



Because learning changes everything.®

# Privacy, Security, and Ethics

## Chapter 9

---

Computing Essentials 2023  
O'Leary



# Learning Objectives

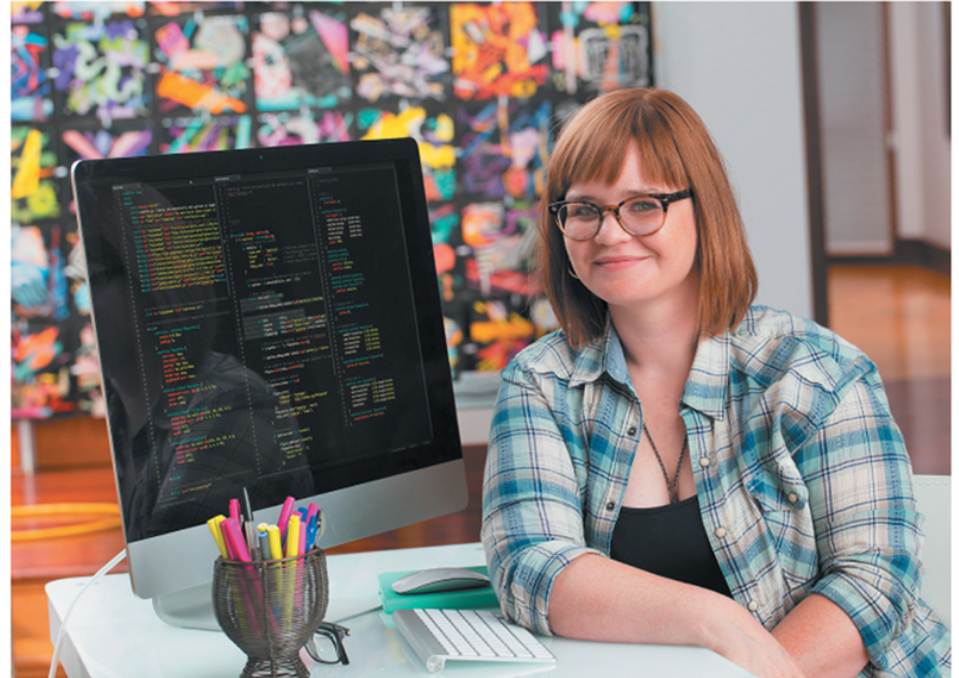
1. Describe the impact of large databases, private networks, the Internet, and the web on privacy.
2. Discuss online identity and major laws on privacy.
3. Discuss cybercrimes including identity theft, Internet scams, data manipulation, ransomware, and denial of service.
4. Describe social engineering and malicious software, including crackers, malware, viruses, worms, and Trojan horses.
5. Discuss malicious hardware, including zombies, botnets, rogue Wi-Fi networks, and infected USB flash drives.
6. Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
7. 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.

To efficiently and effectively use computers, you need to be aware of the potential impact of technology on people and how to protect yourself on the web.

Copyright © McGrawHill LLC permission required for reproduction or display



Ariel Skelley/Getty Images

# People

Technology has had a very positive impact on people, but some of the impact could be negative.

Most significant concerns:

- 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

## Accuracy

- Responsibility of those who collect data
- Ensure data is correct

## Property

- Relates to who owns the data

## Access

- Responsibility of those who control data and use that data

# Large Databases

Large organizations compile information about us daily

Big Data is exploding and ever-growing

## Information Resellers/ Brokers

- Collect and sell personal data
- Create electronic profiles

Copyright © McGrawHill LLC permission required for reproduction or display

The screenshot shows the Acxiom website with a navigation bar containing 'What We Do', 'Industries', 'Resources', 'Partners', 'About Us', 'Careers', and 'Login'. A search bar and a 'CONTACT US' button are also visible. The main content area is divided into four blue panels, each with a title, a brief description, and a background image. The 'DATA' panel features a crowd of people. The 'IDENTITY RESOLUTION' panel shows a blurred street scene. The 'DIGITAL TRANSFORMATION SOLUTIONS' panel depicts two people working at a computer. The 'CUSTOMER INTELLIGENCE PLATFORMS' panel shows a group of people in a cafe setting. A 'Chat with an Expert' button is located in the bottom right corner of the page.

**DATA**  
Leverage comprehensive global data and insights with over 11,000 data attributes in over 60 countries helping brands connect to 2.5 billion people ethically.

**IDENTITY RESOLUTION**  
Manage and maintain identity across your enterprise by leveraging 50 years of data and identity expertise combined with the latest artificial intelligence and machine learning techniques.

**DIGITAL TRANSFORMATION SOLUTIONS**  
Leverage powerful performance marketing solutions and services connect marketing technology with advertising execution to maximize business performance and address today's channel-free

**CUSTOMER INTELLIGENCE PLATFORMS**  
Deliver connected and relevant experiences leveraging a full suite of customer data platform solutions that support the entire customer journey leveraging over 50 years of data management expertise.

Acxiom

# Large Databases, continued

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
  - Entitlement to look at your records held by government agencies



# Private Networks

Employee monitoring software

Employers can monitor e-mail legally

- A proposed law could prohibit this type of electronic monitoring or at least require the employer to notify the employee first



# The Internet and the Web

## Illusion of anonymity

- People are not concerned about privacy when surfing the Internet or when sending e-mail

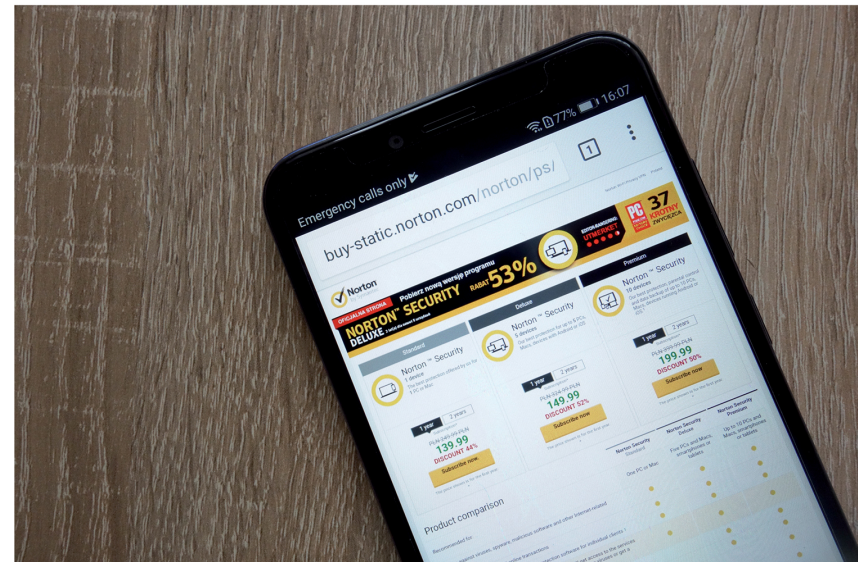
When browsing the web, critical information is stored on the hard drive in these locations:

- History Files
- Temporary Internet Files, or Browser cache
- Cookies

Privacy Mode to block recording

Spyware is the most dangerous type of privacy threat,

Copyright © McGraw-Hill Education. Permission required for reproduction or display.



Piotr Swat/Shutterstock

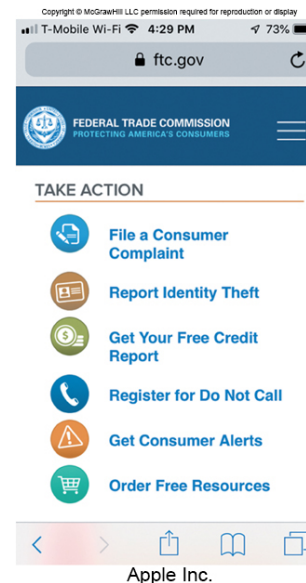
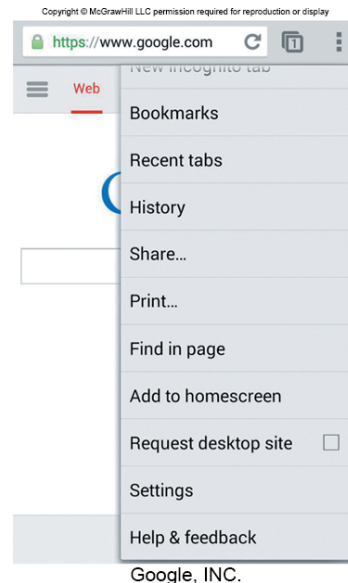
# History Files and Temporary Internet Files

## History Files

- Include locations or addresses of sites you have recently visited

## Temporary Internet Files / Browser Cache

- Saved files from visited websites
- Offers quick display of previously stored content when you return to the site



# Cookies

Small data files that are deposited on your hard disk from websites you have visited

- First-party cookies - generated only by websites you are visiting
- Third-party cookies - generated by an advertising company that is affiliated with the website
- Also known as tracking cookies that keep track of your Internet activities through 3<sup>rd</sup> party cookies

# Privacy Modes

Incognito  
Mode

- Google Chrome

Private  
Browsing

- Safari

# Privacy Threats

## Web bugs

- Invisible images or HTML code hidden within an e-mail message or web page

## Spyware

- Record and report Internet activities
- Change browser to manipulate what you view

## Computer monitoring software

- Most invasive and dangerous
- Keystroke Loggers
  - Record activities and keystrokes

## Anti-Spyware programs

- Detect and remove privacy threats

Copyright © McGrawHill LLC permission required for reproduction or display

Program	Website
Ad-Aware	<a href="http://www.adaware.com">www.adaware.com</a>
Norton Security	<a href="http://www.norton.com">www.norton.com</a>
Windows Defender	<a href="http://www.microsoft.com">www.microsoft.com</a>
AVG Antitrack	<a href="http://avg.com">avg.com</a>

# 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 personal financial information
  - **Health Insurance Portability and Accountability Act (HIPAA)** protects medical records
  - **Family Educational Rights and Privacy Act (FERPA)** resists disclosure of educational records

# Security

Involves protecting individuals or organizations from theft and danger

## Cybercrime / Computer Crime

- Criminal offense that involves a computer and a network
  - Effects over 400 million people annually
  - Costs over \$400 billion each year

# Forms of Computer Crime

Computer Crime	Description
Identity theft	Illegal assumption of a person's identity for economic gain
Internet scams	Scams over the Internet
Data manipulation	Unauthorized access of a computer network and copying files to or from the server
Ransomware	Malicious software that encrypts your computer's data and ransoms the password to the user
DoS, Denial of service	Attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data
DDoS, Distributed denial of service	Coordinates several computers making repeated requests for service



# Internet Scams

## Scams using the Internet

Internet scams have created financial and legal problems for many thousands of people

Majority are initiated by a mass mailing to unsuspecting individuals

Copyright © McGraw-Hill Education. Permission required for reproduction or display.

Type	Descriptions
Phishing	Communications via e-mail or social media pretend to be from an official organization and trick you into giving them sensitive data, such as passwords, bank account numbers, etc. Often these communications include a link to a website that looks like an official log-in screen but in fact is a fake website designed to trick people into giving up their username and password.
Nigerian scam	A classic e-mail scam. The recipient receives an e-mail from a wealthy foreigner in distress who needs your bank account information to safely store his or her wealth, and for your troubles you will receive a large amount of money. Of course, once the scammer has your bank account information, your accounts will be drained and he or she will disappear.
Greeting card scam	An e-mail or social media communication informs you that a friend has sent you a greeting card and you need to download software to view it. In fact, the software is malware that can steal your data and infect your computer.
Bank loan/credit card scam	Criminals acting as bank or credit card officials offer you unusually good deals on bank loans or credit cards—but these are just attempts to get you to pay huge “processing fees” and to get your personal information.
Lottery scam	An e-mail informs you that you have won the lottery and to claim your prize, you need to pay processing fees. Criminals will take the processing fees, but you will not receive any lottery winnings.

# Social Engineering

Practice of manipulating people to divulge private data.

Played a key role in:

- Identity theft
- Internet scams
- Data manipulation

## Phishing

- Attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legitimate

# Malicious Software

## Malicious Software or Malware

- Designed by crackers, computer criminals, to damage or disrupt a computer system
- 3 most common programs
  - Viruses – migrate through networks and attach to different programs
  - Worms – fills the computer with self-replicating information
  - Trojan horse – programs disguised as something else

# Malicious Hardware

Criminals use hardware for crimes

Most common are:

- **Zombies**
  - Computers infected by a virus, worm, or Trojan Horse
  - Botnet or Robot Network is a collection of Zombies
- **Rogue Wi-Fi Hotspots**
  - Imitating legitimate free Wi-Fi
  - Capture data coming through the Rogue Wi-Fi
- **Infect USB Flash Drives**
  - Left on purpose in hopes for people to pick up and use
  - Have malicious software contained on them

# Computer Security Measures

## Principle measures to ensure computer security

- Computer Fraud and Abuse Act
  - Crime for unauthorized person to view, copy or damage data using computers across state lines
  - Prevents use of any government or federally insured financial institution computers

Measure	Description
Restricting access	Limit access to authorized persons using such measures as passwords, picture passwords, and biometric scanning.
Encrypting data	Code all messages sent over a network.
Anticipating disasters	Prepare for disasters by ensuring physical security and data security through a disaster recovery plan.
Preventing data loss	Routinely copy data and store it at a remote location.

# Restricting Access

## Passwords

- Dictionary attack
  - Uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account

## Biometric scanning

- Fingerprint scanners
- Iris (eye) scanners
- Facial recognition

Copyright © McGrawHill LLC permission required for reproduction or display



Prostock-studio/Shutterstock

Copyright © McGrawHill LLC permission required for reproduction or display



Michael Dwyer/Alamy Stock Photo

# Security Tasks

## Ways to perform and automate important security tasks

- Security Suites
  - Provide a collection of utility programs designed to protect your privacy and security
- Firewalls
  - Security buffer between a corporation's provide network and all external networks
- Password Managers
  - Helps to create strong passwords
- Authentication
  - Process of ensuring the integrity of a user

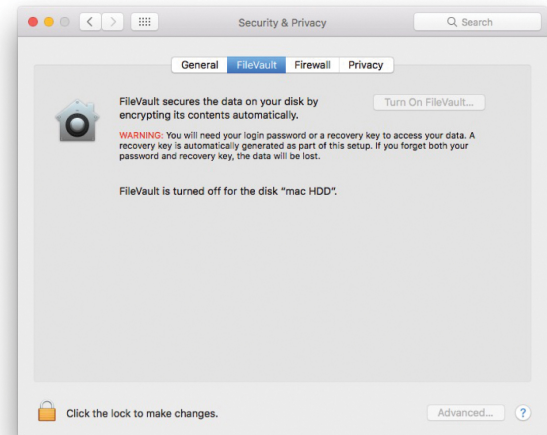
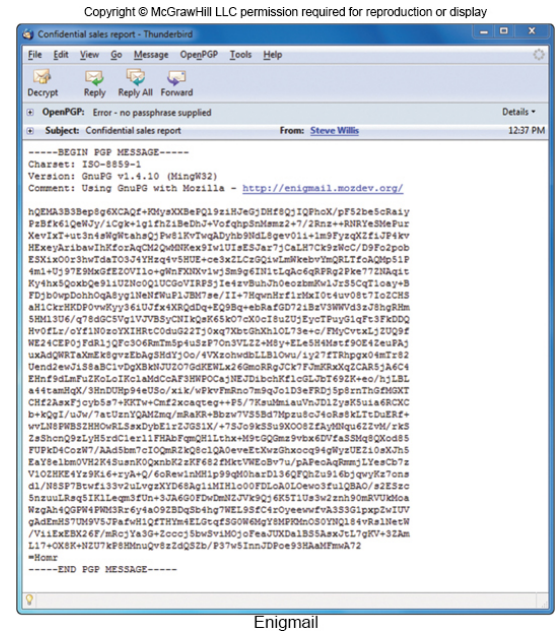
# Encryption

Coding information to make it unreadable, except to those who have the encryption key, or simply, the key

- The key will decrypt the information into a readable format

## Common uses for encryption:

- E-mail encryption
- File encryption
- Website encryption
  - HTTPS – hypertext transfer protocol secured
- Virtual private networks (VPNs)
- Wireless network encryption restricts access to authorized users
- WPA2 – Wi-Fi Protected Access





# Anticipating Disasters and Preventing Data Loss

## Anticipating Disasters

- Physical security protects hardware
- Data security protects software and data from unauthorized tampering or damage
- A disaster recovery plan describes ways to continue operating in the event of a disaster

## Preventing Data Loss

- Frequent backups
- Redundant data storage
  - Store off-site in case of loss of equipment

# Ethics

Standards of moral conduct

Computer Ethics – guidelines for the morally acceptable use of computers

- Cyberbullying
- Copyright and Digital Rights Management
- Plagiarism

# Copyright and Digital Rights Management

## Copyright

- Gives content creators the right to control the use and distribution of their work
- Paintings, books, music, films, video games

## Software piracy

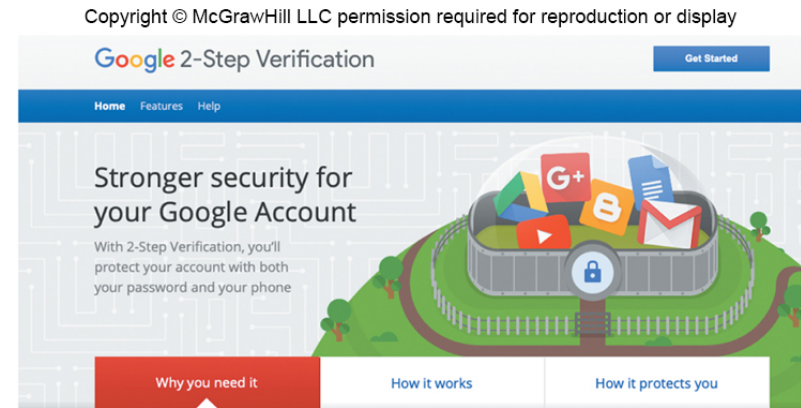
- Unauthorized copying and distribution of software
  - Digital rights management (DRM) controls access to electronic media
  - Digital Millennium Copyright Act protects against piracy



# Making IT Work for You

## Security and Technology

- Precautions you as an individual can and should take to make sure that you aren't the victim of high-tech criminals
  - Update software
  - Regularly back up your data
  - Be careful when browsing
  - Be alert to e-mail scams
  - Use antivirus software
  - Strong passwords



It's easier than you think for someone to steal your password

Any of these common actions could put you at risk of having your password stolen:

- Using the same password on more than one site
- Downloading software from the Internet
- Clicking on links in email messages

2-Step Verification can help keep bad guys out, even if they have your password.

Google, INC.

# Cyberbullying and Plagiarism

## Cyberbullying

- Use of the Internet to send or post content intended to harm another person

## Plagiarism

- Representing some other person's work and ideas as your own without giving credit to the original person's work and ideas


Copyright © McGrawHill LLC permission required for reproduction or display

Introducing Draft Coach, feedback for students while they write. [Learn More](#)

Change language | English | Search | [Create Account](#) | [Login](#)

[turnitin](#) [Products](#) [Solutions](#) [Resources](#) [Support](#) [Contact Sales](#)

Empower students to do their best, original work



Student success starts here  
Turnitin

# Careers in IT

## IT Security Analysts

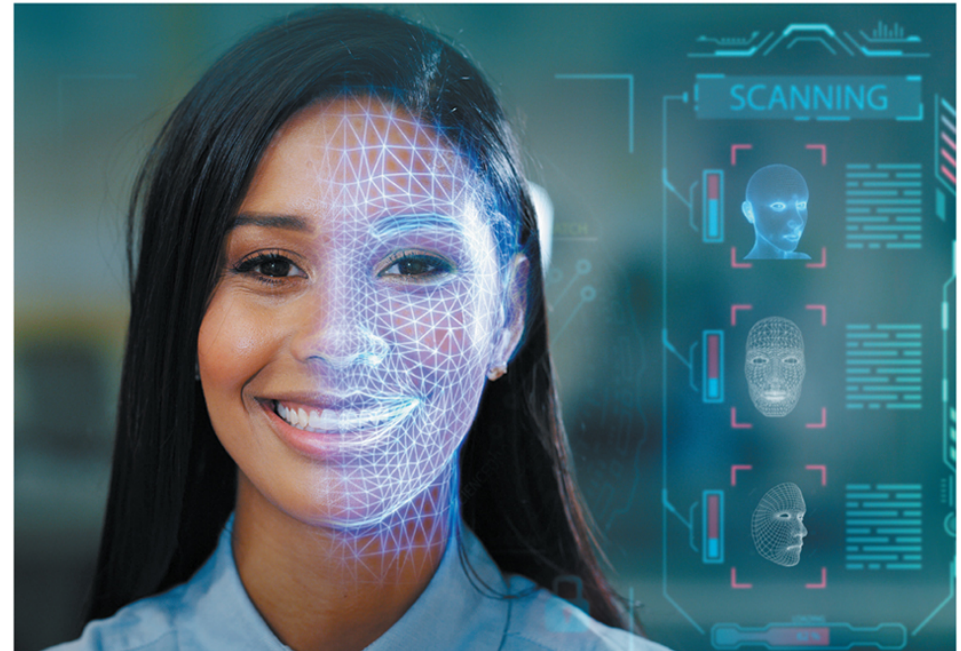
- Maintain the security of a company's network, systems, and data
- Bachelors or associates degree in information systems or computer science
- Experience is usually required
- Must safeguard information systems against external threats
- Annual salary is usually from \$49,000 to \$99,000
- Demand for this position is expected to grow

# A Look to the Future

## The End of Anonymity

- Most forums and comment areas on websites allow users to post messages anonymously
- Future software can identify you and track your moves through a mall or store

Copyright © McGrawHill LLC permission required for reproduction or display



HQuality/Shutterstock

# Open Ended Questions

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, social engineering, malicious software, and malicious hardware including identity theft, Internet scams, data manipulations, ransomware, DoS attacks, viruses, worms, Trojan horses, zombies, rogue Wi-Fi hotspots, and infected USB flash drives.
4. Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
5. Define ethics, copyright law, cyberbullying, and plagiarism.





Because learning changes everything.®

[www.mheducation.com](http://www.mheducation.com)