Chapter = 05

Computer Security and Ethics

Q1. What do you know about computer security?

COMPUTER SECURITY

The computer has become an important part of our life. We store important data on our computers in the shape of documents, pictures, programs, etc. Therefore, we expect that all our information must remain safe and our computer runs properly without any problem. Few threats can cause problems for our computers. These threats may be different types of viruses or unauthorized use of a computer. To prevent our computer from such threats, we need to abide by computer security. Computer security is the protection against theft or damage to our computer hardware, software and information present on it.

Q2. Why computer security is important

Importance of Computer Security

Computer security is important for our computer's overall health. It keeps our information protected and helps prevent viruses and malware, which allows programs to run quicker and smoother. It safeguards confidential and sensitive information

Q3. What is cyber crime

Cybercrime

Cybercrime is the crime that is committed through a computer and network. Cybercriminal uses devices to gain unauthorized access to important information. Stealing passwords and important information, hacking social media accounts, accessing anyone else's account and making transactions, committing online frauds are some of the examples of cybercrime. Cybercrime is illegal and also punishable. According to Pakistan's Cybercrime Law, any offender who interrupts the privacy of a person or organization and harms their repute may be sent to jail for three to five years including a heavy fine.

Q4. What do you know about hacker and crackers?

HACKERS

Hacker can be a person who has in-depth knowledge of computer systems, networks, and programs. Hacker maybe someone who uses his or her extensive skills to identify and overcome a network loophole. Hackers constantly seek further knowledge and freely share what they have discovered. Hackers are generally considered as bad people however, hackers can also help us to improve the data and network security

CRACKERS

Crackers are persons who gain unauthorized access to another system. They bypass passwords or licenses of computer programs, change source code or intentionally breach computer security. They do it with negative intentions. Crackers can also make targeted system unavailable or non-functional. They commit these activities generally for money but they may do it for fame or just for challenge or fun.

Q5. List some computer crimes (cyber crime) in real life.

There are many genres of computer crime or now called cyber-crimes. Some examples are

1. Hacking
2. Credit and Debit Card Scam
3. Phishing
4. Clickjacking
5. Cyber Bullying or Harassment

Hacking

Hacking is perhaps the most common crime in the computer world. Hackers can steal our WiFi, email or social media accounts' passwords. Hackers also attack a website and take it down. However, the scope of hacking is much wider. The

hackers can also steal sensitive information from government and business organizations, make fraudulent transactions and erase data on the cloud or network computers.

Credit and Debit Card Scam

Keeping debit or credit cards is a common practice but insecure use of these cards can be dangerous. If a person has information about our debit or credit card he or she can make fraudulent transactions. There are various ways to get this information. One way is through scamming. Scammers set small machines inside an ATM or credit card machine. These machines copy the data which is then misused by the scammers. Debit and credit cards are also secured with PIN codes. User has to keep this code secret otherwise any person can use the card for online shopping and other purposes.

Phishing

Phishing is a method of trying to gather personal information using false e-mails and websites. In Phishing, perpetrators contact the target person through email, telephone or text message and pose as a legitimate and trusted individual. He or she asks the target to provide sensitive data such as personally identifiable information, banking and credit card details and passwords for different reasons. The information is then used to access different accounts and can result in identity theft and financial loss.

Clickjacking

Have you ever seen any video tagged as “OMG? You won't believe what this boy has done!” or did you nd a button on a website that asked to click to claim a reward you had never applied for? This is a kind of fraud which is called Clickjacking. Usually, culprits target children or novice internet users to click on a link containing malware or trick them into sharing private information via social media sites.

Cyber Bullying or Harassment

Electronic means like a computer, mobile phone or internet are also used for online bullying or harassment. Harmful bullying behavior can include posting rumors, threats, passing inappropriate remarks, leaking personal information,

blackmailing and committing hate speech. The perpetrator does it with the intent to cause harm to the victim. Victims may experience lower self-esteem, intent to commit suicide and a variety of negative emotional responses, including being scared, frustrated, angry and depressed.

Q6. What is malware? Name and discus different malware.

MALWARE

The term malware is the contraction of malicious software. Malware is a broad term that encompasses computer viruses, worms, spyware, adware and others. Malware is a program that is written generally to cause a mess. They can be so dangerous that they can also damage devices.

(i) Computer Virus
(ii) Worm
(iii) Adware

(v) Spyware

(i) Computer Virus

A computer virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user's knowledge. It can also modify other computer programs, insert its own code and change computer settings. Viruses are harmful. Viruses generally latch on a host file and when they execute they infect other files or programs.

Example

Boot Sector, Resident, Macro Viruses and File Infector

(ii) Worm

A computer worm spreads copies of itself from computer to computer. A worm can replicate itself without any human interaction. It does not need to attach itself to a file or program to cause damage. It can do several malicious tasks, such as dropping other malware, copying itself onto devices physically attached to the affected system, deleting files, and consuming internal storage and memory resources.

(iii) Adware

Adware is advertising-supported software. They present endless ads and pop-up windows that could potentially consume memory and processing resources. Adware can also change the different settings of
internet browsers like homepage and default search engine. Normally, these are not as dangerous as other malware.

(iv) Spyware

Spyware is a malware that monitors a device and steals important information about a person or organization without their consent and sends such information to another person or organization. Spyware takes control over a mobile phone or computer without the user's knowledge. They capture information like web browsing history, e-mail messages, usernames and passwords and online payment information.

Q7. What is antivirus? Name Some antivirus software

1. Avast
2. Norton
3. McAfee

Q8. What are the types of Security Mechanism?

(i) Username and Password:

A username and password are the pair of keywords known by the user. They are presented to the computer to authenticate the user. Usernames and passwords are the default authentication mechanism on the web today. However, recent large scale computer attacks have made usernames and passwords an unacceptable authentication mechanism.

Personal Identification Number

PIN stands for Personal Identification Number. It is a security code for verifying your identity. Similar to a password, your PIN should be kept secret because it allows access to important services such as financial transactions and

confidential emails. The PIN provides security when a credit/debit card is lost or stolen because the PIN must be known before making money withdrawal or transfer.

Biometric Verification

Unlike authentication processes, biometrics verification makes sure that the real person gets access to the data or device. Biometric authentication relies on the unique biological characteristics of a person. Biometric authentication systems captures data in real-time and compare it with existing data in database. If both samples of the biometric data match, authentication is confirmed. Scanning fingerprints are the most common way of biometric.

Q9. What is Intellectual Property Right?

Intellectual Property Right

When any person develops software, writes a book or research paper or invents any method or the machine, it becomes the intellectual property of that person. Intellectual property is intangible creations of the human intellect. Just like other property the intellectual property can be stolen. To prevent theft or illegal use or spread of intellectual property, Intellectual Property Right is exercised. Through these rights, intellectual property is protected with the help of copyrights, patents, and trademarks.

Q10. What do you know about patent, copyright and trademark?

(i) Patent

A patent is a grant of exclusive rights for an invention to make, use and sell the invention for a limited period, in Pakistan 20 years. Owning a patent gives the patent holder the right to stop someone else from making, using or selling his or her invention without permission.

(ii) Copyright

Copyright is a legal instrument that provides legal rights to the creator of artwork, literature, or a work that conveys information or ideas. In simple words, copyright is the right of copying. Copyright gives control over how the

work is used. The © sign is also often displayed on copyrighted objects.

(iii) Trademark

Trademark identifies a product or service and distinguishes it from other products and services. Trademarks are protected by intellectual property rights which identifies that the product or service belongs to a specific organization. It can be an easily recognizable word, phrase, logo, or symbol and often mentioned as TM (Trade Mark).

Q11. Write short note on software piracy.

Software Piracy

Software piracy is referred to the illegal use, copying or distribution of copyrighted software. Software piracy is a huge threat to the software industry. It causes a significant loss of revenue for developers and vendors. Since they earn less profit, they are forced to pass these costs on to their customers.

Software companies have tried various techniques to stop software piracy but most of them have remained unsuccessful. They applied for copy- protection which demands the user to enter certain keys or credentials. Today, most software require registration which is mainly online. However, these measures could not stop software piracy.
Using pirated software is also risky for users. Aside from the legal consequences of using pirated software, users of pirated software lose some practical benefits as well. Pirated software may not work properly or stop working at any time.

Q12. What is plagiarism?

Plagiarism

Plagiarism is presenting someone else's work or ideas as your own without full acknowledgment to the author or conceiver. Academic honesty demands that the users of any ideas, words and data should
acknowledge the originators. Plagiarism is unethical and can have serious consequences. Colleges and universities encourage students to submit their

original work and cite the ideas and words borrowed from any other sources. Failing to this may cause serious penalties. There are online services to check and FIx the plagiarism issues. Academic organizations hire the plagiarism detection service. One of the most used services is Turnitin.