They have also made it easier to recognize and catch plagiarists.
  - Example
    - Turnitin

Careers in IT

- IT Security Analysts maintain the security of a company's network, systems, and data.
- Must safeguard information systems against external threats
- Annual salary is usually from $62,000 to $101,000
- Demand for this position is expected to grow



A Look to the Future

- The End of Anonymity
- A Webcam on Every Corner
  - Images of public places are more accessible than ever before (e.g., Google Street View)
  - "Virtual site-seeing tours"
  - Public webcams continue to grow in popularity

Open-Ended Questions (Page 1 of 3)

- Define privacy and discuss the impact of large databases, private networks, the Internet, and the Web.
- Define and discuss online identity and the major privacy laws.
- Define security. Define computer crime and the impact of malicious programs, including viruses, worms, Trojan horses, and zombies, as well as cyberbullying, denial of service attacks, Internet scams, social networking risks, rogue Wi-Fi hotspots, thefts, data manipulation, and other hazards.

Open-Ended Questions (Page 2 of 2)

- Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
- Define ethics, and describe copyright law and plagiarism.