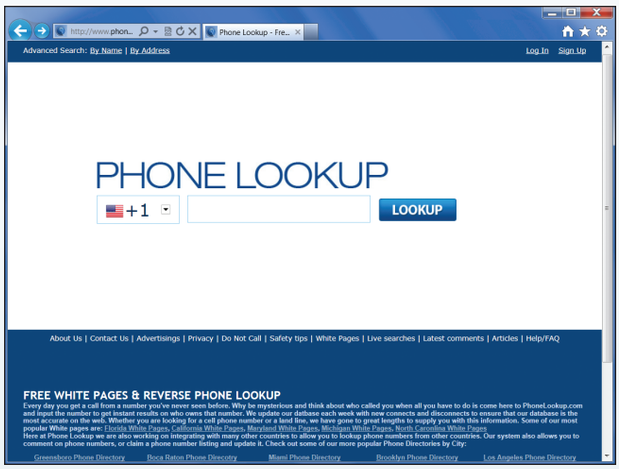
# VISUAL SUMMARY

Privacy, Security, and Ethics

## PRIVACY




**Privacy** concerns the collection and use of data about individuals. There are three primary privacy issues: **accuracy** (who is responsible to ensure data is correct), **property** (who owns data and rights to software), **access** (who controls access to data).

### Large Databases

Large organizations are constantly compiling information about us. **Reverse directories** list telephone numbers followed by subscriber names. **Information resellers (information brokers)** collect and sell personal data. **Electronic profiles** are compiled from databases to provide highly detailed and personalized descriptions of individuals.

**Identity theft** is the illegal assumption of someone's identity for the purposes of economic gain. **Mistaken identity** occurs when an electronic profile of one person is switched with another. **The Freedom of Information Act** entitles individuals access to governmental records relating to them.

### Private Networks

Many organizations monitor employee e-mail and computer files using special software called **employee-monitoring software.**

### The Internet and the Web

Many people believe that, while using the web, little can be done to invade their privacy. This is called the **illusion of anonymity.**

## PRIVACY


Information stored by browsers includes **history files** (record sites visited) and **temporary Internet files** or **browser cache** (contain website content and display instructions). **Cookies** store and track information. **Privacy mode (InPrivate Browsing; Private Browsing)** ensures that your browsing activity is not recorded.

**Spyware** secretly records and reports Internet activities. **Computer monitoring software** (or **keystroke loggers**) are particularly dangerous. **Antispyware (spy removal programs)** detects and removes various privacy threats.

### Online Identity

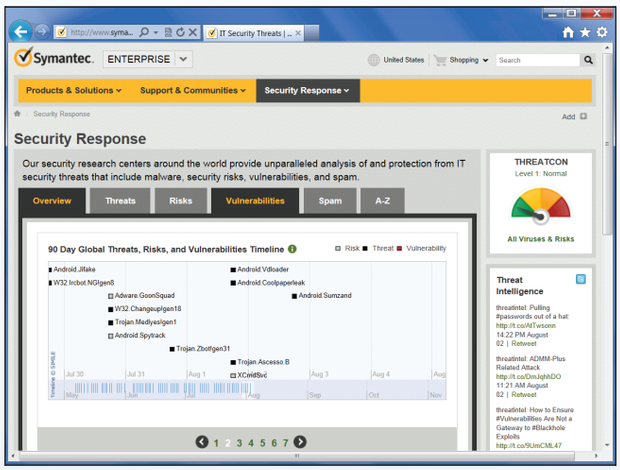
Many people post personal information and sometimes intimate details of their lives without considering the consequences. This creates an **online identity.** With the archiving and search features of the web, this identity is indefinitely available to anyone who cares to look for it.

### Major Laws on Privacy

The **Gramm-Leach-Bliley Act** protects personal financial information; the **Health Insurance Portability and Accountability Act (HIPAA)** protects medical records; and the **Family Educational Rights and Privacy Act (FERPA)** restricts disclosure of educational records.

**To be a competent end user, you need to be aware of the potential impact of technology on people. You need to be sensitive to and knowledgeable about personal privacy, organizational security, and ethics.**

## SECURITY




Computer **security** focuses on protecting information, hardware, and software from unauthorized use as well as preventing damage from intrusions, sabotage, and natural disasters. Someone who gains unauthorized access to computers that contain information about us is commonly known as a computer **hacker**. Not all hackers are intent on malicious actions and not all are criminals.

### Cybercrime

**Cybercrime (computer crime)** is an illegal action involving special knowledge of computer technology.

- Malicious programs **(malware)** include **viruses** (the **Computer Fraud and Abuse Act** makes spreading a virus a federal offense), **worms**, and **Trojan horses. Zombies** are remotely controlled infected computers used for malicious purposes. A collection of zombie computers is known as a **botnet**, or **robot network**.
- **Denial of service (DoS) attack** is an attempt to shut down or stop a computer system or network. It floods a computer or network with requests for information and data.
- **Scams** are designed to trick individuals into spending their time and money with little or no return. Common **Internet scams** include identity theft, chain letters, auction fraud, vacation prizes, and advance fee loans. These are frequently coupled with **phishing** websites or e-mails.

## SECURITY

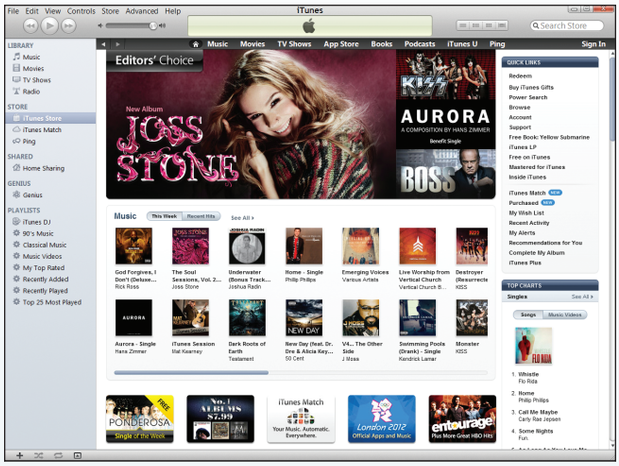

- Social networking risks include posting work-related criticisms and disclosure of personal information.
- **Cyberbullying** is the use of the Internet, cell phones, or other devices to send or post content intended to hurt or embarrass another person.
- **Rogue Wi-Fi hotspots** imitate legitimate hotspots to capture personal information.
- Theft takes many forms including stealing hardware, software, data, and computer time.
- Data manipulation involves changing data or leaving prank messages. **The Computer Fraud and Abuse Act** helps protect against data manipulation.

### Measures to Protect Computer Security

There are numerous ways in which computer systems and data can be compromised and many ways to protect computer security. These measures include

- Access can be restricted through **biometric scanning** devices and **passwords** (secret words or phrases; **dictionary attacks** use thousands of words to attempt to gain access).
- **Encrypting** is coding information to make it unreadable except to those who have the **encryption key**. **Virtual private networks (VPNs)** encrypt connections between company networks and remote users. **WPA2 (Wi-Fi Protected Access)** is the most widely used wireless network encryption for home wireless networks.
- Anticipating disasters involves physical security, data security, and disaster recovery plans.
- Preventing data loss involves protecting data by screening job applicants, guarding passwords, and auditing and backing up data.

## ETHICS




What do you suppose controls how computers can be used? You probably think first of laws. Of course, that is right, but technology is moving so fast that it is very difficult for our legal system to keep up. The essential element that controls how computers are used today is *ethics.*

**Ethics** are standards of moral conduct. **Computer ethics** are guidelines for the morally acceptable use of computers in our society. We are all entitled to ethical treatment. This includes the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands.

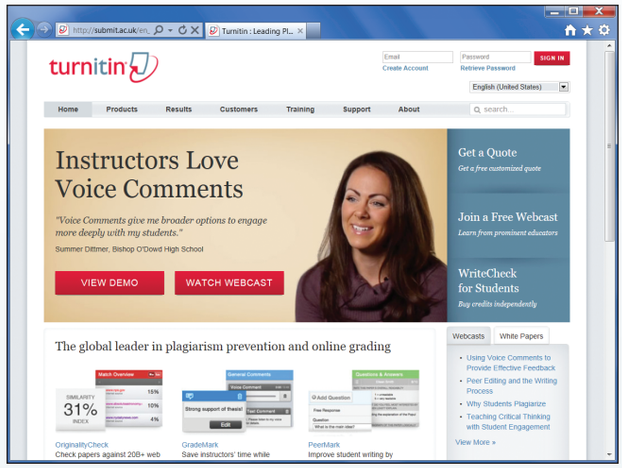
### Copyright and Digital Rights Management

**Copyright** is a legal concept that gives content creators the right to control use and distribution of their work. Materials that can be copyrighted include paintings, books, music, films, and even video games.

**Software piracy** is the unauthorized copying and distribution of software. The software industry loses over $30 billion annually to software piracy. Two related topics are the Digital Millennium Copyright Act and digital rights management.

- **Digital Millennium Copyright Act** establishes the right of a program owner to make a backup copy of any program and disallows the creation of copies to be sold or given away. It is also illegal to download copyright-protected music and videos from the Internet.
- **Digital rights management (DRM)** is a collection of technologies designed to prevent copyright violations. Typically, DRM is used to (1) control the number of devices that can access a given file and (2) limit the kinds of devices that can access a file.

## ETHICS




Today, many legal sources for digital media exist, including

- Television programs that can be watched online, often for free, on television-network-sponsored sites.
- Sites like Pandora that allow listeners to enjoy music at no cost.
- Online stores that legally sell music and video content. A pioneer in this area is Apple's iTunes Music Store.

### Plagiarism

**Plagiarism** is the illegal and unethical representation of some other person's work and ideas as your own without giving credit to the original source. Examples of plagiarism include cutting and pasting web content into a report or paper.

Recognizing and catching **plagiarists** is relatively easy. For example, services such as **Turnitin** are dedicated to preventing Internet plagiarism. This service examines a paper's content and compares it to a wide range of known public electronic documents including web page content. Exact duplication or paraphrasing is readily identified.

## CAREERS IN IT

**IT security analysts** are responsible for maintaining the security of a company's network, systems, and data. Employers look for candidates with a bachelor's or advanced specialized associate's degree in information systems or computer science and network experience. Salary range is $62,000 to $101,000.

# KEY TERMS

access (243)
accuracy (243)
antispyware (249)
biometric scanning (255)
botnet (252)
browser cache (247)
computer crime (251)
computer ethics (263)
Computer Fraud and Abuse Act (251, 254)
computer monitoring software (249)
cookies (247)
copyright (263)
cracker (251)
cyberbullying (253)
cybercrime (251)
data security (260)
denial of service (DoS) attack (253)
dictionary attack (256)
Digital Millennium Copyright Act (263)
digital rights management (DRM) (263)
disaster recovery plan (260)
electronic profile (244)
employee-monitoring software (246)
encryption (256)
encryption key (259)
ethics (263)
Family Educational Rights and Privacy Act (FERPA) (250)
firewall (256)
first-party cookie (247)
Freedom of Information Act (246)
Gramm-Leach-Bliley Act (250)
hacker (251)
Health Insurance Portability and Accountability Act (HIPAA) (250)
history file (247)
http (hypertext transfer protocol) (260)
https (hypertext transfer protocol secure) (260)
identity theft (245)
illusion of anonymity (247)
information broker (244)
information reseller (244)
InPrivate Browsing (248)
Internet scam (253)
IT security analyst (265)
key (259)
keystroke loggers (249)
malware (251)
mistaken identity (246)
online identity (250)
password (256)
phishing (253)
physical security (260)
plagiarism (264)
plagiarist (264)
privacy (243)
privacy mode (248)
Private Browsing (248)
property (243)
reverse directory (243)
robot network (252)
rogue Wi-Fi hotspot (254)
scam (253)
security (251)
security suites (256)
software piracy (263)
spy removal program (249)
spyware (249)
temporary Internet file (247)
third-party cookie (248)
tracking cookies (248)
Trojan horse (252)
virtual private network (VPN) (260)
virus (251)
web bugs (249)
wireless network encryption (260)
worm (251)
WPA2 (Wi-Fi Protected Access 2) (260)
zombie (252)

To test your knowledge of these key terms with animated flash cards, visit us at www.computing2014.com and enter the keyword terms9. Or use the free *Computing Essentials 2014* app.

# MULTIPLE CHOICE

Circle the letter of the correct answer.

1. The three primary privacy issues are accuracy, property, and:
   a. access
   b. ethics
   c. ownership
   d. security

2. To get the name, address, and other details about a person using only his or her telephone number, you could use a:
   a. third-party cookie
   b. keystroke logger
   c. reverse directory
   d. worm

3. Browsers store the locations of sites visited in a:
   a. history file
   b. menu
   c. tool bar
   d. firewall

4. The browser mode that ensures your browsing activity is not recorded.
   a. detect
   b. insert
   c. privacy
   d. sleep

5. The information that people voluntarily post in social networking sites, blogs, and photo- and video-sharing sites is used to create their:
   a. access approval
   b. firewall
   c. online identity
   d. phish

6. Computer criminals who create and distribute malicious programs.
   a. antispies
   b. crackers
   c. cyber traders
   d. identity thieves

7. Programs that come into a computer system disguised as something else are called:
   a. Trojan horses
   b. viruses
   c. web bugs
   d. zombies

8. The use of the Internet, cell phones, or other devices to send or post content intended to hurt or embarrass another person is known as:
   a. cyberbullying
   b. online harassment
   c. social media discrimination
   d. unethical communication

9. Special hardware and software used to control access to a corporation's private network is known as a(n):
   a. antivirus program
   b. communication gate
   c. firewall
   d. spyware removal program

10. To prevent copyright violations, corporations often use:
    a. ACT
    b. DRM
    c. VPN
    d. WPA2

For an interactive multiple-choice practice test, visit us at www.computing2014.com and enter the keyword multiple9. Or use the free *Computing Essentials 2014* app.

# MATCHING

**Match each numbered item with the most closely related lettered item. Write your answers in the spaces provided.**

**a.** accuracy
**b.** biometric
**c.** cookies
**d.** encryption
**e.** information brokers
**f.** malware
**g.** phishing
**h.** plagiarism
**i.** spyware
**j.** zombies

___ **1.** Privacy concern that relates to the responsibility to ensure correct data collection.
___ **2.** Individuals who collect and sell personal data.
___ **3.** Small data files deposited on your hard disk from websites you have visited.
___ **4.** Wide range of programs that secretly record and report an individual's activities on the Internet.
___ **5.** Malicious programs that damage or disrupt a computer system.
___ **6.** Infected computers that can be remotely controlled.
___ **7.** Used by scammers to trick Internet users with official-looking websites.
___ **8.** A type of scanning device such as fingerprint and iris (eye) scanner.
___ **9.** Process of coding information to make it unreadable except to those who have a key.
___ **10.** An ethical issue relating to using another person's work and ideas as your own without giving credit to the original source.

**For an interactive matching practice test, visit our website at www.computing2014.com and enter the keyword matching9. Or use the free *Computing Essentials 2014* app.**

# OPEN-ENDED

**On a separate sheet of paper, respond to each question or statement.**

1. Define privacy, and discuss the impact of large databases, private networks, the Internet, and the web.
2. Define and discuss online identity and the major privacy laws.
3. 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, theft, data manipulation, and other hazards.
4. Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
5. Define ethics, and describe copyright law and plagiarism.