DIPLOMA IN CYBER SECURITY

DCS-03

INFORMATION SECURITY

BLOCK

3

ETHICAL ISSUES IN INFORMATION SECURITY AND PRIVACY

Unit-1

Information Security, Privacy and Ethics

Unit-2

Cyber Crime and Cyber Terrorism

Unit-3

Hacking: Ethical Issues

EXPERT COMMITTEE

Dr P.K.Behera (Chairman)
Reader in Computer science
Utkal University
Bhubaneswar, Odisha

Dr.J.R.Mohanty (Member)
Professor and HOD
KIIT University
Bhubaneswar, Odisha

Sh. PabitranandaPattnaik (Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Sh. Malaya Kumar Das (Member)
Scientist-E, NIC
Bhubaneswar, Odisha

Dr. Bhagirathi Nayak (Member)
Professor and Head (IT & System)
Sri Sri University
Bhubaneswar,Odisha

Dr.ManoranjanPradhan (Member)
Professor and Head (IT & System)
G.I.T.A
Bhubaneswar, Odisha

Sr V.S Sandhilya(Convener)
Academic Consultant (I.T)
Odisha State Open University
Sambalpur, Odisha

DIPLOMA IN CYBER SECURITY

Course Writer
Chandrakant Mallick
Consultant (Academic)
School of Computer and Information Science
Odisha state Open University

UNIT-1: INFORMATION SECURITY, PRIVACY AND ETHICS

1.1 INTRODUCTION

This unit will review ethical aspects of computer and information security and privacy. Ethics is a field of study that is concerned with distinguishing right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures. Ethicists attempt to justify their moral judgments by reference to ethical principles of theories that attempt to capture our moral intuitions about what is right and wrong. Ethical principles often inform legislation, but it is recognized in ethics that legislation cannot function as a substitute for morality. It is for this reason that individuals and corporations are always required to consider not only the legality but also the morality of their actions. Ethical analysis of security and privacy issues in information technology primarily takes place in computer ethics which emerged in the 1980s as afield. Computer ethics analyzes moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use. It asks such questions as:

- Is it wrong for corporations to read their employee‘s e-mail?
- Is it morally permissible for computer users to copy copyrighted software?
- Should people be free to put controversial or pornographic content online without censorship?

Ethical issues and questions like these require moral or ethical analysis: analysis in which the moral dilemmas contained in these issues are clarified and solutions are proposed for them. Moral analysis aims to get clear on the facts and values in such cases, and to find a balance between the various values, rights and interests that are at stake and to propose or evaluate policies and courses of action.

1.2 LEARNING OBJECTIVES

A student after going through this unit will be able to understand concepts of:

- Ethical aspects involved in Information Security
- Information Privacy and Ethics
- Tactics for ensuring proper information security
- How Information Security as a part of National Security Policy.

1.3 INFORMATION SECURITY AND ETHICS

We will now turn to ethical issues in computer and information security. In this section, the moral importance of computer security will be assessed, as well as the relation between information or computer security and national security.

1.3.1 The Moral Importance of Information Security

Computer security is a field of computer science concerned with the application of security features to computer systems to provide protection against the unauthorized disclosure, manipulation, or deletion of information, and against denial of service. The condition resulting from these efforts is also called computer security. The aim of computer security professionals is to attain protection of valuable information and system resources. A distinction can be made between the security of system resources and the security of information or data. The first may be called system security, and the second information security or data security. System security is the protection of the hardware and software of a computer system against malicious programs that sabotage system resources. Information security is the protection of data that resides on disk drives on computer systems or is transmitted between systems. Information security is customarily defined as concerned with the protection of three aspects of data: their confidentiality, integrity and availability.

1.3.2 How does Information security pose ethical issues?

As explained earlier, ethics is mostly concerned with rights, harms and interests. We may therefore answer this question by exploring the relation between computer security and rights, harms and interests.

- What morally important benefits can computer security bring?
- What morally important harms or violations of moral rights can result from a lack of computer security?
- Can computer security also cause harms or violate rights instead of preventing and protecting them?

A first and perhaps most obvious harm that can occur from breaches of computer security is economic harm. When system security is undermined, valuable hardware and software may be damaged or corrupted and service may become unavailable, resulting in losses of time, money and resources. Breaches of information security may come at an even higher economic cost. Valuable data may be lost or corrupted that is worth much more than the hardware on which it is stored, and this may cause severe economic losses. Stored data may also have personal, cultural or social value, as opposed to economic value, that can be lost

when data is corrupted or lost. Any type of loss of system or data security is moreover likely to cause some amount of psychological or emotional harm.

Breaches of computer security may even cause grave harms like injury and death. This may occur in so-called safety-critical systems, which are computer systems with a component or real-time control that can have a direct life-threatening impact. Examples are computer systems in nuclear reactor control, aircraft and air traffic control, missile systems and medical-treatment systems. The corruption of certain other types of systems may also have life-threatening consequences in a more indirect way.

These may include systems that are used for design, monitoring, diagnosis or decision-making, for instance systems used for bridge design or medical diagnosis. Compromises of the confidentiality of information may cause additional harms and rights violations. Third parties may compromise the confidentiality of information by accessing, copying and disseminating it. Such actions may, first of all, violate property rights, including intellectual property rights, which are rights to own and use intellectual creations such as artistic or literary works and industrial design. The information may be exclusively owned by someone who has the right to determine who can access and use the information, and this right can be violated.

Second, compromises of confidentiality may violate privacy rights. This occurs when information that is accessed includes information about persons that is considered to be private. In addition to violations of property and privacy rights, breaches of confidentiality may also cause a variety of other harms resulting from the dissemination and use of confidential information. For instance, dissemination of internal memos of a firm damages its reputation, and compromises of the confidentiality of online credit card transactions undermine trust in the security of online financial transactions and harms e-banking and e-commerce activity.

Compromises of the availability of information can, when they are prolonged or intentional, violate freedom rights, specifically rights to freedom of information and free speech. Freedom of information is the right to access and use public information. Jeroen van den Hoven has argued that access to information has become a moral right of citizens in the information age, because information has become a primary social good: a major resource necessary for people to be successful in society. Shutting down vital information services could violate this right to information. In addition, computer networks have become important as a medium for speech. Websites, e-mail, bulletin boards, and other services are widely used to spread messages and communicate with others. When access to such services is blocked, for instance through denial of service attacks or hijackings of websites, such acts are properly classified as violations of free speech. Computer security measures normally prevent harms and protect rights, but they can also cause harm and violate rights. Notably, security measures may

be so protective of information and system resources that they discourage or prevent stakeholders from accessing information or using services. Security measures may also be discriminatory: they may wrongly exclude certain classes of users from using a system, or may wrongly privilege certain classes of users over others.

1.3.3 Information Security and National Security

Developments in computer security have been greatly influenced by the September 11, 2001 terrorist attacks in the United States and their aftermath. In response to these attacks, national security has become a major policy concern of Western nations. National security is the maintenance of the integrity and survival of the nation-state and its institutions by taking measures to defend it from threats, particularly threats from the outside. Many new laws, directives and programs protective of national security have come into place in Western nations after 9/11, including the creation in the U.S. of an entire Department of Homeland Security. The major emphasis in these initiatives is the protection of state interests against terrorist attacks. Information technology has acquired a dual role in this quest for national security. First of all, computer security has become a major priority, particularly the protection of critical information infrastructure from external threats. Government computers, but also other public and private infrastructure, including the Internet and telephone network, have been subjected to stepped-up security measures. Secondly, governments have attempted to gain more control over public and private information infrastructures. They have done this through wiretapping and data interception, by requiring Internet providers and telephone companies to store phone and e-mail communications records and make them available to law enforcement officials, by attempting to outlaw certain forms of encryption, or even through attempts to require companies to reengineer Internet so that eavesdropping by the government is made easier. Paradoxically, these efforts by governments to gain more control over information also lessen certain forms of security: they make computers less secure from access by government agencies.

Philosopher Helen Nissenbaum has argued that the current concern for national security has resulted in a new conception of computer security next to the classical one. The classical or ordinary conception of computer security is the one used by the technical community and defines computer security in terms of systems security and integrity, availability and confidentiality of data. Nissenbaum calls this technical computer security. The other, which she calls cyber security, involves the protection of information infrastructure against threats to national interests. Such threats have come to be defined more broadly than terrorism, and have nowadays come to include all kinds of threats to public order, including internet crime, online child pornography, computer viruses, and racist and hate-

inducing websites. At the heart of cyber security, however, are concerns for national security, and especially the state's vulnerability to terrorist attacks.

Nissenbaum emphasizes that technical computer security and cyber security have different conceptions of the aims of computer security and the measures that need to be taken. Technical computer security aims to protect the private interests of individuals and organizations, specifically owners and users of computer systems and data. Cyber security aims to protect the interests of the nation-state and conceives of computer security as a component of national security. Technical computer security measures mostly protect computer systems from outside attacks. Cyber security initiatives include such protective measures as well, but in addition include measures to gain access to computer systems and control information. The two conceptions of security come into conflict when they recommend opposite measures. For instance, cyber-security may require computers system to be opened up to remote government inspection or may require government access to websites to shut them down, while technical computer security may prohibit such actions. The different interests of technical computer security and cyber security can in this way create moral dilemmas: should priority be given to state interests or to the interests and rights of private parties? This point to the larger dilemma of how to balance national security interests against civil rights.

1.4 ETHICAL ISSUES IN INFORMATION SECURITY

In this section, ethical aspects of specific practices in relation to computer security will be analyzed. In this section we will focus on practices that undermine computer security: hacking, computer crime, and cyber terrorism and information warfare.

1.4.1Hacking and Computer Crime

A large part of computer security is concerned with the protection of computer resources and data against unauthorized, intentional break-ins or disruptions. Such actions are often called hacking. Hacking is the use of computer skills to gain unauthorized access to computer resources. Hackers are highly skilled computer users that use their talents to gain such access, and often form communities or networks with other hackers to share knowledge and data. Hacking is often also defined, more negatively, as the gaining of such unauthorized access for malicious purposes: to steal information and software or to corrupt data or disrupt system operations. Self-identified hackers, however, make a distinction between non-malicious break-ins, which they describe as hacking, and malicious and disruptive break-ins, which they call cracking. Self-identified hackers often justify their hacking activities by arguing that they cause no real harm and instead have a positive impact. The positive impact of hacking, they argue, is that it frees data to the benefit of all, and improves systems and software by exposing security holes.

The reconsiderations are part of what has been called the hacker ethic or hacker code of ethics, which is a set of (usually implicit) principles that guide the activity of many hackers. Such principles include convictions that information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world. Various professionals have argued that many principles of the hacker ethic cannot be sustained. The belief that information should be free runs counter to the very notion of intellectual property, and would imply that creators of information would have no right to keep it to themselves and have no opportunity to make a profit from it. It would moreover fundamentally undermine privacy, and would undermine the integrity and accuracy of information, as information could be modified and changed at will by anyone who would access it. A school of thought that the helpfulness of hacking in pointing to security weaknesses may not outweigh the harm it does, and that activities in cyberspace can do harm in the real world. Both hacking and cracking tend to be unlawful, and may therefore be classified as a form of computer crime, or cybercrime, as it has also been called. There are many varieties of computer crime, and not all of them compromise computer security. There are two major types of cybercrime that compromise computer security:

- Cyber trespass, which is defined as the use of information technology to gain unauthorized access to computer systems or password-protected websites, and
- Cyber vandalism, which is the use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data. Another type of cybercrime that sometimes includes breaches of computer security, cyber piracy.

Cyber piracy, also called software piracy, is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network. Cyber piracy is much more widespread than cyber vandalism or cyber trespass, because it does not require extensive computer skills and many computer users find it morally permissible to make copies of copyrighted software and data. Cyber piracy involves breaches in computer security when it includes the cracking of copyright protections. Another type of cybercrime that sometimes involves breaches of computer security is computer fraud, which is deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data. Computer fraud may depend on acts of cyber trespass to obtain passwords, digital identities, or other transaction or access codes, and acts of cyber vandalism involving the modification of data. Other types of cybercrime, such as the online distribution of child pornography or online harassment and libel, usually do not involve breaches of computer security.

1.4.2 Cyber terrorism and Information Warfare

A recent concern in computer and national security has been the possibility of cyber terrorism, which is defined by Herman Tavani as the execution of ―politically motivated hacking operations intended to cause grave harm that is, resulting in either loss of life or severe economic loss, or both‖. The possibility of major attacks on information infrastructure, intending to debilitate or compromise this infrastructure and harm economic, industrial or social structures dependent on it, has become a major concern since the attacks. Such attacks could be both foreign and domestic. Controversy exists on the proper scope of cyber terrorism‖. Where the boundaries should be drawn between cyber terrorism, cybercrime, and cyber vandalism? Should a teenager who releases a dangerous virus that turns out to cause major harm to government computers be persecuted as a cyber terrorist? Are politically motivated hijackings of the homepages of major organizations acts of cyber terrorism? A distinction between cyber terrorism and other kinds of cyber attacks may be found in its political nature: cyber terrorism consists of politically motivated operations that aim to cause harm. Yet, Mark Mainon and Abby Good rum have argued that not all politically motivated cyber attacks should be called cyber terrorism. They distinguish cyber terrorism from activism, which are hacking operations against an internet site or server with the intent to disrupt normal operations but without the intent to cause serious damage. Hacktivists may make use of e-mail bombs, low-grade viruses, and temporary homepage hijackings. They are politically motivated hackers who engage in a form of electronic political activism that should be distinguished from terrorism .Information warfare is an extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare. Information warfare may include the use of information media to spread propaganda, the disruption, jamming or hijacking of communication infrastructure or propaganda feeds of the enemy, and hacking into computer systems that control vital infrastructure (e.g., oil and gas pipelines, electric power grids, or railway infrastructure).

1.4.3 Moral Responsibilities of Information Security Professionals

Information security (IS) professionals are individuals whose job it is to maintain system and information security. By standing of their profession, they have a professional responsibility to assure the correctness, reliability, availability, safety and security of all aspects of information and information systems. The discussion in the above sections makes clear that this responsibility has a moral dimension: professional activities in computer security may protect people from morally important harms but could also cause such harms, and may either protect or violate people‘s moral rights. In case of safety-critical systems, the decisions of information security professionals may even be a matter of life or death. That IS professionals have moral responsibilities as part of their profession is reflected in

codes of ethics used by various organizations for computer and information security. These codes of ethics rarely go into detail, however, on the moral responsibilities of IS professionals in specific situations. For instance, the code of ethics of the Information Systems Security Association (ISSA), an international organization of information security professionals and practitioners, only states that members should ―perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles‖ but does not go on to specify what these ethical principles are or how they should be applied and balanced against each other in specific situations For IS professionals, as well as for other computer professionals who have a responsibility for computer security, a code of ethics clearly is not enough. To appreciate the moral dimension of their work, and to cope with moral dilemmas in it, they require training in information security ethics. Such training helps professionals to get clear about interests, rights, and moral values that are at stake in computer security, to recognize ethical questions and dilemmas in their work, and to balance different moral principles in resolving such ethical issues.

1.5 INFORMATION PRIVACY AND ETHICS

We will now turn to issues of privacy in modern data management. In this section, it will be considered what privacy is, why it is important and how it is impacted by information technology.

1.5.1 What is Privacy and why is it important?

In Western societies, a broad recognition exists of a right to personal privacy. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis, who defined privacy as ―the right to be let alone‖. Privacy is a notion that is difficult to define, and many more precise definitions have since been presented. Often, the right to privacy is defined as the right of individuals to control access or interference by others into their private affairs. Philosopher Ferdinand Schoeman has defined it thus: ―A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body.‖ Schoeman‘s definition shows that the concept of privacy does not only apply to the processing of personal information. It also applies to the observation of and interference with human behaviors and relations, the human body, and one‘s home and personal belongings. Privacy is held to be valuable for several reasons. Most often, it is held to be important because it is believed to protect individuals from all kinds of external threats, such as defamation, ridicule, harassment, manipulation, blackmail, theft, subordination, and exclusion. James Moor has summed this up by claiming that privacy is an articulation of the core value of security, meant to protect people from all kinds of harm done by others. It has also been argued that privacy is a necessary condition for autonomy: without privacy, people could not

experiment in life and develop their own personality and own thoughts, because they would constantly be subjected to the judgment of others. The right to privacy has also been claimed to protect other rights, such as abortion rights and the right to sexual expression. Privacy moreover has been claimed to have social value in addition to individual value. It has, for instance, been held to be essential for maintaining democracy.

The right to privacy is not normally held to be absolute: it must be balanced against other rights and interests, such as the maintenance of public order and national security. Privacy rights may also vary in different contexts. There is, for example, a lesser expectation of privacy in the workplace or in the public sphere than there is at home. An important principle used in privacy protection in Western nations is that of informed consent: it is often held that citizens should be informed about how organizations plan to store, use or exchange their personal data, and that they should be asked for their consent. People can then voluntarily give up their privacy if they choose.

1.5.2 Information Technology and Privacy

Privacy is a value in modern societies that corresponds with the ideal of the autonomous individual who is free to act and decide his own destiny. Yet, modern societies are also characterized by surveillance, a practice that tends to undermine privacy. Surveillance is the systematic observation of (groups of) people for specific purposes, usually with the aim of exerting some form of influence over them. Sociologist David Lyon has argued that surveillance has always been an important part of modern societies. The state engages in surveillance to protect national security and to fight crime, and the modern corporation engages in surveillance in the workplace to retain control over the workforce. Computerization from the 1960s onward has intensified surveillance by increasing its scale, ease and speed. Surveillance is partially delegated to computers that help in collecting, processing and exchanging data. Computers have not only changed the scale and speed of surveillance, they have also made a new kind of surveillance possible: dataveillance, which is the large-scale, computerized collection and processing of personal data in order to monitor people‘s actions and communications. More and more, information technology is not just used to record and process static information about individuals, but to record and process their actions and communications. New detection technologies like smart closed-circuit television (CCTV), biometrics and Intelligent User Interfaces, and new data processing techniques like data mining further exacerbate this trend. As Lyon has argued, the ease with which surveillance now takes place has made it a generalized activity that is routinely performed in all kinds of settings by different kinds of organizations. Corporations, for instance, have extended surveillance from the workplace to their customers (consumer surveillance). In addition, the 9/11 terrorist attacks have drastically expanded surveillance activities by the state. Many privacy disputes in today‘s society result from tensions between people‘s

right to privacy and state and corporate interests in surveillance. In the information society, privacy protection is realized through all kinds of information privacy laws, policies and directives, or data protection policies, as they are often called in Europe. These policies regulate the harvesting, processing, usage, storage and exchange of personal data. They are often overtaken, however, by new developments in technology. However, privacy protection has also become a concern in the design and development of information technology. Information privacy has also become a major topic of academic study. Studies of information privacy attempt to balance privacy rights against other rights and interests, and try to determine privacy rights in specific contexts and for specific practices. Specialized topics include workplace privacy, medical privacy, genetic privacy, Internet privacy, and privacy in public.

1.6 PRIVACY ISSUES IN MODERN DATA MANAGEMENT

1.6.1 Internet Privacy

The Internet raises two kinds of privacy issues. First, the posting and aggregation of personal information on Internet websites sometimes violates privacy. Websites on the Internet contain all sorts of personal information that is made publicly available, often without the bearer‘s explicit consent. They may contain, for instance, one‘s phone number and address, archived bulletin board messages from years past, information about one‘s membership of organizations, online magazines and newspapers in which one is mentioned, online databases with public records, pictures and video clips featuring oneself, etc. Using search engines, this information can easily be located and be used to create elaborate composite records about persons. Should there be limits to this? When should someone‘s consent be asked when his personal information is posted on the web, or when such information is used for specific purposes? A second type of privacy issue involves the online monitoring of internet users. Their connection to the internet may be used by third parties to collect information about them, in a way that is often invisible to them. Online privacy risks include cookies (small data packets placed by servers on one‘s computer for user authentication, user tracking, and maintaining user-specific information), profiling or tracking (recording the browsing behavior of users), and spyware (computer programs that maliciously collect information from a user‘s computer system or about a user‘s browser behavior and send this information over the internet to a third party). In addition, private e-mail and data traffic may be intercepted at various points, for instance by employers, internet service providers, and government agencies. When do such actions violate privacy, and what should be done to protect internet privacy?

1.6.2 Record Merging and Matching and Data Mining

It frequently happens that different databases with personal information are combined to produce new data structures. Such combinations may be made in two ways. First, the records in two databases may be merged to produce new

composite records. For instance, a credit card company may request information about its prospective customers from various databases (e.g., financial, medical, insurance), which are then combined into one large record. This combined record is clearly much more privacy-sensitive than the records that compose it, as the combined record may generate perceptions and suggest actions that would not have resulted from any of the individual records that make it up. Second, records in databases may be matched. Computer matching is the cross-checking in two or more unrelated databases for information that fits a certain profile in order to produce matching records or ―hits‖. Computer matching is used often by government agencies to detect possible instances of fraud or other crimes. For instance, ownership records of homes or motorized vehicles may be matched with records of welfare recipients to detect possible instances of welfare fraud. Computer matching has raised privacy concerns because it is normally done without the consent of the bearers of personal information that are involved. Moreover, matches rarely prove facts about persons but rather generate suspicions that require further investigation. In this way, record matching could promote stereotyping and lead to intrusive investigations. Data Mining is a technique that is usually defined over a single database. It is the process of automatically searching large volumes of data for patterns, using techniques like statistical analysis, machine learning and pattern recognition. When data mining takes place in databases containing personal information, the new information thus gained may be privacy sensitive or confidential even when the old information is not. It may for instance uncover patterns of behavior of persons that were not previously visible. Data mining may also be used to stereotype whole categories of individuals. For instance, a credit card company may use data mining on its customer database to discover that certain zip codes correlate strongly with loan defaults. It may then decide not to extend credit anymore to customers with these zip codes. In summary, data mining may violate individual privacy and may be used to stereotype whole categories of individuals. Ethical policies are needed to prevent this from happening.

1.6.3 Privacy in Public

It is sometimes believed that privacy is a right that people have when they are in private places like homes, private clubs and restrooms, but that is minimized or forfeited as soon as they enter public space. When you walk in public streets or are on the road with your car, it is sometimes believed, you may retain the right not to be seized and searched without probable cause, but your appearance and behavior may be freely observed, surveilled and registered. Many privacy scholars, however, have argued that this position is not wholly tenable, and that people have privacy rights in public areas that are incompatible with certain registration and surveillance practices. The problem of privacy in public applies to the tracking, recording, and surveillance of public appearances, movements and behaviors by individuals and their vehicles. Techniques that are used for this including video surveillance (CCTV), including smart CCTV for facial

recognition, infrared cameras, satellite surveillance, GPS tracking, RFID tagging, electronic checkpoints, mobile phone tracking, audio bugging, and ambient intelligence techniques. Does the use of these techniques violate privacy even when they are used in public places? The problem of privacy in public also applies to publicly available information on the Internet. Does the fact that personal information is available on a public forum make it all right to harvest this information, aggregate it and use it for specific purposes?

Helen Nissenbaum has argued in an influential paper that surveillance in public places that involves the electronic collection, storage and analysis of information on a large scale often amounts to a violation of personal privacy. She argues that people often experience such surveillance as an invasion of their privacy if they are properly informed about it, and that such electronic harvesting of information is very different from ordinary observation, because it shifts information from one context to another and frequently involves record merging and matching and data mining. She concludes that surveillance in public places violates privacy whenever it violates contextual integrity: the trust that people have that acquired information appropriate to one context will not be used in other contexts for which it was not intended.

1.6.4 Biometric Identification

Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics. Biometric technologies provide a reliable method of access control and personal identification for governments and organizations. However, biometrics has also raised privacy concerns. Widespread use of biometrics would have the undesirable effect of eliminating anonymity and pseudonymity in most daily transactions, because people would leave unique traces everywhere they go. Moreover, the biometric monitoring of movements and actions gives the monitoring organization insight into a person‘s behaviors which may be used against that person‘s interests. In addition, many people find biometrics distasteful, because it involves the recording of unique and intimate aspects of (rather than about) a person, and because biometric identification procedures are sometimes invasive of bodily privacy. The challenge for biometrics is therefore to develop techniques and policies that are optimally protective of personal privacy.

1.6.5 Ubiquitous Computing and Ambient Intelligence

Ubiquitous Computing is an approach in information technology that aims to move computers away from the single workstation and embed microprocessors into everyday working and living environments in an invisible and unobtrusive way. Ambient Intelligence is an advanced form of ubiquitous computing that incorporates wireless communication and Intelligent User Interfaces, which are interfaces that use sensors and intelligent algorithms for profiling (recording and adapting to user behavior patterns) and context awareness (adapting to different situations). In Ambient Intelligence environments, people are surrounded with possibly hundreds of intelligent, networked computers that are aware of their presence, personality and needs, and perform actions or provide information based on their perceived needs. Marc Langheinrich has claimed that ubiquitous computing has four unique properties that are potentially threatening to privacy:

1. ubiquity;
2. invisibility
3. sensing;
4. memory amplification (the continuous recording of people‘s actions to create searchable logs of their past). Ambient Intelligence adds two properties to this list:
5. user profiling; and
6. Connectedness (wireless communication between smart objects).

These unique features of the two technologies make the protection of privacy in them a major challenge. As critics have argued, ubiquitous computing and ambient intelligence have the ability to create a Big Brother society in which every human activity is recorded and smart devices probe people‘s actions, intentions and thoughts. The distinction between the private and the public sphere may be obliterated as dozens of smart devices record activity in one‘s home or car and connect to corporate or government computers elsewhere. Major privacy safeguards will be needed to avoid such scenarios.

1.7 TACTICS TO ENSURE INFORMATION SECURITY AND MAINTAIN PRIVACY

These tactics guides cover the basics of digital security and recommend tools you can use

- Protect your device from malware and hackers: Prevent worms, viruses and Trojans
- Protect your information from physical threats: Ensure your workplace and devices are secure
- Create and maintain secure passwords: Learn to manage strong passwords
- Protect the sensitive files on your computer : Learn to encrypt data and files

- Recover from information loss : Back up your devices and data
- Destroy sensitive information : Delete data permanently
- Keep your online communication private: Encrypted chat and email.
- Remain anonymous and bypass censorship on the Internet: Using Tor and VPNs
- Protect yourself and your data when using social networking sites: Using Facebook, Twitter and Flickr safely.

1.8 SUMMARY

Privacy is a moral right of individuals that is frequently and increasingly at issue when information systems are used. It was explained in this essay why privacy is important and how it is impacted by information technology, and various ethical issues in information privacy were reviewed. Computer security is not itself a moral right or moral value, but it has been argued that maintaining computer security may be morally necessary to protect correlated rights and interests: privacy rights, property rights, freedom rights, human life and health and national security. It was argued that computer security can also work to undermine rights. Ethical analysis of privacy and security issues in computing can help computer professionals and users recognize and resolve moral dilemmas and can yield ethical policies and guidelines for the use of information technology. In addition, it has been recognized in computer ethics that not only the use of information systems requires moral reflection, but also their design, as system designs reflect moral values and involve moral choices. A system can for example be designed to protect privacy, but it can also be designed to give free access to personal information to third parties. This fact is taken up in value-sensitive design, an approach to the design of information systems that attempts to account for values in a principled fashion. Ideally, ethical reflection on information technology should not wait until products hit the market, but should be built in from the beginning by making it part of the design process. Digital world poses great danger to privacy and security; however it can be tackled to a great extent by adhering to disciplined approach as prescribed. Freeware and Open Source Software are of great help in achieving Information Security to a fairly great extent.

1.9 CHECK YOUR PROGRESS

A. Fill in the blanks.

1. Ethical principles often inform legislation, but it is recognized in ethics that legislation cannot function as a substitute for_____.
2. _____ is the protection of data that resides on disk drives on computer systems or is transmitted between systems.
3. _____ is the use of computer skills to gain unauthorized access to computer resources.
4. _____ is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network.
5. _____ is defined as politically motivated hacking operations intended to cause grave harm that is, resulting in either loss of life or severe economic loss, or both.
6. _____ is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics.

1.10 MODEL QUESTIONS

1. What are ethics?
2. What is the moral importance of Computer Security?
3. How does computer security pose ethical issues?
4. How compromises of confidentiality may violate privacy rights?
5. What are the moral responsibilities of Information Security professionals?
6. What are the ethical issues in Information security?
7. What is hacking? How it is different from cracking?
8. What are the two kinds of privacy issues raised by the Internet?
9. What is Ubiquitous Computing?
10. What are the different tactics to ensure computer security and maintain privacy?

1.11 ANSWERS TO CHECK YOUR PROGRESS

1. Morality
2. Information security
3. Hacking
4. Cyber piracy
5. Cyber terrorism
6. Biometrics

1.12REFERENCES AND SUGGESTED REDING

1. Study Material "Fundamentals of Information Security, (PGDCS-01), Certificate in e-Governance and Cyber Security", Uttrakhand Open University,Haldwani, made available under a Creative Commons Attribution Share-Alike 4.0 Licence (International), http://creativecommons.org/licenses/by-sa/4.0/

UNIT-2 CYBER CRIME AND CYBER TERRORISM

UNIT STRUCTURE

2.0 INTRODUCTION

Cyber-space refers to the boundless space known as the internet. It refers to the interdependent network of information technology components that underpin many of our communications technologies in place today. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user‘s assets. Organization and user‘s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user‘s assets against relevant security risks in the cyber environment.
In this unit we will discuss different reasons and kinds of cyber-crimes and terrorism.

2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- define cyber crime
- Know the reasons for commission of cyber crimes
- Know different types of cyber crime
- Understand cyber stalking
- Know spamming
- Understand cross site scripting
- Know online auction frauds
- Know cyber squatting
- Understand web jacking

2.2 CYBER CRIME

The term **cyber-crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often committedby the people of destructive and criminal mindset either for revenge, greed or adventure.

2.2.1 Classification of Cyber Crimes

The cyber-criminal could be internal or external to the organization facing the cyber-attack. Based on this fact, the cyber-crime could be categorized into two types:

1. **Insider Attack:** An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber-attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker has an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when an employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a Vulnerability window for the attacker. The insider attack could be prevented by planning and installing an internal intrusion detection system (IDS) in the organization.

2. **External Attack:** When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber-attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log generated by the firewalls as external attacks can be traced out by carefully analyzing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

- Unstructured attacks: These attacks are generally performed by amateurs who don‘t have any predefined motives to perform the cyber-attack. Usually these amateurs try to test a tool readily available over the internet on the network of a random company.
- Structure Attack: These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems (IDSs). Moreover, these attackers have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival

countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

2.2.2 Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

a) **Money:** People are motivated towards committing cyber crime is to make quick and easy money.
b) **Revenge:** Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
c) **Fun:** The amateur do cyber-crime for fun. They just want to test the latest tool they have encountered.
d) **Recognition:** It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
e) **Anonymity:** Many time the anonymity that a cyber space provide motivates the person to commit cyber-crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.
f) **Cyber Espionage:** At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

It is much easier to get away with criminal activity in a cyber-world than in the real world. There is a strong sense of anonymity that can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.

2.3 KINDS OF CYBER CRIME

This section describes various types of cyber-crimes. Some of the important ones are:

2.3.1 Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behaviour includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

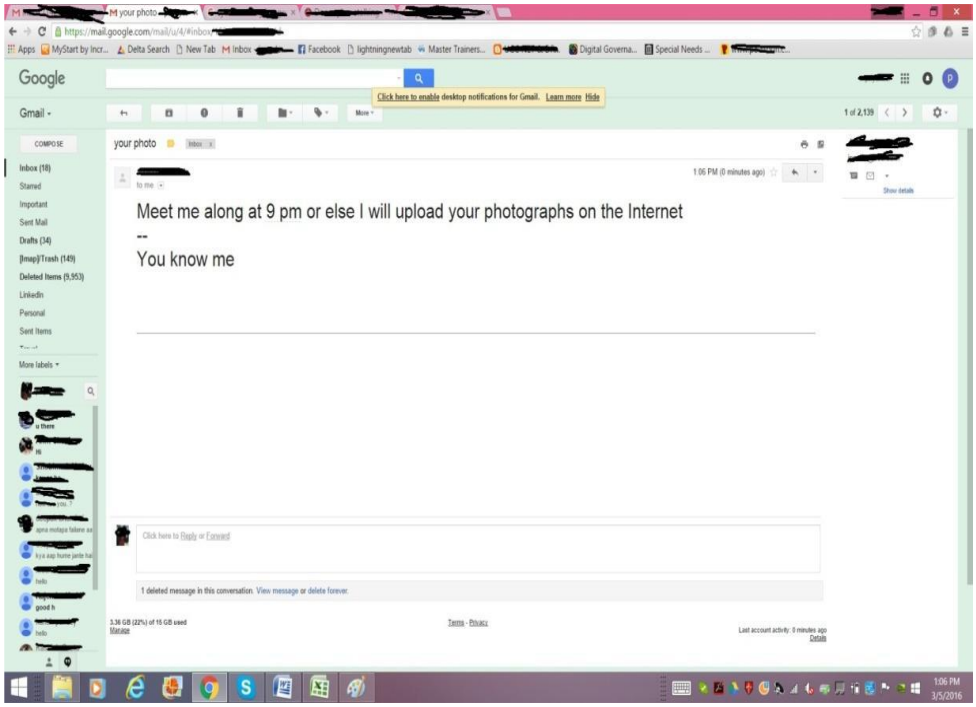


Fig: Sample stalking email

2.3.2 Child Pornography

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct. Nowadays, internet use and access is becoming increasingly common as a great entertainment, communication and educational resource for children as well as for adults39. Internet is a perfect environment for children, for exploring the world, learning and having fun. However, accesses to illegal sites that contain violence and sexuality, and contact dangerous people are among the particular risks for children using the internet. It is a known fact that, internet and developing technology make the production and distribution of child pornography cheaper and easier.

2.3.3 Forgery and Counterfeiting

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgment.

Surcharge Forgery Genuine Surcharge

2.3.4 Software Piracy and Crime related to IPRs

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

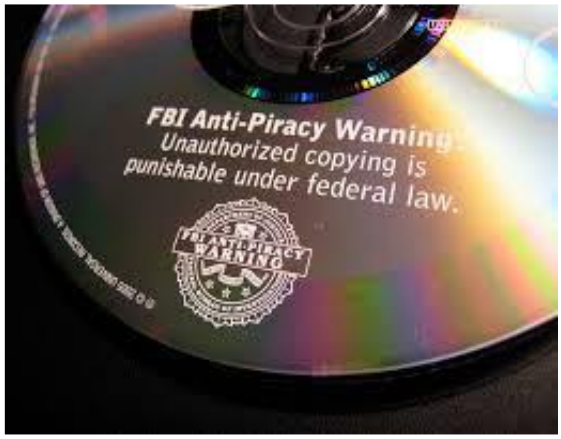


Fig: FBI warning for anti-software piracy

2.3.5 Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives. It is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses42. Cyber terrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this can be seen as a form of terrorism.

2.3.6 Phishing

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as Vishing (voice phishing). Another form of phishing is Smishing, in which sms is used to lure customers.

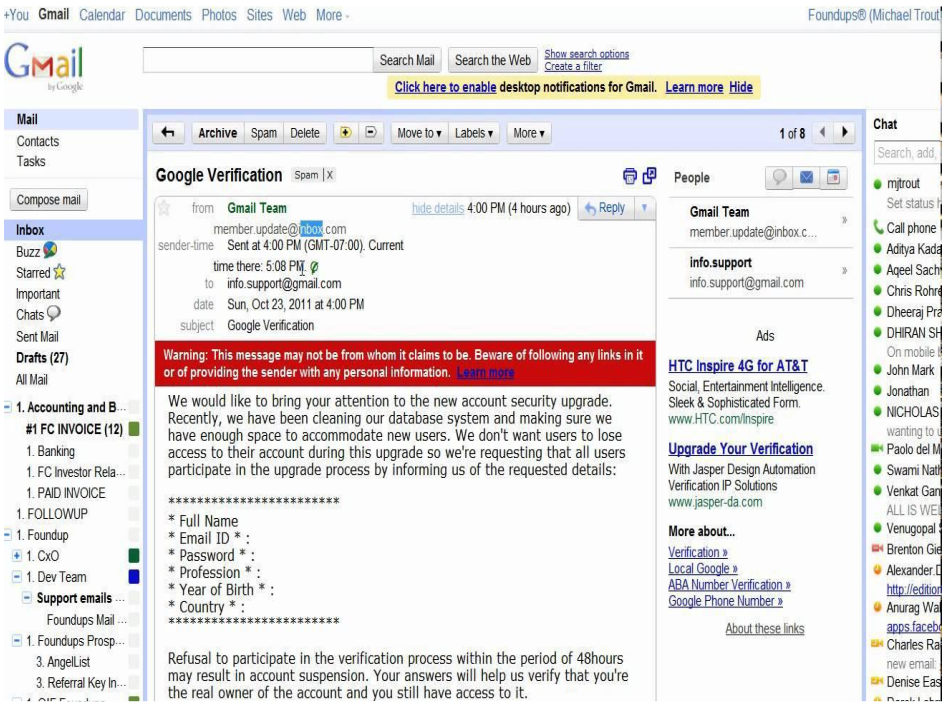


Fig: Phishing

2.3.7 Computer Vandalism

Vandalism is action involving deliberate destruction of or damage to public or private property. The term also includes criminal damage such as graffiti and defacement directed towards any property without permission of the owner. The term finds its roots in an Enlightenment view that the Germanic Vandals were a uniquely destructive people. Computer Vandalism is an act of physical destroying computing resources using physical force or malicious code.

Fig: Broken computer screen due to the act of vandalism

2.3.8 Computer Hacking

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator‘s original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities. The hackers may be classified as:

- White Hat: white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.
- Black Hat: in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions.
- They find the security loopholes the system, and keep the information themselves and exploit the system for personal or organizational benefits till organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.
- Grey Hat: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

2.3.9 Creating and distributing viruses over internet

A Computer virus46 is a parasitic program written intentionally to enter a computer without the user's permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some viruses do little but replicate others can cause serious damage or effect program and system performance. A virus should never be assumed harmless and left on a system–Symantec. Five most common types:

1. Macro virus - this type of virus usually comes as part of a document or spreadsheet, often in email.
2. Boot sector virus - this type of virus overwrites the boot sector on your hard drive or floppy drive.
3. File infector virus - this type of virus attaches itself to executables, for example .com and .exe files.
4. Stealth virus - this type of virus tries to fool antivirus software by catching its requests tothe operating system (asking to open a file, for example).
5. Self-modifying virus - this type of virus was designed to avoid detection by antivirus software by changing itself internally.

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

2.3.10 Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming. An email can be classified as spam, if it meets following criteria:

a) Mass mailing: - the email is not targeted to one particular person but to a large number of peoples.

b) Anonymity: - The real identify of the person not known.

c) Unsolicited: - the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

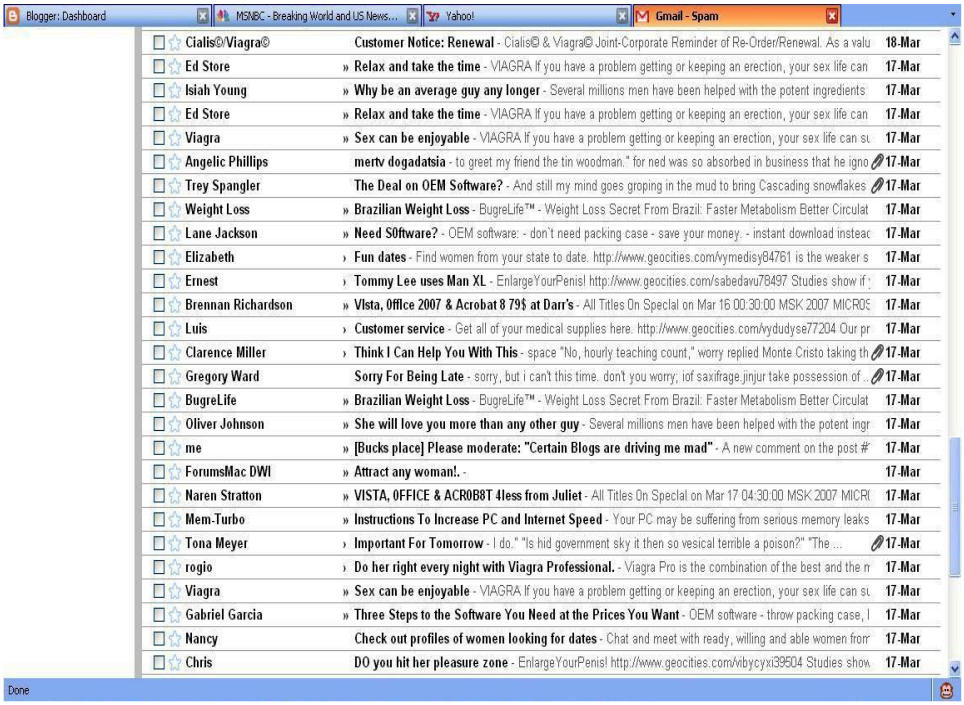


Fig: Spam mail

2.3.11 Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.

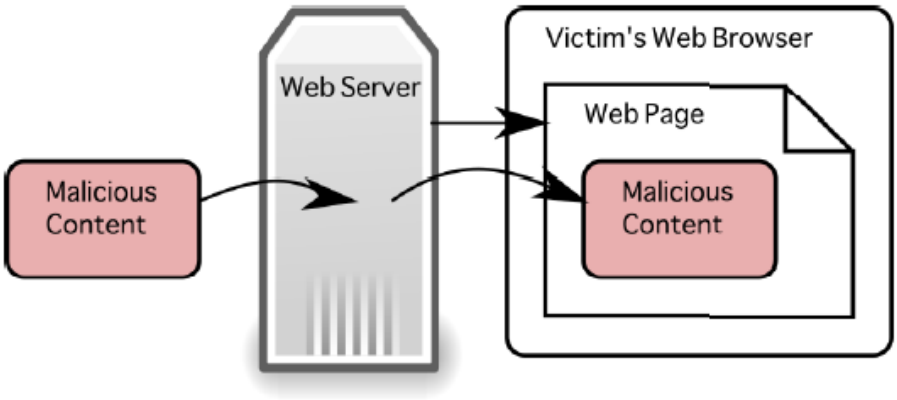


Fig: Cross site scripting process

2.3.12 Online Auction Fraud

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either

overpayment of the product or the item is never delivered once the payment is made.

2.2.13 Cyber Squatting

It is an act of reserving the domain names of someone else‘s trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price

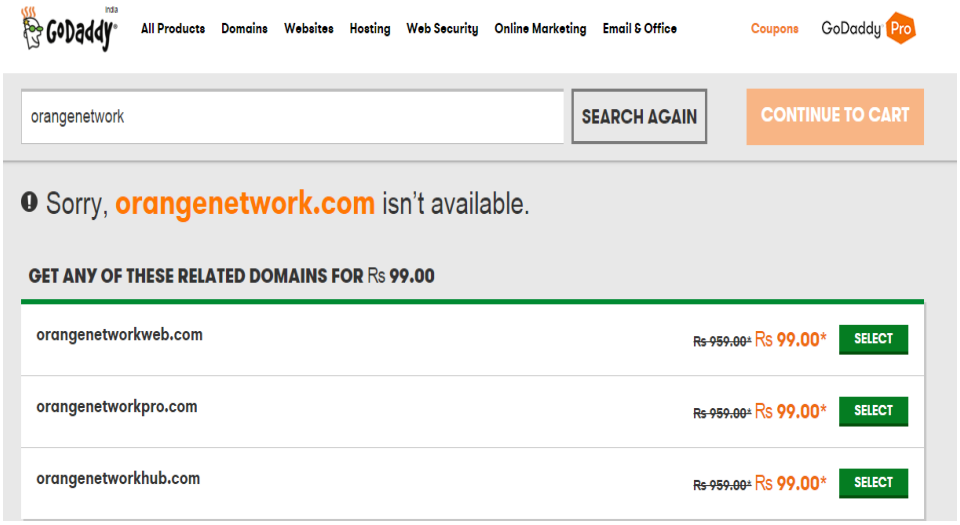


Fig: Cyber squatting

2.3.14 Logic Bombs

In a computer program, a logic bomb50, also called slag code (because all that's left after it detonates is computer slag), is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company. To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software.

It's secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs. This event might be a positive trigger, such as a

specific date. Trojans that activate on certain dates are often called "time bombs". Negative triggers are considered to be more dangerous than positive ones, since the risk of accidentally triggering the bomb increases dramatically.
A logic bomb could also be programmed to wait for a certain message from the programmer. The logic bomb could, for example, check a web site once a week for a certain message. When the logic bomb sees that message, or when the logic bomb stops seeing that message, it activates and executes its code. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects. Because a logic bomb does not replicate itself, it is very easy to write a logic bomb program. This also means that a logic bomb will not spread to unintended victims. In some ways, a logic bomb is the most civilized programmed threat, because a logic bomb must be targeted against a specific victim.

2.3.15 Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

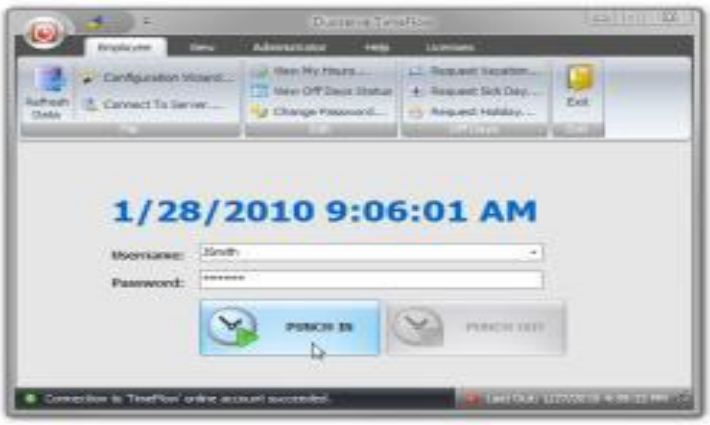


Fig: Steeling other's username and password for internet access.

2.3.16 Web Jacking

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India in 2014.

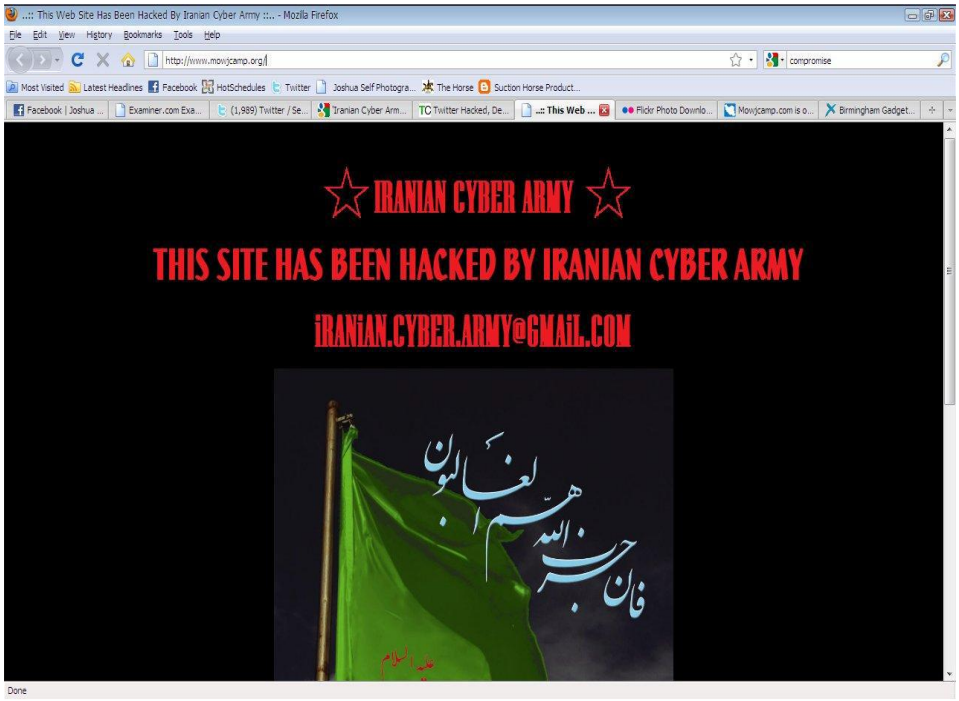


Fig: Web jacking by Iranian hackers

2.3.17 Denial of Service Attack

It is a cyber-attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

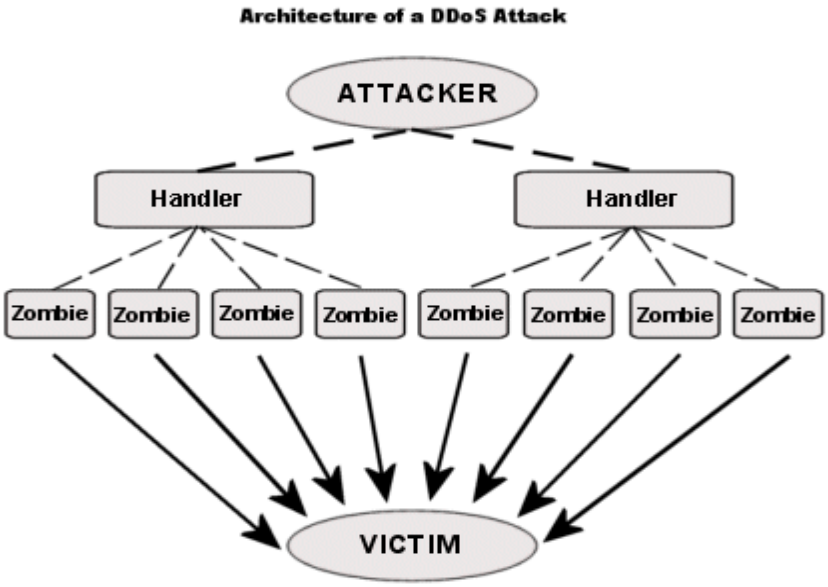


Fig: Denial of Service attack

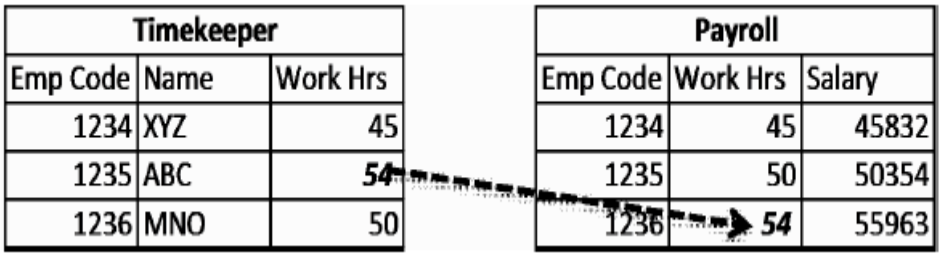
2.3.18 Salami Attack

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example

of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

2.3.19 Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report. The example below shows how Employee numbers were switched so overtime was credited to wrong employee.



Timekeeper		
Emp Code	Name	Work Hrs
1234	XYZ	45
1235	ABC	54
1236	MNO	50

Payroll		
Emp Code	Work Hrs	Salary
1234	45	45832
1235	50	50354
1236	54	55963

Fig: Example of data diddling

2.3.20 Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

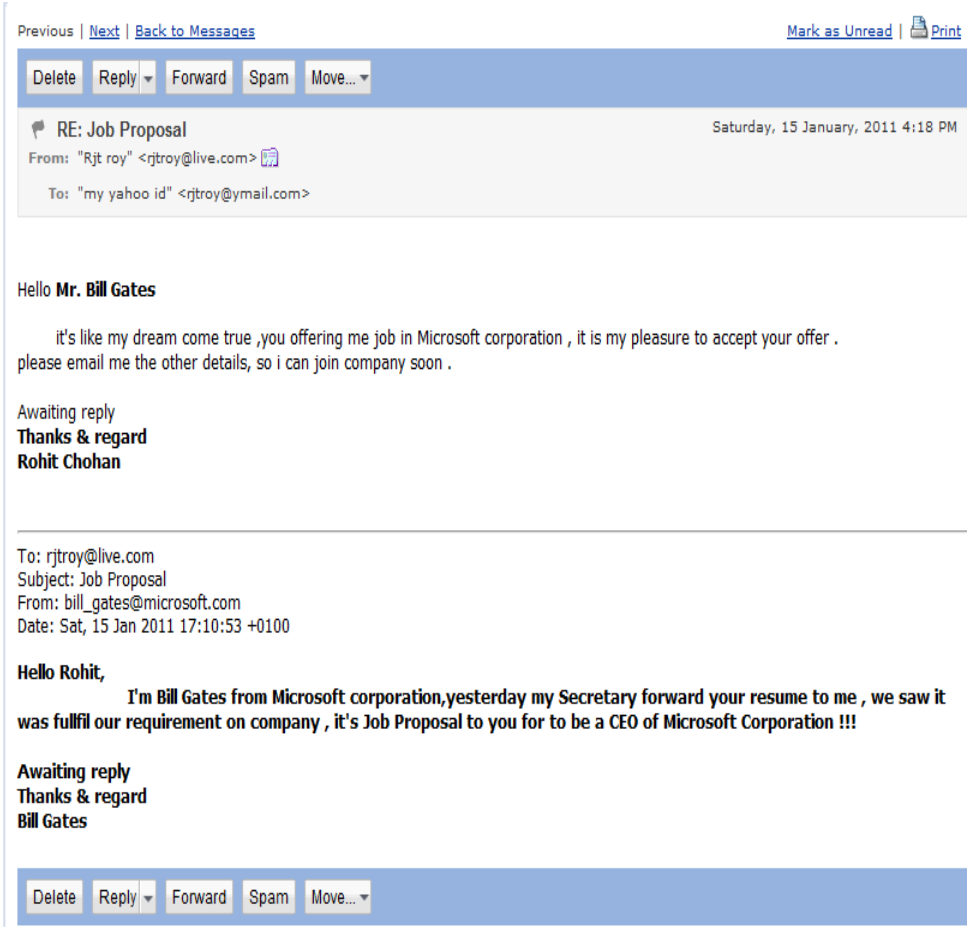


Fig: Example of email spoofing

2.4 CYBER CRIME AND CYBER TERRORISM

Cyber criminals perform various acts like cyber stalking, on-line harassment, on-line defamation, hacking, and so forth collectively we call it cybercrime58. When these activities are managed by organized group systematically and deliberately we term it as CYBER TERRORISM. Cyber terrorism is a well-planned and organized use of technologies by cyber experts resides inside and outside the country for anti-national activities. We can divide these activities as follows:

1. Crime against a Person- These types of crimes are targeted towards a person.
2. Crime against a Nation- These types of crimes are targeted towards a Nations or groups of nations following same ideology.

2.5 SUMMARY

1. Cyber stacking is an act of stalking, harassing or threatening someone using Internet/computer as a medium.
2. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgment.
3. Hacking is a practice of modifying computer hardware and software to accomplish a goal outside the creator‘s original purpose.
4. The spreading of a virus can cause business and financial loss to an organization.
5. The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest.
6. Salami attack is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed.

2.6 CHECK YOUR PROGRESS

A. Fill in the blanks.

1. _____ is an illegal reproduction and distribution for personal use or business.
2. If a telephone is used as a medium for identity theft, it is known as _____.
3. _____ hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers.
4. _____ is an act of reserving the domain names of someone else‘s trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.
5. _____ is a cyber-attack in which the network is chocked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.
6. _____ Virus usually comes as part of a document or spreadsheet, often in email.

2.7 MODEL QUESTIONS

1. Mention the names of different types of cyber-crimes.
2. What is cyber stalking?
3. What is phishing?
5. What is spamming? Define the criteria based on which an email can be classified as spam.
6. What is computer virus? Define various type of virus.
7. What is cross site scripting?

2.8 ANSWERS TO CHECK YOUR PROGRESS

1. Software piracy
2. Vishing (voice phishing)
3. White hat
4. Cyber Squatting
5. Denial of service attack
6. Macro

2.9 REFERENCES AND SUGGESTED REDINGS

1. Study Material "Fundamentals of Information Security, (PGDCS-01), Certificate in e-Governance and Cyber Security", Uttrakhand Open University, Haldwani, made available under a Creative Commons Attribution Share-Alike 4.0 Licence (International), http://creativecommons.org/licenses/by-sa/4.0/

UNIT-3 HACKING: ETHICAL ISSUES

UNIT STRUCTURE

3.0 INTRODUCTION

Hacking is any technical effort to manipulate the normal behavior of network connections andconnected computers or systems. A hacker is any person engaged in hacking.

Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. Those individuals who engage in computer hacking activities are typically referred to as "hackers."

The majority of hackers possess an advanced understanding of computer technology. The typical computer hacker will possess an expert level in a particular computer program and will have advanced abilities in regards to computer programming.

Unlike the majority of computer crimes which are regarded as clear cut in terms of legality issues, computer hacking is somewhat ambiguous and difficult to define. In all forms, however, computer hacking will involve some degree of infringement on the privacy of others or the damaging of a computer-based property such as web pages, software, or files.

3.1 LEARNING OBJECTIVES

After going through this unit you will understand

- What is the meaning of hacking?
- Who is a Hacker?
- What are different ways of hacking?
- What are different types of hackers?
- What are the tools and techniques of hacking?
- What are the ways to prevent computer hacking?

3.2 WHAT IS HACKING?

Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose.

3.3 WHO IS A HACKER?

A **security hacker** is someone who seeks to breach defences and exploit weaknesses in a computer system or network. Hackers may be motivated by a multitude of reasons, such as profit, protest, challenge, recreation, or to evaluate system weaknesses to assist in formulating defences against potential hackers. The subculture that has evolved around hackers is often referred to as the computer underground.

A hacker may be defined as any person who enjoys exploring the intricacies of programmable systems and how to stretch their capabilities. This definition is held in contrast to a generic computer user, who prefers to access a computer's minimal functions;

One who programs or who enjoys programming, as opposed to those individuals who simply theorize about programming;

An individual who possesses exceptional skill regarding computer programming;

A malicious meddler, who attempts to discover and subsequently tamper with sensitive information through poking around computer-based technologies,. These individuals are commonly referred to as "network hackers" or "password hackers."

Regardless of the definition, there are unwritten rules or principles that a hacker will ultimately live by. The belief that information sharing is a powerful exercise and that is the ethical duty of hackers to share their expertise through the creation of free software and through facilitating access to information and to computing resources is a fundamental code for which the majority of hackers follow. In addition, computer hacking as a practice revolves around the belief that system-cracking as a hobby or for fun is ethically okay so long as the hacker commits no vandalism, theft, or a breach of confidentiality.

3.4 DIFFERENT WAYS OF HACKING

Hackers follow different ways of techniques for hacking, including:

- Vulnerability scanner: checks computers on networks for known weaknesses
- Password cracking: the process of recovering passwords from data stored or transmitted by computer systems
- Packet sniffer: applications that capture data packets in order to view data and passwords in transit over networks
- Spoofing attack: involves websites which falsify data by mimicking legitimate sites, and they are therefore treated as trusted sites by users or other programs
- Root kit: represents a set of programs which work to subvert control of an operating system from legitimate operators
- Trojan horse: serves as a back door in a computer system to allow an intruder to gain access to the system later
- Viruses: self-replicating programs that spread by inserting copies of the same program into other executable code files or documents
- Key loggers: tools designed to record every keystroke on the affected machine for later retrieval.

3.5 HACKING: ETHICAL ISSUES

Computer hacking possesses a mixed perception. Due to our reliance on computer technologies and the critical information shared on networks, the art of computer hacking has been skeptically viewed. That being said, there is also a "Robin Hood" mentality attached to the practice, where free programs or facilitated measures have been awarded to the average computer user.

The primary issue attached to computer hacking stems from an individual's ability to access crucial or personal information that is found on a computer network. The ability to retrieve and subsequently tamper with such information will give way to the potential to commit heinous criminal acts.

3.6 NATURE AND CULTURE OF A HACKER

To be accepted as hacker one should have the attitude, behave as though one have the attitude,and belief in that. Some of them can be listed as follows:

- Strong zeal to learn and obtain more knowledge
- Breaking law
- Anonymity
- Stealing confidential information.

3.7 TYPES OF HACKERS

Hackers can be classified in to the following types based on their depth of knowledge andactivities.

a) **White Hats**: White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.

b) **Black Hats**: Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious. This is the traditional definition of a hacker and what most people consider a hacker to be.

c) **Gray Hats:** Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between

hacker and cracker. Grayhat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools.

d) **Suicide Hackers:** Individuals who will aim to bring down the critical infrastructure whatever the consequence may be.

e) **Script Kiddies:** In hacker culture a script kiddie or skiddie are unskilled individuals who use scripts or programs developed by others to attack computer systems and networks and deface websites. It is generally assumed that script kiddies are juveniles who lack the ability to write sophisticated hacking programs or exploits on their own, and that their objective is to try to impress their friends or gain credit in computer-enthusiast communities. The term is typically intended as an insult.

f) **Hacktivist:** Detects and sometimes reports or exploits security vulnerabilities as a form of social activitism. A hacktivist is a hacker who utilizes technology to announce a social ideological, religious or political message. In general most hacktivism involve defacement or denial of service attacks. Hacktivits are also known as Neo hackers

g) Nation state: Intelligence agencies and cyberwarfare operatives of nation states.

h) **Organized criminal gangs:** Groups of hackers that carry out organized criminal activities for profit.

3.8 HACKING TOOLS AND TECHNIQUES

There are several recurring tools of the trade and techniques used by computer criminals and

security experts used as per the situation. Some of the prominent ones are:

a) **Security exploit**: A security exploit is a prepared application that takes advantage of a known weakness. A common example of a security exploit is an SQL injection, which abuses security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some webpages. These are very common in website/domain hacking.

b) **Vulnerability scanner**: A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Note that firewalls defend computers from intruders by limiting access to ports/machines both inbound and outbound, but can still be circumvented).

c) **Packet sniffer**: A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

d) **Spoofing attack**: A spoofing attack involves one program, system, or website successfully masquerading as another by falsifying data and thereby being treated as a trusted system by a user or another program. The purpose of this is usually to fool programs, systems, or users into revealing confidential information, such as user names and passwords, to the attacker.

e) **Rootkit:** A rootkit is designed to conceal the compromise of a computer's security, and can represent any of a set of programs which work to subvert control of an operating system from its legitimate operators. Usually, a rootkit will obscure its installation and attempt to prevent its removal through a subversion of standard system security. Rootkits may include replacements for system binaries so that it becomes impossible for the legitimate user to detect the presence of the intruder on the system by looking at process tables.

f) **Social engineering**: Social Engineering is the art of getting persons to reveal sensitive information about a system. This is usually done by impersonating someone or by convincing people to believe you have permissions to obtain such information.

g) **Trojan horse:** A Trojan horse is a program which seems to be doing one thing, but is actually doing another. A Trojan horse can be used to set up a back door in a computer system such that the intruder can gain access later

h) **Virus:** A virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents. Therefore, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. While some are harmless or mere hoaxes most computer virus are considered malicious.

i) **Worm:** Like a virus, a worm is also a self-replicating program. A worm differs from a virus in that it propagates through computer networks without user intervention. Unlike a virus, it does not need to attach itself to an existing program.

j) **Key loggers**: A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. Some key loggers uses virus-, Trojan, and rootkit-like methods to remain active and hidden.

k) **Client side attacks:** These are attacks that target vulnerabilities in client applications that interact with a malicious server or process malicious data.

Here, the client initiates the connection that could result in an attack. Following are some techniques used for client side attacks.

- Phishing
- Cross Site Scripting (XSS)
- Man in the Middle Attack (MITM)
- Pharming
- Malware Web Page
- Trojan Horse Program
- Botnets

l) **Phishing:** Phishing is a type of Internet fraud that seeks to acquire a user‘s credentials by deception. It includes theft of passwords, credit card numbers, bank account details and other confidential information.

m) **Vishing:** Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Criminals also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on ―social engineering techniques to trick you into providing information that others can use to access and use your important accounts.

3.9 WAYS TO PREVENT COMPUTER HACKING

Educational institutions must clearly establish use policies and delineate appropriate and inappropriate actions to all individuals who access information via a computer. The use of filters or firewalls may be considered to reduce access to unauthorized software serial numbers and other hacking-related materials.

Precaution measures like Intrusion detection systems and strong testing mechanisms like penetration testing are required to avoid hacking of websites and other software systems.

3.10 CHECK YOUR PROGRESS

A. Fill in the blanks

1. Those individuals who engage in computer hacking activities are typically referred to as _____.
2. _____hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement countermeasures.
3. _____ are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes.
4. _____ is the art of getting persons to reveal sensitive information about a system.
5. Individuals who will aim to bring down the critical infrastructure whatever the consequence may be are called_____.

3.11MODEL QUESTIONS

1. What is the meaning of hacking?
2. Who is a Hacker?
3. What are different types of hackers?
4. Write the names of different tools and techniques of hacking?
5. Mention different ways in which you can prevent computer hacking?

3.12ANSWER TO HECK YOUR PROGRESS

1. Hackers
2. White Hat
3. Black Hat
4. Social Engineering
5. Suicide Hackers

3.13 REEFERENCES AND SUUGGESTED READING

1. Study Material "Information System(CEGCS-04), Certificate in e-Governance and Cyber Security", Uttrakhand Open University,Haldwani, made available under a Creative Commons Attribution Share-Alike 4.0 Licence (International), http://creativecommons.org/licenses/by-sa/4.0/
2. http://cyber.laws.com/hacking
3. https://www.techopedia.com/definition/26361/hacking
4. https://en.wikipedia.org/wiki/Security_hacker

3.14 GLOSSARY

1. **Information security** (sometimes shortened to InfoSec), as the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
2. **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
3. **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
4. **Availability:** Ensuring timely and reliable access to and use of information.
5. **Threat:** A threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
6. **Attack:** An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.
7. **Vulnerability:** This is a weakness in a system that can be attacked and used as an entry point into an environment.
8. **Masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attack.
9. **Backdoors** – Backdoors4 is bypassing normal authentication. Backdoor is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system? This threat can turn out to be potentially serious as it allows for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer.
10. **Denial-of-Service Attack** – A denial-of-service (DoS) attack is attacking the network to bring it down completely with useless traffic by affecting the host device which isconnected to the Internet. DoS attack targets websites or services which are hosted on the servers. This type of attack can aim bank servers and credit card payment gateways.
11. **Direct-access Attack** – A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security.

The attacker can install software loaded with worms or download important data, using portable devices.

12. **Eavesdropping** – As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network.
13. **Spoofing** – Spoofing is a cyber-attack where a person or a program impersonates another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender‘s address is spoofed.
14. **Tampering** – Tampering is a web based attack where certain parameters in the URL are changed without the customer‘s knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.
15. **Repudiation Attack** – A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.
16. **Information Disclosure** – Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements that are not trustworthy.
17. **Privilege Escalation Attack** – A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.
18. **Exploits –** An exploit attack is basically software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.
19. **Social Engineering** – An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.
20. **Indirect Attack** – Indirect attack means an attack launched from a third party computer as it becomes more difficult to track the origin of the attack.
21. **Computer Crime** – A crime undertaken with the use of a computer and a network is called as a computer crime.

22. **Malware** – Malware refers to malicious software that is being designed to damage or perform unwanted actions into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer‘s hard drive. They can either delete some files or a directory or simply gather data without the actual knowledge of the user.

23. **Adware** – Adware is software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.

24. **Bots** – Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be malicious, but they are usually found to initiate a DoS attack or a click fraud while using the internet.

25. **Ransom-ware** – Ransom ware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.

26. **Rootkits** – A rootkit is malicious software designed in such a way that hides certain process or programs from normal anti-virus scan detection and continues to enjoy a privilege access to your system. It is that software which runs and gets activated each time you boot your system and are difficult to detect and can install various files and processes in the system.

27. **Spyware** – Spyware, as the name suggests, is a software which typically spies and gathers information from the system through a user‘s internet connection without the user‘s knowledge. Spyware software is majorly a hidden component of a freeware program which can be downloaded from the internet.

28. **Scareware** – Scareware is a type of threat which acts as a genuine system message and guides you to download and purchase useless and potentially dangerous software. Such scareware pop-ups seem to be similar to any system messages, but actually aren‘t. The main purpose of the scareware is to create anxiety among the users and use that anxiety to coax them to download irrelevant software.

29. **Trojan Horses** – Trojan Horses are a form of threat that are malicious or harmful codes hidden behind genuine programs or data which can allow complete access to the system and can cause damage to the system or data corruption or loss/theft of data. It acts as a backdoor and hence it is not easily detectable.

30. **Virus** – A computer virus is a self-replicating program which, when executed, replicates or even modifies by inserting copies of itself into another computer file and infects the affected areas once the virus succeeds in replicating. This virus can be harmful as it spreads like wildfire and can infect majority of the system in no time.

31. **Worm** – Just like a virus, worm is a self-replicating program which relies on computer network and performs malicious actions and spreads itself onto other computer networks. Worms primarily rely on security failures to access the infected system.

32. **Phishing** – Phishing is a cyber-threat which makes an attempt to gain sensitive information like passwords, usernames and other details for malicious reasons. It is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

33. **Identity Theft** – Identity theft is a crime wherein your personal details are stolen and these details are used to commit a fraud. An identity theft is committed when a criminal impersonates individuals and use the information for some financial gain.

34. **Intellectual Property Theft** – Intellectual Property theft is a theft of copyrighted material where it violates the copyrights and the patents. It is a cybercrime to get hands onto some trade secrets and patented documents and research. It is basically a theft of an idea, plan and the methodology being used.

35. **Password Attacks** – Password attack is a form of a threat to your system security where attackers usually try ways to gain access to your system password. They either simply guess the password or use an automated program to find the correct password and gain an entry into the system.

36. **Bluesnarfing** – Bluesnarfing is a threat of information through unauthorized means. The hackers can gain access to the information and data on a Bluetooth enabled phone using the wireless technology of the Bluetooth without alerting the user of the phone.

37. **Blue jacking** – Bluejacking is simply sending of texts, images or sounds, to another Bluetooth enabled device and is a harmless way of marketing. However, there is a thin line between bluejacking and bluesnarfing and if crossed it results into an act of threat.

38. **DDoS** – DDoS basically means a Distributed Denial of Service. It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.

39. **Key-logger** – A key logger is a spyware that has the capability to spy on the happenings on the computer system. It has the capability to record every stroke on the keyboard, web sites visited and every information available on the system. This recorded log is then sent to a specified receiver.

40. **Cyber security** deals with the following aspects.
    a. Securing cyber space
    b. Preventing cyber attacks
    c. Reducing national vulnerability to cyber-attacks.
    d. Minimizing damage and recovery time from cyber attacks
    e. Capacity building