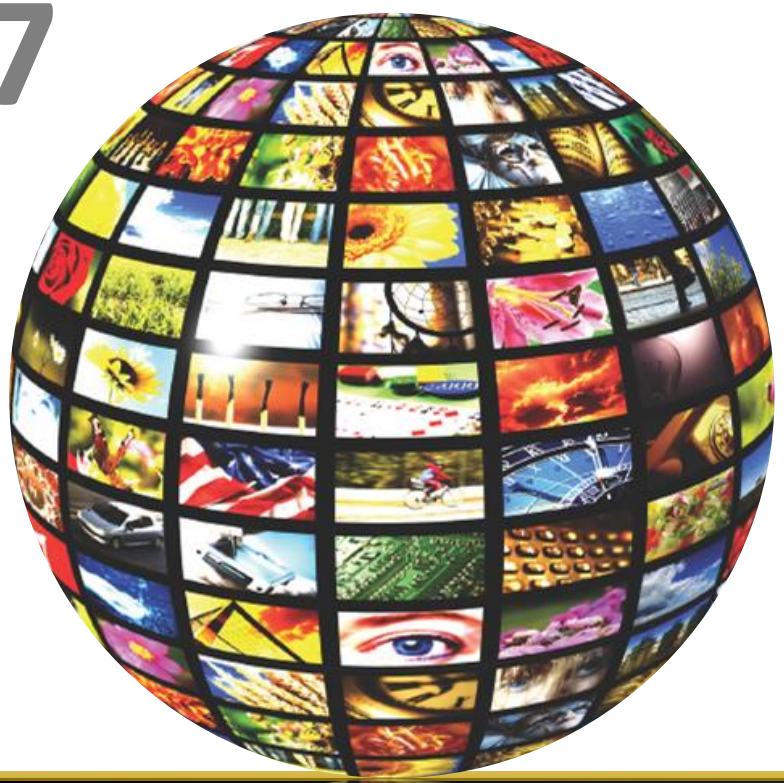
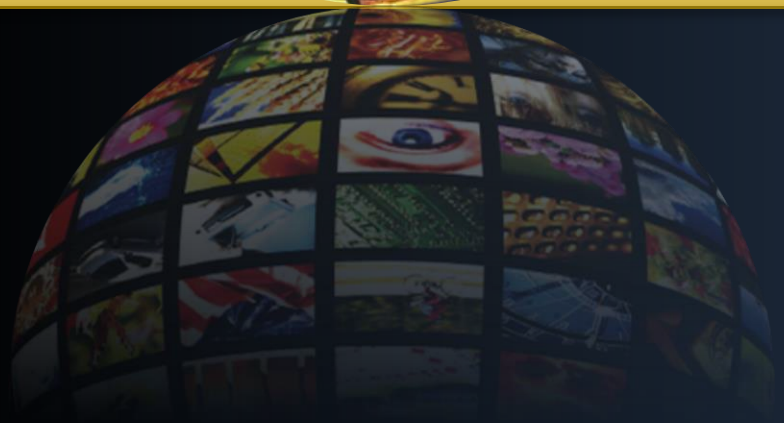
Chapter 7



Privacy, Security, and Ethics



Chapter 7

Learning Objectives

1. Describe the impact of large databases, private networks, the Internet, and the web on privacy.
2. Discuss online identity and the 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
8. management, the Digital Millennium Copyright Act, as well as cyberbullying, plagiarism, and ways to identify plagiarism.

Introduction

- What are the consequences of the widespread presence of this technology? Does technology make it easy for others to invade our personal privacy? When we apply for a loan or for a driver's license, or when we check out at the supermarket, is that information about us being distributed and used without our permission? When we use the web, is information about us being collected and shared with others? How can criminals use this information for ransom, blackmail, or vandalism?

- This chapter covers issues related to the impact of technology on people and how to protect ourselves on the Web.

Yuri Arcurs/E+/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?

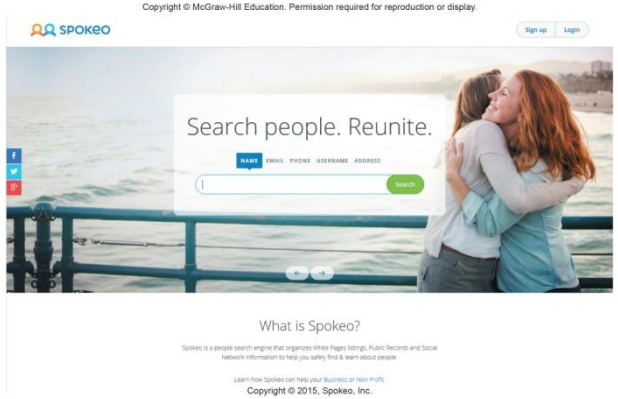
Privacy

- Privacy – concerns the collection and use of data about individuals
- Three primary privacy issues:
  - Accuracy – responsibility of those who collect data
    - Must be secure and correct
  - Property – who owns data and who has rights to software
  - Access – responsibility of those who control data and use of data

Large Databases / Big Data

Large organizations compile information about us daily

- Big Data is exploding and ever-growing
  - The federal government alone has over 2000 database
- Data collectors include
  - Government agencies
  - Telephone companies
  - Credit card companies
  - Supermarket scanners
  - Financial institutions
  - Search engines
  - Social networking sites
- Information Resellers/Brokers
  - Collect and sell personal data
  - Create electronic profiles



Large Databases / Big Data (Cont.)

- 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
    - Browser cache
  - Cookies
    - First-party cookie
    - Third-party cookie
  - Privacy Mode
  - Web bugs
  - Spyware

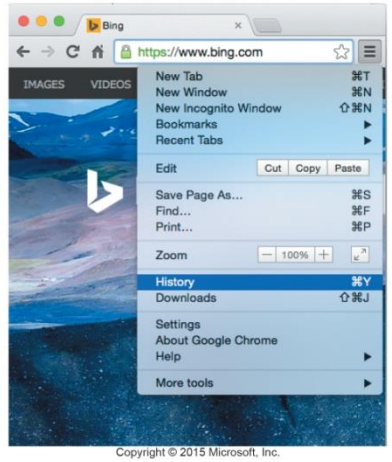
History Files and Temporary Internet Files

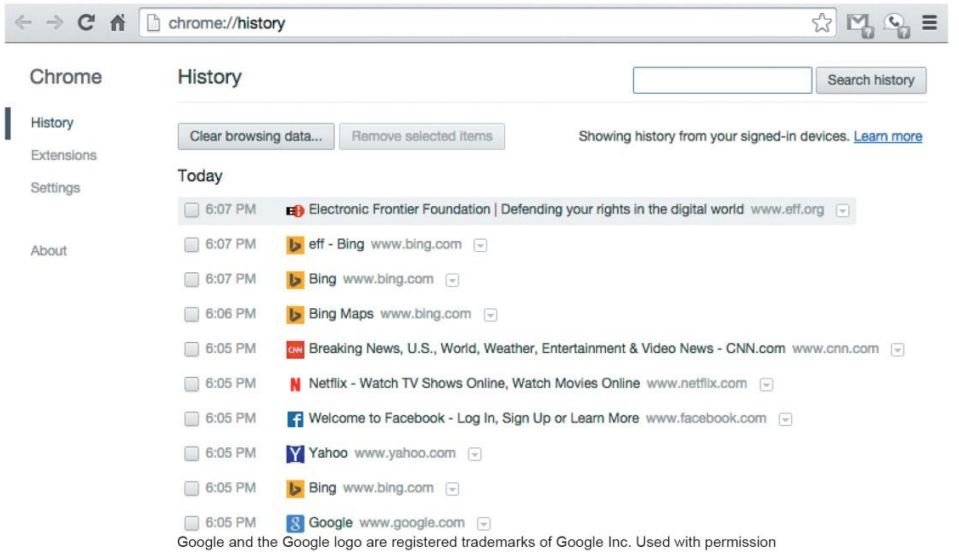
History Files

- Include locations or addresses of sites you have recently visited

Temporary Internet Files / Browser Cache

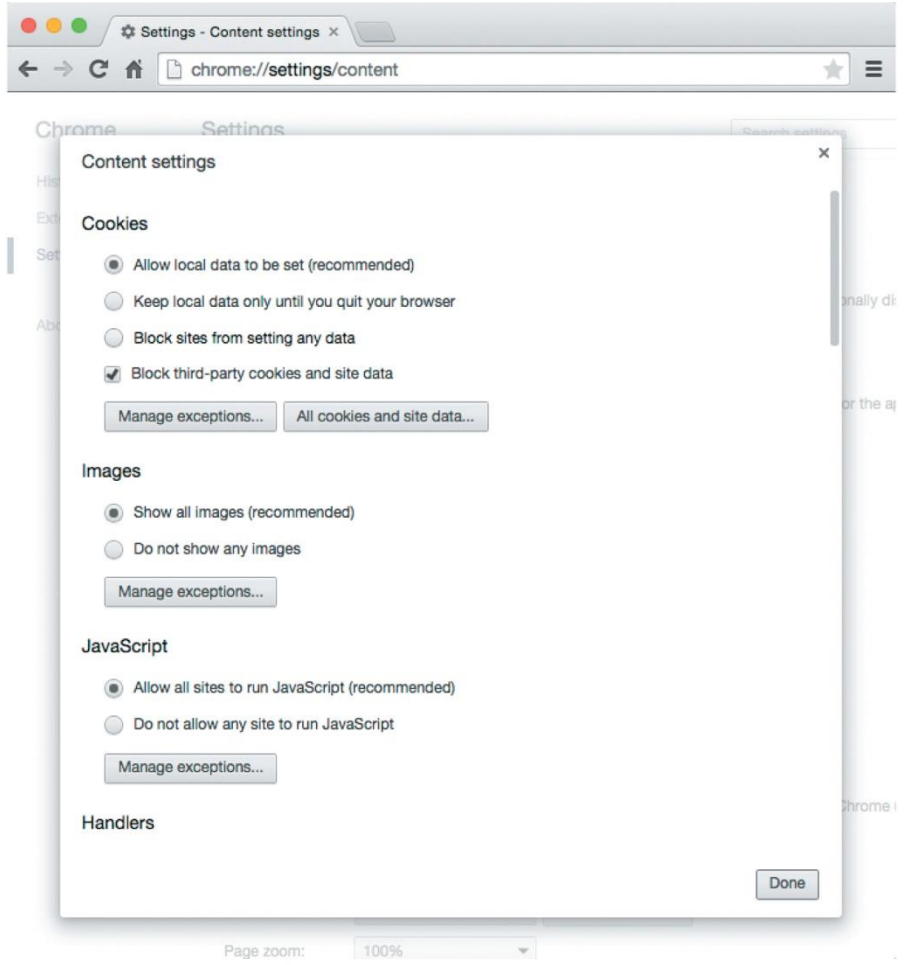
- Saved files from visited websites
- Offers quick re-display when you return to the site





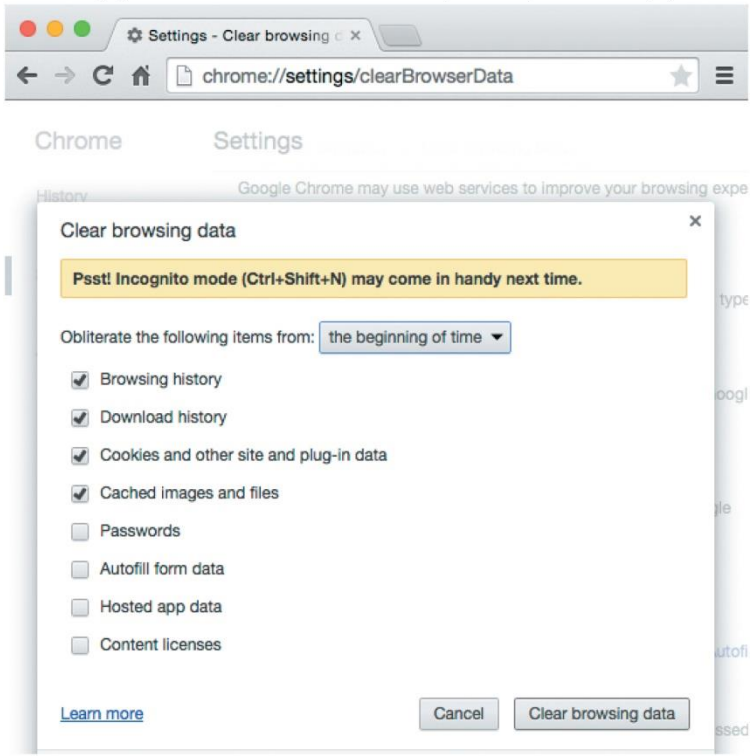
Cookies

- Cookies are small data files that are deposited on your hard disk from web sites you have visited
  - First-party cookies are generated only by websites you are visiting
  - Third-party cookies are generated by an advertising company that is affiliated with the website
    - Also known as tracking cookies that keep track of your Internet activities through 3rd party cookies
    - Refer to the accompanying graphic displaying how to block 3rd party cookies



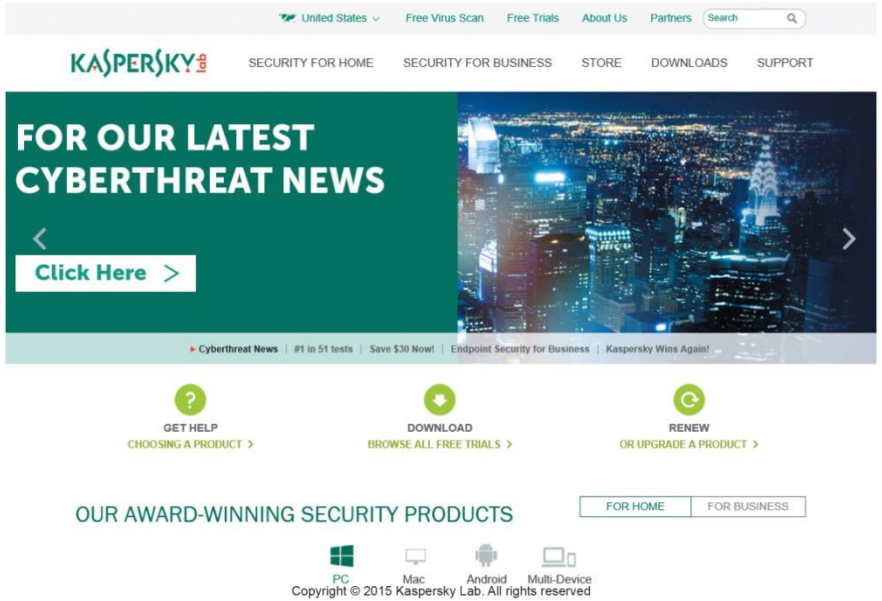
Privacy Modes

- Ensures your browsing activity is not recorded on your hard drive
  - 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
  - When a user opens the message information is sent back to the source of the bug
- Spyware
  - Wide range of programs that are designed to secretly record and report Internet activities, add Internet ad cookies
- Computer monitoring software
  - Invasive and dangerous
  - Keystroke Loggers
    - Record activities and keystrokes
- Anti-Spyware programs
  - Detect and remove privacy threats



Program	Website
Ad-Aware	www.lavasoft.com
Kaspersky Anti-Virus	www.kaspersky.com
Windows Defender	www.microsoft.com

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

- Hackers
  - Gain unauthorized access with malicious intent
  - Not all hackers are illegal

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
Malicious programs	Include viruses, worms, and Trojan horses
DoS	Causes computer systems to slow down or stop
Rogue Wi-Fi hotspots	Imitate legitimate Wi-Fi hotspot in order to capture personal information
Data manipulation	Involves changing data or leaving prank messages
Identity theft	Is illegal assumption of a person's identity for economic gain
Internet scams	Are scams over the Internet usually initiated by e-mail and involving phishing
Cyberbullying	Is using the Internet, smartphones, or other devices to send/post content intended to hurt or embarrass another person

Cyber Crime

- Denial of Service
  - (DoS) attack attempts to slow down or stop a computer system or network by flooding it with requests for information or data
- Rogue Wi-Fi hotspots
  - Imitate free Wi-Fi networks and capture any and all information sent by the users to legitimate sites including usernames and passwords
- Data manipulation
  - Finding entry into someone's computer network and leaving a prankster's message

Internet Scams

A fraudulent or deceptive act or operation to trick someone into providing personal information or spending money for little or no return

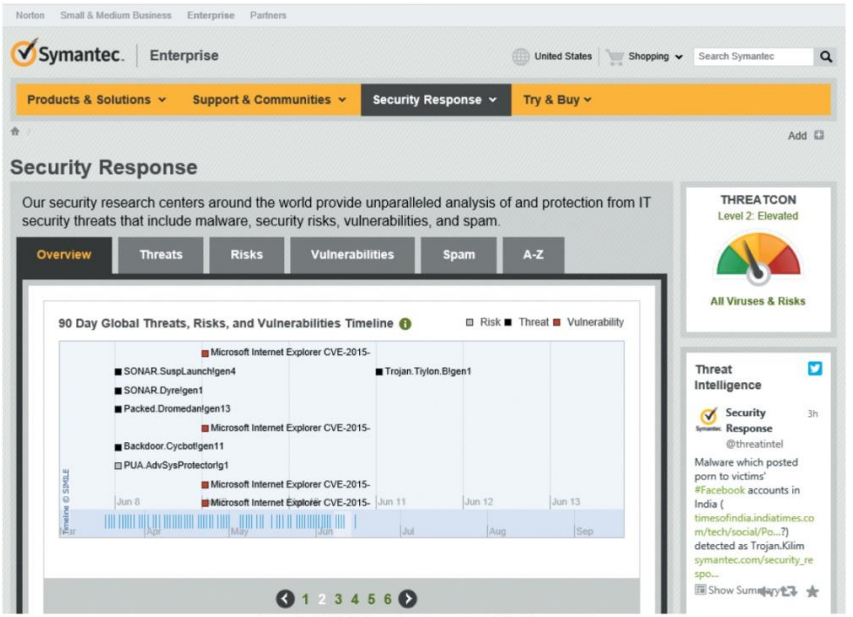
- Identity Theft
  - Illegal assumption of someone's identity for purpose of economic gain
- Cyber-bullying
  - Use of the Internet, cell phones, or other devices to send or post content intended to harm
- Phishing
  - Attempts to trick Internet users into thinking a fake but official-looking website is legitimate

Types of Internet Scams

Type	Description
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."

Malicious Software

- Malicious Programs or Malware
  - Designed by crackers, computer criminals, to damage or disrupt a computer system
  - Computer Fraud and Abuse Act makes spreading a virus a federal offense
  - 3 most common programs
    - Viruses – migrate through networks an attach to different programs
    - Worms – fills the computer with self-replicating information
    - Trojan horse – programs disguised as something else



Malicious Hardware

- 3 most common malicious hardware
  - Zombies – infected computers allow them to be remotely controlled for malicious purpose.
  - Rogue WiFi hotspot – imitate free Wi-Fi networks.
  - Infected USB flash drives – contain viruses and other malicious software

Measures to Protect Computer Security

Principle measures to ensure computer security

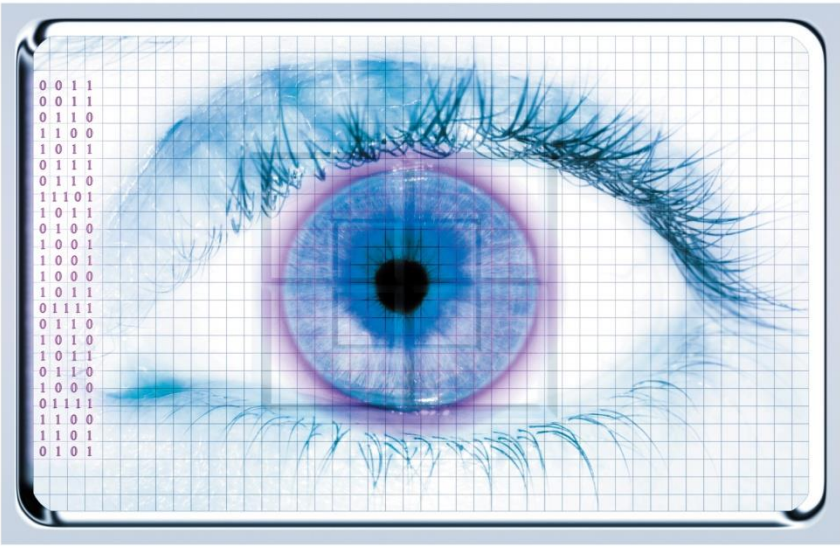
- Restricting access
- Encrypting data
- Anticipating disasters
  - Physical security
  - Data security
  - Disaster recovery plan
- Preventing data loss

Measure	Description
Restricting access	Limit access to authorized persons using such measures as passwords and firewalls.
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

- Firewalls
- Authentication
- Encrypting Data
  - Email Encryption
  - File Encryption
  - Website Encryption
- Biometric scanning
  - Fingerprint scanners
  - Iris (eye) scanners
- Passwords
  - Dictionary attack
    - Uses software to try thousands of common words sequentially to gain unauthorized access to a user's account

Fingerprint scan

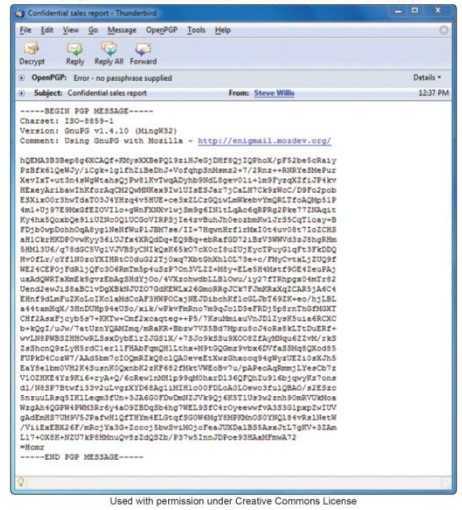


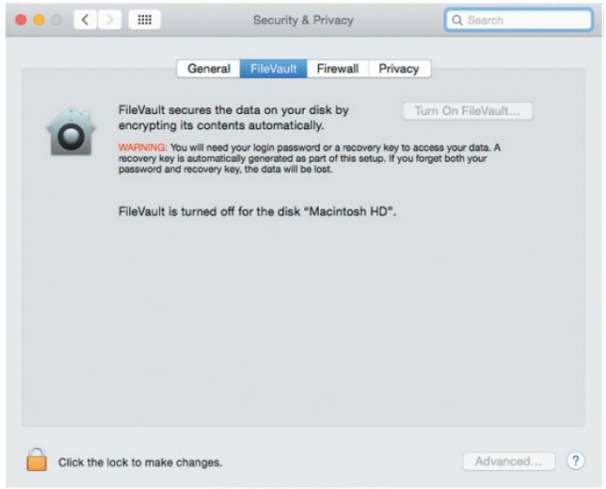
Iris scan

Encryption

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

- E-mail encryption protects emails
- File encryption protects files
- Web site encryption uses HTTPS protocol for protection
  - HTTPS – hypertext transfer protocol secured
- Virtual private networks (VPNs)
  - Encrypts connects between company networks and their remote users
- Wireless network encryption restricts access to authorized users
  - WPA2 – Wi-Fi Protected Access





Anticipating Disasters

- Anticipating Disasters
  - Physical Security protects hardware
  - Data Security protects software and data from unauthorized tampering or damage
  - 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

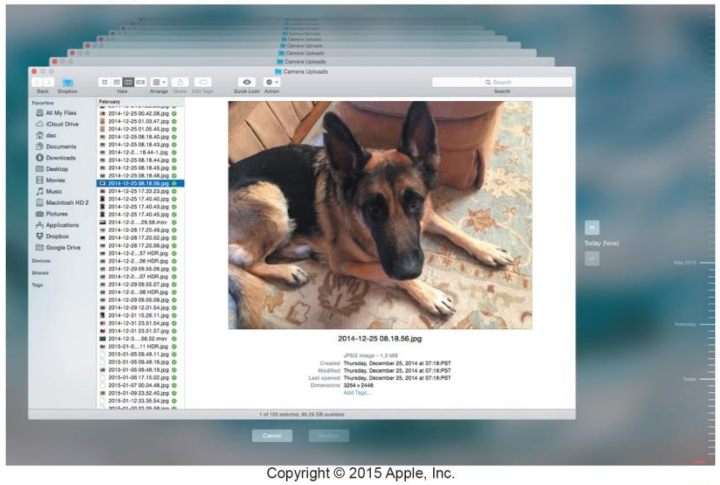
Recent Data Privacy Trends

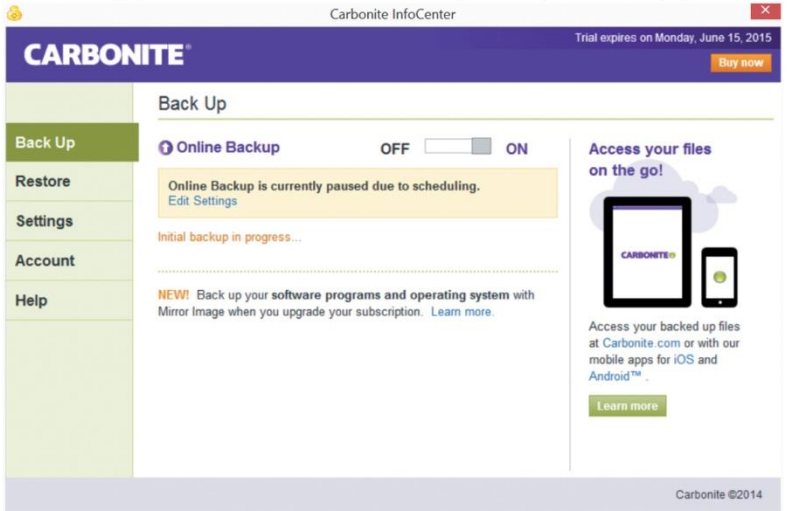
- Recent trends seek to strike a balance between our data against our privacy.
  1. **Cookies-less future** - Publishers, advertisers, and Big Tech will need to alter how they monetize their content and gather data in the future.
  2. **Consumers demand more control over their data** – customers will choose companies that are transparent with their personal data.
  3. **Addressing privacy with technology** – employ centralize PrivacyOps platform to fulfill users request faster
  4. **Public awareness leads to corporate transparency** – expect clear data policies.
  5. **Governing bodies will enforce more fines.**

[https://www.invisibly.com/learn-blog/data-privacy-trends/]

Making IT Work for You ~ Cloud-Based Backup

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



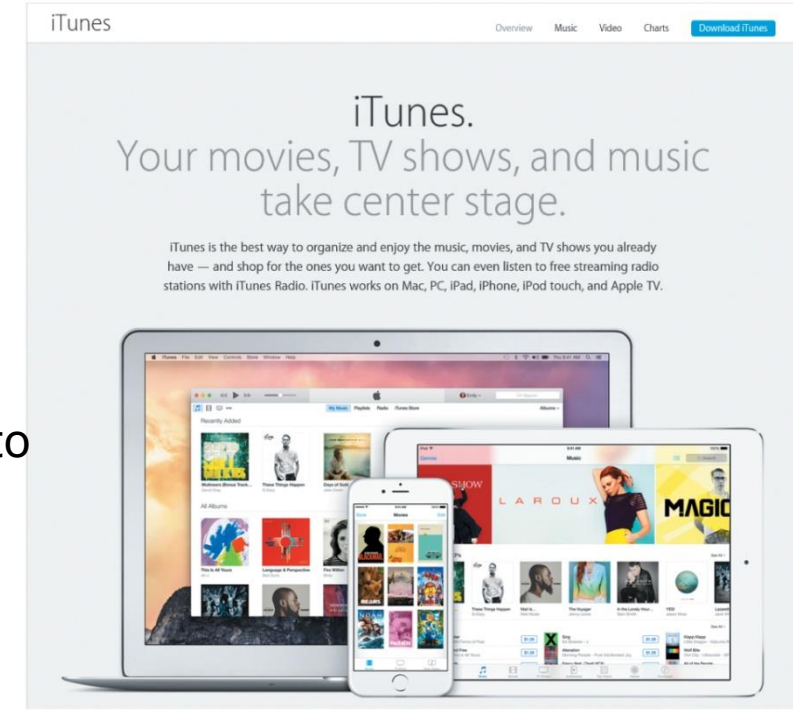


Ethics

Standards of moral conduct

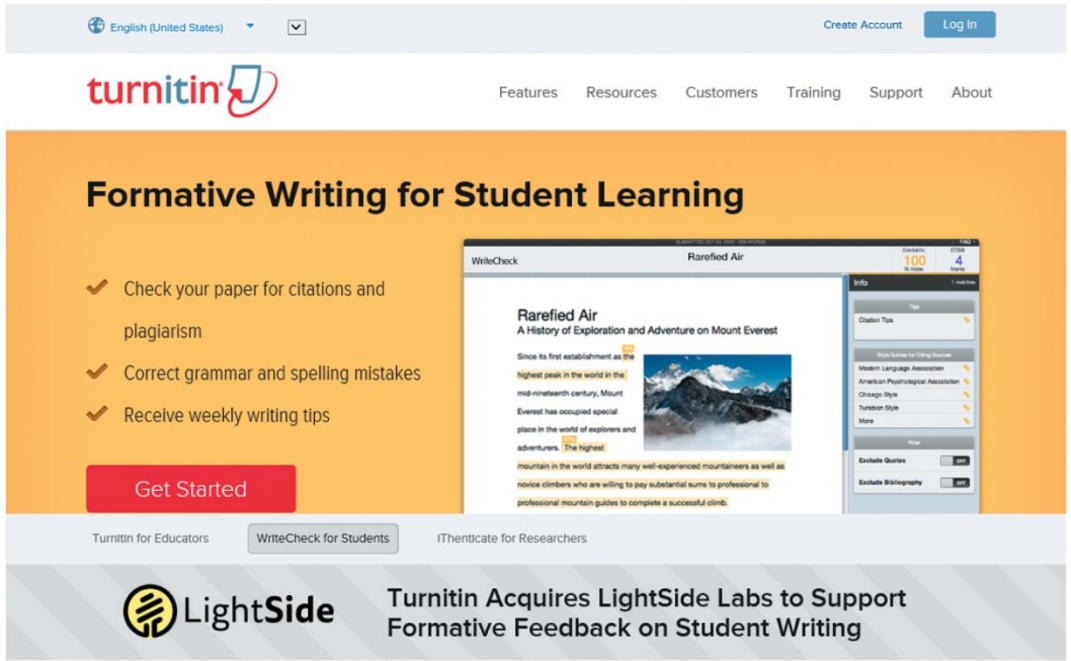
Computer Ethics – guidelines for the morally acceptable use of computers

- 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



Plagiarism

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



The National Cyber Security Agency (NACSA) in Malaysia

- was officially established in February 2017 as the national lead agency for cyber security matters, with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyber attacks, by co-ordinating and consolidating the nation's best experts and resources in the field of cyber security.
- **VISION**
- Establishing a stable, safe and resilient cyber environment to meet the economic and social needs of Malaysia.

https://www.nacsa.gov.my/index.php

CYBER SECURITY ACT 2024 (ACT 854)

- The Cyber Security Act 2024 has been officially gazetted by the Attorney General's Chambers on 26 June 2024. This legislation is a major milestone in strengthening Malaysia's cyber defenses and enhancing our resilience against emerging threats.
- The Cyber Security Act 2024 introduces several important features, such as the establishment of the National Cyber Security Committee.

https://www.nacsa.gov.my/act854.php

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
- Demand for this position is expected to grow


Yuri Arcurs/E+/Getty Images

Cyber Security Analyst?

The average monthly salary for Cyber Security Analyst jobs in Malaysia ranges from **RM 5,500** to **RM 6,800**. (jobstreet.com)

Job Title	Range	Average
Cyber Security Analyst	RM 5k - RM 103k	RM 46,540
Cyber Security Engineer	RM 3k - RM 138k	RM 50,868
Security Analyst	RM 6k - RM 103k	RM 48,683
Security Engineer	RM 4k - RM 266k	RM 51,923
Information Security Analyst	RM 31k - RM 92k	RM 51,900
Information Security Manager	RM 99k - RM 256k	RM 146,939
Chief Information Security Officer	RM 196k - RM 240k	RM 222,480

Open-Ended Questions (Page 1 of 3)

1. Define privacy and discuss the impact of large databases, private networks, the Internet, and the Web.

1. Define and discuss online identity and the major privacy laws.

1. Define security. Define computer crime and the impact of malicious programs, including viruses, worms, Trojan horses, and zombies, as well as denial of service attacks, rogue Wi-Fi hotspots, data manipulation, identity theft, Internet scams, and cyberbullying.

Open-Ended Questions (Page 2 of 2)

4. Discuss ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.

4. Define ethics, and describe copyright law and plagiarism.