Module 9 - Privacy, Security, and Ethics

People

Information Systems Components

- People
- Procedures
- Software
- Hardware
- Data
- Internet

Impact of Technology on People

- Positive impact
- Negative impact

Maximizing Positive Effects and Minimizing Negative Effects

- Privacy concerns
- Security concerns
- Ethics concerns

Privacy Concerns

- Threats to personal privacy
- Ways to protect ourselves

Security Concerns

- Controlling access to sensitive information
- Securing hardware and software

Ethics Concerns

- How individual users and companies affect society

Conclusion

- Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects.
- Key concerns are privacy, security, and ethics.
- It is important to recognize the negative impacts of technology on people and address them.

Additional information:

- Privacy concerns include identity theft, data breaches, and online tracking.
- Ways to protect personal privacy include using strong passwords, enabling two-factor authentication, and avoiding sharing personal information online.
- Security concerns include malware, phishing attacks, and unauthorized access to sensitive information.
- Ways to secure hardware and software include installing antivirus software, keeping software up to date, and using firewalls.
- Ethics concerns include online harassment, cyberbullying, and the impact of technology on job displacement.
- Ways to address ethics concerns include promoting responsible use of technology and developing regulations to prevent negative impacts on society.

Privacy

Privacy concerns the collection and use of data about individuals. With the digital revolution, new tools such as cell phones provide camera, microphone, and sensors to share every experience with the world. However, this presents new challenges to old ways of thinking about privacy.

Three primary privacy issues:

1. Accuracy: The responsibility of those who collect data to ensure that the data is correct.
2. Property: Who owns the data.

3. Access: The responsibility of those who have data to control who is able to use that data.

Big Data

Big data refers to the unprecedented amount of digital information being stored, including almost all human events recorded digitally. The collection of data can be searched to find all the actions of one person, creating a **digital footprint** that reveals a highly detailed account of their life.

Information resellers

An industry of data gatherers known as **information resellers** or **information brokers** exists that collects, analyzes, and sells personal data. This personal data can reveal more than what one might wish to make public and have an impact beyond what one might imagine.

Three important issues related to digital footprints:

1. **Collecting public, but personally identifying, information:** Google's Street View project allows anyone in the world to view detailed images of individuals, their homes, or vehicles. Such a combination of computing technologies could make real-time tracking of individuals in public places possible.

2. **Spreading information without personal consent:** Employers use social networking profiles to make decisions about hiring, placement, promotion, and firing. Social networking sites can put individuals at risk since deeper analysis of a social networking profile may reveal even more about the individual than they intend.

3. **Spreading inaccurate information:** Errors in credit history or giving someone a serious criminal history can happen due to simple clerical errors.

Mistaken identity is when the digital footprint of one person is switched with another. The Freedom of Information Act allows individuals to gain access to

records held by credit bureaus and government agencies. Portions may be deleted for national security reasons.

Community

Sharing personal information on social media is a necessary part of creating and participating in an online community. However, many individuals do not fully understand the complex sharing and privacy policies of these networks. This often causes unintentional sharing with people outside their intended social circle. Social networks have come under fire from privacy groups, who say that these companies use complex settings and policies to get users to share more information than intended. This information is in turn shared with advertisers.

Private Networks

Employee-monitoring software is commonly used to record virtually everything employees do on their work computers and networks. Employees should never do anything on a work computer or a work network connection that they wouldn’t want shared with their employer.

Concept Check

- Big data can affect our privacy by creating a digital footprint that reveals a highly detailed account of our life. Information resellers exist that collect, analyze, and sell such personal data.
- Big data refers to the unprecedented amount of digital information being stored, including almost all human events recorded digitally. Information resellers or information brokers collect, analyze, and sell personal data. A digital footprint is a record of an individual's online activity.
- Three important issues related to digital footprints are: collecting public, but personally identifying, information, spreading information without personal consent, and spreading inaccurate information. Mistaken identity is when the digital footprint of one person is switched with another. The Freedom of Information Act allows individuals to gain access to records held by credit bureaus and government agencies.
- Private networks are networks where electronic communication occurs. Employee-monitoring software is used to record virtually everything employees

do on their work computers and networks. Employees should never do anything on a work computer or a work network connection that they wouldn't want shared with

The Internet and the Web

Privacy Concerns and Illusion of Anonymity

- Many people believe that they are anonymous when using the internet and that little can be done to invade their personal privacy, but this is an illusion.
- Every computer on the internet is identified by a unique IP address, which can be used to trace internet activities to their origin.
- Deep web websites can allow communication in a secure and anonymous manner, and the dark web can hide a user's IP address, attracting criminals and political activists.

Browsing and Privacy

- Browsers store critical information, including **history** and **temporary internet files**, which can be used to quickly redisplay web content.
    - **History files** include the locations, or addresses, of sites that you have recently visited.
    - **Temporary Internet files**, also known as the **browser cache**, contain web page content and instructions for displaying this content.
- **Cookies**, which are small data files, can store information about a user's preferences and browsing habits and can be used by websites to deliver a personalized experience.
- **First-party cookies** are generated and read by the website being visited, while **third-party** cookies are generated by an advertising company affiliated with the website and used to track a user's web activity.
- Google Chrome's Incognito mode erases records of web activities on the user's computer but not on the computers running the websites visited.

Privacy Threats

- **Web bugs**, which are invisible images or HTML code, can transmit information

without a user's knowledge, making it possible to identify active e-mail addresses.

- **Spyware** is software designed to secretly record and report a user's activities
  on the internet, including keystrokes and personal information.
- **Computer monitoring software** is perhaps the most invasive and dangerous type of spyware.
- Such as **keyloggers**.
- **Antispyware** or spy removal programs can detect and remove various types of privacy threats.

Anti-spyware Programs

Program	Website
Ad-Aware	<www.adaware.com>
Norton Security	<www.norton.com>
Windows Defender	<www.microsoft.com>
AVG Antitrack	avg.com

Ethics

- Data encryption protects privacy but also allows criminals to hide evidence from police, leading to debates about whether governments should have a way to bypass encryption.

Online Identity

- Online identity is the information that people voluntarily post about themselves online and is available indefinitely to anyone who cares to look.
- People have lost jobs due to posts on social networking sites, highlighting the potential consequences of online identity.

Major Laws on Privacy

- Federal laws such as the **Gramm-Leach-Bliley Act**, **Health Insurance Portability and Accountability Act (HIPAA)**, and **Family Educaitonal Rights and Privacy Act (FERPA)** protect personal financial, medical, and educational information, respectively.

Conclusion

Internet privacy is a complex issue with various threats and challenges. While there are federal laws in place to protect personal information, much of the data collected by private organizations is not covered. Users must exercise caution when browsing and consider the potential consequences of their online identity. Encryption provides privacy but also poses challenges for law enforcement. Antispyware programs and other tools can help protect against privacy threats.

Security

Personal security protects us from crime and danger in the physical world. To protect ourselves from new threats, computer security needs to protect our information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters.

Cybercrime

Cybercrime or computer crime is any criminal offense that involves a computer and a network. It was estimated that cybercrime affects over 400 million people and costs over $400 billion each year. Cybercrimes can take various forms, including:

Identity Theft

- Illegal assumption of someone’s identity for the purposes of economic gain.
- Stolen identities are used to steal credit cards and mail and to commit other crimes.
- Identity thieves stole $16 billion and victimized 15.4 million individuals.

Internet Scams

- Scams using the Internet and have created financial and legal problems for many thousands of people.
- Almost all the scams are initiated by a mass mailing to unsuspecting individuals.
- Common types of Internet scams include phishing, advanced fee scam, greeting card scam, bank loan/credit card scam, and lottery scam.

Common Internet Scams

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

Data Manipulation

- Unauthorized access of a computer network and copying files to or from the server.
- Unlike other cybercrimes, data manipulation can occur for months, even years, without the victims being aware of the security breach, making it hard to

detect.

Ransomware

- Malicious software that encrypts your computer's data and ransoms the password to the user.
- Ransomware criminals have targeted food processing plants, hospitals, and police stations, endangering the health and safety of millions.

Denial of Service (DoS) Attacks

- Attempt to slow down or stop a computer system or network by flooding it with requests for information and data.
- Targets are usually ISPs and specific websites, resulting in shutting down the servers at the ISP or the website and unable to respond to legitimate users.

Tips

Identity theft is a growing problem and can be financially devastating if you are a victim. Here are some steps to help protect your identity:

1. Be careful what you post on the Internet. Never post personal information on forums or social networking areas that are public or in response to an e-mail from someone you do not know or trust.
2. Only do business on the Internet with companies you know to be legitimate.
3. When selling a computer, be sure to completely remove all personal information from the hard drive. To ensure that your personal information is erased, consider using a free erasure software tool, such as Dban.
4. Monitor your credit. Each year, you are entitled to a free personal credit report from each of the three major credit reporting agencies. Monitor your credit by requesting a report every four months from a different reporting agency. The official site for this service is <www.annualcreditreport.com>.

Concept Check

- Cybercrime is any criminal offense that involves a computer and a network.
- Identity theft is the illegal assumption of someone's identity for the purposes of economic gain.

- Internet scams are scams using the Internet.
- Data manipulation is the unauthorized access of a computer network and copying files to or from the server.
- Ransomware is malicious software that encrypts your computer's data and ransoms the password to the user.
- **Denial of Service (DoS)** attacks attempt to slow down or stop a computer system or network by flooding a computer or network with requests for information and data.

Conclusion

As technology continues to advance, cybercrime will continue to be a growing problem. It is important to protect ourselves by being aware of the various types of cybercrime, taking steps to protect our personal information, and monitoring our accounts and credit reports. Understanding the tools used by cybercriminals can also help us make smarter choices and better protect ourselves from becoming victims.

Social Engineering

- Manipulating people to divulge private data
- Often the least secure parts of a network or computer are the humans who work with it
- Common techniques include phishing, where Internet users are tricked into divulging their financial information by a fake but official-looking website or e-mail

Malicious Software

- **Cracker:** a computer criminal who creates and distributes malicious programs or malware
- **Malware:** specifically designed to damage or disrupt a computer system
- Three most common types of malware:
    - **Viruses:** migrate through networks and operating systems, and mostly attach themselves to other programs and databases
    - **Worms:** replicate themselves over and over again, clogs computers and networks until their operations are slowed or stopped

    - **Trojan horses:** appear to be harmless but contain malicious programs, not viruses but can be carriers of viruses

Malicious Hardware

- Criminals use computer hardware to steal information, infect computers with malicious software, and disrupt computer systems
- Most common malicious hardware includes:
    - **Zombies:** computers infected by a virus, worm, or Trojan horse that allows them to be remotely controlled for malicious purposes, a collection of zombie computers is known as a **botnet**, or **robot network**
    - **Rogue Wi-Fi hotspots:** imitate free Wi-Fi networks, capture any and all information sent by the users to legitimate sites, including usernames and passwords
    - **Infected USB flash drives:** contain viruses and other malicious software, typically distributed in public spaces or at conferences

Privacy

- Some websites are designed to be hidden from standard search engines and allow people to communicate in a secure and anonymous manner, known as the dark web
- Dark web makes it nearly impossible to identify who is using it, attracts criminals who want to engage in illegal activities
- Same anonymity allows people in countries where political dissent is dangerous and free speech is censored to communicate, plan, and organize toward a more free and open society without fear of jail or execution

Concept Check

- **Social engineering:** manipulating people to divulge private data
- **Phishing:** attempts to trick Internet users into divulging their financial information by a fake but official-looking website or e-mail
- **Malicious software:** specifically designed to damage or disrupt a computer system, includes viruses, worms, and Trojan horses
- **Cracker:** a computer criminal who creates and distributes malicious programs or malware
- **Zombies:** computers infected by a virus, worm, or Trojan horse that allows them to be remotely controlled for malicious purposes, a collection of zombie

computers is known as a botnet, or robot network

- **Rogue Wi-Fi hotspots:** imitate free Wi-Fi networks, capture any and all information sent by the users to legitimate sites, including user names and passwords
- **Infected USB flash drives:** contain viruses and other malicious software, typically distributed in public spaces or at conferences.

Conclusion

- Security and privacy are important issues in the digital age.
- Social engineering, phishing, malicious software, and malicious hardware are common threats to our security and privacy.
- The dark web offers anonymity to those seeking to engage in illegal activities, but it can also provide a platform for political dissenters in oppressive regimes.
- To protect ourselves, it is important to stay informed about these threats and take appropriate measures to safeguard our information and systems.

Measures to Protect Computer Security

Computer systems and data can be compromised in numerous ways. The Computer Fraud and Abuse Act prohibits unauthorized persons from accessing data using any computer across state lines, and offenders can be sentenced up to 20 years in prison and fined up to $100,000.
However, the best protection for computer security is to be prepared.
The following are some of the main measures to ensure computer security:

Restricting Access

- Security experts are constantly devising ways to protect computer systems from access by unauthorized persons. The most common way to restrict access is the use of a password. Passwords are secret words or phrases that must be keyed into a computer system to gain access. For many applications on the web, users assign their own passwords.
- Security professionals warn that most people use passwords that are too easily guessed. Passwords should have at least eight characters, not include personal information, and contain at least one uppercase letter, one lowercase letter, one number, and one symbol.

- Newer technology allows access to be restricted by passwords that do not require secret words or phrases, such as Picture Password or biometric scanning devices such as fingerprint and iris scanners.

Ethics

- Software companies have discovered flaws in cell phone security and sell software that exploit these flaws and break open locked cell phones. However, this software is also purchased and used by dictators and tyrants to spy on their populace and imprison political dissenters. Companies that discover security flaws have an ethical responsibility to work with cell phone companies to eliminate the flaws instead of exploiting them.

Security Suites

- Security suites provide a collection of utility programs designed to protect your privacy and security while on the web. Two widely used security suites are Avast! Free Antivirus and Microsoft Windows Defender. Services that keep track of viruses on a daily basis, such as Symantec, McAfee, and Microsoft, are also important to stay current with virus threats.

Firewalls

- Act as a security buffer between a corporation’s private network and all external networks, including the Internet.

Password Managers

- Password managers help you create strong passwords and store all your passwords in one location, automatically providing the appropriate password when requested. However, this master list of passwords is protected by one *master* password, which, if forgotten or revealed, could pose a risk.

Authentication

- **Authentication** is the process of ensuring the identity of a user. **Two-factor authentication** uses two types (or factors) of data to verify your identity, such as knowledge, possession, and biometric data. Two-step authentication uses one type of authentication twice.

Encrypting Data

Overview

- Encryption is the process of coding information to make it unreadable except to those who have a special piece of information known as an encryption key or a key.
- Encryption is used to protect information as it moves over a network or is stored on a computer system.

Common uses for encryption include:

1. E-mail encryption
2. File encryption
3. Website encryption
4. Virtual private networks (VPNs)
5. Wireless network encryption

E-mail Encryption

- Protects e-mail messages as they move across the Internet.
- One of the most widely used personal e-mail encryption programs is Pretty Good Privacy (PGP).
- A PGP e-mail message window displays message text as a long string of letters, numbers, and symbols.

File Encryption

- Protects sensitive files by encrypting them before they are stored on a hard drive.
- Files can be encrypted individually or specialized software can be used to encrypt all files automatically each time they are saved to a certain hard drive location.

- Apple's File Vault is an example of file encryption software.

Website Encryption

- Secures web transactions, especially financial transactions.
- Web pages that accept passwords or confidential information like a credit card number are often encrypted.
- **HTTPS (Hypertext Transfer Protocol Secure)** is the most widely used Internet protocol, which requires that the browser and the connecting site encrypt all messages, providing a safer and more secure transmission.

Virtual Private Networks (VPNs)

- Encrypt connections between company networks and remote users such as workers connecting from home.
- This connection creates a secure virtual connection to a company LAN across the Internet.

Wireless Network Encryption

- Restricts access to authorized users on wireless networks.
- **WPA2 (Wi-Fi Protected Access)** is the most widely used wireless network encryption for home wireless networks.
- **WPA2** is typically established for a wireless network through the network's wireless router.

Anticipating Disasters

Overview

- Companies (and even individuals) should prepare themselves for disasters.
- Physical security is concerned with protecting hardware from possible human and natural disasters.
- Data security is concerned with protecting software and data from unauthorized tampering or damage.

Disaster Recovery Plans

- Most large organizations have disaster recovery plans describing ways to continue operating until normal computer operations can be restored.

Preventing Data Loss

- Making frequent backups of data is essential to prevent data loss.
- Backups are often stored at an off-site location to protect data in case of theft, fire, flood, or other disasters.
- Incremental backups store multiple versions of data at different points in time to prevent data loss due to unwanted changes or accidental deletion.

Measures to Protect Computer Security (Figure 9-13)

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

Ethics

- New technologies create new opportunities and interactions, including new computer crimes for criminals and new cybercrime laws and ways to serve and protect for police officers. Therefore, computer ethics are guidelines for the morally acceptable use of computers in our society.
- Ethical treatment is important to all, including the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands.
- Three important issues in computer ethics for average users are cyberbullying, copyright and digital rights management, and net neutrality.

Cyberbullying

- Cyberbullying is the use of the Internet to send or post content intended to hurt or embarrass another person, and it can lead to criminal prosecution.
- Examples of cyberbullying include sending unwanted e-mails, ganging up on victims in electronic forums, posting false statements, maliciously disclosing personal data, and sending any type of communication that is threatening or harassing.
- Cyberbullying is dangerous and hateful, and users should never participate in it or encourage others to do so.
- If someone is the victim of cyberbullying, they can get help and advice from stopbullying.gov.

Copyright and Digital Rights Management

- A **copyright** is a legal concept that gives content creators the right to control use and distribution of their work, including paintings, books, music, films, and video games.
- **Software piracy** is the unauthorized copying and/or distribution of software, and it costs the software industry over $60 billion annually.
- To prevent copyright violations, corporations use **digital rights management (DRM)** to control access to electronic media and files by limiting the number and kinds of devices that can access a file.
- However, some users feel they should have the right to use the media they buy as they choose, and the Digital Millennium Copyright Act makes it illegal to deactivate or disable any antipiracy technologies, including DRM technologies.
- It is also illegal to sell or use programs or devices that are used to illegally copy software, music, or videos from the Internet without appropriate authorization.
- Today, there are many legal sources for digital media, such as online stores and television-network-sponsored sites.

Net Neutrality

- Net neutrality is the policy that **Internet Service Providers (ISPs)** should deliver all data to customers at the same speed, regardless of the content.
- Opponents of net neutrality would allow ISPs to charge companies to deliver some websites faster, arguing that ISPs should be allowed to charge however they like.
- Proponents of net neutrality argue that the Internet has always had equal and unbiased access to information, and allowing ISPs to vary access to websites based on content is a new form of censorship.
- Net neutrality is an important defense of Internet freedom of speech, and it is important to prevent ISPs from discriminating against certain websites or users.

Plagiarism

- Plagiarism means representing someone else's work and ideas as your own without giving credit to the original source, and computer technology has made plagiarism easier than ever.
- Cutting and pasting content from a web page into a report or paper is a common form of plagiarism.
- Services such as Turnitin are dedicated to preventing Internet plagiarism by examining the content of a paper and comparing it to a wide range of known public electronic documents, including web page content.
- It is unethical and most likely illegal to copy parts of a web page from a variety of sites and combine them to form a term paper, and many schools and universities use plagiarism checking programs to compare the content of a student's paper to published material on the web and to previously submitted papers.

Concept Check

- Ethics are guidelines for the morally acceptable conduct of individuals and organizations, while computer ethics are guidelines for the morally acceptable use of computers in our society.

- Copyright is a legal concept that gives content creators the right to control use and distribution of their work, while software piracy is the unauthorized copying and/or distribution of software. Digital rights management (DRM) is used to control access to electronic media and files, and the Digital Millennium Copyright Act makes it illegal to deactivate or disable any antipiracy technologies, including DRM technologies.
- Cyberbullying is the use of the Internet to send or post content intended to hurt or embarrass another person. It includes sending unwanted e-mails, ganging up on victims in electronic forums, posting false statements, maliciously disclosing personal data, and sending any type of communication that is threatening or harassing. Cyberbullying is dangerous and hateful, and users should never participate in it or encourage others to do so. If someone is the victim of cyberbullying, they can get help and advice from stopbullying.gov.
- Plagiarism means representing someone else's work and ideas as your own without giving credit to the original source. Computer technology has made plagiarism easier than ever, such as cutting and pasting content from a web page into a report or paper. Services such as Turnitin are dedicated to preventing Internet plagiarism by examining the content of a paper and comparing it to a wide range of known public electronic documents, including web page content. It is unethical and most likely illegal to copy parts of a web page from a variety of sites and combine them to form a term paper, and many schools and universities use plagiarism checking programs to compare the content of a student's paper to published material on the web and to previously submitted papers.

Conclusion

In conclusion, as new technologies create new opportunities and interactions, computer ethics are guidelines for the morally acceptable use of computers in our society. Users should avoid cyberbullying and plagiarism, and respect copyrights and digital rights management. Net neutrality is an important defense of Internet freedom of speech, and ISPs should not be allowed to discriminate against certain websites or users. It is important to reexamine our standards of moral conduct, or ethics, in the context of these new opportunities and interactions.

Careers in IT

IT security analysts are responsible for maintaining the security of a company's networks, systems, and data.