Exercise

A. Multiple choice questions
1. Which of the following is not an external threat to a computer or a computer network
   (a) Ignorance     (b) Trojan horses     (c) Adware     (d) Crackers

2. When a person is harassed repeatedly by being followed, called or be written to he / she is a target of
   (a) Bullying     (b) Identity theft     (c) Stalking     (d) Phishing

3. With genetic and genomics research which of the following issues is of specific concern
   (a) Anonymity     (b) Intellectual property
   (c) Software piracy     (d) Concerns about biochip implants

4. Which of the following is a class of computer threat
   (a) Phishing     (b) DoS attacks     (c) Soliciting     (d) Stalking

5. A license allows a user to use copyrighted material.
   (a) True     (b) False

6. It is a program or hardware device that filters the information coming through an internet connection to a network or computer system.
   (a) Anti virus     (b) Firewall     (c) Cookies     (d) Cyber safety

7. It allow a visited website to store its own information about a user on the user’s computer.
   (a) Spam     (b) Malware     (c) Cookies     (d) Adware

8. It is stealing ideas or creations of others.
   (a) Plagiarism     (b) Piracy     (c) Intellectual Property Rights     (d) All of the above

9. Hacking a computer is always illegal and punishable by law.
   (a) True     (b) False

10. Exploring appropriate and ethical behaviors related to online environments and digital media.
    (a) Cyber ethics     (b) Cyber safety     (c) Cyber security     (d) Cyber law

11. A license allows a user to use copyrighted material.
    (a) In some situations this statement is correct     (b) This statement is not true at all.
    (c) In is not necessary to use license.     (d) All the above statements are not applicable.

B. Answer the following questions:
Q1. Differentiate between a workstation license and a site license.
   Ans. Workstation licenses: are licenses that permit the installation of an application on a single computer. Before installing it on a different machine the software must be removed from the first machine.

   Site licenses: permit the use of software on any computer at a specified site. Unlimited site licenses allow the installation of the software on any number of computers as long as those computers are located at the specified site.

Q2. Write a short note on your understanding of ‘cracking’ a software.
Cracking a software means to copy commercial software illegally by breaking the various copy-protection and registration techniques being used. Crackers also modify or disable features of a software application. They usually mean to harm the software, the hardware using this software or the end user of the software.

Q3. What are the categories of Cyber crime. Explain them.
   Ans. Cyber crime can be categorized as given here.
   ❖ General Intrusions
     ✧ Hacking, spyware, phishing, pharming,
     ✧ Sending computer viruses & worms to invade computers
     ✧ Causing denial of service attacks
     ✧ Creating bots, Trojan horses, zombie machines
   ❖ Nuisances (usually non-violent activities)
     ✧ Sending spam
     ✧ Changing web page text and images
     ✧ Redirecting websites
   ❖ Personal Identity Theft (using someone else’s name or credit)
     ✧ Phishing for private information, passwords, code numbers
     ✧ Making unauthorized purchases with stolen credit cards or ID
     ✧ Destroying personal reputation
     ✧ Damaging personal credit ratings
   ❖ Theft of Intellectual Property (stealing ideas or creations of others)
     ✧ Downloading copyrighted music & videos
     ✧ Plagiarism, cheating
     ✧ Software piracy
   ❖ Physical or Mental Damage
     ✧ Cyberbullying, harassment
     ✧ Cyberstalking
     ✧ Sexual exploitation of minors, child pornography
   ❖ Terrorism
     ✧ Stealing military and private industry secrets - espionage
     ✧ Brainwashing and recruiting new followers
     ✧ Building terrorist communications network

Q4. Define the following terms: (a) Spyware     (b) Malware     (c) Virus   (d) Worms
   Ans. (a) Spyware: Spyware is simply software that literally spies on what is being done on a computer. Spyware can be as simple as a cookie used by a website or a more dangerous type such as a key logger that records every keystroke one makes on a keyboard.

(b) Malware: software that has a mischievous purpose such as virus attacks, worms, adware, Trojan horses, and spyware. This is the most prevalent danger to a system.

(c) Virus: A computer virus is a program that replicates itself. A computer virus attaches itself to a program or file to help it spread from one computer to another. Almost all viruses are attached to an executable file, which means the virus may exist on a computer but it actually cannot infect the computer unless one runs or opens the malicious program. A virus will also have some other unpleasant functions.

(d) Worms: A worm is similar to a virus and is considered to be a sub-class of a virus. It spreads from computer to computer, as it has the capability to travel without any human action. A worm takes advantage of file or information transport features on a system, which is what allows it to travel unaided. Worms cause harm to the infected network.

Q5. Read about ethical hacking and write a short note on your understanding of the topic.
   Ans. Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or red teaming. An ethical hacker is a security
professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. An ethical hacker operates with the knowledge and permission of the organization for which they are trying to defend.

Q6. Why Cyber security should be taken care by the user while working on internet?
Ans. Cyber security should be taken care by the user while working on internet due to a number of problems arising when users are not aware about security external and internal threats on the internet. These threats include:
Malware: -- explain this in few lines --
Adware: -- explain this in few lines --
Hackers and Crackers: -- explain this in few lines –

The internal threats are misbehavior or simple ignorance.

Q7. Discuss all the point which should be kept in mind while working on computers.
Ans. Cyber ethics must be practiced at every level of computer use—from the novice user to an information technology professional whose job requires significant use of online resources. Those who use the internet must be follow ethical practices in every aspect of its use.

Q8. What is Denial of Service attack? How it affects the systems performance?
Ans. A denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

System affected by DoS attack shows:
1. unusually slow network performance (opening files or accessing web sites)
2. unavailability of a particular web site
3. inability to access any web site
4. dramatic increase in the number of spam emails received

Q9. What is the difference between Shareware and Freeware software’s?
Ans. Shareware are copyrighted software that can be shared for a limited on a trial basis with the understanding that if the user decides to use it, he will pay for it.

Some copyrighted software is made available for use, free of charge for an unlimited time. These are called freeware. The copyright still remains with the producer / owner for any future development.

Q10. Mention the list of the licenses used by the users.
Ans. Types of software licenses:
1. Proprietary license
2. GNU general Public licenses
3. End user license agreement (EULA)
4. Workstation licenses
5. Concurrent use licenses
6. Site licenses
7. Perpetual licenses
8. Non-perpetual licenses
9. License with Maintenance

Q11. What do you mean by open source software’s? How are they different from proprietary software’s?
Ans. Open-source software (OSS) is computer software with its source code made available. It is very often developed in a public, collaborative manner. A license for open sources software allows the end user to study, change and distribute the software for any purpose. While in proprietary
license the copyright stays with the producer and it does not allow in modification or further distribution of the software. Proprietary software's source code is never made public.

Q12. In groups of 4-5 discuss how software cookies can be ‘helpful’ to both the user of the computer and the websites that created them. Document your understanding. It could be a poster, a brochure, a poem or a skit.
Ans. --- Home Work / Class Work --

Q13. What all do you usually do while you are connected to the net? Make a list and then plan all the security measures that you could take to safeguard yourself. Share this list with at least two of your peers and compare it to their lists.
Ans. --- Home Work / Class Work –

<table>
<thead>
<tr>
<th>Activity</th>
<th>Safety Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browsing website</td>
<td>1. Not downloading suspicious files with .exe extension</td>
</tr>
<tr>
<td></td>
<td>2. Using updated ver. of browser, OS and Antivirus</td>
</tr>
<tr>
<td></td>
<td>3. Using Firewall</td>
</tr>
<tr>
<td>Using social media</td>
<td>1. Keeping private information hidden</td>
</tr>
<tr>
<td></td>
<td>2. No interaction with unknown people / strangers</td>
</tr>
<tr>
<td></td>
<td>3. Not clicking on suspicious links send by strangers</td>
</tr>
</tbody>
</table>

C. Categorize the following under ethical / safety / security precaution
1. Do not share your password - security precaution
2. Do not use foul language. - ethical
3. Immediately report any suspect data or security breaches to your supervisor and/or authorities. - safety
4. Install firewalls and antivirus software's - safety
5. Do not copy information from the Internet and claim it as yours (plagiarism). - ethical
6. Be wary of strangers and cautious of potentially misleading or false information. - safety
7. Manage your computer settings to allow only data that comes from a known or safe place - security precaution
8. Do not download copyrighted materials. - ethical
9. Download only trusted applications from reputable sources or marketplaces - security precaution
10. Pay attention to the URLs of websites you visit - security precaution
11. Do not use someone else’s password or break into his computer. - ethical
12. Restrict access and make personal information secure to prevent identity theft. - security precaution

D. State whether the following statements are true or false
1. Hacking a computer is always illegal and punishable by law. - False
2. A license allows a user to use copyrighted material. - True
3. Software can only be licensed for a specific period of time. - False
4. A firewall is a virtual ‘wall’ that protects data on computers and computer networks. - True
5. Cyber law oversees only crimes that are committed by computers. - True
6. Crackers use physical tools to break into a computer and steal data. - False