McGraw Hill Education

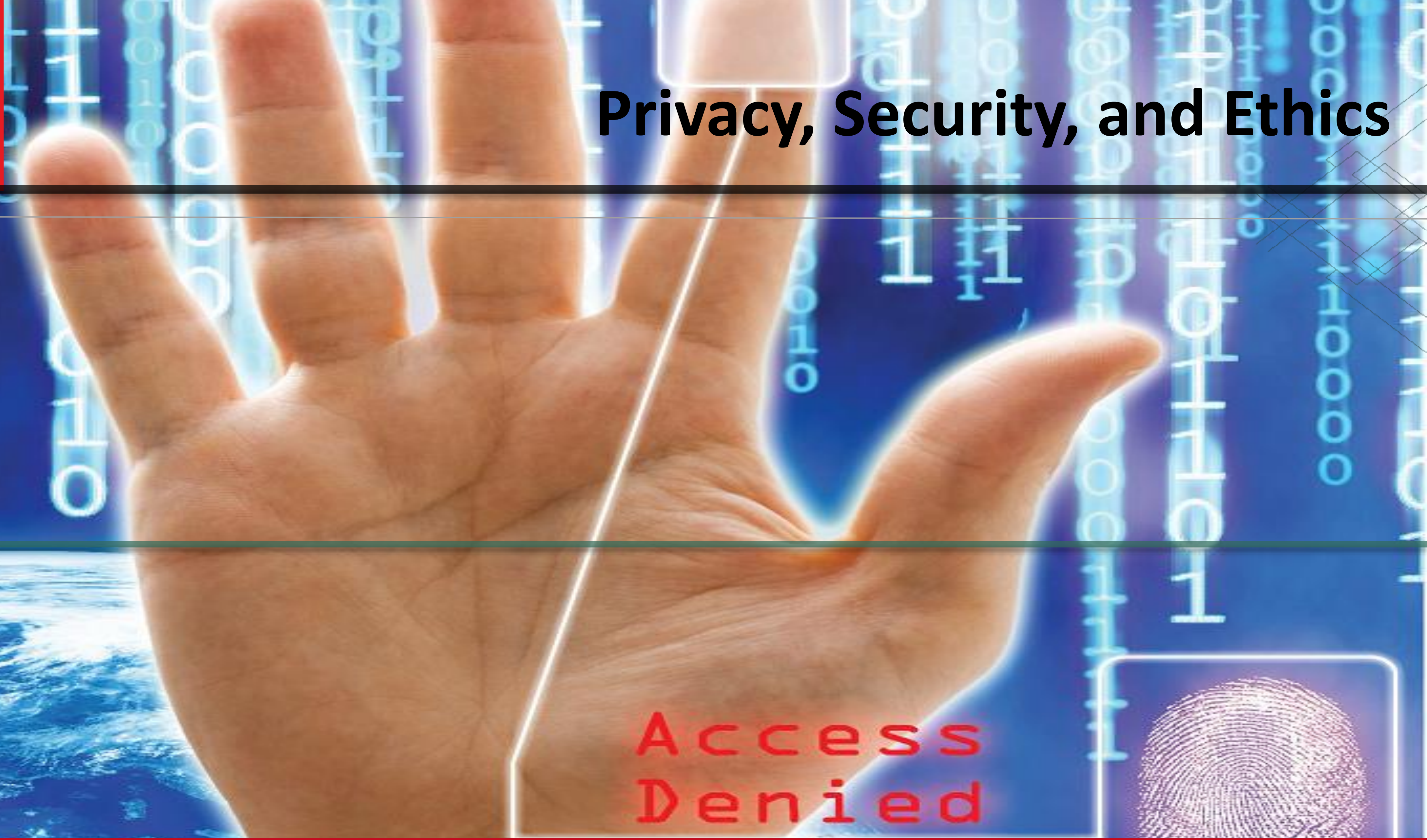
Privacy, Security, and Ethics

Lecture 3

Dr. Hala Najwan Sabeh

Email: hala.najwan@tiu.edu.iq

Privacy, Security, and Ethics



Because learning changes everything.™

People

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

- Negative impact concerns of technology:

1) Privacy – What are the threats to personal privacy and how can we protect ourselves?
2) Security – How can access to sensitive information be controlled and how can we secure hardware and software?
3) Ethics – How do the actions of individual users and companies affect society?

Privacy

- Privacy – concerns the collection and use of data about individuals

There are three primary privacy issues:

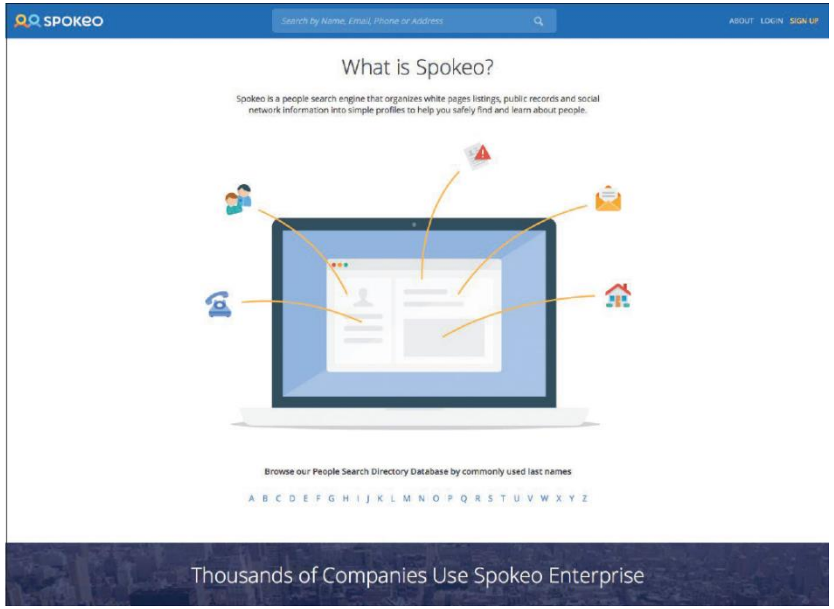
1) Accuracy – responsibility of those who collect data
   – Must be secure and correct
2) Property – relates to who owns the data
3) Access – responsibility of those who control data and use that data

Large Databases

Large organizations compile information about us daily

Big data - ever growing volume of data

- Big Data is exploding and ever-growing



What is Spokeo?

Spokeo is a people search engine that organizes white pages listings, public records and social network information into simple profiles to help you safely find and learn about people.

Browse our People Search Directory Database by commonly used last names

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

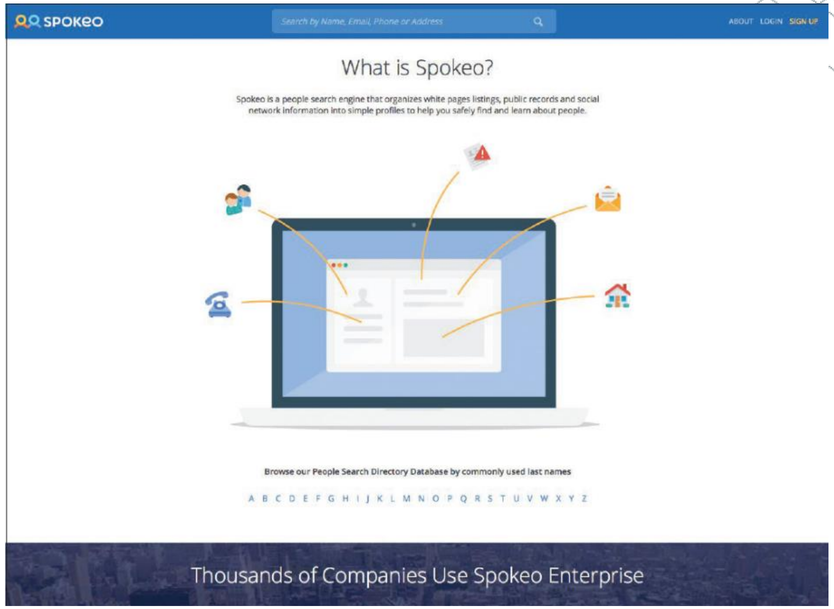
Thousands of Companies Use Spokeo Enterprise

Large Databases (Cont.)

Data collected and stored on citizens every day

Collectors' companies or websites include :

1. Telephone companies
2. Credit card companies
3. Supermarket scanners
4. Financial institutions
5. Search engines
6. Social networking sites



What is Spokeo?

Spokeo is a people search engine that organizes white pages listings, public records and social network information into simple profiles to help you safely find and learn about people.

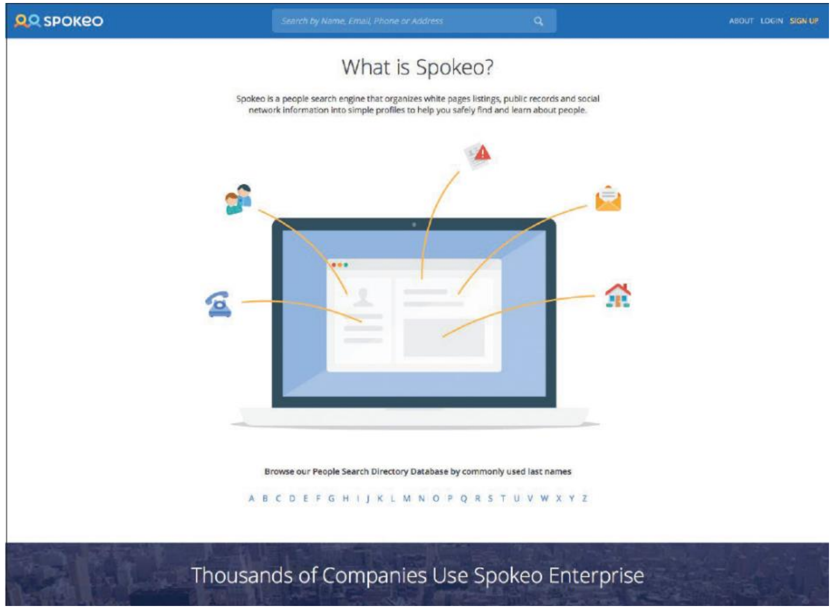
Browse our People Search Directory Database by commonly used last names

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Thousands of Companies Use Spokeo Enterprise

Large Databases (Cont.)

- Information Resellers/Brokers
  - Collect and sell personal data
  - Using publicly available databases and in many cases nonpublic databases, information resellers create **electronic profiles**, or highly detailed and personalized descriptions of individuals.


spokeo
Search by Name, Email, Phone or Address
ABOUT
LOGIN
SIGN UP

What is Spokeo?

Spokeo is a people search engine that organizes white pages listings, public records and social network information into simple profiles to help you safely find and learn about people.

Browse our People Search Directory Database by commonly used last names

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Thousands of Companies Use Spokeo Enterprise

Electronic profiles

(List three important issues related to electronic profiles)

These electronic profiles can reveal more than you might wish to make public and have an impact beyond what you might imagine. This raises many important issues, including:

1) Collecting public, but personally identifying information (e.g., Google's Street View)

2) Spreading information without personal consent, leading to identity theft

3) Spreading inaccurate information

Electronic profiles (Cont.)

These electronic profiles can reveal more than you might wish to make public and have an impact beyond what you might imagine. This raises many important issues, including:

1) Collecting public, but personally identifying information (e.g., Google's Street View)

Electronic profiles (Cont.)

These electronic profiles can reveal more than you might wish to make public and have an impact beyond what you might imagine. This raises many important issues, including:

2) Spreading information without personal consent, leading to identity theft

Example: collecting your shopping habits and sharing; or medical records, or driver's license number

Electronic profiles (Cont.)

These electronic profiles can reveal more than you might wish to make public and have an impact beyond what you might imagine. This raises many important issues, including:

3) Spreading inaccurate information

once you are tagged that photo can become a part of your electronic profile

- **Mistaken identity – an electronic profile of one person is switched with another**

Freedom of Information Act

Freedom of Information Act

- Entitlement to look at your records held by government agencies

Private Networks

Many businesses search employees' electronic mail and computer files using **employee-monitoring software.** These programs record virtually everything you do on your computer.

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

Concept check

1) Define privacy and list the three primary privacy issues.
2) Define privacy and explain the three primary privacy issues.
3) Every day, data is gathered about us and stored in large databases. Give six examples of collector companies or websites.
4) What is big data? Information resellers? Electronic profiles?
5) List three important issues related to electronic profiles.
6) What is mistaken identity?
7) What is the Freedom of Information Act?
8) What is employee-monitoring software?

Mc Graw Hill Education

The Internet and the Web

- When browsing the web, critical information is stored on the hard drive in these locations:
  1) **History Files**
  2) **Temporary Internet Files**
     - **Browser cache**
  3) **Cookies**
  4) **Spyware**

Because learning changes everything.™

History Files and Temporary Internet Files

History Files

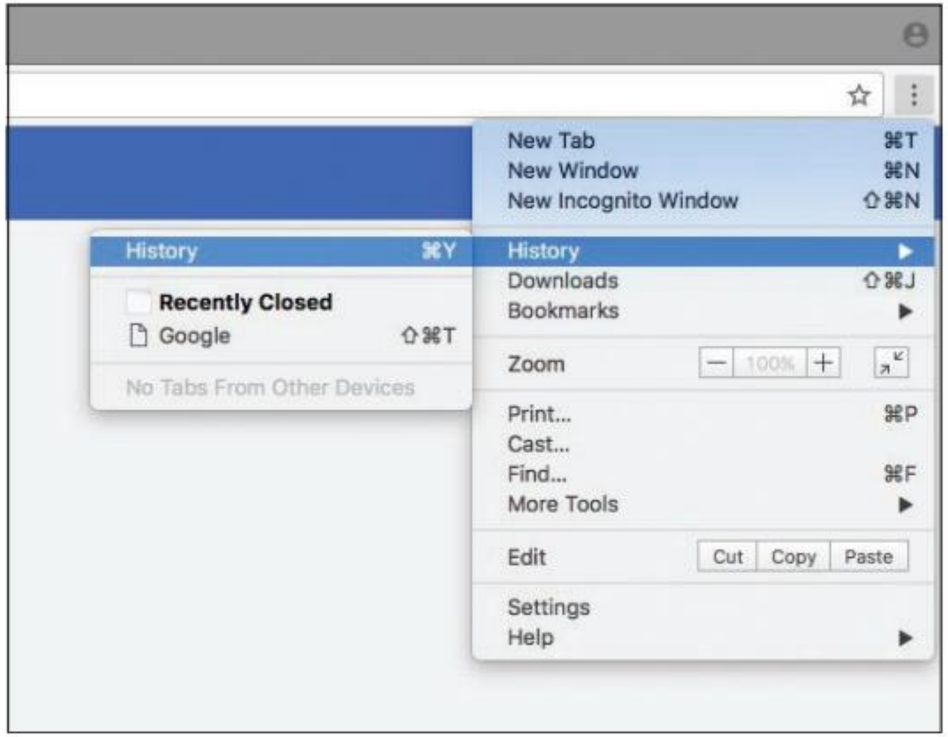
- History Files include locations or addresses of sites you have recently visited.

Temporary Internet Files / Browser Cache

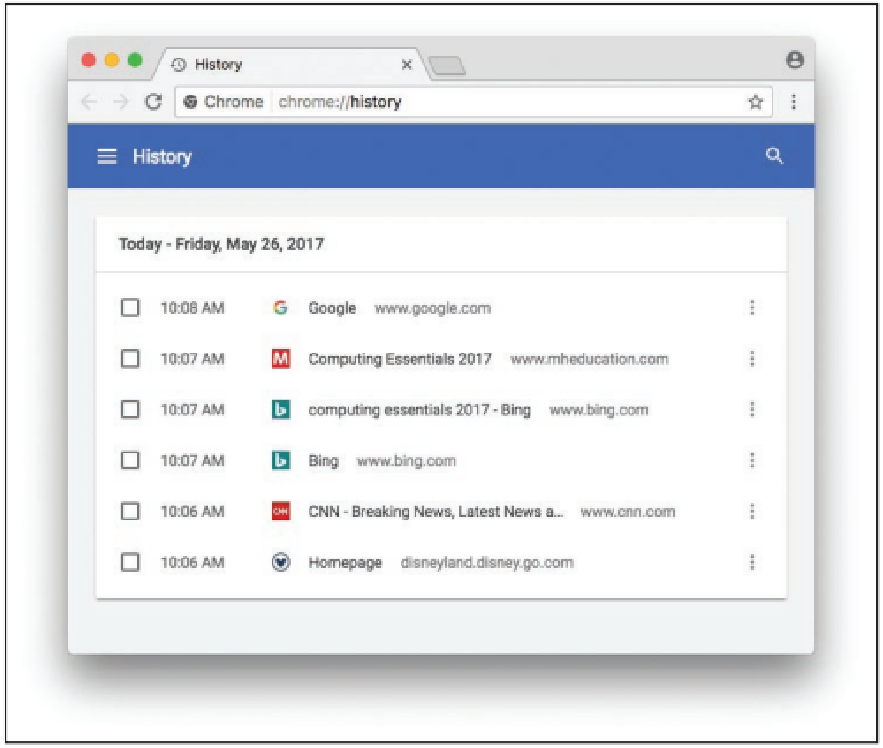
- Temporary Internet Files / Browser Cache saved files from visited website
- Temporary Internet Files / Browser Cache contain web page content and instructions for displaying this content.
- Temporary Internet Files / Browser Cache offers quick re-display when you return to the site

History Files

1 In the top-right corner of the browser window, select the *Chrome Menu* button.



2 Select *History*.



Today - Friday, May 26, 2017

□	10:08 AM	Google	www.google.com
□	10:07 AM	Computing Essentials 2017	www.mheducation.com
□	10:07 AM	computing essentials 2017 - Bing	www.bing.com
□	10:07 AM	Bing	www.bing.com
□	10:06 AM	CNN - Breaking News, Latest News a...	www.cnn.com
□	10:06 AM	Homepage	disneyland.disney.go.com

Figure. Viewing history files

Because learning changes everything.™

Cookies

- **Cookies:** Small data files that are deposited on your hard disk from web sites you have visited

- Most cookies are harmless and are intended to provide customized service

Cookies

There are **two** basic types of **cookies**:

1) **First-party cookies**
2) **Third-party cookies**

Cookies

1) **First-party cookies** - is one that is generated (and then read) only by the website you are currently visiting.

- Many websites use first-party cookies to store information about the current session, your general preferences, and your activity on the site. The intention of these cookies is to provide a personalized experience on a particular site.

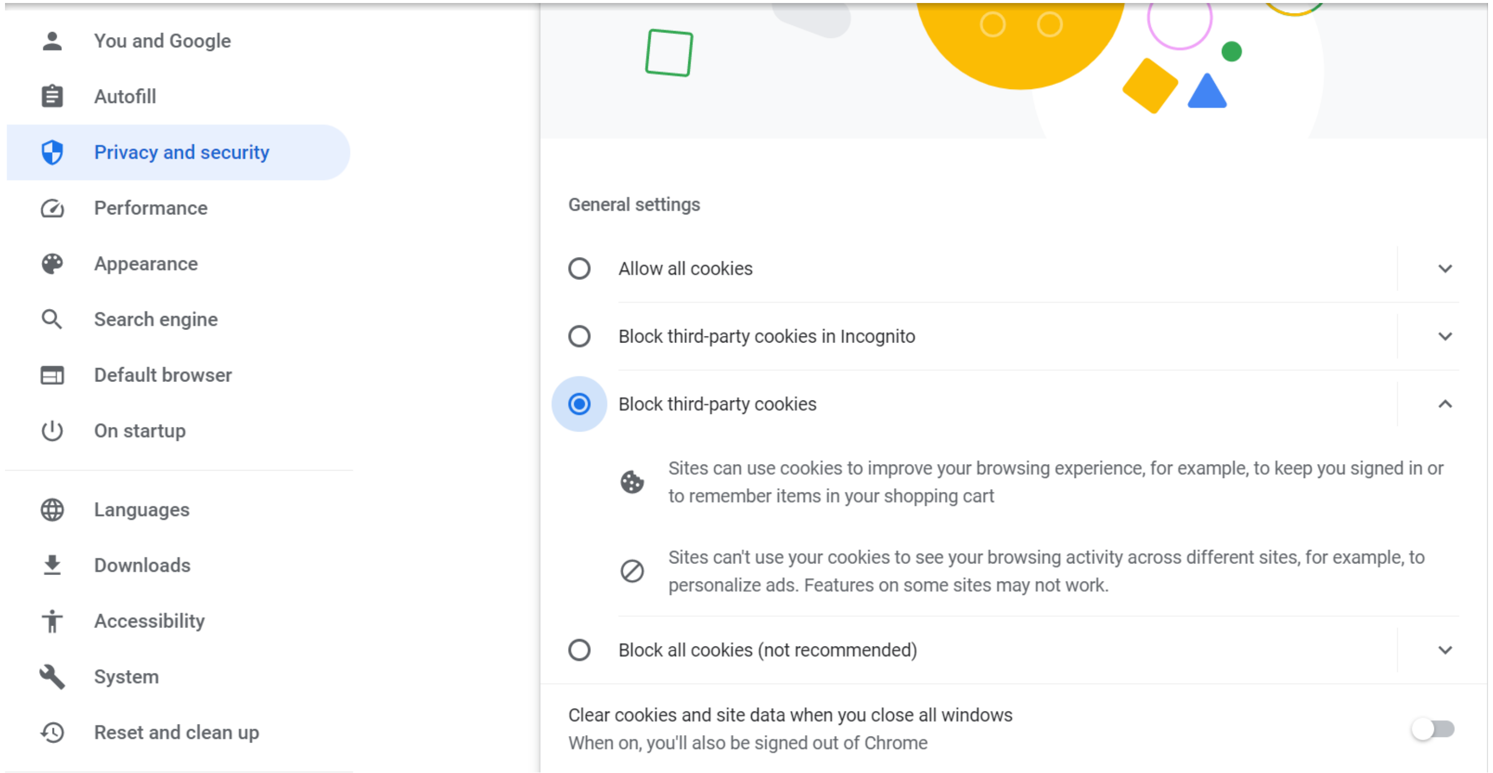
- For example, when you revisit a particular electronic commerce site, a previously deposited cookie can provide information so that you can be greeted by name and presented with sales and promotions that interest you.

Cookies

2) **Third-party cookies** - generated by an advertising company that is affiliated with the website you are currently visiting.

- Third-party cookies also known as **tracking cookies** that keep track of your Internet activities
- For example, suppose you visit four different websites that employ the same advertising agency. The first three sites are about cars, but the fourth is a search engine. When you visit the fourth site, you will likely see a car advertisement because your cookie showed that you had been visiting car-related websites

Cookies



General settings

○ Allow all cookies

○ Block third-party cookies in Incognito

● Block third-party cookies

Sites can use cookies to improve your browsing experience, for example, to keep you signed in or to remember items in your shopping cart

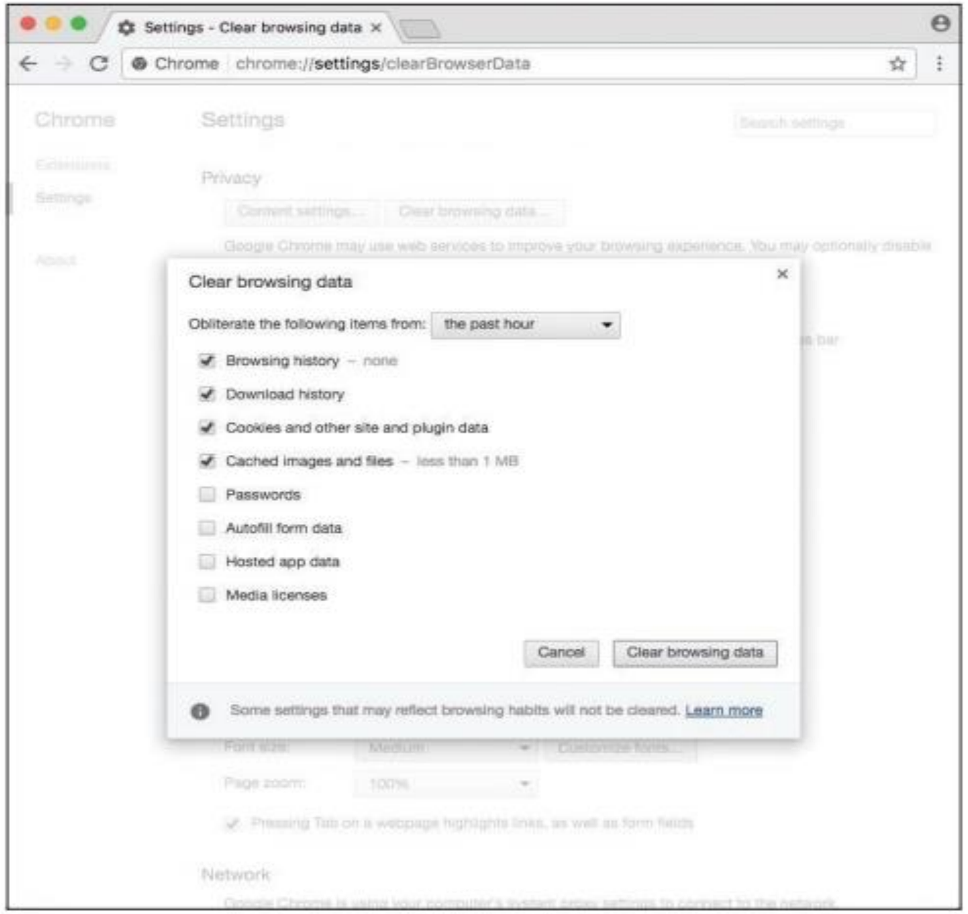
Sites can't use your cookies to see your browsing activity across different sites, for example, to personalize ads. Features on some sites may not work.

○ Block all cookies (not recommended)

Clear cookies and site data when you close all windows
When on, you'll also be signed out of Chrome

Figure. Blocking cookies

Deleting browsing history


Settings - Clear browsing data ×
Chrome chrome://settings/clearBrowserData
Chrome
Settings
Privacy
Network

Clear browsing data

Obliterate the following items from: the past hour

☑ Browsing history – none

☑ Download history

☑ Cookies and other site and plugin data

☑ Cached images and files – less than 1 MB

□ Passwords

□ Autofill form data

□ Hosted app data

□ Media licenses

Cancel | Clear browsing data

Some settings that may reflect browsing habits will not be cleared. Learn more

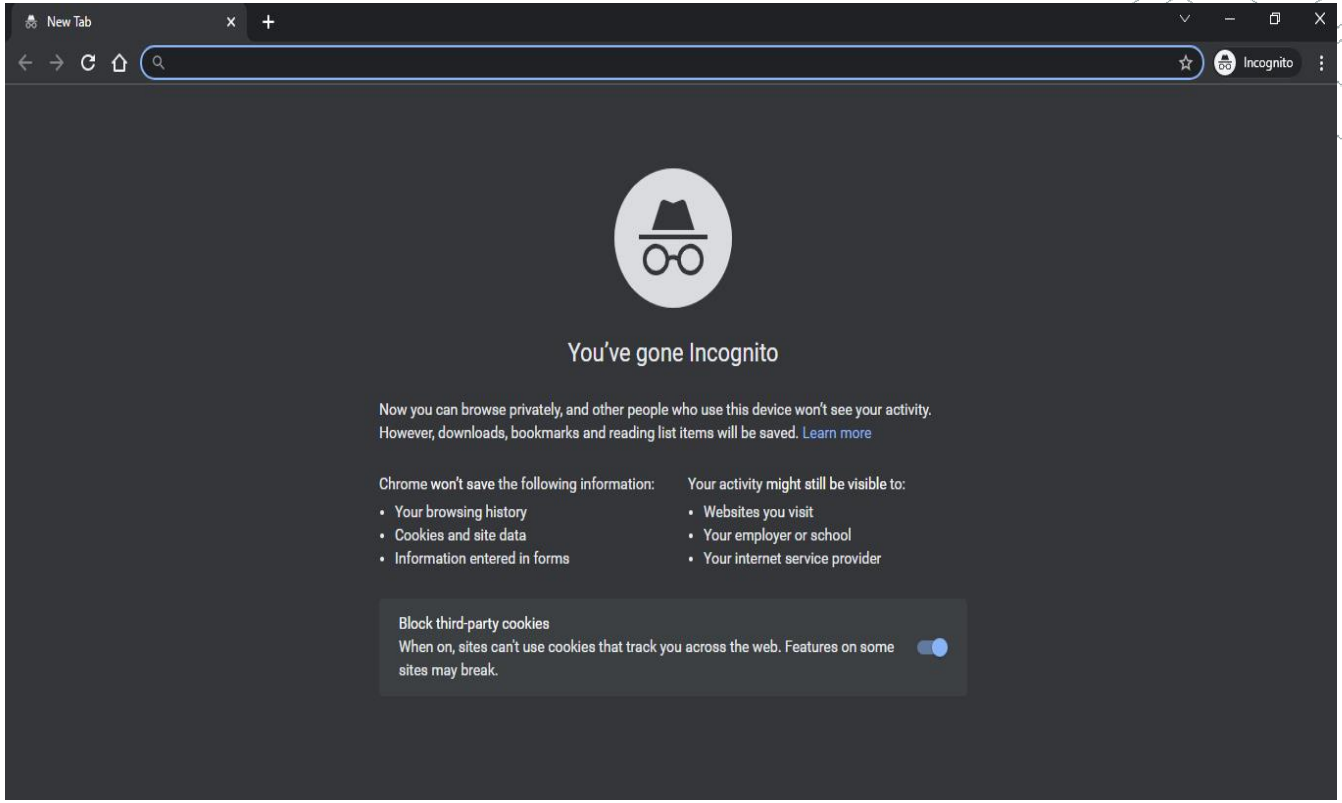
Figure. Deleting browsing history

Privacy Modes

- Most browsers also offer a **privacy mode**, which ensures that your browsing activity is not recorded on your hard disk.

For example

- **Google Chrome** provides **Incognito Mode** accessible from the Chrome menu.
- **Safari** provides **Private Browsing** accessible from the Safari option on the main menu.



You've gone Incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Privacy Modes

Privacy mode: eliminates history files as well as blocks most cookies.

Incognito mode: privacy mode for Chrome

Private Browsing: privacy mode for Safari

Privacy Threats

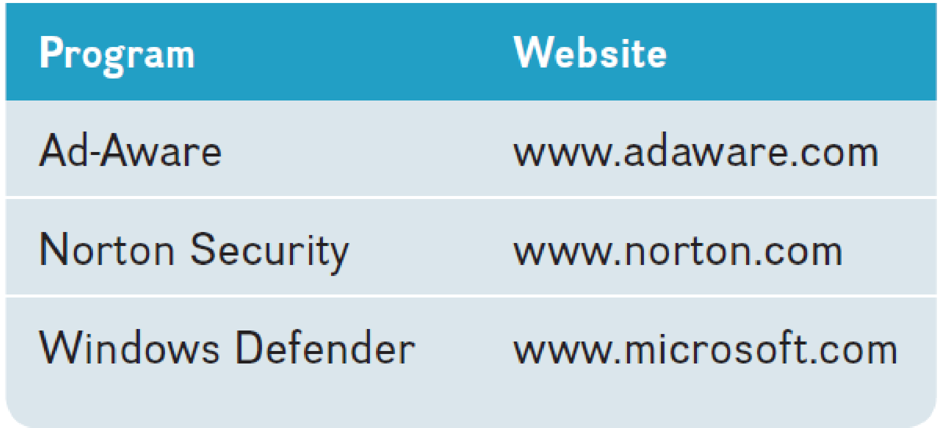
- **Web bugs**
  - Web bugs are invisible images or HTML code hidden within an e-mail message or web page
- **Spyware**
  - Spyware is the most dangerous type of privacy threat
  - Spyware is secretly record and report the internet activities of an individual's.
  - Spyware can change browser to manipulate what you see online

Privacy Threats

- **Computer monitoring software**
  - Most dangerous type of spyware
  - Programs record every activity and keystroke made on a computer system including credit card numbers, bank account numbers, and e-mail messages
  - Keystroke Loggers - can be deposited on a hard drive without detection from the Web or by someone installing programs directly onto a computer
    - Record activities and keystrokes

Privacy Threats

- **Anti-Spyware programs / spy removal programs**
  - Detect and remove privacy threats
  - A category of programs known as spy removal programs designed to detect Web bugs and monitoring software



Program	Website
Ad-Aware	www.adaware.com
Norton Security	www.norton.com
Windows Defender	www.microsoft.com

Figure . **Antispyware programs**

Online Identity

Online identity: can be defined as the information that people voluntarily post about themselves online

- Archiving and search features of the Web make it available indefinitely

Online Identity

- **Major Laws on Privacy related to the online identity**
  1) **Gramm-Leach-Bliley Act** protects personal financial information
  2) **Health Insurance Portability and Accountability Act (HIPAA)** protects medical records
  3) **Family Educational Rights and Privacy Act (FERPA)** resists disclosure of educational records

Concept check

1) Define history files
2) Define temporary Internet files/ Browser Cache
3) Define Privacy mode
4) What is a cookie? A first-party cookie? A third-party cookie?
5) What is a web bug? Spyware? Keystroke Loggers ? Antispyware programs? Online identity?

Concept check

6) List the two basic types of cookies

7) Define Incognito mode

8) Define Private Browsing

9) List the major laws on privacy related to online identity and explain one of them in detail.

Security

Security: Involves protecting individuals or organizations from theft and danger.

- People who gain unauthorized access to computers are hackers
- Not all hackers are illegal

Cybercrime / Computer Crime: can be defined as the 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

List some of the most common forms of Computer Crime

Computer Crime	Description
1) Identity theft	Illegal assumption of a person's identity for economic gain
2) Internet scams	Scams over the Internet
3) Data manipulation	Unauthorized access of a computer network and copying files to or from the server
4) Ransomware	Malicious software that encrypts your computer's data and ransoms the password to the user
5) 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

Internet Scams

Internet scams are 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

Common Internet Scams

Lists some of the most common Internet Scams:

1) Advance fee loans
2) Auction fraud
3) Fake antivirus software
4) Nigerian Scam

Common Internet Scams

Lists some of the most common Internet Scams

Type	Description
1) 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."
2) Auction fraud	Merchandise is selected and payment is sent. Merchandise is never delivered.
3) Fake antivirus software	A website or e-mail warns you that you are at risk of being infected by a computer virus and you need to download and install the security software they recommend. The security software is fake and will install malicious software on your computer.
4) 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 their 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 they will disappear

Concept check

1) Define security, hackers.
2) What is cybercrime?
3) List some of the most common forms of computer crime and explain one of them in detail.
4) What are identity theft and Internet scams?
5) What are data manipulation, ransomware, and denial of service attacks?
6) Lists some of the most common Internet Scams and explain one of them in detail.

Social Engineering

Social engineering is the practice of manipulating people to divulge private data.

Played a key role in:

1) Identity theft
2) Internet scams
3) Data manipulation

Social Engineering

- The most common social engineering technique is Phishing

- Phishing can be defined as the attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legal.

Malicious Programs - Malware

- **Malicious Programs or Malware**
  - 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
  - **The three most common Malicious Programs / Malware**
    1) Viruses – migrate through networks and attach to different programs; can alter and/or delete files; can damage system components.
    2) Worms – a special type of virus fills the computer with self-replicating information
    3) Trojan horse – programs disguised as something else; The most common type of Trojan horses appear as free computer games.

Malicious Hardware

Criminals use hardware for crimes.

Most common malicious hardware are:

1) **Zombies**
2) **Rogue Wi-Fi Hotspots**
3) **Infect USB Flash Drives**

Malicious Hardware

Cyber criminals can use computer hardware to steal information.

Three types of malicious hardware:

1) Zombies

- **Zombies** are computers infected by a virus, worm, or Trojan Horse that allows them to be remotely controlled for malicious purposes.
- Botnet or Robot Network is a collection of Zombies

Malicious Hardware

Cyber criminals can use computer hardware to steal information.

Three types of malicious hardware:

2) **Rogue Wi-Fi Hotspots**

Imitate a legitimate free Wi-Fi hotspot. When users connect to this rogue Wi-Fi, their data and private information is captured and used for illegal activities

Malicious Hardware

Cyber criminals can use computer hardware to steal information. Three types of malicious hardware:

3) Infect USB Flash Drives

- Crackers load malicious software on the USB drives and left on purpose in hopes for people to pick up and use.
- Infect USB flash drives have malicious software contained on them.

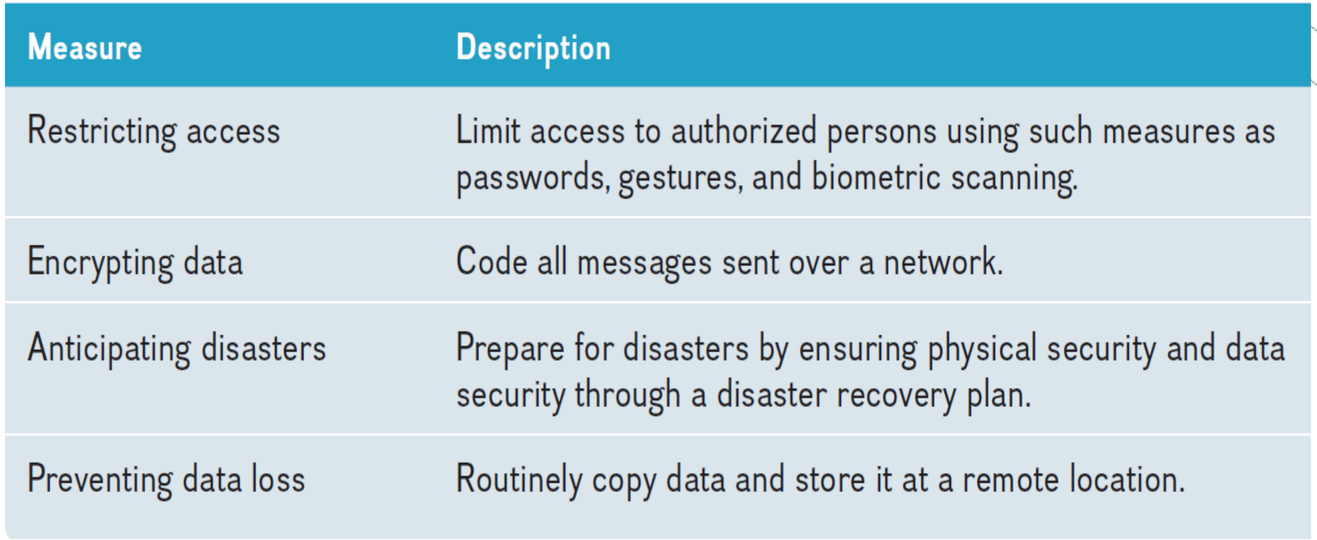
Concept check

1) What is social engineering? What is phishing?
2) What is malicious Programs / Malware
3) List the three most common Malicious Programs / Malware and explain one of them in detail.
4) Define Viruses, Worms, and Trojan horses.
5) What is malicious hardware? Zombies? Botnets? Rogue Wi-Fi hotspots? Infected USB flash drives?
6) List the three types of malicious hardware and explain one of them in detail.

Measures to Protect Computer Security

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, gestures, 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

- Computers should be protected from unauthorized access by using **Passwords** or **Biometric scanning devices**

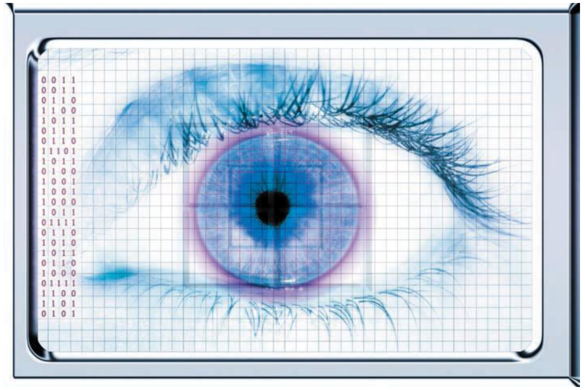
Passwords: is the most common way to restrict access

  - **Dictionary attack**

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

Restricting Access

- Computers should be protected from unauthorized access
- Biometric scanning devices such as Fingerprint scanners and Iris (eye) scanners
- Facial recognition (technology that recognizes your face and logs you into your computer)



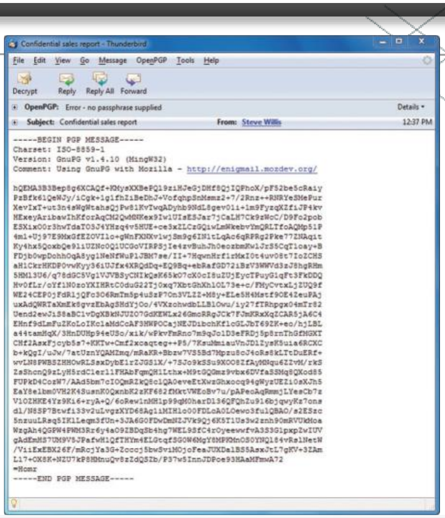
Automated Security Tasks

Ways to perform and automate important security tasks

1) Security Suites
   - Provide a collection of utility programs designed to protect your privacy and security
2) Firewalls
   - Security buffer between a corporation's provide network and all external networks
3) Password Managers
   - Helps to create strong passwords

Encryption

- **Encryption** is the process of coding information to make it unreadable except to those who hold an encryption key.
- **Encryption key** is used to decrypt the information into a readable format.

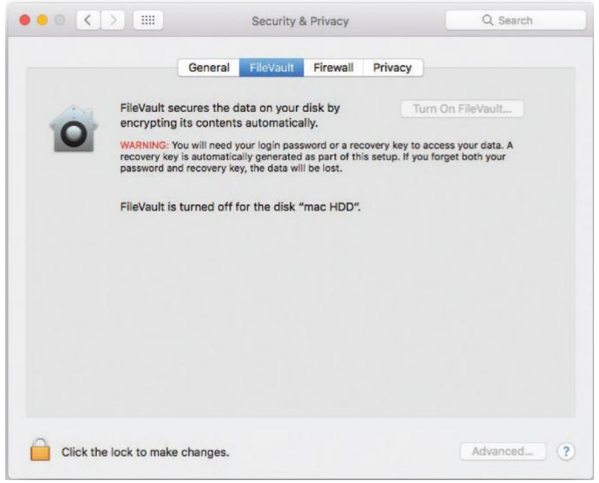


OpenPGP: Error - no passphrase supplied

Subject: Confidential sales report From: Steve Willis 12:37 PM

```
-----BEGIN PGP MESSAGE-----
Charset: ISO-8859-1
Version: GnuPG v1.4.10 (MingW32)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org/

hQEMA3B3Bep8g6XCAQf+KMysXXBePQ19ziMJeGjDMf8QjIQPhoX/pF52be5cRaiy
PzBfk61QeWJy/iCgk+1g1fhZiBeDhJ+VofqhpSnMemz2+7/2Rnz++RNRYeSMePur
XevIxT+ut3n4sWgWtahsQjPw81KvTwqADyhb9NdL8gev01i+1m9FyzqXZfiJP4kv
HExeyAribawIhKforAqCM2QwMNKex9Iw1UIsESJar7jCaLH7Ck9zWoC/D9Fo2pob
ESXixO0r3hwTdaTO3J4YHzq4v5HUE+ce3xZLCzGQiwLmWkebvYmQRLTfoAQMp51P
4m1+Uj97E9MxGfEZOVIlo+gWnFXNXv1wjSm9g6IN1tLqAc6qRPRg2Pke77ZNAqit
Ky4hx5QoxbQe91iUZNc0Q1UCGoVIRPSjIe4zvBuhJh0eozbmKw1JrS5CqT1oay+B
FDjb0wpDohhOqA8yg1NeNfWuPlJBM7se/II+7HqwnHrf1rMxI0t4uv08t7IoZCHS
aH1CkrHKDP0vwKyy36iUJfx4XRQdDq+EQ9Bq+ebRafGD72iBzV3WWVd3zJ8hgRHm
5HMl3U6/q78dGC5Vg1VJVBSyCNIkQsK65k07cX0cI8uZUjEycTPuyG1qFt3FkDDQ
Mv0fLr/oYf1N0zoYXIHRtC0duG22Tj0xq7XbtGhXhlOL73e+c/FMyCvtxLjZUQ9f
WE24CEP0jFdR1jQFc3O6RmTm5p4u8zP7On3VLZZ+M8y+ELe5H4Mstf9OE4ZeuPAj
uxAdQWRTaXmEk8gvzEbAgSMdYjOo/4VXzohwdbLLB1Owu/iy27fTRhpgx04mTr82
Uend2ewJiS8aBC1vDgXBkNJUZO7GdKEWLx26GmoRRgJCk7FJmKRxXqZCAR5jA6C4
EHnf9dLmFuZKoLoIKclaMdCcAF3MWPOCajNEJDibchKf1cGLJbT69ZK+eo/hjLBL
a44tamMqX/3HnDUMp94eUSo/xik/wPkvFmRno7m9qJo1D3eFRDj5p8rnThGfMGXT
CMf2AsxFjcyb5s7+KKTw+Cmf2xcaqteg++P5/7KsuMmiauVnJD1ZysK5uia6RCXC
b+kQgI/uJw/7atUznYQAMZmq/mRaKR+Bbzw7VS5Bd7Mpzu8cJ4oRs8kLTtDuERf+
wvLN8PWB5ZHHOwRLSaxDybE1rZJGS1X/+7SJo9kSSu9XOO8ZfAyMNqu6ZZvM/rkS
ZsShcnQ9zLyH5rdC1er11FHAbFqmQH1Lthx+M9tGQGmz9vbx6DVfaSSMq8QXod85
FUPkD4CozW7/AAd5bm7cIOQmRZkQ8c1QA0eveEtXwzGhxocq94gWyzUEZi0sXJh5
EaY8elbm0VH2K4SusnK0QxnbK2zKF682fMktVWZoBv7u/pAPeoAqRmmjLYesCb7z
V1OZHKE4Yz9Ki6+ryA+Q/6oRew1nMH1p99qM0harD136QFQhZu916bjqwyKz7ons
dl/N8SP7Btwfi33v2uLvgzXYD68Ag1iMIHlo00FDLoA0LOewo3fulQBAO/s2ESzc
5nzuuLRsq5IK1Leqm3fUn+3JA6G0FDwDmNZJVk9Qj6K5T1Us3w2znh90mRVUkMoa
WzgAh4QGPW4PWM3Rr6y4a09ZBDqSb4hg7WEL9SfC4rOyeewwfvA3S3G1pxpZwIUV
gAdEmMS7UM9V8JPafwM1QfTMYm4ELGtqfSG0W6MgY8MPKMnO5OYNQ184vRslNetW
/ViiExEBX26F/mRcjYa3G+Zoccj5bwSviMOjoFeaJUXDalBS5AsxJtL7gKV+3ZAm
L17+OX8K+NZU7kP8HMnuQv8zZdQ5Zb/P37w5InnJDPoe93HAaMFmwA72
=Homr
-----END PGP MESSAGE-----
```



FileVault secures the data on your disk by encrypting its contents automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned off for the disk “mac HDD”.

Click the lock to make changes.

Because learning changes everything.™

Encryption

- **Common uses for encryption:**
  1) E-mail encryption (protects emails)
  2) File encryption (protects files)
  3) Website encryption
     - HTTPS – hypertext transfer protocol secured: is the most common protocol for website encryption

Anticipating Disasters and Preventing Data Loss

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

Anticipating Disasters and Preventing Data Loss

Preventing Data Loss can be done through:

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

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

1) Update software
2) Be careful when browsing
3) Be alert to e-mail scams
4) Use antivirus software
5) Strong passwords

Concept check

1. Define each of the following: password, dictionary attack, facial recognition, security suite, firewalls, and password managers.
2. What are encryption and an encryption key?
3. List the common uses for encryption.
4. Define physical security, data security, and disaster recovery plans.
5. Describe how to prevent data loss.
6. What are the precautions that you should take to make sure that you aren't the victim of high-tech criminals?

Ethics

- **Computer Ethics** – guidelines for the morally acceptable use of computers
  - Copyright and Digital Rights Management
  - Cyberbullying
  - 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

iTunes.

Your music, movies, and TV shows take center stage.

iTunes is the best way to organize and enjoy the music, movies, and TV shows you already have — and shop for the ones you want to get. It's home to Apple Music, which gives you unlimited access to millions of songs, curated playlists,[1] and Beats 1 radio, hosted by Zane Lowe and a team of acclaimed DJs. Enjoy all the entertainment iTunes has to offer on your Mac and PC.

Copyright and Digital Rights Management

- Software piracy: unauthorized copying and distribution of software
- Digital Millennium Copyright Act makes it illegal to deactivate or disable antipiracy technologies, to copy, resale, or give away commercial programs or to sell or use programs or devices that are illegally copying software.

Copyright and Digital Rights Management

- 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

(2) Limit the kinds of devices that can access a file.

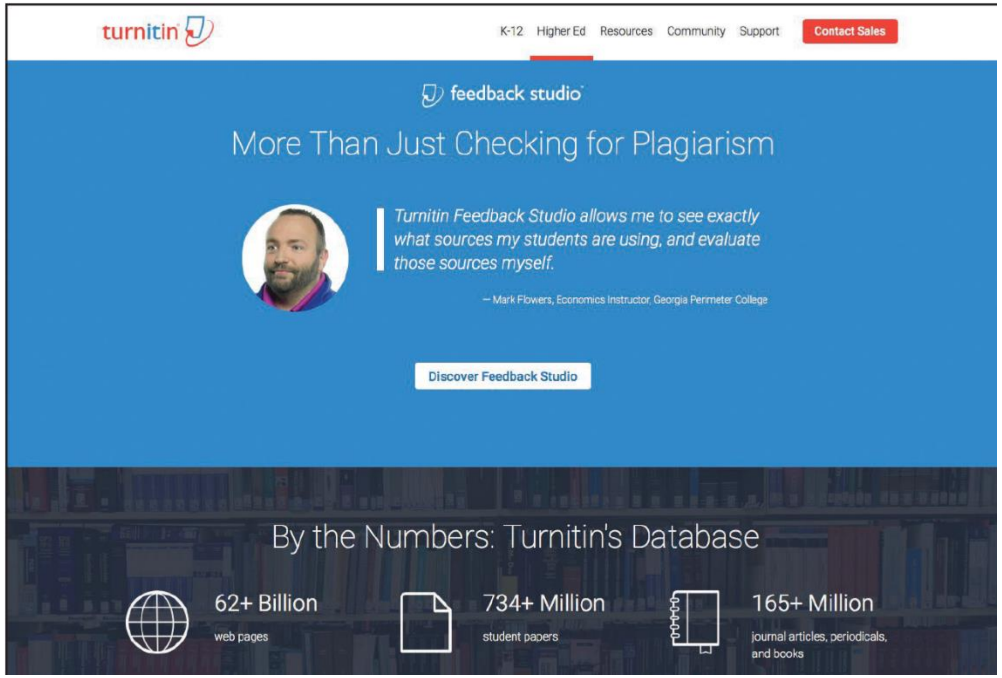
Cyberbullying and Plagiarism

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



More Than Just Checking for Plagiarism

> *Turnitin Feedback Studio allows me to see exactly what sources my students are using, and evaluate those sources myself.*
>
> — Mark Flowers, Economics Instructor, Georgia Perimeter College

By the Numbers: Turnitin's Database

62+ Billion web pages

734+ Million student papers

165+ Million journal articles, periodicals, and books

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 $58,000 to $86,000
- Demand for this position is expected to grow

Concept check

1) Define computer ethics.
2) Define copyright, software piracy, digital rights management, and the Digital Millennium Copyright Act.
3) What is cyberbullying?
4) What is plagiarism?