



Unit 3 Tutorials: Networks and the Internet

INSIDE UNIT 3

Computer Networks

- [Introduction to Computer Networks](#)
- [Computer Network Components](#)
- [Computer Network Types](#)
- [Network Security and Cybersecurity](#)

The Internet, Online Risks, and Social Media

- [The World Wide Web](#)
- [Website Development](#)
- [Protecting Minors from Online Dangers](#)
- [Computer Addiction](#)
- [Benefits and Risks of Social Media](#)

Ethical and Legal Considerations

- [Copyright, Trademark and Intellectual Property](#)
- [Ethical Behavior in the Digital World](#)
- [Professional Code of Ethics](#)

Introduction to Computer Networks

by Sophia



WHAT'S COVERED

In the early days of computing, computers were seen as devices for making calculations, storing data, and automating business processes. However, as the devices evolved, it became apparent that many of the functions of telecommunications could be integrated into the computer. During the 1980s, many organizations began combining their once-separate telecommunications and information-systems departments into an information technology, or IT, department. This ability of computers to communicate with one another and, maybe more importantly, to facilitate communication between

individuals and groups, has been an important factor in the growth of computing over the past several decades. In this tutorial, we will take a closer look at computer networks, and why businesses rely so heavily on them.

Our discussion will break down as follows:

1. Networks

A **network** is a group of people, or devices, connected for the sole purpose of collaborating and sharing resources. Not all networks involve computers or the Internet. Telephone networks provide people with the ability to engage in conversations with one another over large distances. A satellite network provides GPS devices with directions to locations.



TERM TO KNOW

Network

Group of people or devices connected for the sole purpose of sharing data or resources.

2. Computer Networks

A **computer network** is a group of computers, servers, peripheral devices, and network hardware all connected for the purpose of sharing data. Computer networks can be categorized based on the proximity of the network's devices to one another. A **local area network (LAN)** is a computer network where all of the equipment is in close proximity to one another, usually in an office building or on the same campus. LANs are typically confined to a small local area and can be wired or wireless.

Conversely, a **wide area network (WAN)** is a computer network with all of the equipment spread over a large geographic area. It is typically inclusive of many small networks or LANs. WANs can be wired or wireless. The most common example of a WAN is the Internet. In fact, computer networking really began in the 1960s with the birth of the Internet. However, while the Internet was evolving and creating a way for organizations to connect to each other and the world, another revolution was taking place inside organizations. The proliferation of personal computers inside organizations led to the need to share resources such as printers, scanners, and data. Organizations solved this problem through the creation of local area networks (LANs), which allowed computers to connect to each other and to peripherals. These same networks also allowed personal computers to hook up to legacy mainframe computers. When an organization needed to provide a network over a wider area (with locations in different cities or states, for example), they would build a wide area network (WAN).



TERMS TO KNOW

Computer Network

A group of computers connected for the purpose of communication-sharing of data and resources.

Local Area Network (LAN)

Computer network that links computers within a building.

Wide Area Network (WAN)

Computer network with all of the equipment spread over a large geographic area, and is typically inclusive of many small networks or LANs.

3. Benefits of Computer Networks

The personal computer originally was used as a stand-alone computing device. However, with the advent of networking and local area networks, computers could work together to solve problems. Higher-end computers were installed as servers, and users on the local network could run applications and share information among departments and organizations. This is called client-server computing. The ability for networked computers to quickly share information is by far one of the most popular reasons for networking computers. To illustrate this idea, consider email applications. The Internet was originally designed as a way for scientists and researchers to share information and computing power among themselves. However, as soon as electronic mail was invented, it began driving demand for the Internet. This wasn't what the developers had in mind, but it turned out that people connecting to people was the killer app for the Internet. Lots of businesses and organizations have also adopted computer networks just to be able to utilize email. The table below lists some more benefits of networked computers.

Networked Computers Allow For:	Translates Into The Following Benefits:
Quick sharing of information (audio, video, text)	--Electronic mail (Email) --Multiple computers can be assigned to solve one problem --Fosters collaboration between users --Decreased need for paper-based communication
Sharing of hardware and software	--One printer can be used to print documents from more than one computer --One computer can be used to serve others (deliver application software)

4. Protocols

Computers and devices on a network use various protocols to facilitate communication between them. A **protocol** is a format or rule for transmitting data between devices. The protocol determines things such as how the sending device notifies the receiving device that there is data to be sent, what data compression method will be used, and how to check for errors in the data. It is critical that the protocol be executed in the same way on each device; otherwise, no communication can take place.

The most common protocol utilized today is the **TCP/IP** used on the Internet. TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a group of protocols that function together for web-based communication.



TERMS TO KNOW

Protocol

Format or rule for transmitting data between devices.

TCP/IP

Transmission Control Protocol/Internet Protocol; a group of protocols that functions together for web-based communication.



SUMMARY

The networking revolution has completely changed how the computer is used. Today, no one would imagine using a computer that was not connected to one or more **networks**. The development of the Internet, combined with wireless access, has made information available at our fingertips. For businesses and organizations, **computer networks help** to increase productivity and efficiency. Because resources can be shared over a **computer network**, businesses are also able to reduce costs by **sharing data** and other resources such as software and hardware.

Source: Derived from Chapter 5 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

Computer Network

A group of computers connected for the purpose of communication-sharing of data and resources.

Local Area Network (LAN)

Computer network that links computers within a building.

Network

Group of people or devices connected for the sole purpose of sharing data or resources.

Protocol

Format or rule for transmitting data between devices.

TCP/IP

Transmission Control Protocol/Internet Protocol; a group of protocols that functions together for web-based communication.

Wide Area Network (WAN)

Computer network with all of the equipment spread over a large geographic area and is typically inclusive of many small networks or LANs.

Computer Network Components

by Sophia



WHAT'S COVERED

Having a basic understanding of networks and networking concepts can provide you with the tools to be able to differentiate between the various types of networks. Regardless of the type of network you are trying to connect to, you will need to have the proper combination of hardware and software in order to make full use of a computer network. In this tutorial, we will take a closer look at network hardware and software.

Our discussion will break down as follows:

1. Network Hardware

A computer network can be either wired or wireless. A **wired network** is one that uses physical cables and connection boxes to connect devices to the network. **Ethernet** is the standard interface for all wired networks. A **wireless network** uses radio frequency signals to transmit data. Each device on a wireless network is required to have its own antenna to receive signals. **Wireless Fidelity (Wi-Fi)** is the standard interface technology for wireless networks.

Every device on a computer network is required to have a **network adapter**. The network adapter translates instructions from the operating system into information that can be transmitted over the network. It also manages the incoming and outgoing network request. A network adapter can be either wired or wireless. It is either built onto the computer's motherboard or connected as a peripheral device, such as a USB connected device.

A network must have a point at which all devices can connect. On a wired network, a switch or router functions in this capacity. A switch is a network connection box that manages traffic on devices that are plugged into it. A **router** is a switch that is able to route local network requests out to other networks, such as the Internet. On a wireless network, the point at which all devices can connect is called a **wireless access point (WAP)**. Sometimes there are situations in which two or more LANs, or devices on a LAN, have to be connected. In this situation, a network bridge is required. A bridge is a device that gives two or more LAN networks the ability to connect to one another without the use of protocol. By avoiding the use of protocol, a bridge can pass information between networks and devices on a LAN network without the need to route the information.

Listed below are common network hardware and the function of each.

Network Hardware	Function
Network Adapter	Translates instructions from the operating system into data that can be sent over a network

Switch	A network connection box that all the cables for the computers on a network connect to
Router	An upper tier switch that can connect and route network local network traffic as well as traffic from outside networks such as the Internet
Wireless Access Point (WAP)	A wireless network connection box that enables computers on a network to connect wirelessly
Ethernet	The standard interface for all wired networks
Wireless Fidelity (Wi-Fi)	Standard interface technology for wireless networks
Bridge	A network device that connects two networks together



Learn more about the common network hardware below.



Wired Network

Network that uses physical cables and connection boxes to connect devices.

Ethernet

The standard interface for all wired networks.

Wireless Network

Network that uses radio frequency signals to transmit data.

Wireless Fidelity (Wi-Fi)

The standard interface technology for wireless networks.

Network Adapter

Translates instructions from the operating system into data that can be sent over a network.

Router

An upper tier switch that can connect and route network local network traffic, as well as traffic from outside networks such as the Internet.

Wireless Access Point (WAP)

Wireless network connection box that enables computers on a network to connect wirelessly.

2. Network Software

On a broad level, network software refers to software used to manage and monitor computer networks. Network administrators use network software to facilitate communication between computers, and to give access to shared files and programs to the computers in the network. Recall that computers and devices on a network use various protocols to facilitate communication between them. The most common protocol utilized today is the Transmission Control Protocol/Internet Protocol (TCP/IP). This is a type of networking software, because it provides a way for various computers to communicate with one another, specifically via the Internet.

Other types of network software allow computers within the network to share files, applications, or programs. Network software is not the same as software applications, such as a computer’s operating system or word processing and spreadsheet software. Rather, network software is a “behind the scenes” set of software that allows network administrators to understand how the computer network functions. Network software also provides administrators with tools to control and manage how the computers in the network are connected.

Like many aspects of computer technology, the architecture of networks is changing and evolving.**Software-defined networking (SDN)** makes it easier to innovate and adapt the network to quickly meeting changing network demands. (Some more general information here about how SDN achieves these goals (agile and flexible to meet changing demands)).

The basic functionality of network software includes:

Network Software Provides	Description of Function
User Management	Enables administrators to add or remove users from the network
File Management	Allows administrators to define the location of data storage and user access to that data

 TERM TO KNOW

Software-Defined Networking (SDN)

Computer networking concept that separates the software from the hardware, making it easier to innovate and adapt the network to quickly meet changing network demands.

 SUMMARY

Computer networks play a critical role in the overall functionality of today’s computer. Users expect to have access to information on demand and computer networks aid in the routing and delivery of information to computer users. In this tutorial, we discussed the **hardware** components of a computer **network** and how these components rely on **network software** to ensure that the computer network will function appropriately.

Source: Derived from Chapter 5 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.
[https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Text book.html](https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Text%20book.html)

 TERMS TO KNOW

Ethernet

The standard interface for all wired networks.

Network Adapter

Translates instructions from the operating system into data that can be sent over a network.

Network Software Application

Software used to manage and monitor networks of all sizes; helps administrators deploy, manage and monitor a network.

Router

An upper tier switch that can connect and route network local network traffic as well as traffic from outside networks such as the Internet.

Software-Defined Networking (SDN)

Computer networking concept that separates the software from the hardware, making it easier to innovate and adapt the network to quickly meet changing network demands.

Wired Network

Network that uses physical cables and connection boxes to connect devices.

Wireless Access Point (WAP)

Wireless network connection box that enables computers on a network to connect wirelessly.

Wireless Fidelity (Wi-Fi)

The standard interface technology for wireless networks.

Wireless Network

Network that uses radio frequency signals to transmit data.

Computer Network Types

by Sophia



WHAT'S COVERED

Computer networks provide users, businesses, and organizations with the ability to share information and resources such as hardware and software. When resources such as these are shared, users are able to increase their capabilities by multiplying and adding capacity. Because computers are deployed in many different situations, various types of computer networks have been developed. These networks have been developed in order to satisfy the needs of computer users who require a network, depending on the situation the user and computer are in. In this tutorial, we will discuss the various types of networks and the situations in which each network type is most appropriate.

Our discussion will break down as follows:

1. Types of Computer Networks

Computers are able to be networked with other computers in the same office building, neighborhood, or with computers in other countries. One way to describe a computer network is based on the physical proximity of the network's devices in relation to each other. A **local area network or LAN** is a network in which the devices connected are located in a relatively small local area, such as a residential home. A subcategory of LAN is a personal area network (PAN). A **personal area network (PAN)** describes a small network in which personal devices such as a cell phone and a tablet PC are sharing data in a very close range (i.e. the same room). Listed below are the common types of computer networks.



TERMS TO KNOW

Personal Area Network (PAN)

A smaller local network in which personal devices are in close range with one another.

Local Area Network (LAN)

Computer network that links computers within a building.

Metropolitan Area Network (MAN)

A network within a large confined area such as a college campus, or company within an urban or suburban area.

Wide Area Network (WAN)

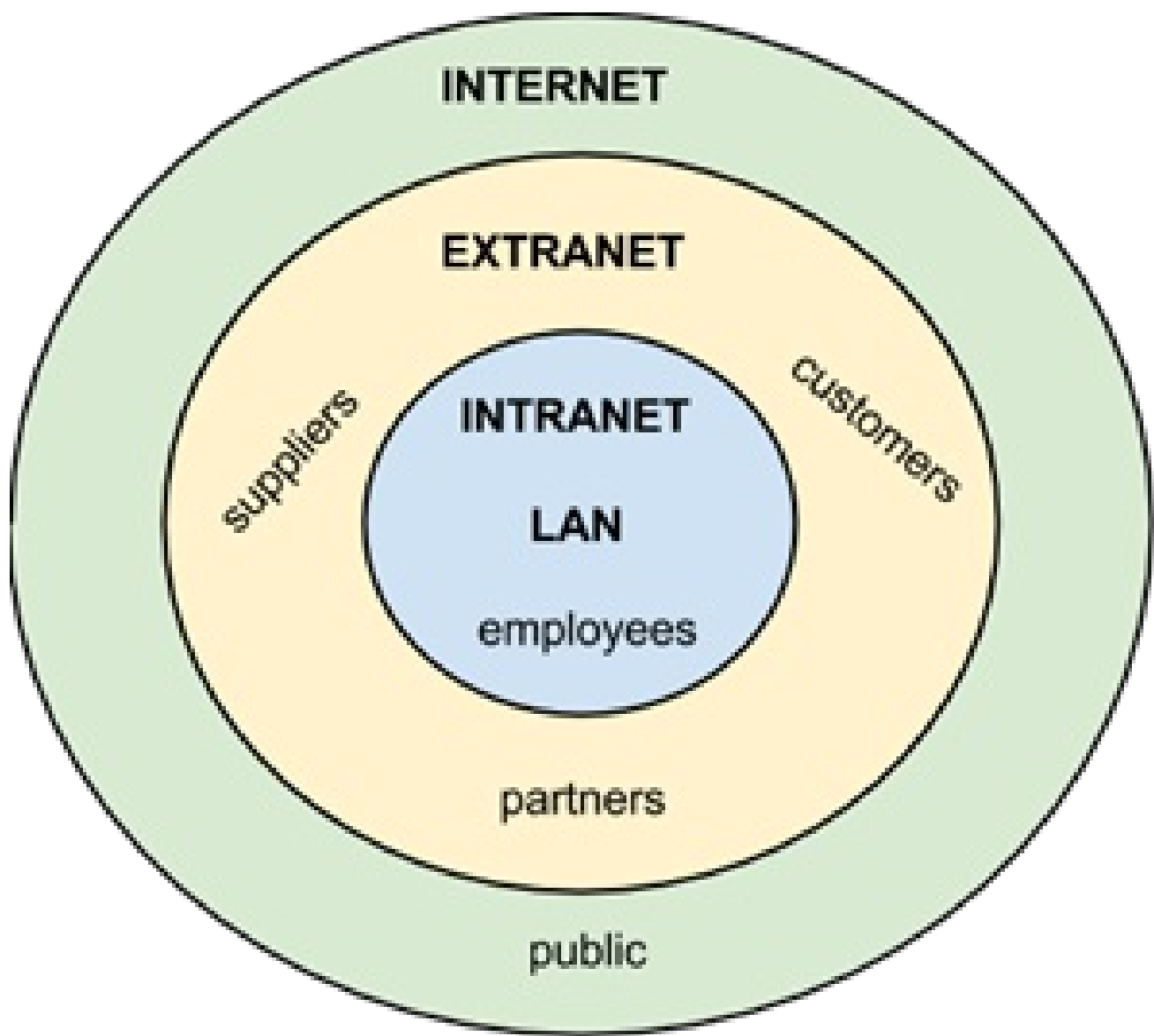
A computer network with all of the equipment spread over a large geographic; is typically inclusive of many small networks or LANs.

2. Internet, Intranet, and Extranet

As information technology has advanced, people have been afforded the ability to access information in a variety of ways at virtually any time needed. The modes by which people can access and share information has also diversified. One of the main ways in which people access information today is via the **Internet**. The Internet is a global network of smaller networks connecting devices using Transmission Control Protocol/Internet Protocol (TCP/IP). Recall that TCP/IP is what governs transmission on the Internet and on most Windows networks.

However, just as organizations set up websites to provide global access to information about their business, they also set up internal web pages to provide information about the organization to the employees. This internal set of web pages is called an **intranet**. An intranet is a private network that can only be accessed by users with special permission. It is typically set up in a private company or organization. Web pages on the intranet are not accessible to those outside the company; in fact, those pages would come up as “not found” if an employee tried to access them from outside the company’s network.

Sometimes an organization wants to be able to collaborate with its customers or suppliers while at the same time maintaining the security of being inside its own network. In cases like this, a company may want to create an **extranet**. An extranet is a LAN that can be accessed by users with special access rights outside of a business or organization. The extranet, which is a part of the company’s network, can be made available securely to those outside of the company. Extranets can be used to allow customers to log in and check the status of their orders, or for suppliers to check their customers’ inventory levels.



Scope of computer networks for business



TERM TO KNOW

Internet

Global network of smaller networks linking devices through TCP/IP.

Intranet

Private network that can only be accessed by users with special permission and is typically set up in a private company or organization.

Extranet

A LAN that can be accessed by users with special access rights outside of a business or organization.

3. Wireless Networking

Today we are used to being able to access the Internet wherever we go. Our smartphones can access the Internet; even Starbucks provides wireless “hotspots” for our laptops or iPads. These wireless technologies

have made Internet access more convenient, and they have made devices such as tablets and laptops much more functional. Let's examine a few of these wireless technologies.

- **Wi-Fi:** **Wi-Fi, short for wireless-fidelity**, is a technology that takes an Internet signal and converts it into radio waves. These radio waves can be picked up within a radius of approximately 65 feet by devices with a wireless adapter. One of the primary places where Wi-Fi is being used is in the home. Home users are purchasing Wi-Fi routers, connecting them to their broadband connections, and then connecting multiple devices via Wi-Fi. Wi-Fi can be used to set up a PAN or LAN.
- **Mobile Network:** As the cellphone has evolved into the smartphone, the desire for Internet access on these devices has led to data networks being included as part of the mobile phone network. While Internet connections were technically available earlier, it was really with the release of the 3G networks in 2001 (2002 in the US) that smartphones and other cellular devices could access data from the Internet. This new capability drove the market for new and more powerful smartphones, such as the iPhone, introduced in 2007. In 2011, wireless carriers began offering 4G data speeds, giving the cellular networks the same speeds that customers were used to getting via their home connection.
- **Bluetooth:** Although **Bluetooth** is not generally used to connect a device to the Internet, it is an important wireless technology that has enabled many functionalities that are used every day. When created it was intended to replace wired connections between devices. Today, it is the standard method for connecting nearby devices wirelessly. Bluetooth has a range of approximately 300 feet and consumes very little power. Some applications of Bluetooth include: connecting a printer to a personal computer, connecting a mobile phone and headset, connecting a wireless keyboard and mouse to a computer, and connecting a remote for a presentation made on a personal computer.
- **Near Field Communication:** **Near-field communication (NFC)** is a set of communication protocols that enables two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within four centimeters (1.6 inches) of each other. NFC devices are used in contactless payment systems, similar to those used in credit cards and electronic ticket smart cards. These devices allow mobile payment to replace/supplement these systems. NFC is used for social networking, and for sharing contacts, photos, videos or files. NFC-enabled devices can act as electronic-identity documents and key cards. NFC offers a low-speed connection with a simple setup that can be used to bootstrap more capable wireless connections.



TERMS TO KNOW

Wireless Fidelity (Wi-Fi)

The standard interface technology for wireless networks.

Near-Field Communication (NFC)

Set communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone.

Bluetooth

Transmission standard that provides the protocol for mobile devices, computers, or smartphones to connect in order to communicate.

4. Appropriate Network Use Cases

Computer networks have made information readily available to users with devices that can connect to them.

As a computer user, you may find that, while your computer is able to connect to a network, the network you are connected to will enable you to share or access resources (information, hardware, software, etc.) depending on the type of network you are connected to. Below is a table listing the various types of computer networks and some example scenarios of how they can be used.

Network Type	Typical Use	Example Scenario
Personal Area Network (PAN)	Sharing data between personal devices in close range, such as a tablet PC and mobile phone, gaming console and a tablet PC, etc.	In a coffee shop with no wireless network, users can utilize their mobile phone network to provide Internet service to a computer or tablet
Local Area Network (LAN)	Sharing data between network devices in a small local area such as an entire home or group of homes	In a company office, users can connect to a company-owned LAN to share data and hardware such as a network printer, or to access company email messages
Metropolitan Area Network (MAN)	Sharing data and resources in a large but confined area, such as a college campus or large company	In a hotel, guests may connect to the hotel's network while at the hotel, or across the street at a restaurant close to the hotel
Wide Area Network (WAN)	Sharing data and resources over a very large geographic area, such as across states and countries	You need to access email; you need to share a file with your friend in another country; the Internet



SUMMARY

Computer networks are a valuable tool, used by people within business situations and outside of business situations, to share information and resources. There are multiple types of computer networks each with their own advantages for users, depending on the situation the user is in. Knowing what the various network types—**internet**, **intranet**, and **extranet**—are and how they work will only enhance your experience while **using a networked computer**.

Source: Derived from Chapter 5 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

Bluetooth

Transmission standard that provides the protocol for mobile devices, computers, or smartphones to connect to communicate.

Extranet

A LAN that can be accessed by users with special access rights outside of a businesses or organization.

Internet

Global network of smaller networks linking devices through TCP/IP.

Intranet

Private network that can only be accessed by users with special permission and is typically set up in a private company or organization.

Local Area Network (LAN)

Computer network that links computers within a building.

Metropolitan Area Network (MAN)

A network within a large confined area such as a college campus, or company within in urban or suburban area.

Near-Field Communication (NFC)

Set communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone.

Personal Area Network (PAN)

A smaller local network in which personal devices are in close range with one another.

Wide Area Network (WAN)

A computer network with all of the equipment spread over a large geographic and is typically inclusive of many small networks or LANs.

Wireless Fidelity (Wi-Fi)

The standard interface technology for wireless networks.

Network Security and Cybersecurity

by Sophia



WHAT'S COVERED

When a computer is connected to a network, a user is afforded the ability to share files, folders, software applications, and hardware such as a printer. However, a computer is also susceptible to attack that can ultimately lead to information theft, data loss, invasion of privacy, virus infection, and service denial, among other things. Because of these threats, it is critical that information is shared carefully and selectively. In this tutorial, we will discuss network security, and how to protect a computer and data from attack.

Our discussion will break down as follows:

1. Information Security Triad

The information security triad refers to three pillars of a secure network: confidentiality, integrity, and availability. This is also sometimes referred to as CIA, although it must not be confused with the governmental bureau with the same acronym.



The security triad

- **Confidentiality:** When protecting information, we want to be able to restrict access to those who are allowed to see it; everyone else should be disallowed from learning anything about its contents. This is the essence of confidentiality. For example, federal law requires that universities restrict access to private student information. The university must be sure that only those who are authorized have access to view the grade records.
- **Integrity:** Integrity is the assurance that the information being accessed has not been altered and truly represents what is intended. Just as a person with integrity means what he or she says and can be trusted to consistently represent the truth, information integrity means information truly represents its intended meaning. Information can lose its integrity through malicious intent, such as when someone who is not authorized makes a change to intentionally misrepresent something. An example of this would be when a hacker is hired to go into the university's system and change a grade. Integrity can also be lost unintentionally, such as when a computer power surge corrupts a file, or someone authorized to make a change accidentally deletes a file or enters incorrect information.
- **Availability:** Information availability is the third part of the CIA triad. Availability means that information can be accessed and modified by anyone authorized to do so in an appropriate timeframe. Depending on the type of information, appropriate timeframe can mean different things. For example, a stock trader needs information to be available immediately, while a salesperson may be happy to get that day's sales numbers in a report the next morning. Companies such as Amazon.com will require their servers to be

available twenty-four hours a day, seven days a week. Other companies may not suffer if their web servers are down for a few minutes once in a while.

2. Access Control

Access control describes the technology and techniques that can be used to control who has access to a computer system. Access control can be implemented in a number of ways, such as physical security (locking the door to a computer lab) or user authentication. User authentication refers to the ways in which a person's identity is verified by a computer system. The most common form of user authentication is through the use of a user ID and password login system.

- **User ID and Password:** User IDs and passwords are the most popular method of access control. A user ID and password combination is required to log in to systems with this type of access control. Windows, websites, and many other systems relying on computers utilize this method. A user chooses a user ID and password, and this information is encrypted and stored on the computer. Access remains local to the computer in which the user ID and password information are stored. The main security risk is that someone or something (i.e. malware) could break the encryption code on the file where the passwords are stored, and then could gain access to the system.
- **Smart Cards:** Another way to provide access control is through the use of **smart cards**. A smart card is a plastic card that contains a microchip that a card reader can scan to verify a person's identity. Smart cards are often used as student ID cards and employee badges, thereby giving access to restricted areas or hardware to people with the proper credentials. Smart cards can also be used to restrict access to computers. Smart cards are typically used as a way to replace the user ID and password combination. The main security risk here is an unauthorized person obtaining access to the card.
- **Biometric Readers:** A **biometric reader** identifies users by scanning for one or more physical traits. Some examples of biometric devices are for fingerprint recognition, facial recognition, voice recognition, and retina scanning. Many law enforcement and government agencies utilize this form of access control, as this is one of the most secure access control methods, due to the uniqueness of the metrics required to obtain access. For example, for over 100 years, police departments have used fingerprint scanners and no two prints have ever been found to be identical.
- **2-Factor Authentication:** For more advanced security, additional authentication may be required along with user IDs and passwords. A user may log in with the traditional information, but then may be required to authenticate with a special one-time code provided through text, email, or an authentication app. These types of additional authentications build in another layer of security when a password may have been compromised. If the user is not able to provide the special code, they are not permitted access to the account and cannot steal valuable information.



TERMS TO KNOW

Access Control

The technology and techniques that can be used to control who has access to a computer system.

Smart Card

Plastic card that contains a microchip that a card reader can scan to verify a person's identity.

Biometric Reader

Identifies users by scanning for one or more physical traits.

3. Wireless Network Security

Wireless networks are a great security risk, due to the fact that there is no physical security. The only way access to a wireless network can be obtained is through connecting to the router or switch. Additionally, anyone within close proximity to a wireless router can access the network if proper security measures haven't been taken. To limit access to a wireless network, administrators can set up encryption on the router, so that users must type an encryption key to connect to the network. The following table lists the wireless encryption types.

Encryption Type	Description
Wired Equivalent Privacy (WEP)	Controls wireless router using 128 bit or 256 bit key
Wi-Fi Protected Access (WPA)	Improves upon WEP; allows for encrypting larger networks
Wi-Fi Protected Access 2 (WPA2)	New version of WPA



TERMS TO KNOW

Wired Equivalent Privacy (WEP)

Commonly used method of network encryption; controlled by entering in a 128 bit or 256 bit key.

Wi-Fi Protected Access (WPA)

Method of wireless encryption that offers capabilities for a large wireless network.

4. Common Network Attacks (Malware)

All operating systems and applications have vulnerabilities that can be exploited. When criminals use a vulnerability to attack a system, the attack is called an **exploit**. To protect against exploits, Windows, Mac OS, and Linux have ways to update their operating systems when people become aware of ways in which to attack. The term used to describe malicious software used to launch attacks on a computer system is **malware**. Listed below are the common types of malware.

- **Virus:** A **virus** is a computer code that inserts itself into an executable file. When the infected executable file is run, the virus's code executes along with the application's code. Viruses are programmed to hide inside of a host file so that it is not obvious to the operating system or user that a virus is there. Once executed, a virus's code can cause pop-up windows to continually appear, files to be corrupted, files to be deleted, and a host of other system issues. Virus's code can also be copied into RAM and from there it can attach itself to other executable files. A virus can be detected and removed by utilizing **anti-virus software**.
- **Trojan Horse:** A **Trojan horse** is an application that appears to do something useful while secretly causing damage to your computer system. Although a Trojan horse can be detected and removed with anti-virus software, it is not a virus because Trojan horses do not hide inside of executable files. Typically, this form of malware seeks to install software designed to compromise privacy. For example, a common Trojan horse is a **keystroke logger**. A keystroke logger records keystrokes in a file and sends the file to the author of the program. The creator of the logger can then open the file and access user IDs and passwords.

- **Worms:** A **worm** is an application that carries harmful programs, such as a Trojan horse or virus. Worms can be either active or passive. An active worm can transport itself, while a passive worm relies on a user to move it from one location to another. This is often accomplished by fooling users into opening email attachments and/or forwarding emails containing the worm to other users. Anti-virus software can be used to detect and destroy worms.
- **Adware:** **Adware** is software that displays advertisements on a user's computer without the user's permission or prompting. People who write adware make money based on how many times an advertisement is clicked. Many types of adware come in the form of an add-on toolbar for your web browser. Adware can be difficult to remove once installed on your computer. Anti-virus software can be of some help; however, in most cases, you will need to research to find the solution for removing adware.
- **Spyware:** **Spyware** is software that makes recordings of your computer's usage without your knowledge or consent. Spyware creators are paid for collecting information about people for marketing purposes. Keystroke loggers are an example of spyware. Most spyware is very difficult to remove once installed on your computer. Anti-virus software will remove some spyware but in most cases, special **anti-spyware software** has to be used. Anti-spyware software is software that defends against spyware and adware.



TERMS TO KNOW

Exploit

An attack that uses a vulnerability to harm a system.

Malware

Malicious software used to launch attacks on a computer system.

Virus

Computer code that inserts itself into an executable file.

Anti-Virus Software

Software that defends against malware (viruses, worms, and Trojan horses).

Trojan Horse

An application that appears to do something useful while secretly causing damage to your computer system.

Worm

An application that carries harmful programs such as a Trojan horse or virus.

Keystroke Logger

Records keystrokes in a file and sends the file to the author of the program.

Anti-Spyware Software

Software that defends against spyware and adware.

5. Malware Defense

Recall that there are quite a few types of malware all designed to cause your computer system harm, spy on your activities, or to obtain data without your knowledge. There are two types of software that are designed to protect your system against malware attacks: anti-virus software and anti-spyware software.

- **Anti-Virus Software:** Anti-virus software is software designed to defend against malware. The software

works by opening a file, scanning the code, and looking for a virus. Anti-virus software also scans executable files to locate viral content. Typically, anti-virus software maintains a large database of known viruses.

- **Anti-Spyware Software:** Anti-spyware software is software designed to defend against spyware and malware. These packages look for known spyware and/or adware, so that they can remove them.

6. Cybersecurity

Cybersecurity is similar to network security but is focused on protecting organizational and user data from unauthorized users and mitigating potential attacks across all devices regardless of being on a specific computer network or not. Cybersecurity teams deal with the softwares and attacks mentioned above, identify potential threats and points of vulnerability in systems, and build in security measures to identify, mitigate, and resolve these types of attacks.

There is an influx of newer forms of attacks to target organizations and their users in attempts to steal information.

- **Phishing/Smishing:** Phishing is a digital practice of sending an email or text (SMS, hence Smishing) to trick users into revealing sensitive information such as passwords, social security numbers, and security questions. These digital communications can involve hackers pretending to be someone they aren't, organizations or its members, to gain trust and this sensitive information. Communications may suggest a reward or consequence for not urgently following up
- **Whale and Spear Phishing:** A type of phishing, these attacks involve scammers targeting and impersonating executive leaders to steal sensitive information.

6a. Trends in Cybersecurity

As more of the world joins the digital space, more data is at risk of being stolen by attackers. Cybersecurity and other specialists have and continue to develop and produce technologies and tools to protect their data and improve user knowledge of potential attacks. Some of these tools and measures include:

- **Blockchain:** Blockchain is an advanced form of a database technology and is commonly associated with cryptocurrency. In this type of data keeping, a large group of data is stored in a block and added to a digital chain and timestamped. The chain works across computers and networks, and every time a new block of data is added, it is added to the end of the chain. It's nearly impossible to alter data on blockchain without extensive money and resources, making it a growing trend for research and cybersecurity measures.
- **Artificial Intelligence Monitoring:** Artificial intelligence (AI) is being used to monitor global trends and vulnerabilities. AI gives cybersecurity insight for prioritization of security measures and preventative solutions.
- **User Training and Education:** As more organizations have users across time zones, locations, devices, and networks, training and education has been a critical component for onboarding and yearly training requirements. Informed users help reduce the risk of cybercrimes.



SUMMARY

In this tutorial, we took a look at **network security** and some of the common issues associated with **securing a computer network**. **Malware** refers to malicious software including viruses, spyware, Trojan horses, and worms that seek to exploit your computer system. Installing **anti-virus** or **anti-spyware software** helps to defend against attacks on your system.

Source: Derived from Chapter 6 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

Access Control

The technology and techniques that can be used to control who has access to a computer system.

Anti-Spyware Software

Software that defends against spyware and adware.

Anti-Virus Software

Software that defends against malware (viruses, worms, and trojan horses).

Biometric Reader

Identifies users by scanning for one or more physical traits.

Exploit

An attack that uses a vulnerability to harm a system.

Keystroke Logger

Records keystrokes in a file and sends the file to the author of the program.

Malware

Malicious software used to launch attacks on a computer system.

Smart Card

Plastic card that contains a microchip that a card reader can scan to verify a person's identity.

Trojan Horse

An application that appears to do something useful while secretly causing damage to your computer system.

Virus

Computer code that inserts itself into an executable file.

Wi-Fi Protected Access (WPA)

Method of wireless encryption that offers capabilities for a large wireless network.

Wired Equivalent Privacy (WEP)

Commonly used method of network encryption; controlled by entering in a 128 bit or 256 bit key.

Worm

An application that carries harmful programs such as a trojan horse or virus.

The World Wide Web

by Sophia



WHAT'S COVERED

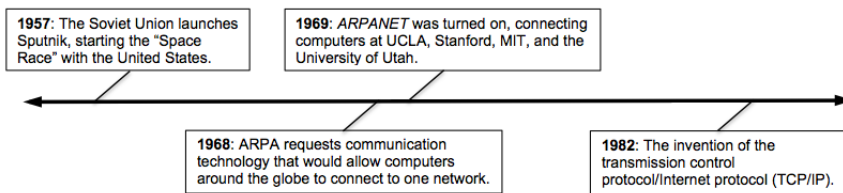
Computer networking really began in the 1960s with the birth of the Internet. However, in the 1990s, when the Internet came of age, Internet technologies began to pervade all areas of personal and organizational life. Now, with the Internet a global phenomenon, it would be unthinkable to have a computer that did not include the ability to access the Internet. In this tutorial, we will discuss the Internet, its history, and how the Internet differs from the World Wide Web.

Our discussion will break down as follows:

1. History of the Internet

The story of the Internet can be traced back to the late 1950s. The United States was in the depths of the Cold War with the former Soviet Union (USSR), and each nation closely watched the other to determine which one would gain a military or intelligence advantage. In 1957, the Soviets surprised the United States with the launch of Sputnik, propelling us into the space age. In response to Sputnik, the U.S. Government created the Advanced Research Projects Agency (ARPA), whose initial role was to ensure that the United States was not surprised again. The Internet sprang from the ARPA, now called DARPA (Defense Advanced Research Projects Agency).

ARPA was the center of computing research in the 1960s, but there was just one problem: many of the computers could not talk to each other. In 1968, ARPA sent out a request for proposals for a communication technology that would allow different computers located around the country to be integrated together into one network. Twelve companies responded to the request, and a company named Bolt, Beranek, and Newman (BBN) won the contract. They began work right away, and were able to complete the job just one year later. In September 1969, the ARPANET was turned on. The first four nodes were at UCLA, Stanford, MIT, and the University of Utah. Over the next decade, the ARPANET grew and gained popularity. During this time, other networks also came into existence. Different organizations were connected to different networks. This led to a problem: the networks couldn't talk to each other. Each network used its own proprietary language, or protocol, to send information back and forth. This problem was solved by the invention of Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP was designed to allow networks running on different protocols to have an intermediary protocol that would allow them to communicate. So as long as your network supported TCP/IP, you could communicate with all of the other networks running TCP/IP. TCP/IP quickly became the standard protocol and allowed networks to communicate with each other. From this breakthrough came the term **Internet**, which simply means "an interconnected network of networks."



A timeline of events that motivated the invention of the internet



TERM TO KNOW

Internet

Global network of smaller networks linking devices through TCP/IP.

2. The Internet

At its core, the Internet is a global wide area network (WAN) comprised of smaller networks owned by businesses, educational institutions, individuals, and governments all working together under a common protocol (TCP/IP). The Internet enables people to communicate and share information within the same home, business, and school, or across the globe.

The benefits of the Internet are tremendous for businesses, governments, and individuals. For example, students can use the Internet to take courses online, communicate with instructors, or research topics for reports. Employees and businesses can use the Internet to advertise products and services for sale, provide benefits information to employees, or to educate potential buyers. Government institutions can use the Internet to collect taxes, provide forms and manuals, and inform the public about new laws.

The Internet's primary protocol is TCP/IP. Under TCP/IP, each computer is identified by an **Internet Protocol (IP) address**, which is a numeric address that provides an ID for a computer on a network. A domain name is a string of text that uniquely identifies a company or server on the Internet. For example, if you want to visit Apple's website, instead of typing the IP address for it into your web browser, you would type `www.apple.com`. **Domain Name Service (DNS)** servers convert the request between IP addresses and domain names. This process is called **resolving** an IP address and happens almost instantaneously.



TERMS TO KNOW

IP Address

Short for Internet Protocol address; numeric address that provides an ID number for a computer on a network.

Domain Name Service (DNS)

Converts the request between IP addresses and domain names.

Resolve

The process of converting a domain name to an IP address.

3. The World Wide Web

On a fairly regular basis, people use the term **“World Wide Web”** to describe the Internet. However, the World Wide Web is only a part of the Internet. In essence, the World Wide Web is an interconnected network of documents written in Hypertext Markup Language (HTML) that can be accessed through the Hypertext Transfer Protocol (HTTP). Information on the World Wide Web is contained in web pages. A **web page** is a document written in HTML format that contains content prepared for the web. A **website** is a group of interconnected webpages with a system for navigation through all of the pages. The navigation scheme uses **hyperlinks** to connect to other pages within the site. A hyperlink is a link to a web page or other type of content.



TERMS TO KNOW

World Wide Web

An interconnected network of documents written in Hypertext Markup Language (HTML) that can be accessed through the Hypertext Transfer Protocol (HTTP).

Web Page

Document written in HTML format that contains content prepared for the web.

Website

A group of interconnected web pages with a system for navigation through all of the pages.

Hyperlinks

Link to a web page or other type of content.

4. Web 2.0

In the first few years of the World Wide Web, creating and putting up a website required a specific set of knowledge: you had to know how to set up a server on the World Wide Web, how to get a domain name, how to write web pages in HTML, and how to troubleshoot various technical issues as they came up. Someone who did these jobs for a website became known as a webmaster. As the web gained in popularity, it became more and more apparent that those who did not have the skills to be a webmaster still wanted to create online content and have their own piece of the web. This need was met with new technologies that provided a website framework for those who wanted to put content online.

➞ **EXAMPLE** Blogger and Wikipedia are examples of these early Web 2.0 applications. They provided anyone who had something to say a place to say it, without the need for understanding HTML or web-server technology.



DID YOU KNOW

Starting in the early 2000s, Web 2.0 applications began a second bubble of optimism and investment. It seemed that everyone wanted his or her own blog or photo-sharing site. Here are some of the companies that came of age during this time: MySpace (2003), Photobucket (2003), Flickr (2004), Facebook (2004), WordPress (2005), Tumblr (2006), and Twitter (2006). The ultimate indication that Web 2.0 had taken hold was when Time magazine named “You” its “Person of the Year” in 2006.



WATCH

This video introduces a digital platform that connects women who are returning to the workforce with employers.



SUMMARY

In this tutorial, we took a deeper look at what the Internet is and how the **World Wide Web** fits into the overall scope of the Internet. The **development of the Internet** and World Wide Web, combined with wireless access, has made information available at our fingertips. The **Web 2.0** revolution has made us all authors of web content. As networking technology has matured, the use of Internet technologies has become a standard for every type of organization. The use of intranets and extranets has allowed organizations to deploy functionality to employees and business partners alike, increasing efficiencies and improving communications.

Source: Derived from Chapter 5 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

Domain Name Service (DNS)

Converts the request between IP addresses and domain names.

Hyperlinks

Link to a webpage or other type of content.

IP Address

Short for internet protocol address; numeric address that provides an ID number for a computer on a network.

Internet

Global network of smaller networks linking devices through TCP/IP.

Resolve

The process of converting a domain name to an IP address.

Web Page

Document written in HTML format that contains content prepared for the web.

Website

A group of interconnected webpages with a system for navigation through all of the pages.

World Wide Web

An interconnected network of documents written in Hypertext Markup Language (HTML) that can be accessed through the Hypertext Transfer Protocol (HTTP).

Website Development

by Sophia



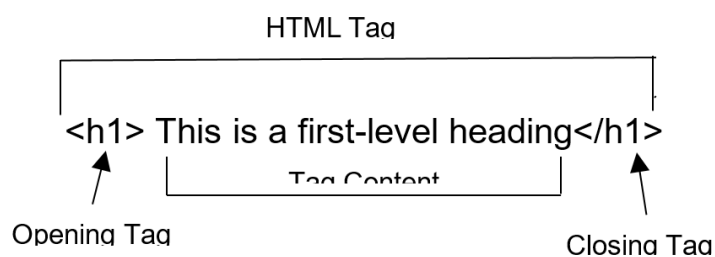
WHAT'S COVERED

The World Wide Web (commonly referred to as the Web) is one of the most popular parts of the Internet. In the early days of the World Wide Web, the creation of a website required knowing how to use Hypertext Markup Language (HTML). Today, most websites are built with a variety of tools, but the final product that is transmitted to a browser is still HTML. In this tutorial, we will discuss the significance of HTML as the main way in which information is communicated via the Web.

Our discussion will break down as follows:

1. What is HTML?

Recall that information on the World Wide Web is contained in web pages, and that a web page is a document written in **Hypertext Markup Language (HTML)** format that contains content prepared for the web. For the most part, the Web is merely a network of documents written in HTML and supported by a network protocol called **Hypertext Transfer Protocol (HTTP)**. At its simplest, HTML is a text language that allows you to define the different components of a web page. The markup part of the name refers to how the HTML defines blocks of text to receive formatting instructions. These definitions are handled through the use of **HTML tags**. An HTML tag is an HTML markup code enclosed in angle brackets `<>` (greater than, less than symbols), that alters how content is formatted, or it does something such as link to another page. For example, an HTML tag can tell the browser to show a word in italics, to link to another web page, or to insert an image. HTML forms the basic programming language of websites. Listed below is the structural breakdown of an HTML tag.



HTML tag

In the above example, the opening tag, `<h1>`, signals the web browser that the tag content is to be treated as a heading, and should display on screen as a heading utilizing an increased font and bold. The closing tag, `</h1>` signals to the web browser the end of the text that will be treated by the `<h1>`.



HINT

An HTML tag must begin with an opening tag and a closing tag. Failure to properly open < or close > a tag can result in no action being performed on the tag's content, or improper display of the tag's content. Additionally, failure to close an HTML tag may also prevent any subsequent tags from being opened, thereby leading to an error or crash of the website.

In the example below, some text is being defined as a heading, while other text is being emphasized:

```
<h1>This is a first-level heading</h1>  
Here is some text. <em>Here is some emphasized text.</em>  
<h2>Here is a second-level heading</h2>  
Here is some more text.
```

Simple HTML

The HTML contained in the picture outputs the following when viewed in a web browser:

This is a first-level heading

Here is some text. *Here is some emphasized text.*

Here is a second-level heading

Here is some more text.

HTML in web browser



Following the steps to create a web page using notepad:

1. Open Notepad
2. In Notepad type the following:

```
<!DOCTYPE HTML>
```

```
<html>
```

```
<head>
```

```
<title> My first web page </title>
```

```
</head>
```

```
<body>
<h1> I am learning computer science </h1>
<p> This page is in progress </p>
</body>
</html>
```

3. Click on File in the menu bar and then select Save
4. In the Save As dialog, type in MyFirstPage.htm
5. Click Save
6. Open Windows Explorer and navigate to the file you just created and double click it. You should see this file open in your web browser.



TERMS TO KNOW

Hypertext Markup Language (HTML)

Programming language used to create websites.

Hypertext Transfer Protocol (HTTP)

Networking protocol used to distribute websites.

HTML Tag

HTML markup code enclosed in < > brackets; used to define how content is displayed on screen.

2. Web Addresses

A requirement of publishing Web content via a website is that the site must have a unique address. This unique address is called a **Uniform Resource Locator (URL)**. Typically, an URL begins with the text “www.” followed by the domain name of the site. The “www” indicates to the web browser that the URL is referencing a web server as opposed to some other type of server such as an email server. Consider the URL, <http://www.sophia.org> The http:// indicates that the HTTP protocol should be used to retrieve the page. When a web browser sends out a request to retrieve a web page, the request goes to a domain name server (DNS), which translates the domain name into the IP address. The server sends the requested page back to the web browser and the browser displays the requested page.



TERM TO KNOW

Uniform Resource Locator (URL)

Address of an Internet resource such as a website; must begin with a communication protocol such as HTTP.

3. Using HTML

The process of developing web pages, websites, or any web content can be complex, and may involve an entire group of web designers and programmers. Depending on the size and scope, a web development project may also involve several programming languages. There are, however, some instances in which a web development project may be as simple as one person using HTML to code a web page or website. If you know HTML, then one way to develop web content is to create it in a software application such as MS Word or Notepad. These applications give users the ability to save documents in a web-enabled format. Listed below are some common HTML tags:

Opening Tag	Closing Tag	Description
<html>	</html>	Opens and closes an HTML document
<head>	</head>	The <head>section is used to provide information about the document for use by search engines and browsers
<title>	</title>	The title of the document. This element is inside the <head> section.
<body>	</body>	The <body>section contains all the content of the web page
	none	Inserts an image into a web page. To insert an image hosted on another site, paste the image URL between the quotation marks.
<h1> to <h6>	</h1> to </h6>	Headings; H1 is the main heading, H2 is secondary, etc.
<p>	</p>	Paragraph
		A container for inline content, such as text inside a paragraph.
<div>	</div>	A container for a block of content
		Gives the contained text emphasis (usually as italics)
		Makes the contained text bold
		Creates a hyperlink of the text between the tags. Paste the URL of the webpage between the quotation marks.
		Creates an ordered (numbered) list of items. 1, 2, 3, etc.
		Creates an unordered (bulleted) list of items. Additional attributes can change the shape of the bullet.
		The list tag separates items in an ordered or unordered list. Use these tags to indicate a new entry to the list.



DID YOU KNOW

Most of the social networking websites such as Facebook and Twitter provide their users with HTML web pages (also called profiles or profile pages) that users can then add content to for friends and followers to view. The key to completely customizing your profile page is to know HTML and some of the common tags. Users who wish to change the navigation on a social network page can open the HTML for the page (if access is allowed by the social network) and locate the <nav>, </nav> tags and insert whatever information is needed in between the tags. The newly edited profile will be displayed immediately after changing the content within the tags.



SUMMARY

Hypertext Markup Language is the language in which web pages are created. **HTML** uses tags to define how content should be displayed on screen. Having some basic knowledge of HTML can help with developing simple **web pages** and with customizing a social networking profile page. In this tutorial, we covered HTML and the common tags used to develop web pages.

Source: Derived from Chapter 10 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

HTML Tag

HTML markup code enclosed in < > brackets; used to define how content is displayed on screen.

Hypertext Markup Language (HTML)

Programming language used to create websites.

Hypertext Transfer Protocol (HTTP)

Networking protocol used to distribute websites.

Uniform Resource Locator (URL)

Address of an internet resource such as a website; must begin with a communication protocol such as HTTP.

Protecting Minors from Online Dangers

by Sophia



WHAT'S COVERED

Individuals, businesses, and organizations all utilize the Internet, due to its value as a resource for sharing information, communicating, and many other things. Unfortunately, there are also risks associated with Internet usage, such as exposure to inappropriate content, privacy, and cyberbullying. These risks are only greater when the person using the Internet is a minor. Being aware of the risks of using the Internet can be very helpful in staying safe while online. In this tutorial, we will identify potential online dangers, and some procedures for keeping minors safe online.

Our discussion will break down as follows:

1. Online Dangers

There are many potential risks for minors when online. Often times while exploring a website or social media, children will be confronted with vulgar content, such as inappropriate language. Furthermore, the potential exists for children to be exposed to pornographic content. Listed below are some common online dangers.

Online Danger	Characteristics
Phishing	Scam in which a user is tricked into providing personal information. Usually involves an email, website, or online form that appears to be from a legitimate source (bank, government institution, etc.) soliciting a user for personal information.
Cyberbullying	Online bullying that takes place via social media, message boards, forums, and email. Cyberbullying usually refers to online bullying of children and teenagers, but anyone can be a victim. Those who would bully others face-to-face are likely to bully others online as well. However, due to the distance/lack of physical connection between a cyberbully and their victims, some people, who might not bully someone otherwise, are emboldened to bully others online.
Cyberstalking	Online harassment that usually involves the communication of threats online through social media, forums, email, and message boards. Cyberstalking is similar to cyberbullying, but the main difference is that cyberstalkers are unusually obsessed with their victims, and seek to collect any information about them.
Malware	Malicious software used to launch attacks on a computer system. Some attacks include malicious software that is designed to steal personal information from users; examples of malware include Trojan horses, worms, and viruses.
Inappropriate	Term used to describe posting text messages, videos, and photos that may be inappropriate

Content	for certain situations or age groups, i.e., children, professional situations.
Web Sites and Chat Rooms	<p>As websites are the primary vehicle through which information is delivered online, children must be shown how important it is to protect their personal information and the information of their family and friends. Many child-oriented websites solicit information from kids in surveys and forms in exchange for prizes, and get them to register online for fan clubs. In chat rooms, sharing their gender, age, and favorite hangout could seem harmless, but predators can easily use this information to locate and harass the child. Predators may even masquerade as children in order to gather information, and ultimately meet their unsuspecting victims. With websites and chatrooms, the potential does exist for kids to pretend to be older than they actually are, not thinking about the potential results of such actions.</p> <p>Chatrooms and online forums are typically where children get into online fights or become the target of bullying via email, chat, and instant messaging.</p>
Blogs and Social Networking	Blogs and social networking websites such as Facebook, Twitter, Instagram, SoundCloud, and YouTube are places where children sometimes share too much information — not only names and addresses, but also personal photos that sometimes show illegal acts, such as underage drinking. Minors should be instructed to share their blogs or online profiles with a parent or guardian so content can be filtered for appropriateness. You can also use Google, along with the search tools on social networking sites, to search for profiles your child may have posted. Use your child's full name, phone number, and other identifying information.
Peer to Peer (P2P) File Sharing Software	Peer-to-peer (P2P) file sharing invites new privacy problems. These types of programs allow people to browse and download files from Internet-connected personal computers of anyone else who uses the same program. This makes it easy for cybercriminals to spread viruses, Trojan horses, and spyware. Children can also accidentally download inappropriate content, such as pornography, that is labeled misleadingly.

2. COPPA and CIPA

As the popularity of PCs increased and the Internet evolved, the need to protect minors utilizing the Internet became increasingly evident. To do this, the U.S. government drafted legislation to address the access that children would have to inappropriate content, as well as legislation to address websites that collect information from children.

- **CIPA:** The **Children's Internet Protection Act (CIPA)** requires that public schools and organizations receiving Internet service at a discounted rate (through the federal E-rate program) provide an Internet safety policy that contains information as to how minors will be protected online. Specifically, CIPA requires that any obscene or pornographic pictures be blocked or filtered, thereby restricting a minor's access to harmful content. CIPA also requires that entities subject to CIPA have a hearing or forum to notify the public of its Internet safety policy.
- **COPPA:** Websites that are collecting information from children under the age of 13 are required to comply with the **Children's Online Privacy Protection Act (COPPA)**, which is enforced by the Federal Trade Commission (FTC). To comply with COPPA, organizations must make a good-faith effort to determine the age of those accessing their websites. If users are under 13 years old, organizations must obtain parental consent before collecting any information.

**CIPA**

Short for Children's Internet Protection Act; requires public schools and organizations to block or filter pictures that may be obscene or pornographic in nature.

COPPA

Short for Children's Online Privacy Protection Act; requires parental consent before collecting information from people under 13 years old.

3. Online Safety Tips

- **Learn the Online Dangers:** Knowing the pitfalls prior to your encountering them will help to make your online experience more effective, by increasing the time you have to be productive. You will also be better prepared to talk to children about the online dangers.
- **Set Rules to Govern Computer and Internet Usage for Children:** Establishing rules for computer and Internet use sets behavioral expectations in the same way that an AUP does for employees and guest users. It is also important to set limits for when children can use the Internet. By not allowing children to use the Internet at night, or when responsible adults are not present, children are less likely to intentionally or unintentionally put their safety at risk. Monitoring software is also available to help monitor Internet usage of users when you are unable to physically monitor online use.
- **Explain the Importance of Maintaining Personal Information:** To keep criminals away from you or loved ones, it is always a good idea to keep your personal information private. Posting your personal information on websites or social media can give criminals access to it.
- **Understand How to Use Social Media:** Understanding how to use social media sites such as Twitter, Facebook, and Instagram can help you to avoid the pitfalls with regard to how people interact on them. These sites tend to be very popular with children and teens. Often social media sites will require personal information from their subscribers. Minors should guard their passwords, and never post personally identifying information or inappropriate photos. Blogs and social networking sites offer privacy tools that can be turned on to restrict potentially dangerous users. The sites automatically provide these protective tools to kids under 15. Kids should share information only with people they know from the real world. It's imperative that your kids let you know if they arrange in-person meetings with people they meet online. Before any such meeting, you should confirm the person's identity, and you should accompany your child to the meeting in a public place. When using P2P file-sharing programs, kids should not download files from users whom they don't know. They could be downloading infected files, pictures, games, and music that are inappropriate, or media files protected by copyright law. Don't allow kids to fill out online forms or surveys.
- **Malware Protection:** Installing anti-virus and anti-malware software is an effective way to keep your computer safe from malicious software that can cause harm to your computer. This software automatically scans email attachments and other downloadable files for viruses before they are downloaded or installed on your computer. Some malware protection software can also filter inappropriate content and block access to sites that might expose minors to graphic content and online predators.



It is important to be safe while **online**, as there are a number of **dangers** to both minors and adults. Knowing the risk associated with the Internet can be the best way in which to defend yourself and your information from malicious attacks. In this tutorial, we discussed the potential threats that exist for online users. We also discussed ways in which to **keep minors safe** while online.

Source: Derived from Chapter 12 of “Information Systems for Business and Beyond” by David T. Bourgeois. Some sections removed for brevity.

[https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Text book.html](https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Text%20book.html)



TERMS TO KNOW

CIPA

Short for Children’ Internet Protection Act; requires public schools and organizations block or filter pictures that may be obscene or pornographic in nature.

COPPA

Short for Children’s Online Privacy Protection Act; requires parental consent before collecting information from people under thirteen years old.

Computer Addiction

by Sophia



WHAT'S COVERED

Although a computer is a valuable tool with many productive applications, some people develop usage habits that are counterproductive and can actually cause harm to their lives or the lives of others. This type of behavior tends to be categorized as addiction, due to the signs and consequences associated with it. In this tutorial, we will discuss computer addiction and how to receive assistance for it.

Our discussion will break down as follows:

1. Computer Addiction

Computer addiction refers to the excessive use of a computer as a primary form of stress relief. Computer addiction is characterized by continued excessive use, in spite of serious negative consequences in the addict's personal life. It, often times, manifests as uncontrolled gaming, uncontrolled viewing of pornography, or immoderate text messaging. There is no commonly accepted number of usage hours to describe a computer addict, as it is typically based on the consequences associated with a person's usage habits.



TERM TO KNOW

Computer Addiction

Excessive use of a computer as a primary form of stress relief.

2. Signs of Computer Addiction

As with all addictions, people will usually display signs or symptoms that they are in some way dependent. Listed below are some signs of computer addiction.

Symptom	Description
Downplaying Computer Use	--Lying about time spent using a computer
Lack of Control	--Difficult time trying to quit using the computer --Habitually losing track of time while using the computer --Poor performance in school or at work as a result of time spent on computer and the type of information shared or activities participated in
Neglect	--Neglecting family and friends --Personal responsibilities (i.e. bills, school assignments)

Uncomfortable Feelings	--Upset or angry when time on computer is cut short --Using computer when upset, sad, or depressed --Anxious when not able to use a computer
------------------------	--

3. Help for Computer Addiction

There are many resources for a person who has admitted to, or who displays, the signs of computer addiction. When in this situation, it is important to be very truthful about your feelings or the feelings of a loved one. Furthermore, limiting computer usage, engaging in other activities, and finding professional addiction counseling is highly advisable. The table below provides suggestions on how to cope with computer addiction.

Guideline	Activities
Set limits and restrictions on computer usage	--Schedule computer usage for designated times during the day --Ask friends or family to recommend amount of time to spend on the computer --Maintain a usage time limit (i.e., one hour on the computer only per day) --Use a stopwatch or timer to enforce usage time limits --Use computer for school work or professional reasons only --Use passwords to block access to unproductive or inappropriate websites --Uninstall unproductive software applications (games, entertainment software) --Restrict computer usage to certain places (i.e., library, school, job)
Engage in other activities	--Engage in physical activities (i.e., jogging, sports, walking, karate, etc.) --Pursue a hobby (i.e., painting, musical instrument, traveling) --Examine new ways of entertainment such as going to the movies, playing board games, or going to museums --Spend time with friends and family
Seek professional counseling	--Know the signs of addiction --Talk with a therapist --Join a support group --Seek help and support from family and friends

Recovering from computer addiction is not impossible, as there are many therapies for computer addicts today. It is important to understand that computer addiction should be treated individually and not similar to the treatment plans for addicts of other things such as drugs and alcohol. For example, drug addicts in treatment are often encouraged to completely abstain from the source of their addiction. The goal for computer addicts should not be to abstain completely from computers, as computers are a valuable tool. However, if there are problematic applications, then those should be avoided.



SUMMARY

Computer addiction, or excessive use of a computer with negative consequences, is a problem for some people. Knowing the **warning signs** or symptoms of computer addiction can **help** to prevent a situation from getting out of control. In this tutorial, we discussed what computer addiction is and the

associated warning signs.



TERMS TO KNOW

Computer Addiction

Excessive use of a computer as a primary form of stress relief.

Benefits and Risks of Social Media

by Sophia



WHAT'S COVERED

Recall that the Internet is a global network of computers linked by the Transmission Control Protocol/Internet Protocol (TCP/IP). This provides computer users with the ability to share information in ways only imagined in years past. As the Internet has evolved, virtual communities or networks have emerged as the standard by which computer users communicate and share information. In this tutorial, we discuss social media and its benefits and risks.

1. Social Networking

A very popular component of the Internet today is the social network. A **social network** is a website that connects its users by allowing them to communicate with each other, share pictures, share information, and share ideas. Social networks also make it easy for people to form groups of friends based on common interest. **Social media** is the term used to describe the sharing of media (photos, videos, audio, text messages) via a social network. Many people feel that social networking sites, such as Facebook, Twitter, and Instagram, have changed the way people use the Internet. Listed below are some of the most popular social networking websites.

Website	Number of Users Per Month	Description
Facebook	1.87 Billion as of January 2017	Most popular social network on the Internet. Allows users to set up a profile that can be used as a custom web page, where users can share photos, videos, audio, text, web links, etc. Users can choose who has access to the content shared by specifying "friends."
Twitter	313,000,00 as of 2016	Allows users to set up a profile that can be used as a custom web page. Users can only share 280-character messages per post; users can share photos, videos, and audio by sharing links to the content. Users can choose who has access to shared content by specifying "followers."
Instagram	100,000,000 as of 2016	Mobile photo sharing application. Users can share photo and video with others. Users can choose who has access to shared content by specifying "followers."
LinkedIn	433,000,000 as of 2016	Professional social network allowing users to connect with past, current, or prospective employers, employees, or colleagues. Provides services for job search and resume posting. Users can make a profile to share employment history and related information. Users can choose who has access to posted content by making "connections" with other users.
	110,000,000	Idea-sharing website where users can share images or videos to their "boards"

Pinterest	as of 2016	and browse content shared by other users.
YouTube	Over 1 Billion users monthly as of 2016	Most popular video sharing network where users can upload video, create channels, and video blog.
WhatsApp	Over 1 Billion as of 2016	Messaging application that gives users the ability to communicate and share via text or voice instantly.
QQ	853,000,000 as of 2016	Instant messaging (chat-based) social media platform. It became international (with more than 80 countries using it), after it was launched in China. It can be used to stay in touch with friends through texts, video calls, and voice chats. It even has a built-in translator to translate your chats.
WeChat	697,000,000 as of 2016	All-in-one communications app for messaging and calling (similar to WhatsApp) that enables you to connect with the people of your choice. It was also developed by Tencent in China and can easily work alongside QQ.
Qzone	640,000,000 as of 2016	Similar to QQ and WeChat, Qzone is another social networking service developed by Tencent. It enables you to share photos, watch videos, listen to songs, write blogs, maintain diaries, and so on. It also empowers you to choose the accessories and customize the look and feel of your Qzone web pages.
Tumblr	227,000,000 as of 2016	Tumblr serves as a social media and microblogging platform that can be used to find and follow things that you like. You can also use it to post anything, including multimedia, to a short-form blog.



TERMS TO KNOW

Social Network

Website that connects its users by allowing them to communicate with each other, share pictures, share information, and share ideas.

Social Media

Term used to describe the sharing of media (photos, videos, audio, text messages) via a social network.

2. Social Networking: Pros and Cons

There is no doubt that social networks have had a huge impact on how people use the Internet. For many individuals, social networks are a major part of their lives. Businesses and organizations are realizing the potential of social networks as they seek to develop more personal relationships with customers and clients. While there are many benefits to social networking, recall that there are also risks associated with social networking as well. Listed below are some of the pros and cons of social networks.

Pros	Cons
Social networking sites encourage greater	The potential for cyber bullying is increased as users

collaboration amongst users	collaborate with one another
Social networking sites build communities around special interest	Social networks can increase the risk of computer addiction as users engage more with friends Social networks can increase the amount of time wasted engaging in social media as opposed to being productive
Social networks increase community access to information	Social networks increase the potential for personal information to be compromised or stolen
Social networks enable people with common interest to meet	Social media can cause relationship problems
Social networks provide fast sharing of information	Social media sometimes provides false information
Social networks are a great way to market or promote a product	Social media can be used for cyberbullying Social media can be used to discriminate against other people
Social networks can aid law enforcement agencies in catching criminals	Social media can compromise personal privacy



As you watch the short video below, think about how you could use social media to advance your own career.

SUMMARY

As the Internet evolves, **social networks** will play an important role in how people use it. Knowing what social networks are available, and the general **pros and cons of social networking** will enhance the experience of users. In this tutorial, we took a look at what a social network is, as well as pros and cons of social networks in general.

TERMS TO KNOW

Social Media

Term used to describe the sharing of media (photos, videos, audio, text messages) via a social network.

Social Network

Website that connects its users by allowing them to communicate with each other, share pictures, share information, and share ideas.

Copyright, Trademark and Intellectual Property

by Sophia



WHAT'S COVERED

Information systems have had an impact far beyond the world of business. New technologies create new situations that we have never dealt with before. How do we handle the new capabilities that these devices empower us with? What new laws are going to be needed to protect us from ourselves? In this tutorial, we will discuss the impact that information systems have on intellectual property, and the methods used by individuals, organizations, and businesses to protect their intellectual property.

Our discussion will break down as follows:

1. Intellectual Property

One of the domains that has been deeply impacted by digital technologies is the domain of intellectual property. **Intellectual property** is defined as property (as an idea, invention, or process) that derives from the work of the mind or intellect. Song lyrics, a computer program, a new type of toaster, or even a sculpture, are all examples of intellectual property. Digital technologies have driven a rise in new intellectual property claims. However, it is very difficult to protect an idea. Instead, intellectual property laws are written to protect the tangible results of an idea. As an example, coming up with a song in your head is not protected, but if you write the song down it can be protected. Three of the most commonly known and used intellectual property protections are copyright, patent, and trademark. In the next section, we will review each type of intellectual property protection.



TERM TO KNOW

Intellectual Property

Property (as an idea, invention, or process) that derives from the work of the mind or intellect.

2. Intellectual Property Protection

Protection of intellectual property is important, because it gives people an incentive to be creative. Innovators with great ideas will be more likely to pursue those ideas if they have a clear understanding of how they will benefit. Outside of the United States, intellectual property protections vary. You can find out more about a specific country's intellectual property laws by visiting the World Intellectual Property Organization.

2a. Copyright

Copyright is the protection given to songs, computer programs, books, and other creative works; any work that has an "author" can be copyrighted. Under the terms of copyright, the author of a work controls what can

be done with the work, including:

- Who can make copies of the work
- Who can make derivative works from the original work
- Who can perform the work publicly
- Who can display the work publicly
- Who can distribute the work

Many times, a work is not owned by an individual, but is instead owned by a publisher with whom the original author has an agreement. In return for the rights to the work, the publisher will market and distribute the work, and then pay the original author a portion of the proceeds.

Copyright protection lasts for the life of the original author, plus 70 years. In the case of a copyrighted work owned by a publisher or another third party, the protection lasts for 95 years from the original creation date. For works created before 1978, the protections vary slightly. You can see the full details on copyright protections by reviewing the Copyright Basics document available at the U.S. Copyright Office's website.



DID YOU KNOW

The first sale doctrine, codified at 17 U.S.C. § 109, provides that an individual who knowingly purchases a copy of a copyrighted work from the copyright holder receives the right to sell, display or otherwise dispose of *that particular copy*, notwithstanding the interests of the copyright owner.



TERM TO KNOW

Copyright

Protection given to songs, computer programs, books, and other creative works; any work that has an “author.”

2b. Trademark

A **trademark** is a word, phrase, logo, shape, or sound that identifies a source of goods or services. For example, the Nike “Swoosh,” the Facebook “f”, and Apple’s apple (with a bite taken out of it) are all trademarked. The concept behind trademarks is to protect the consumer. Imagine going to the local shopping center to purchase a specific item from a specific store, and finding that there are several stores all with the same name! Being able to recognize a trademarked logo or slogan will help ensure that you are buying the product that you want, and not from another company using the same name.

Two types of trademarks exist — a **common-law trademark** and a **registered trademark**. As with copyright, an organization will automatically receive a trademark if a word, phrase, or logo is being used in the normal course of business. A common-law trademark is designated by placing “TM” next to the trademark. A registered trademark is one that has been examined, approved, and registered with the trademark office, such as the Patent and Trademark Office in the United States. A registered trademark has the circle-R (®) placed next to the trademark. While almost any word, phrase, logo, shape, or sound can be trademarked, there are a few limitations. A trademark will not hold up legally if it meets one or more of the following conditions:

1. The trademark is likely to cause confusion with a mark in a registration or prior application.
2. The trademark is merely descriptive of the goods or services. For example, trying to register the trademark “blue” for a blue product you are selling will not pass muster.
3. The trademark is a geographic term.
4. The trademark is a surname. You will not be allowed to trademark “Smith’s Bookstore.”

5. The trademark is ornamental as applied to the goods. For example, a repeating flower pattern that is a design on a plate cannot be trademarked.

As long as an organization uses its trademark and defends it against infringement, the protection afforded by it does not expire. Because of this, many organizations defend their trademark against other companies whose branding even only slightly copies their trademark. For example, Chick-fil-A has trademarked the phrase “Eat Mor Chikin” and has vigorously defended it against a small business using the slogan “Eat More Kale.” Coca-Cola has trademarked the contour shape of its bottle, and will bring legal action against any company using a bottle design similar to theirs.



DID YOU KNOW

Some trademarks have been diluted and have lost their protection in the United States; for example, “aspirin” (originally trademarked by Bayer), “escalator” (originally trademarked by Otis), and “yo-yo” (originally trademarked by Duncan).



TERMS TO KNOW

Trademark

A word, phrase, logo, shape, or sound that identifies a source of goods or services.

Common Law Trademark

Designated by placing “TM” next to the trademark.

Registered Trademark

Trademark that has been examined, approved, and registered with the trademark office, such as the Patent and Trademark Office in the United States.

2c. Patent

Another important form of intellectual property protection is the patent. A **patent** creates protection for someone who invents a new product or process. The definition of invention is quite broad and covers many different fields. Here are some examples of items receiving patents:

- circuit designs in semiconductors;
- prescription drug formulas;
- firearms;
- locks;
- plumbing;
- engines;
- coating processes; and
- business processes.

Once a patent is granted, it provides the inventor with protection from others who may be infringing on his or her patent. A patent holder has the right to “exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States for a limited time in exchange for public disclosure of the invention when the patent is granted.” As with copyright, patent protection lasts for a limited period of time, before the invention or process enters the public domain. In the United States, a patent lasts 20 years. This is why generic drugs are available to replace brand-name drugs after 20 years.



Patent

Protection for the invention of a new product or process.

3. Obtaining Intellectual Property Protection

In the United States, a copyright is obtained by the simple act of creating the original work. In other words, when an author writes down that song, makes that film, or designs that program, he or she automatically has the copyright. However, for a work that will be used commercially, it is advisable to register for a copyright with the U.S. Copyright Office if you are working in the United States. If you plan on deploying your work internationally, then an international copyright would be highly advised. A registered copyright is needed in order to bring legal action against someone who has used a work without permission.

Unlike copyright, a patent is not automatically granted when someone has an interesting idea and writes it down. In most countries, a patent application must be submitted to a government patent office. A patent will only be granted if the invention or process being submitted meets certain conditions:

- It must be original. The invention being submitted must not have been submitted before.
- It must be non-obvious. You cannot patent something that anyone could think of. For example, you could not put a pencil on a chair and try to get a patent for a pencil-holding chair.
- It must be useful. The invention being submitted must serve some purpose or have some use that would be desired.

4. Fair Use

Another important provision within copyright law is that of **fair use**. Fair use is a limitation on copyright law, that allows for the use of protected works without prior authorization in specific cases. For example, if a teacher wanted to discuss a current event in her class, she could pass out copies of a copyrighted news story to her students without first getting permission. Fair use is also what allows a student to quote a small portion of a copyrighted work in a research paper. Unfortunately, the specific guidelines for what is considered fair use and what constitutes copyright violation are not well-defined. Fair use is a well-known and respected concept and will only be challenged when copyright holders feel that the integrity or market value of their work is being threatened. The following four factors are considered when determining if something constitutes fair use:

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work;
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
4. The effect of the use upon the potential market for, or value of, the copyrighted work.

If you are ever considering using a copyrighted work as part of something you are creating, you may be able to do so under fair use.



Fair Use

A limitation on copyright law that allows for the use of protected works without prior authorization in specific cases.

5. Open Source Licensing

While electronic media, such as computer software, is afforded the same copyright protection as non-electronic media, there are some situations in which software developers allow others to freely modify their software in spite of its copyright or licensing agreement. In fact, it has become commonplace among software developers to provide a way for others to modify software without fear of penalty. Open source is the term used to describe software that can be modified by anyone. Businesses and organizations that utilize open source software packages often times modify the software to suit the particular needs of their situation. Open source licenses are licenses that comply with the Open Source definition and are packaged with open source software, thus allowing for the software to be freely used, modified, and shared. To be approved by the Open Source Initiative (also known as the OSI), a license must go through the Open Source Initiative's license review process. The following OSI-approved licenses are popular, widely used, or have strong communities:

- Apache License 2.0
- BSD 3-Clause "New" or "Revised" license
- BSD 2-Clause "Simplified" or "FreeBSD" license
- GNU General Public License (GPL)
- GNU Library or "Lesser" General Public License (LGPL)
- MIT license
- Mozilla Public License 2.0
- Common Development and Distribution License
- Eclipse Public License



TERM TO KNOW

Open Source

Term used to describe software that can be modified by anyone.



SUMMARY

The rise of information systems has forced us to rethink how we deal with **intellectual property**. From the increase in patent applications swamping the government's patent office, to the new laws that must be put in place to enforce copyright protection, digital technologies have impacted our behavior. In this tutorial, we covered the various methods, **copyright**, **trademark**, and **patent** used to protect intellectual property.

Source: Derived from Chapter 12 of "Information Systems for Business and Beyond" by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>

**Common Law Trademark**

Designated by placing “TM” next to the trademark.

Copyright

Protection given to songs, computer programs, books, and other creative works; any work that has an “author.”

Fair Use

A limitation on copyright law that allows for the use of protected works without prior authorization in specific cases.

Intellectual Property

Property (as an idea, invention, or process) that derives from the work of the mind or intellect.

Patent

Protection for the invention of a new product or process.

Registered Trademark

Trademark that has been examined, approved, and registered with the trademark office, such as the Patent and Trademark Office in the U.S.

Trademark

A word, phrase, logo, shape, or sound that identifies a source of goods or services.

Ethical Behavior in the Digital World

by Sophia



WHAT'S COVERED

The introduction of new technology can have a profound effect on human behavior. New technologies give us capabilities that we did not have before, which in turn create environments and situations that have not been specifically addressed in ethical terms. Today's digital technologies have created new categories of ethical dilemmas. For example, the ability to anonymously make perfect copies of digital music has tempted many music fans to download copyrighted music for their own use without making payment to the music's owner. Many of those who would never have walked into a music store and stolen a CD find themselves with dozens of illegally downloaded albums. In this tutorial, we will take a closer look at ethics and ethical issues related to the use of information technology.

Our discussion will break down as follows:

1. Information System Ethics

The term **ethics** is defined as a set of moral principles, or the principles of conduct governing an individual or a group. One method for navigating new ethical waters is a **code of ethics**. A code of ethics is a document that outlines a set of acceptable behaviors for a professional or social group; generally, it is agreed to by all members of the group.

The code of ethics document details different actions that are considered appropriate and inappropriate. One of the major advantages of creating a code of ethics is that it clarifies the acceptable standards of behavior for a professional group. While to many, the guidelines may seem obvious, having these items detailed provides clarity and consistency. The varied backgrounds and experiences of the members of a group lead to a variety of ideas regarding what is acceptable behavior. Explicitly stating standards communicates the common guidelines to everyone in a clear manner. A good example of a code of ethics is the Software Engineering Code of Ethics and Professional Practice. It was developed by the Association for Computing Machinery (ACM) and the Institute for Electrical and Electronics Engineers (IEEE). Their code of ethics provides many straightforward ethical instructions, such as the commitment to honesty and integrity.



TERMS TO KNOW

Ethics

A set of moral principles or the principles of conduct governing an individual or a group.

Code of Ethics

Document that outlines a set of acceptable behaviors for a professional or social group; generally, it is agreed to by all members of the group.

2. Acceptable Use Policies

Many organizations that provide technology services to the public require agreement to an **acceptable use policy (AUP)** before those services can be accessed. Similar to a code of ethics, this policy outlines what is allowed and what is not allowed while someone is using the organization's services. Essentially, by agreeing to the AUP, you are committing to a set of acceptable behavior. Many AUPs have similar pieces of information, although the specific text may vary depending on the organization. The table below details the general components of an AUP.

AUP Section	Description
Preface or Introduction	Provides details as to why the AUP is needed and how it will be implemented
Definition of Terms	Provides definitions of all terms unique to the AUP that are used within the policy
AUP Coverage	Explains to users the specific technology services covered by the AUP
Acceptable Use Policy	Explains to users what is appropriate. Details all specifics as to what is acceptable use of technology, software, network, etc.
Unacceptable Uses	Explains to users what is inappropriate. Details all specifics as to what is not acceptable use of technology, software, hardware, etc.
Consequences for violation	Details for users the actions that will be taken if the policy is violated

An everyday example of this is the terms of service that must be agreed to before using the public Wi-Fi at Starbucks, McDonald's, or even a university. Violations of these policies have various consequences. In most cases, such as with Wi-Fi, violating the acceptable use policy will mean that you will lose your access to the resource. While losing access to Wi-Fi at Starbucks may not have a lasting impact, a university student getting banned from the university's Wi-Fi (or possibly all network resources) could have a serious impact on the student's success.



TERM TO KNOW

Acceptable Use Policy (AUP)

Policy that outlines what is allowed and what is not allowed while someone is using an organization's technology services.

3. Infringement

Recall that under the terms of copyright, the author of a work controls what can be done with the work, including:

- Who can make copies of the work
- Who can make derivative works from the original work
- Who can perform the work publicly
- Who can display the work publicly
- Who can distribute the work

Infringement refers to the violation of the rights of a copyright holder by using copyrighted works without

permission. Infringement is a very broad term, as it encompasses a variety of activities that violate the rights of copyright holders. A good example of infringement would be if you made copies and distributed a music CD without permission.



TERM TO KNOW

Infringement

The violation of the rights of a copyright holder by using copyrighted works without permission.

4. Plagiarism

Plagiarism refers to the taking of another person's work without any attribution and presenting it as your own. Typically, plagiarism is much broader, as its definition can also be inclusive of ideas, words, and other things that cannot be copyrighted. Although not always the case, many cases of plagiarism are also cases of infringement. A good example of plagiarism would be copying a paragraph from a published book and using it in your research paper without a citation or acknowledgement that the paragraph was written by someone else.



TERM TO KNOW

Plagiarism

Taking of another person's work without any attribution and presenting it as your own.



WATCH

Take a look at this short video to better understand the importance of using credible resources.



SUMMARY

The rapid changes in **information technology** in the past few decades have brought a broad array of new capabilities and powers to governments, organizations, and individuals alike. These new capabilities have required thoughtful analysis and the creation of new **norms, regulations, and laws**. In this tutorial, we took a look at **ethics** and the impact that information technology has on ethical considerations when using electronic media.

Source: Derived from Chapter 12 of "Information Systems for Business and Beyond" by David T. Bourgeois. Some sections removed for brevity.

<https://www.saylor.org/site/textbooks/Information%20Systems%20for%20Business%20and%20Beyond/Textbook.html>



TERMS TO KNOW

Acceptable Use Policy (AUP)

Policy that outlines what is allowed and what is not allowed while someone is using an organization's technology services.

Code of Ethics

Document that outlines a set of acceptable behaviors for a professional or social group; generally, it is agreed to by all members of the group.

Ethics

A set of moral principles or the principles of conduct governing an individual or a group.

Infringement

The violation of the rights of a copyright holder by using copyrighted works without permission.

Plagiarism

Taking of another person's work without any attribution and presenting it as your own.

Professional Code of Ethics

by Sophia



WHAT'S COVERED

Digital technologies have opened the possibility to many new capabilities that simplify and expedite processes that were, at one time, complex and time-consuming. However, these new capabilities have also called into question the ethical use of digital technologies. The Software Engineering Code of Ethics and Professional Practice provides principles that detail a commitment to the health, safety, and welfare of the public. In this tutorial, we will apply the Software Engineering Code of Ethics to a few case studies of situations in which ethical behavior may be unclear.

Our discussion will break down as follows:

1. Software Engineering Code of Ethics and Professional Practice

The Association for Computing Machinery (ACM) has published a short and full version of the Software Engineering Code of Ethics. The short version summarizes the guiding principles, and the full version provides additional details and examples. The full version can be found on their [website](#). Below is the short version of the Software Engineering Code of Ethics and Professional Practice.

Software engineers shall commit themselves to making the analysis, specification, design, development, testing, and maintenance of software a beneficial and respected profession. In accordance with their commitment to the health, safety, and welfare of the public, software engineers shall adhere to the following Eight Principles:

1. **PUBLIC** - Software engineers shall act consistently with the public interest.
2. **CLIENT AND EMPLOYER** - Software engineers shall act in a manner that is in the best interests of their client and employer, consistent with the public interest.
3. **PRODUCT** - Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
4. **JUDGMENT** - Software engineers shall maintain integrity and independence in their professional judgment.
5. **MANAGEMENT** - Software engineering managers and leaders shall subscribe to, and promote, an ethical approach to the management of software development and maintenance.
6. **PROFESSION** - Software engineers shall advance the integrity and reputation of the profession, consistent with the public interest.
7. **COLLEAGUES** - Software engineers shall be fair to, and supportive of, their colleagues.
8. **SELF** - Software engineers shall participate in lifelong learning regarding the practice of their profession,

2. Case Study: Jonathan, a Software Engineer

Jonathan Cameron is a software engineer working for LFB Software Company. He is currently working on a project, for the Whitestone County School System, that will provide students, teachers, and parents with a way to electronically receive access to a student's transcript upon request. Jonathan's current role on the team is as a software tester. Early tests show that, while the software is functional, it does not take measures to fully authenticate users, and could result in private student data being given to the wrong people, or even criminals. Jonathan would like to develop a patch for the software, but the project is severely over budget. Further complicating the situation is the fact that the project is two months late. Jonathan feels that he can resolve the problem, but it will take another month of software design, development, and implementation. Jonathan has raised his concerns with his supervisor, and has been instructed to complete development on the patch to fix the problem; however, the patch will be released next year in the second version of the software. Jonathan is under a tremendous amount of pressure from the company to sign off on the software so that it can be released to the school system. His supervisor has even suggested that Jonathan's employment with LFB Software company may be terminated. What should Jonathan do?



THINK ABOUT IT

What principles in the Software Engineering Code of Ethics are relevant to Jonathan's situation?

Relevant Clauses:

Principle 1. Public Software engineers shall act consistently with the public interest. In particular, software engineers shall as appropriate:

1.03. Approve software only if they have a well-founded belief that it is safe, meets Specifications, passes appropriate test, and does not diminish quality of life, diminish Privacy, or harm the environment. The ultimate effect of the work should be good to the Public.

1.04. Disclose to appropriate persons or authorities any actual or potential danger to the User, the public, or the environment, that they reasonably believe to be associated with Software or related documents.

Principle 5. Management. Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance. In particular, those managing or leading software engineers shall, as appropriate:

5.01. Ensure good management for any project on which they work, including effective Procedures for promotion or quality and reduction of risk.

5.11. Not ask a software engineer to do anything inconsistent with this code.

Applying the Code:

According to Principle 1, Section 1.03, of the Software Engineering Code of Ethics, a software engineer should only approve software that does not diminish privacy. Section 1.04 stipulates that the engineer should disclose potential dangers associated with the product being developed. In this case, Johnathan does comply with Section 1.04 of the code, as he did attempt to explain his concerns with his supervisor. Furthermore, the software, if released, would be in direct violation of Principle 1 Section 1.03 of this policy, as the software could possibly diminish the privacy of its users.

Principle 5 of the code addresses the behavior or management. Based on the code, Jonathan's manager would be in violation based on Sections 5.01 and 5.11. Section 5.01 addresses the reduction of risk, while 5.11 stipulates that a manager not ask an engineer to do anything in violation of the code.

In this example, Jonathan finds himself in a tough situation. On one hand, he would like to act ethically as a software engineer, but faced with tight deadlines, the overall quality of the application could be diminished, and user privacy may be compromised. To further complicate things, it has been implied that Jonathan's job could be on the line if the software is not released on time. With this being the case, it would be advisable that Jonathan, as he rightly did, express his concerns to his manager regarding end users' privacy being compromised if the application is deployed. If Jonathan is still concerned about the software, he may even ask that a team meeting be called (or ask to put his concerns on an agenda for another already scheduled meeting) with all key development personnel in attendance, where he can then express his specific concern to the entire team, thereby ensuring that other team members understand the ethical ramifications of going forward with the software release. After initially listening to Jonathan's concerns, his manager might want to commission a software test in which Jonathan's concerns are documented and tested. If it turns out that his concerns are valid, then the manager should address this issue with his supervisor and the development team. If the manager has the authority to stop work on the project until the issue is resolved, then the manager should have development stopped. It would not be advisable for the manager to sign off on the software and wait until the second version to fix or patch the software.

3. Case Study: Chris, a Computer Engineering Professor

Chris Sellers is a computer engineering professor who sits on the board of directors for Sophia University. His role on the board of directors is to serve as the chair of the technology committee. It is his responsibility to evaluate the University's technology needs and make recommendations based on the assessment of the board's technology committee. Chris has been asked by the dean of the chemical engineering department to assist with evaluating process simulation software packages that will be used by students, professors, and researchers at the University. The University provided Chris with software applications from several different companies. After carefully evaluating each application based on the University's expressed needs, Chris recommended an application developed by Bison Software Firm (BSF). His recommendation included a report on the software, and why he felt the BSF application was best suited for the needs of the University's chemical engineering department. Chris did not inform the University or the board of directors that he currently owns 35% of BSF's stock, and that the purchase of a software application by the University will significantly increase the value of Chris's stock. Assuming that Chris's evaluation of the software packages was fair and balanced, were Chris's actions in not informing the University or board of directors ethical?



THINK ABOUT IT

What principles in the Software Engineering Code of Ethics are relevant to Chris's situation?

Relevant Clauses:

Principle 4. Judgement. Software engineers shall maintain integrity and independence in their professional judgement. In particular, software engineers shall, as appropriate:

4.05. Disclose to all concerned parties those conflicts of interest that cannot reasonably be avoided or escaped.

Applying The Code

Section 4.05 speaks to judgement. In this case, Chris Sellers's positions — as board chair and the chief evaluator of the software applications to be purchased, as well as owning a large share of a company whose software he is evaluating — are a direct conflict of interest. Chris should have disclosed his conflict of interest

to the board of directors and the University immediately. He could have, thereby, recused himself or given the University an opportunity to decide whether or not to recuse him from the software evaluation and recommendation process. The issue here is not about whether or not Mr. Sellers was fair in the process of evaluating the software, but rather that the University has invested a high level of trust in Mr. Sellers. He did maintain integrity and independence, as his evaluation of the software was fair and unbiased. However, by not disclosing his interests and the inherent conflicts up front, Chris is breaking the University's trust. If he disclosed his monetary interests in BSF, and the University still hired him to evaluate the software applications, he could have done so professionally. The code absolutely restricts Mr. Sellers from any conflict(s) of interest.



SUMMARY

In every industry, it is important for the businesses and organizations to maintain a clear code of ethics. The values contained within a business's **code of ethics** are an extension of the organization, and can serve as a way to hold management and employees accountable to a business's ultimate vision. A well-written code of ethics can ensure that a company is viewed positively by customers as well as employees. A well-written code of ethics also goes a long way in explaining to employees what is acceptable conduct versus inappropriate conduct.

Source: Software Engineering Code of Ethics and Professional Practice from <http://www.acm.org/about/se-code>. This Code may be published without permission as long as it is not changed in any way and it carries the copyright notice. Copyright (c) 1999 by the Association for Computing Machinery, Inc. and the Institute for Electrical and Electronics Engineers, Inc.

Terms to Know

Acceptable Use Policy (AUP)

Policy that outlines what is allowed and what is not allowed while someone is using an organization's technology services.

Access Control

The technology and techniques that can be used to control who has access to a computer system.

Anti-Spyware Software

Software that defends against spyware and adware.

Anti-Virus Software

Software that defends against malware (viruses, worms, and trojan horses).

Biometric Reader

Identifies users by scanning for one or more physical traits.

Bluetooth

Transmission standard that provides the protocol for mobile devices, computers, or smartphones to connect to communicate.

CIPA

Short for Children's Internet Protection Act; requires public schools and organizations block or filter pictures that may be obscene or pornographic in nature.

COPPA

Short for Children's Online Privacy Protection Act; requires parental consent before collecting information from people under thirteen years old.

Code of Ethics

Document that outlines a set of acceptable behaviors for a professional or social group; generally, it is agreed to by all members of the group.

Common Law Trademark

Designated by placing "TM" next to the trademark.

Computer Addiction

Excessive use of a computer as a primary form of stress relief.

Computer Network

A group of computers connected for the purpose of communication-sharing of data and resources.

Copyright

Protection given to songs, computer programs, books, and other creative works; any work that has an “author.”

Domain Name Service (DNS)

Converts the request between IP addresses and domain names.

Ethernet

The standard interface for all wired networks.

Ethics

A set of moral principles or the principles of conduct governing an individual or a group.

Exploit

An attack that uses a vulnerability to harm a system.

Extranet

A LAN that can be accessed by users with special access rights outside of a businesses or organization.

Fair Use

A limitation on copyright law that allows for the use of protected works without prior authorization in specific cases.

HTML Tag

HTML markup code enclosed in < > brackets; used to define how content is displayed on screen.

Hyperlinks

Link to a webpage or other type of content.

Hypertext Markup Language (HTML)

Programming language used to create websites.

Hypertext Transfer Protocol (HTTP)

Networking protocol used to distribute websites.

IP Address

Short for internet protocol address; numeric address that provides an ID number for a computer on a network.

Infringement

The violation of the rights of a copyright holder by using copyrighted works without permission.

Intellectual Property

Property (as an idea, invention, or process) that derives from the work of the mind or intellect.

Internet

Global network of smaller networks linking devices through TCP/IP.

Intranet

Private network that can only be accessed by users with special permission and is typically set up in a private company or organization.

Keystroke Logger

Records keystrokes in a file and sends the file to the author of the program.

Local Area Network (LAN)

Computer network that links computers within a building.

Malware

Malicious software used to launch attacks on a computer system.

Metropolitan Area Network (MAN)

A network within a large confined area such as a college campus, or company within in urban or suburban area.

Near-Field Communication (NFC)

Set communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone.

Network

Group of people or devices connected for the sole purpose of sharing data or resources.

Network Adapter

Translates instructions from the operating system into data that can be sent over a network.

Network Software Application

Software used to manage and monitor networks of all sizes; helps administrators deploy, manage and monitor a network.

Patent

Protection for the invention of a new product or process.

Personal Area Network (PAN)

A smaller local network in which personal devices are in close range with one another.

Plagiarism

Taking of another person's work without any attribution and presenting it as your own.

Protocol

Format or rule for transmitting data between devices.

Registered Trademark

Trademark that has been examined, approved, and registered with the trademark office, such as the Patent and Trademark Office in the U.S.

Resolve

The process of converting a domain name to an IP address.

Router

An upper tier switch that can connect and route network local network traffic as well as traffic from outside networks such as the Internet.

Smart Card

Plastic card that contains a microchip that a card reader can scan to verify a person's identity.

Social Media

Term used to describe the sharing of media (photos, videos, audio, text messages) via a social network.

Social Network

Website that connects its users by allowing them to communicate with each other, share pictures, share information, and share ideas.

Software-Defined Networking (SDN)

Computer networking concept that separates the software from the hardware, making it

easier to innovate and adapt the network to quickly meet changing network demands.

TCP/IP

Transmission Control Protocol/Internet Protocol; a group of protocols that functions together for web-based communication.

Trademark

A word, phrase, logo, shape, or sound that identifies a source of goods or services.

Trojan Horse

An application that appears to do something useful while secretly causing damage to your computer system.

Uniform Resource Locator (URL)

Address of an internet resource such as a website; must begin with a communication protocol such as HTTP.

Virus

Computer code that inserts itself into an executable file.

Web Page

Document written in HTML format that contains content prepared for the web.

Website

A group of interconnected webpages with a system for navigation through all of the pages.

Wi-Fi Protected Access (WPA)

Method of wireless encryption that offers capabilities for a large wireless network.

Wide Area Network (WAN)

Computer network with all of the equipment spread over a large geographic area and is typically inclusive of many small networks or LANs.

Wired Equivalent Privacy (WEP)

Commonly used method of network encryption; controlled by entering in a 128 bit or 256 bit key.

Wired Network

Network that uses physical cables and connection boxes to connect devices.

Wireless Access Point (WAP)

Wireless network connection box that enables computers on a network to connect wirelessly.

Wireless Fidelity (Wi-Fi)

The standard interface technology for wireless networks.

Wireless Network

Network that uses radio frequency signals to transmit data.

World Wide Web

An interconnected network of documents written in Hypertext Markup Language (HTML) that can be accessed through the Hypertext Transfer Protocol (HTTP).

Worm

An application that carries harmful programs such as a trojan horse or virus.