**KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY**

**CHEMICAL ENGINEERING DEPARTMENT**

**CHE 158: INTRODUCTION TO INFORMATION TECHNOLOGY**

**INSTRUCTOR:** Dr. (Mrs.) Mizpah A. D. Rockson

LECTURE 10: **PRIVACY, SECURITY AND ETHICS**

**Learning Objectives**

At the end of the lecture the student is expected to be able to do the following:

1. Identify the most significant concerns for effective implementation of computer technology.
2. Discuss the primary privacy issues of accuracy, property, and access.
3. Describe the impact of large databases, private networks, the Internet, and the web on privacy.
4. Discuss online identity and the major laws on privacy.
5. Discuss cybercrimes including creation of malicious programs such as viruses, worms, Trojan horses, and zombies as well as denial of service attacks, Internet scams, identity theft, cyberbullying, rogue Wi-Fi hotspots, and data manipulation.
6. Detail ways to protect computer security including restricting access, encrypting data, anticipating disasters, and preventing data loss.
7. Discuss computer ethics including copyright law, software piracy, digital rights management, the Digital Millennium Copyright Act, as well as plagiarism and ways to identify plagiarism.

**10.0 Introduction**

The tools and products of the information age do not exist in a world by themselves. An information system consists not of only procedures, software, hardware, data and connectivity but also of people. Because of people, computer systems may be used for both good and bad purposes.

There are more that one billion microcomputers in use today. What are the consequences of the widespread presence of this technology? Does technology make it easy for others to invade our personal privacy? When we use the web, is information about us being collected and shared with others?

This technology prompts lots of questions- very important questions. Perhaps these are some of the most important questions for the 21st century. Competent end users need to be aware of the potential impact of technology on people and how to protect themselves on the web. They need to be sensitive to and knowledgeable about personal privacy and organizational security.

**10.1 PEOPLE**

While almost everyone agrees that technology has had a very positive impact on people, it is important to recognize the negative, or potentially negative, impacts as well.

Effective implementation of computer technology involves maximizing its positive effects while minimizing its negative effects. The most significant concerns are:

* **Privacy:** what are the threats to personal privacy, and how can we protect ourselves?
* **Security:** How can access to sensitive information be controlled, and how can we secure hardware and software?
* **Ethics:** How do the actions of individual users and companies affect society?

**10.2 PRIVACY**

Privacy concerns the collection and use of data about individuals. There are three primary privacy issues:

1. **Accuracy** relates to the responsibility of those who collect data to ensure that the data is correct.
2. **Property** relates to who owns data and rights to software
3. **Access** relates to the responsibility of those who have data to control who is able to use that data.

**10.2.1 Large Databases**

Large organizations are constantly compiling information about us. Every day, data *is* gathered about us and stored in large databases. For example, telephone companies compile lists of the calls we make, the numbers called, and so on. By entering just a telephone number, you can determine the name, address, and more information about the person registered with that number.

A vast industry of data gatherers known as information resellers or information brokers now exists that collects and sells such personal data. Using publicly available databases and in many cases non-public databases, information resellers create electronic profiles orhighly detailed and personalized descriptions of individuals.

Your personal information, including preferences, habits, and financial data, has become a marketable commodity. This raises many issues, including:

• ***Collecting public, but personally identifying information:*** What if people anywhere in the world could view detailed images of you, your home, or your vehicle?

*As* digital cameras and webcams become cheaper and software becomes more sophisticated, it is likely that many more issues involving personal privacy in public spaces will need to be addressed. A combination of computing technologies could, for example, make real-time tracking of individuals in public places possible.

• Spreading information without personal consent: How would you feel ifan employer were using your Facebook, Google+, orother social networking profiles to make decisions about hiring, placement, promotion and firing? It is a common practice today for many organizations.

How would you feel if someone obtained a driver's license and credit cards in your name? What if that person then assumed your identity to buy clothes, cars, and a house? It happens every day. It is called ***identity theft.*** Identity theft is the illegal assumption of someone's identity for the purposes of economic gain. It is one of the fastest-growing crimes in the country.

• Spreading inaccurate information: How would you like to be turned down for a home loan because of an error in your credit history? This is much more common than you might expect. What if you could not find a job or were fired from a job because of an error giving you a serious criminal history?

This can and has happened due to simple clerical errors. In one case, an arresting officer while completing an arrest warrant incorrectly recorded the Social Security number of a criminal. From that time forward, this arrest and the subsequent conviction became part of another person's electronic profile. This is an example of mistaken identity in which the electronic profile of one person is switched with another.

**10.2.2 Private Networks**

Suppose you use your company's electronic mail system to send a co-worker an unflattering message about your supervisor or to send a highly personal message to a friend. Later you find the boss has been spying on your exchange. This is legal, and a recent surveyrevealed that nearly 75 percent of all businesses search electronic mail and computer files using so called employee-monitoring software. These programs record virtually everything you do on your computer. One proposed law would not prohibit this type of electronic monitoring but would require employers to provide prior written notice. Employers also would have to alert employees during the monitoring with some sort of audible or visual signal. Ifyou are employed and would like to know your company's current policy on monitoring electronic communication, contact your human relations department.

**10.2.3 The Internet and the Web**

When you send e-mail on the Internet or browse the web, do you have any concerns about privacy? Most people do not. They think that as long as they are using their own computer and are selective about disclosing their names or other personal information, then little can be done to invade their personal privacy. Experts call this the ***illusion of anonymity*** that the Internet brings.

Every computer on the Internet is identified by a unique number known as an IP address. IP addresses can be used to trace Internet activities to their origin, allowing computer security experts and law enforcement officers to investigate computer crimes such as unauthorized access to networks or sharing copyright files without permission.

When you browse the web, your browser stores critical information onto your hard disk, typically without you being aware of it. This information, which contains records about your Internet activities, includes history and temporary Internet files.

• **History files** include the locations, or addresses, of sites that you have recently visited. This history file can be displayed by your browser in various locations, including the address bar (as you type) and the *History tab*.

• **Temporary Internet files**, also known as the browser cache, contain web page content and instructions for displaying this content. Whenever you visit a website, these files are saved by your browser. If you leave a site and then return later, these files are used to quickly redisplay web content.

Another way your web activity can be monitored is with **cookies.** Cookies are small data files that are deposited on your hard disk from websites you have visited. Based on your browser's settings, these cookies can be accepted or blocked. Although you will generally not be aware when a website generates a cookie, the personalized experiences you enjoy on the web are often a result of those cookies. While cookies are harmless in and of themselves, what makes them a potential privacy risk is that they can store information about you, your preferences, and your browsing habits. The information stored generally depends on whether the cookie is a first-party or a third-party cookie.

• A **first-party** cookie is one that is generated (and then read) only by the website you are currently visiting. Many websites use first-party cookies to store information about the current session, your general preferences, and your activity on the site. The intention of these cookies is to provide a personalized experience on a particular site. For example, when you revisit a particular electronic commerce site, a previously deposited cookie can provide information so that you can be greeted by name and presented with sales and promotions that interest you.

• A **third-party cookie** is usually generated by an advertising company that is affiliated with the website you are currently visiting. They are used by the advertising company to keep track of your web activity asyou move from one site to the next. For this reason they are often referred to astracking cookies. Critics of this practice claim that your privacy is being violated because your activity is being recorded across multiple websites. Defenders of this practice argue that these cookies are beneficial because it helps websites deliver ads that interest you. For example, suppose you visit four different websites that employ the same advertising agency. The first three sites are about cars, but the fourth is a search engine. When you visit the fourth site, you will likely see a car advertisement because your cookie showed that you had been visiting car-related websites.

**Web bugs**, which are invisible images or HTML code hidden within a web page or e-mail message, can be used to transmit information without your knowledge. When a user opens an e-mail containing a web bug, information is sent back to the source of the bug. The receiving server will now know that this e-mail address is active. One of the most common web bugs is used by companies that sell active mailing lists to spammers. Because of this deception, many e-mail programs now block images and HTML code from unknown senders. It is up to the user to decide whether or not toallow such content to be displayed for current and future messages.

The most dangerous type of privacy threat comes in the form of **spyware.** The term spyware is used to describe a wide range of programs that are designed to secretly record and report an individual's activities on the Internet. Some of these programs can even make changes to your browser in order to deceive you and manipulate what you see online.

Computer monitoring software, also known as **keystroke loggers**, is perhaps the most invasive and dangerous type of spyware. These programs record every activity and keystroke made on your computer system, including credit card numbers, passwords, and e-mail messages. Computer monitoring software can be deposited onto your hard drive without your knowledge by a malicious website orby someone installing the program directly onto your computer. While such software is deadly in the hands of criminals, it can be legally used by companies monitoring employees or law enforcement officials who are collecting evidence.

Unfortunately, many spyware programs go undetected, largely because users have no idea they are infected. Spyware will run in the background, invisible to the average user. Other times, it disguises itself as useful software, such as a security program. Various studies have demonstrated that an alarming number of computers are infected with spyware. The financial impact to individuals, companies, and financial institutions is estimated at billions of dollars.

One of the best defenses against spyware is to exercise caution when visiting new website and downloading software from an unknown source. Another defense involves using a category of software known as antispyware or spy removal programs, which are designed to detect and remove various types of privacy threats.

**Table 10.1: Antispyware programs**



**10.2.4 Online Identity**

Another aspect of Internet privacy comes from online identity, the information that people voluntarily post about themselves online. With the popularity of social networking, blogging, and photo-and video-sharing sites, many people post intimate details of their lives without considering the consequences. Although it is easy to think of online identity as something shared between friends, the archiving and search features of the web make it available indefinitely to anyone who cares to look. There are many number of cases of people who have lost their jobs on the basis of posts on social media websites. These job losses range from a teacher (using off-color language and photos showing drinking) to a chief financial officer of a major corporation (discussing corporate dealings and financial data). 'The cases include college graduates being refused a job because of Facebook posts. How would you feel if information you posted about yourself on the web kept you from getting a job?

**10.2.5 Major Laws on Privacy**

Some laws governing privacy in Ghana are: Data Protection Act, 2012, Electronic Communications Act, 2008, Electronic Transaction Act, 2008 and Copyright Law. There also exists a draft cyber-crime policy.

**10.3 SECURITY**

We are all concerned with having a safe and secure environment to live in. We are careful to lock our car doors and our homes. We are careful about where we walk at night and whom we talk to. This is personal security. What about computer security? What if someone gains unauthorized access to our computer or other computers that contain information about us? These people are commonly known as computer hackers. It should be noted that not all hackers are intent on malicious actions and that not all are criminals. Security involves protecting individuals and organizations from theft and danger. Computer security specifically focuses on protecting information, hardware, and software from unauthorized use, as well as preventing or limiting the damage from intrusions, sabotage, and natural disasters.

**10.3.1 Cybercrime**

Cybercrime or computer crime is any criminal offense that involves a computer and a network. It was recently estimated that cybercrime affects over 400 million people and costs over $400 billion each year. Cybercrimes can take various forms including the creation of malicious programs, denial of service attacks, Internet scams, theft, and data manipulation.

**Malicious Programs** A cracker is someone who creates and distributes malicious programs. These programs are called malware, which is short for malicious software. They are specifically designed to damage or disrupt a computer system. The three most common types of mal ware are viruses, worms, and Trojan horses.

• **Viruses** are programs that migrate through networks and operating systems, and most attach themselves to different programs and databases. While some viruses are relatively harmless, many can be quite destructive. Once activated, these destructive viruses can alter and/or delete files. Unfortunately, new computer viruses are appearing all the time. The best way to stay current is through services that keep track of viruses on a daily basis. For example, Symantec tracks the most serious virus threats.

• **Worms** are programs that simply replicate themselves over and over again. Once active in a network, the self-replicating activity clogs computers and networks until their operations are slowed or stopped. A recent worm traveled across the world within hours, stopping tens of thousands of computers along its way. Unlike a virus, a worm typically does not attach itself to a program or alter and/ or delete files. Worms, however, can carry a virus. Once a virus has been deposited by a worm onto an unsuspecting computer system, the virus will either activate immediately orlie dormant until some future time. For example in 2010, the Stuxnet worm infected several networks in Iran. One of these networks was used by Iran's nuclear program. Soon after the infection, several key pieces of nuclear equipment became permanently disabled.

Viruses and worms typically find their way into microcomputers through e-mail attachments and programs downloaded from the Internet. Because viruses can be so damaging, computer users are advised to never open an e-mail attachment from an unknown source and to exercise great care in accepting new programs and data from any source.

Antivirus programs alert users when certain kinds of viruses and worms enter their system. Two of the most widely used are McAfee virus Scan and Norton Antivirus. Unfortunately; new viruses are being developed all the time, and not all viruses can be detected.

• Trojan horses are programs that come into a computer system disguised as something else. Trojan horses are not viruses. Like worms,however, they can be carriers of viruses. The most common types of Trojan horses appear as free computer games and free screen saver programs that can be downloaded from the Internet. When a user downloads one of these programs, a virus is deposited on the computer system. The virus then begins its mischief. One of the most dangerous types of Trojan horse claims to provide free antivirus programs. When a user downloads one of these programs, the Trojan horse starts with a virus locates and disables any existing virus protection programs before depositing other viruses.

**Zombies** are computers infected by a virus, worm, orTrojan horse that allows them to be remotely controlled for malicious purposes. A collection of zombie computers is known as a botnet, or robot network. Botnets harness the combined power of many zombies for malicious activities like password cracking or sending junk e-mail. Because they are formed by many computers distributed across the Internet, botnets are hard to shut down even after they are detected. Unfortunately for individual computer owners, italso can be difficult to detect when a personal computer has been compromised.

**Denial of Service:** A denial of service (DoS) attack attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data. The targets of these attacks are usually Internet service providers (ISPs) and specific websites. Once under attack, the servers at the ISP or the website become overwhelmed with these requests for service and are unable to respond to legitimate users. As a result, the ISP or website is effectively shut down.

**Internet Scams**: A scam is a fraudulent or deceptive act or operation designed to trick individuals into providing personal information or spending their time and money for little or no return. An Internet scam is simply a scam using the Internet. Internet scams are becoming a serious problem 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.

A technique often employed by scammers is **phishing** (pronounced "fishing"). Phishing attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legitimate. Phishing has grown in sophistication, replicating entire websites like Pay Pal to try to lure users into divulging their financial information. See Table 10.2 for a list of common types of Internet scams.

**10.3.2 Denial of Service**

A denial of service (DoS) attack attempts to slow down or stop a computer system or network by flooding a computer or network with requests for information and data. The targets of these attacks are usually Internet service providers (ISPs) and specific websites. Once under attack, the servers at the ISP or the website become overwhelmed with these requests for service and are unable to respond to legitimate users. As a result, the ISP or website is effectively shut down.

**10.3.3 Internet Scams**

A scam is a fraudulent or deceptive act or operation designed to trick individuals into providing personal information or spending their time and money for little or no return. An Internet scam is simply a scam using the Internet. Internet scams are becoming a serious problem 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.

A technique often employed by scammers is **phishing** (pronounced "fishing"). Phishing attempts to trick Internet users into thinking a fake but official-looking website or e-mail is legitimate. Phishing has grown in sophistication, replicating entire websites like Pay Pal to try to lure users into divulging their financial information. Table 10.2 lists common types of Internet scams.

**Table 10.2: Common internet scams**



**10.3.4 Social Networking Risk**

Social networking is designed for open sharing of information among individuals that share a common interest. Unfortunately, this openness can put individuals using social networking sites at risk. Some have lost their jobs after posting unflattering remarks about their supervisor or after discussing their dislike of their current job. Others post detailed personal information such as their birth dates, family member names, home addresses, and photos of their children. This information can be used by others to steal personal identities and commit other types of crimes. Always exercise caution when providing information on Facebook, Twitter, and other social networking sites. Always use the privacy settings and controls that are provided at the social networking sites you use.

**10.3.5 Cyberllullying**

A fairly recent and all-too-common phenomenon, cyberbullying is the use of the Internet, cell phones, or other devices to send or post content intended to hurt or embarrass another person. Although not always a crime, it can lead to criminal prosecution. Cyberbullying includes sending repeated unwanted e-mails to an individual who has stated that he or she wants no further contact with the sender, ganging up on victims in electronic forums, posting false statements designed to injure the reputation of another, maliciously disclosing personal data about a person that could lead to harm to that person and sending any type of communication that isthreatening or harassing.

**10.3.6 Rogue WI-FI Hotspots**

Free Wi-Fi networks are available almost everywhere from libraries to fast-food restaurants and coffee shops. Rogue Wi-Fi hotspots imitate these free networks. These rogue networks operate close to the legitimate free hotspots and typically provide stronger signals that many users unsuspectingly connect to. Once connected, the rogue networks capture any and all information sent by the users to legitimate sites including user names and passwords.

**10.3.7 Theft**

Theft can take many forms-of hardware, of software, of data, of computer time. Thieves steal equipment and programs, of course, but there are also white-collar crimes. These crimes include the theft of data in the form of confidential information such aspreferred-client lists. Another common crime *is* the use (theft) of a company's computer time by an employee to run another business.

**10.3.8 Data Manipulation**

Finding entry into someone's computer network and leaving a prankster's message may seem like fun, which is why hackers do it. It isstill against the law. Moreover, even if the manipulation seems harmless, it may cause a great deal of anxiety and wasted time among network users.

**Table 10.3 Summary of computer crimes**



**10.4 Measures to Protect Computer Security**

There are numerous ways in which computer systems and data can be compromised and many ways to ensure computer security. Some of the principal measures to ensure computer security are restricting access, encrypting messages, anticipating disasters, and preventing data loss.

**10.4.1 Restricting Access**

Security experts are constantly devising ways to protect computer systems from access by unauthorized persons. Sometimes security is a matter of putting guards on company computer rooms and checking the identification of everyone admitted. Other times it is using biometric scanning devices such as fingerprint and iris (eye) scanners. There are numerous applications that use face recognition to allow access to a computer system.

For example, many microcomputer systems use Dell's FastAccess face recognition application to prevent unauthorized access. There are also several face recognition apps for mobile devices including Face Recognition by iNFINITE Studios LLC.

Oftentimes it is a matter of being careful about assigning passwords to people and of changing the passwords when people leave a company. Passwords are secret words orphrases (including numbers, letters, and special characters) that must be keyed into a computer system to gain access. For many applications on the web, users assign theirown passwords. The strength of a password depends on how easily it can be guessed. A dictionary attack uses software to try thousands of common words sequentially in an attempt to gain unauthorized access to a user's account. For this reason, words, names, and simple numeric patterns make weak or poor passwords. Strong passwords have at least eight characters and use a combination of letters, numbers, and punctuation marks. It is also important not to reuse passwords for different accounts. If one account is compromised, that password might be tried for access to other systems as well. For example, if a low-security account such as an online web forum is compromised, that password could also be tried on higher-security accounts such as banking websites.

Individuals and organizations use security suites and firewalls to protect and control access to their computers.

• ***Security suites*** provide a collection of utility programs designed to protect your privacy and security while you are on the web.

• ***Firewalls*** act as a security buffer between a corporation's private network and all external networks, including the Internet. All electronic communications coming into and leaving the corporation must be evaluated by the firewall Security is maintained by denying access to unauthorized communications.

**10.4.2 Encrypting Data**

Whenever information is sent over a network orstored on a computer system, the possibility of unauthorized access exists. The solution is encryption, 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, simply, a key. Some common uses for encryption include:

• ***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.

• ***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.

• ***Website encryption:*** Secures web transactions, especially financial transactions. Web pages that accept passwords orconfidential information like a creditcard number are often encrypted. The most common protocol for website encryption is https (hypertext transfer protocol secure). The https adds a security level to http. Every URL that begins with *https* requires that the browser and the connecting site encrypt all messages, providing a safer and more secure transmission.

• ***Virtual private networks:*** 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. While the specifics vary between routers, WPA2 is usually set through the router's settings options.

**10.4.3 Anticipating Disasters**

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

**10.4.4 Preventing Data Loss**

Equipment can always be replaced. A company's *data,* however, may be irreplaceable. Most companies have ways of trying to keep softwareand data from being tampered with in the first place. They include carefulscreening of job applicants, guarding of passwords, and auditing of data and programsfrom time to time. Some systems use redundant storage to prevent loss ofdata even when a hard drive fails. Backup batteries protect against data loss due to file corruption during unexpected power outages.

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, fires, floods, or other disasters. Students and others often use flash drives and cloud storage to back up homework and important papers. Incremental backups store multiple versions of data at different points in time to prevent data loss due to unwanted changes or accidental deletion.

See Table 10.4 for a summary of the different measures to protect computer security.

**Table 10.4 Measures to protect computer security**



**10.5 Ethics**

What do you suppose controls how computers can be used? You probably think first of laws. Of course, that is right, but technology is moving so fast that it is very difficult for our legal system to keep up. The essential element that controls how computers are used today is **ethics.**

Ethics, as you may know, are standards of moral conduct. Computer ethics are guidelines for the morally acceptable use of computers in our society. Ethical treatment is critically important to us all, and we are all entitled to ethical treatment. This includes the right to keep personal information, such as credit ratings and medical histories, from getting into unauthorized hands.

Two important issues in computer ethics where average users have a role to play are:

**10.5.1 Copyright and Digital Rights Management**

Copyright is a legal concept that gives content creators the right to control use and distribution of their work. Materials that can be copyrighted include paintings, books, music, films, and even video games. Some users choose to make unauthorized copies of digital media, which violates copyright. For example, making an unauthorized copy of a digital music file for a friend might be a copyright violation.

Software piracy is the unauthorized copying and/or distribution of software. According to a recent study, software piracy costs the software industry over $30 billion annually. To prevent copyright violations, corporations often use digital rights management **(DRM).** DRM encompasses various technologies that control access to electronic media and files. Typically, DRM is used to

(1) control the number of devices that can access a given file and

(2) limit the kinds of devices that can access a file. Although some companies see DRM as a necessity to protect their rights, some users feel they should have the right to use the media they buy-including movies, music, software, and video games-as they choose.

The Digital Millennium Copyright Act makes it illegal to deactivate or otherwise disable any antipiracy technologies including DRM technologies. The act also establishes that copies of commercial programs may not be legally resold or given away. It further makes it a crime to sell or to use programs or devices that are used to illegally copy software. This may come as a surprise to those who copy software including music and games from a friend or from the Internet. The law is clear: It is illegal to copy or download copyright-protected music and videos from the Internet without appropriate authorization.

Today, there are many legal sources for digital media. Television programs can be watched online, often for free, on television-network-sponsored sites. Sites like Pandora allow listeners to enjoy music at no cost. There are several online stores for purchasing music and video content

A pioneer in this area is Apple's iTunes Music Store.

**10.5.2 Plagiarism**

Another ethical issue is plagiarism, which means representing some other person's work and ideas as your own without giving credit to the original source. Although plagiarism was a problem long before the invention of computers, computer technology has made plagiarism easier. For example, simply cutting and pasting content from a web page into a report or paper may seem tempting to an overworked student or employee.

Correspondingly, computer technology has made it easier than ever to recognize and catch plagiarists. For example, services such as **Turnitin** are dedicated to preventing Internet plagiarism. This service will examine the content of a paper and compare it to a wide range of known public electronic documents including web page content in this way; Turnitin can identify an undocumented paper or even parts of an undocumented paper.