Professional Practice

6. Internet Issues

Level III - Semester 5

Intended Learning Outcomes

At the end of this lesson, you will be able to understand;

- The reasons why misuse of the internet gives cause for concern.
- The role of Internet Service Provider and how far it can be held responsible.
- Different types of concerns raise due to misuse of internet
- Factors caused a dramatic increase in the number, variety, and severity of security incidents
- Different types of cyber attacks can happen
- E-commerce regulations

List of sub topics

6.1. The Effects of the Internet

- 6.1.1 What Is Internet
- 6.1.2 Benefits of Internet
- 6.1.3 Effects of Internet
- 6.1.4 Law Across National Boundaries

6.2. Internet Service Providers

- 6.2.1 What is Internet Service Provider
- 6.2.2 Three roles that an ISP may play
- 6.2.3 How far an ISP can be held responsible

6.3. Defamation

6.4. Pornography

6.5. Spam

List of sub topics

6.6. Cyber Attacks and Cybersecurity

- 6.6.1 What is Cyberattacks and Cybersecurity
- 6.6.2 Why Computer Incidents Are So Prevalent?
- 6.6.3 Types of Perpetrators of Computer Crime and Damage
- 6.6.4 Types of Exploits

6.7. E-commerce Regulations

- 6.7.1 Information Needs from Supplier
- 6.7.2 Areas Need to Consider to Protect the Business

6.1.1 What is Internet

- **Internet is a network of networks and has different types of internet.**
- **It consists of public, private, academic, business, and government networks of local to global scope, linked by a comprehensive arrangement of electronic, wireless, and optical networking technologies.**
- **Through internet users at any one computer can, if they have permission, get information from any other computer.**

6.1.2 Benefits of Internet

- **The benefits that the internet has brought are almost universally recognized.**
  - Made it much simpler to access information of all kinds.
  - Made it significantly simpler for people to communicate with one another, both individually and collectively.
  - Simplified and speeded up many types of commercial transaction.
- **Most importantly, these benefits have been made available to very many people, not just to a small and privileged group**

Inevitably, a development on this scale creates its own problems.

6.1.3 Effects of Internet

- **Every country has laws governing what can be published or publicly displayed.**
- **These are main concerns to everyone professionally involved in the internet**
  - **Defamation**- material that makes unwelcome allegations about people or organizations
  - **Pornography**- material with sexual content.
  - **Spam** - any kind of unwanted, unsolicited digital communication that gets sent out in bulk.
- **These topics cannot sensibly be discussed in technical terms alone. Social, cultural and legal issues must be taken into account.**

Different countries approach these issues in very different ways but the internet itself knows no boundaries.

.

6.1.4 Law Across National Boundaries

- **Although every country has such laws, they are very different from each other.**

  For example:

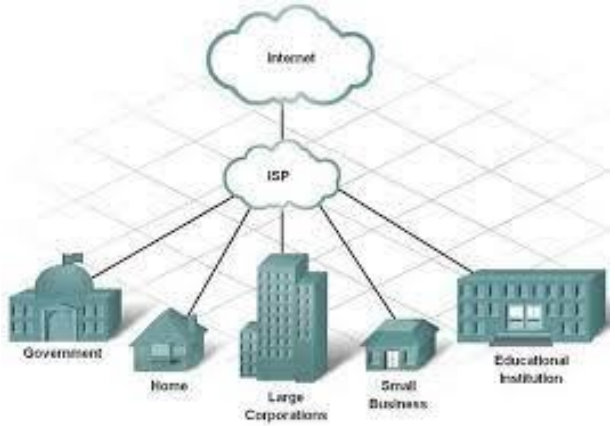
  In some countries, publication of material criticizing the government or the established religion is effectively forbidden, while in others it is a right guaranteed by the constitution and vigorously defended by the courts.

- **Since information can move freely across borders, it is both far more likely that illegally published material will enter a nation and more challenging for that country to enforce its own laws.**

The roles and responsibilities of ISPs are a central element in the way these issues are addressed

6.2.1 What is Internet Service Provider

- **An ISP (internet service provider) is a company that provides individuals and organizations access to the internet and other related services.**
- **An ISP has the equipment and the telecommunication line access required to have a point of presence on the internet for the geographic area served.**
- **ISPs can be organized in various forms, such as,**
  - commercial
  - community-owned
  - non-profit
  - privately owned



An ISP typically serves as the access point or the gateway that provides a user access to everything available on the Internet.

6.2.2 Three roles that an ISP may play

The *mere conduit role* when it transmit the data

This role covers,

- Copies that must necessarily be made during digital communications
- Only intermediate carriers of the communications. Does no more than transmit data. Not the originators or recipients of the communications
    - Does not **initiate transmissions**
    - Does not **select the receivers of the transmissions**
    - Does not **select or modify the data transmitted**.

The regulations provide that an ISP is not liable for damages or for any criminal sanction as a result of a transmission.

6.2.2 Three roles that an ISP may play

The *caching role* covers, when the information is the subject of automatic, intermediate and temporary storage, for the sole purpose of increasing the efficiency of the transmission of the information to other recipients of the service upon their request.

- **An ISP serving as a cache is exempt from liability for damage or other legal repercussions resulting from a transmission if it:**
    1. **Does not modify the information;**
    2. **Complies with conditions on access to the information;**
    3. **Complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by industry;**

6.2.2 Three roles that an ISP may play

The caching role,

4. **Does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;**
5. **Acts quickly to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.**

These conditions are simply designed to ensure that an ISP that claims to be playing a caching role is behaving in accordance with industry practice.

6.2.2 Three roles that an ISP may play

The hosting role,

This role covers,when stores information provided by its customers.

- **ISP is not liable for damage or criminal sanctions provided that:**
  1. **It was unaware that anything unlawful was taking place**
  2. **Where a claim for damages is made, it did not know anything that should have caused it to think that something unlawful might be going on**
  3. **When it found out that that something unlawful was going on, it acted expeditiously to remove the information or to prevent access to it**
  4. **The customer was not acting under the authority or the control of the service provider.**

In the USA, ISPs enjoy much broader immunity than in Europe.

6.2.3 How far an ISP can be held responsible

Removing unlawful material

- **Even after being informed, ISP does not take down illegal content will places it in the position of having to judge whether or not material is unlawful.**
  - ISPs are not qualified to make such judgements and if they are forced to make them they will play safe, that is, they will usually accept that the material complained about is unlawful and will remove it.
  - The ISP, aware that the complainant can deploy an army of expensive lawyers, is likely to play safe by requiring that the material be removed, regardless of whether it is true and in the public interest.

6.2.3 How far an ISP can be held responsible

Releasing information

- **Another concern regarding ISPs is the question of anonymous and pseudonymous postings.**
- **Using a pseudonym when posting on bulletin boards and newsgroups is quite frequent. Their real identity will be known to their ISP. Is the ISP allowed to release, and can it be compelled to release, this information to someone wishing to take legal action against the contributor?**
  - In the UK, the ISP is allowed to release the information and can be compelled to do so by a court.
  - In the USA, ISPs cannot in general be required to release the information, although they may be required to do so in the case of serious crimes.

6.3 What is Defamation

- **Defamation is the act of communicating to a third party false statements about a person, place or thing that results in damage to its reputation.**
- **It can be spoken (slander) or written (libel)**
- **The harm is often of a financial nature, in that it reduces a person's ability to earn a living, work in a profession, or run for an elected office.**

6.4 Pornography

- **Parents, educators, and other child advocates are concerned that children might be exposed to online pornography. They are concerned about,**
  - Potential impact on children
  - Fear that increasingly easy access to pornography encourages pedophiles and sexual predators.
- **Organizations must be very careful when dealing with pornography in the workplace. Reasonable steps include,**
  - Establishing a computer usage policy that prohibits access to pornography sites
  - Identifying those who violate the policy, and taking action against those users, regardless of how embarrassing it is for the users or how harmful it might be for the company.

6.5 Spam

- **Spamming is the use of messaging systems to send multiple unsolicited messages to large numbers of recipients for the purpose of,**
  - Commercial advertising
  - Non-commercial proselytizing
  - Any prohibited purpose
  - Simply repeatedly sending the same message to the same user.

6.5 Spam

- **Email spam is the use of email systems to send unsolicited email to large numbers of people.**
- **Spam used as,**
  - Form of low-cost commercial advertising.
  - Inexpensive marketing tool used by many legitimate organizations.

    For example, a company might send email to a broad cross section of potential customers to announce the release of a new product in an attempt to increase initial sales.

  - Way to deliver harmful worms and other malware.

6.5 Spam

Following are some issues caused due to spam messages

- Reduces receivers' capacity to communicate effectively since their mailboxes are filled and relevant emails are mixed up with a lot of spam messages
- Takes user’s time to scan and delete spam email,
- Entice unsuspecting recipients to take actions that will result in malware being downloaded to their computer.

In early 2015, Symantec, a provider of security, storage, and systems management solutions, began noticing multiple instances of short-duration, high-volume spam attacks targeting millions of users. The messages instructed recipients to click on a link to a URL, which, if done, resulted in the Trojan “Infostealer.Dyranges

6.6.1 What is Cyberattacks and Cybersecurity

Cyberattacks

- Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself

Cybersecurity

- Cybersecurity is the collected set of technologies, processes, and procedures organizations use to protect their computing environments from damage and unauthorized data access perpetrated by cybercriminals or malicious insiders.

6.6.2 Why Computer Incidents Are So Prevalent?

Following are some factors caused a dramatic increase in the number, variety, and severity of security incidents,

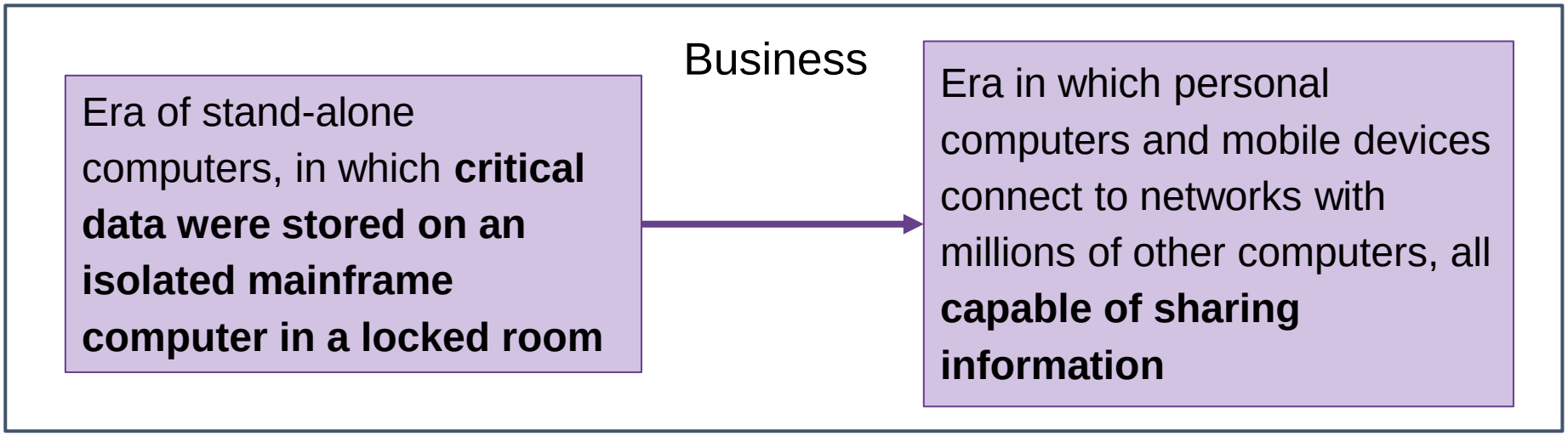
- **Increasing computing complexity**
- **Expanding and changing systems**
- **Increase in the prevalence of bring your own device (BYOD) policies**
- **Growing reliance on software with known vulnerabilities**
- **Increasing sophistication of those who would do harm**

6.6.2.1 Increasing computing complexity

Computing environments have become enormously complex.

- **Cloud computing, networks,computers, mobile devices, virtualization, operating systems, applications, websites,switches, routers, and gateways are interconnected and driven by hundreds of millions of lines of code.**
- **The number of possible entry points to a network expands continually as more devices are added,increasing the possibility of security breaches.**

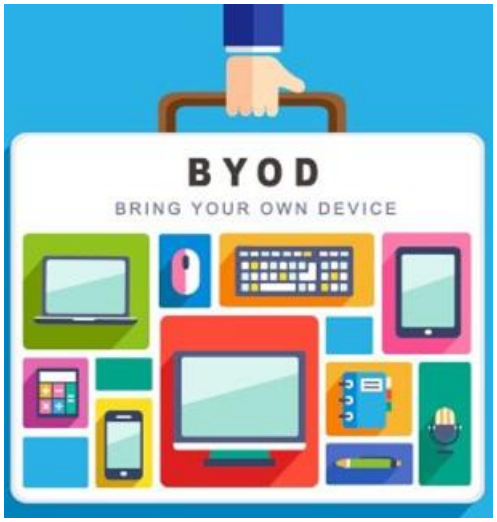
6.6.2.2 Expanding and changing systems



- **Businesses have moved quickly into e-commerce, mobile computing, collaborative work groups, global business, and interorganizational information systems.**
- **Information technology is now widely used and is a crucial tool for businesses to succeed.**
- **IT firms are finding it more challenging to keep up with the rate of technological advancement, properly carry out a continuous evaluation of emerging security risks, and put strategies in place to address them..**

6.6.2.3 Increase in the prevalence of bring your own device (BYOD) policies

- **Bring your own device (BYOD) is a business policy that permits, and in some cases encourages, employees to use their own mobile devices (smartphones, tablets, or laptops) to access,**
  - Company computing resources
  - Applications
  - Email
  - Corporate databases
  - Corporate intranet
  - Internet



- **Proponents of BYOD say it improves employee's productivity by allowing workers to use devices with which they are already familiar**

6.6.2.3 Increase in the prevalence of bring your own device (BYOD) policies

This practice raises many potential security issues as well.

- **These devices are far more commonly exposed to malware than a device used only for business because they are also utilized for non-work activities like,**
  - Browsing websites
  - Shopping
  - Visiting social networks
  - Blogging
- **Many users do not set the timer to automatically lock the device after a few minutes of inactivity or password-protect their computers, tablets, or smartphones.**

6.6.2.4 Growing reliance on software with known vulnerabilities

- In computing, an exploit is an attack on an information system that takes advantage of a particular system vulnerability (poor system design or implementation).
- Once it is discovered, software developers create and issue a “fix,” or patch, to eliminate the problem.
- Users of the system or application are responsible for obtaining and installing the patch, which they can usually download from the web.
- Any delay in installing a patch exposes the user to a potential security breach.

6.6.2.5 Increasing sophistication of those who would do harm

Earlier,

- **The stereotype of a computer troublemaker was that of an introverted “geek” who worked alone and motivated by the desire to gain some degree of notoriety.**
- **This individual was armed with specialized, but limited, knowledge of computers and networks and used rudimentary tools, perhaps downloaded from the Internet, to execute his or her exploits.**

While such individuals still exist, it is not this stereotyped individual who is the biggest threat to IT security.

6.6.2.5 Increasing sophistication of those who would do harm

Today,

- **Computer menace is much better organized and may be part of an organized group, that has an agenda and targets specific organizations and websites.**
  For example:
  - Anonymous
  - Chaos Computer Club
  - Lizard Squad
  - TeslaTeam

- **Some of these groups have ample resources, including money and sophisticated tools to support their efforts, greater depth of knowledge and expertise in getting around computer and network security safeguards.**

6.6.3 Types of Perpetrators of Computer Crime and Damage

- **Black hat hacker**
  Who violates computer or Internet security maliciously or for illegal personal gain.

  White hat hacker is someone who has been hired by an organization to test the security of its information systems

- **Cracker**
  Who causes problems, steals data, and corrupts systems

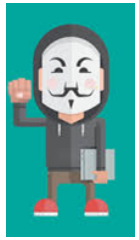
- **Malicious insider**
  An employee or contractor who attempts to gain financially and/or disrupt a company's information systems and business operations

6.6.3 Types of perpetrators of computer crime and damage

- **Industrial spy**
  Who captures trade secrets and attempts to gain an unfair competitive advantage

- **Cybercriminal**
  Who attacks a computer system or network for financial gain

- **Hacktivist**
  Who hacks computers or websites in an attempt to promote a political ideology



- **Cyberterrorist**
  Who attempts to destroy the infrastructure components of governments, financial institutions, and other corporations, utilities, and emergency response units

6.6.4 Types of Exploits

- There are numerous types of computer attacks, with new varieties being invented all the time.
- Not only computers, since smartphones continue to become more computer capable. They also get targeted.
- Smartphone users store an array of personal identity information on their devices, including credit card numbers and bank account numbers. Used to surf the web and transact business electronically.
- The more people use smartphones for these, the more attractive these devices become as targets for cyberthieves. .

6.6.4.1 Ransomware

- Ransomware is malware that stops you from using your computer or data until you meet demands, such as paying a ransom or sending photos to the attacker.
- A computer becomes infected when a user opens an email attachment or is lured to a compromised website by a deceptive email or pop-up window.
- Ransomware can also be spread through removable USB drives or by texting applications such as Yahoo Messenger, with the payload disguised as an image.

6.6.4.1 Ransomware

Ransomware Example:

- **In early February 2016, Hackers encrypted some of Hollywood Presbyterian Medical Center's data and demanded a $12,000 ransom be paid before it would be unlocked.**
- **Initially, the hospital refused to pay the ransom, and hospital employees were forced to resort to paper, pencil, phones, and fax machines to carry out many of their tasks, including accessing patient data.**
- **The hospital sought help from the FBI, the Los Angeles Police Department, and cybersecurity consultants, but it was unable to access the data.**
- **After a week, the hospital paid the ransom and access to the data was fully restored.**

6.6.4.2 Viruses

- A virus is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner.
- A virus may display a certain message on an infected computer's display screen, delete or modify a certain document, or reformat the hard drive.
- Almost all viruses are attached to a file, meaning the virus executes only when the infected file is opened.
- A virus is spread to other machines when a computer user shares an infected file or sends an email with a virus-infected attachment.

Viruses are spread by the action of the "infected" computer user.

6.6.4.2 Viruses

- Macro viruses have become a common and easily created form of virus.
- Attackers use an application macro language (such as Visual Basic or VBScript) to create programs that infect documents and templates.
- Macros can insert unwanted words, numbers, or phrases into documents or alter command functions.
- After a macro virus infects a user's application, it can embed itself in all future documents created with the application.

Viruses Example:

- "WM97/Resume.A" virus is a Word macro virus spread via an email message with the subject line "Resume - Janet Simons." If the email recipient clicks on the attachment, the virus deletes all data in the user's computer or mobile device.

6.6.4.3 Worms

- **A worm is a harmful program that resides in the active memory of the computer and duplicates itself.**
- **A worm is capable of replicating itself on your computer so that it can potentially send out thousands of copies of itself to everyone in your email address book.**
- **The negative impact of a worm attack on an organization's computers can be considerable,**
  - Lost data and programs
  - Lost productivity due to workers being unable to use their computers and to clean up the mess and restore everything to as close to normal as possible.
- **The cost to repair the damage done by each of the *Code Red*, *SirCam*, and *Melissa* worms was estimated to exceed $1 billion, with that of the *Conficker*, *Storm*, and *ILOVEYOU* worms totaling well over $5 billion.**

6.6.4.4 Trojan Horses

- A Trojan horse is a seemingly harmless program in which malicious code is hidden. A victim is usually tricked into opening it because it appears to be useful software from a legitimate source, such as an update for software the user currently has installed on his or her computer.
- The program's harmful payload might be designed to enable the hacker to destroy hard drives, corrupt files, control the computer remotely, launch attacks against other computers, steal passwords, or spy on users by recording keystrokes and transmitting them to a server operated by a third party.
- A Trojan horse often creates a "backdoor" on a computer that enables an attacker to gain future access to the system and compromise confidential or private information.

6.6.4.4 Trojan Horses

- A Trojan horse can be delivered via an email attachment or downloaded to a user's computer, or contracted via a removable media device such as a DVD or USB memory stick.
- Once a user executes the program that hosts the Trojan horse, the malicious payload is automatically launched as well with no telltale signs.
- Common host programs include screensavers, greeting card systems, and games.

6.6.4.4 Trojan Horses

- **Another type of Trojan horse is a logic bomb, which executes when it is triggered by a specific event.**
- **It can be triggered by a change in a particular file, by typing a specific series of keystrokes, or at a specific time or date.**

Logic Bomb Example:

- Malware attacks employing logic bombs compromised some 32,000 Windows, Unix, and Linux systems at half a dozen South Korean organizations, including three major television broadcasters and two large banks.
- A component of the attack was “wiper” malware triggered by a logic bomb set to begin overwriting a computer’s master boot record at a preset time and day.

6.6.4.5 Blended Threat

- A blended threat is a sophisticated threat that combines the features of a virus, worm, Trojan horse, and other malicious code into a single payload.
- A blended threat attack might use server and Internet vulnerabilities to initiate and then transmit and spread an attack on an organization's computing devices, using multiple modes to transport itself, including email, Internet Relay Chat (IRC), and file-sharing networks.
- Rather than launching a narrowly focused attack on specific EXE files, a blended threat might attack multiple EXE files, HTML files, and registry keys simultaneously.

BLENDED THREAT

Multiple malware in one attack

6.6.4.6 DDoS Attacks

Dos / DDos

- A distributed denial-of-service attack is one in which a malicious hacker takes over computers via the Internet and causes them to flood a target site with demands.
- It does not involve infiltration of the targeted system. Instead, it keeps the target so busy responding to a stream of automated requests that legitimate users cannot get in.
- In a DDoS attack, a tiny program is downloaded surreptitiously from the attacker's computer to dozens, hundreds, or even thousands of computers all over the world.
- The term botnet is used to describe a large group of such computers, which are controlled from one or more remote locations by hackers, without the knowledge or consent of their owners.
- The collective processing capacity of some botnets exceeds that of the world's most powerful supercomputers.

6.6.4.6 DDoS Attacks

- **Based on a command by the attacker, the botnet computers (called zombies) go into action, each sending a simple request for access to the target site again and again.**

DDoS Attack Example:

- **Dyn is an Internet performance management company that provides network services including Domain Name System (DNS) services for its many clients.**
- **Starting October 21, 2016, Dyn was hit with a series of massive DDoS attacks. Millions of users on the East coast were unable to reach the websites of Dyn's clients, including Airbnb, Amazon, Comcast, Etsy, GoFundMe, New York Times, PayPal, Shopify, and Twitter.**
- **The attack had a severe impact on the website owners, who were unable to provide customer services or generate e-commerce revenue.**

6.6.4.7 Advanced Persistent Threat

- **A rootkit is a set of programs that enables its user to gain administrator-level access to a computer without the end user's consent or knowledge.**
- **Once installed, the attacker can gain full control of the system and even obscure the presence of the rootkit from legitimate system administrators.**
- **Attackers can use the rootkit to execute files, access logs, monitor user activity, and change the computer's configuration.**
- **Rootkits are one part of a type of blended threat that consists of,**
  - a dropper
  - a loader
  - a rootkit.

ROOTKIT

Hides deep within PC

6.6.4.7 Advanced Persistent Threat

- The dropper code gets the rootkit installation started and can be activated by clicking on a link to a malicious website in an email or opening an infected PDF file.
- The dropper launches the loader program and then deletes itself.
- The loader loads the rootkit into memory; at that point, the computer has been compromised.
- The fundamental problem with trying to detect a rootkit is that the operating system cannot be trusted to provide valid test results.

6.6.4.8 Phishing

- Phishing is the act of fraudulently using email to try to get the recipient to reveal personal data.
- Attacker send legitimate-looking emails urging the recipient to take action to avoid a negative consequence or to receive a reward.
- The requested action may involve clicking on a link to a website or opening an email attachment. These emails, lead consumers to counterfeit websites designed to trick them into divulging personal data or to download malware onto their computers
- It is estimated that bout 156 million phishing emails are sent each day, with 16 million of those successfully evading email filters. Of those, roughly 50 percent (or 8 million) are opened, and 800,000 recipients per day click on malicious URL links contained in the emails.

Phishing Attack

6.6.4.9 Smishing and Vishing

- Smishing is another variation of phishing that involves the use of texting.
- People receive a legitimate-looking text message telling them to call a specific phone number or log on to a website.
- This is often done under the guise that there is a problem with the recipient's bank account or credit card that requires immediate attention.
- The phone number or website is phony and is used to trick unsuspecting victims into providing personal information such as a bank account number, personal identification number, or credit card number, which can then be used to steal money from victims' bank accounts, charge purchases on their credit cards, or open new accounts.

6.6.4.9 Smishing and Vishing

- **Vishing, victims receive a voice-mail message telling them to call a phone number or access a website.**

Vishing Example:

- **One recent vishing campaign captured the payment card information of an estimated 250 Americans per day.**
- **In the attack, users were sent a message that their ATM card had been deactivated.**
- **The users were prompted to call a phone number to reactivate the card by entering their card number and their personal identification number (PIN)—data that were recorded and then used by the criminals to withdraw money from the accounts.**

6.6.4.10 Cyberespionage

- **Cyberespionage involves the deployment of malware that secretly steals data in the computer systems of organizations, such as government agencies, military contractors, political organizations, and manufacturing firms.**
- **Attackers target data that can provide an unfair competitive advantage to the perpetrator. These data are typically not public knowledge and may even be protected via patent, copyright, etc.**
- **High-value data include the following:**
  - Details about product designs and innovative processes
  - Employee personal information
  - Customer and client data
  - Sensitive information about partners and partner agreements

6.6.4.10 Cyberespionage

Example Cyberespionage:

- **U.S. experts claim cyberespionage has helped China accelerate its research and development process.**
- **Alleged targets include aluminum and steel producers, a company that designs nuclear power plants, a solar panel manufacturer, and an aircraft manufacturer.**
- **Meanwhile, China's Foreign Ministry portrays the United States as a hypocrite that engages in cyberespionage by conducting cybertheft, wiretapping, and surveillance activities against Chinese governmental departments, companies, and universities.**
- **President Obama and Chinese President Xi announced in 2015 that the two nations had agreed to initial norms of cyberactivities with the two nations pledging each will avoid conducting cybertheft of intellectual property for commercial gain.**

6.6.4.11 Cyberterrorism

Example Cyberterrorism :

- **In late 2015, cyberterrorists attacked the two electric utility companies in western Ukraine, causing a three-hour power outage affecting some 80,000 customers.**
- **Hackers cut the power and froze the data displayed on the screens of plant operators so they could not view the changing plant conditions; thus, fooling the operators into believing power was still flowing.**
- **To prolong the outage, the attackers also launched a telephone DDoS attack against the utility's call center to prevent customers from reporting the outage, the center's phone system was flooded with bogus calls to prevent legitimate callers from getting through.**
- **Once operators became aware of the outage, the attackers activated KillDisk malware that rendered infected servers and systems unusable. The operators' machines were completely destroyed by the malware.**

6.7 E-commerce Regulations

- Ecommerce is a relatively new branch of retail.
- Similar to other types of online businesses, you need to comply with the general corporate laws and local and international laws applicable to your business, and failure to do so can result in legal issues and lawsuits.
- E-commerce Regulations apply to both goods and services ordered over the telephone or over the internet.

6.7.1 Information Needs from Supplier

Following information must be clear and understandable and it must be provided, along with all terms and conditions.

- **Name of the supplier and an address**
- **Description of the what is being offered**
- **Cost, including tax**
- **Delivery charge, if any, and the method of delivery**
- **Method of payment**
- **Customer's right of cancellation**
- **Communication costs for concluding the contract**
  Ex: the cost of a premium rate telephone call
- **How long the offer is valid for**
- **Duration of the contract, if it is not a one-off**

6.7.2 Areas Need to Consider to Protect the Business

- **See if you need to form a business entity**
- **Ensure you're collecting the proper taxes**
- **Register trademarks and patents**
- **Understand restrictions around the products you sell**
- **Find out if you need business insurance**
- **Choose a Payment Gateway considering**
  - Hosted or not
  - Equipped with anti-fraud features
  - Any restrictions on products
  - Do they handle payment processing issues, chargebacks, and holdbacks
- **Understanding Age Restrictions**
- **Determining Inventory Size**

Summary

Effects of Internet	• Benefits of internet are made available to many people, not only to a small and privileged group • Development on this scale creates its own problems such as defamation, pornography, spam etc. • Different countries approach these issues in different ways but the internet itself knows no boundaries. • The roles and responsibilities of ISPs are a central element in the way these issues are addressed
Internet Service Providers	• ISP is a company that provides access to the internet and other related services • There are three roles that and ISP may play such as mere conduit role, caching role and hosting role.

Summary

Defamation	• Act of communicating to a third party false statements about a person, place or thing that results in damage to its reputation.
Pornography	• Concerned about the potential impact on children and how to deal with it in the workplace.
Spam	• Use of messaging systems to send multiple unsolicited messages to large numbers of recipients
Cyberattacks and Cybersecurity	• There are some factors caused dramatic increase in the number, variety, and severity of security incidents such as Increasing computing complexity, expanding and changing systems, BYOD policies, growing reliance on software with known vulnerabilities, increasing sophistication of those who would do harm. • There are different types of perpetrators and different types of exploits

Summary

E-commerce Regulations	• Similar to other types of online businesses, need to comply with the general corporate laws and local and international laws applicable to your business. • Suppliers need to provide set of information before any contract is agreed • The consumer has an automatic right to cancel the contract for up to seven days after the goods are delivered or, in the case of contracts for the supply of services, up to seven days after the contract has been agreed.