Chapter 6
Cyber Safety

I. Tick (√) the correct option.

1. If someone says they are 16 you should

a. Believe them, they have no reason to lie

b. Not trust anyone you don't personally know

c. Give them your age

d. Meet up with them because they may be someone cool to hang out with

Ans. b. Not trust anyone you don't personally know

2. Who is the most common victim of online predators?

a. Infants

b. Adults

c. 5-9 year olds

d. Teenagers

Ans. d. Teenagers

3. Which among the following is not a malicious website?

a. Address, Phone Number and/or Email address is present.

b. The website address is not mis-spelled.

c. The https:// at the beginning of the web site.

d. The link shows a different address than what is mentioned.

Ans. c. The https:// at the beginning of the website

4. When visiting sites where you win something or they are giving something away

a. Give your name, phone number, and address

b. Give parents information

c. Give no personal information (If it sounds to good to be true, it is)

d. Give whatever information they request

Ans. c. Give no personal information

5. You are online and you get an instant message from your internet service provider needing your password

a. I give it to them because they are my ISP

b. I ask them why they need it

c. I never give my password to anyone

d. I log off without giving any information

Ans. c. I never give my password to anyone

6. _____ is a fraudulent practice of directing Internet users to a bogus website that mimics the appearance of a legitimate one.

a. Virus
b. Malware
c. Pharming
d. Chatting

Ans. c. Pharming

7. What is the private browsing mode in Internet Explorer/Edge called?

a. InPrivate
b. Incognito
c. PrivateIn
d. All of these

Ans. a. InPrivate

8. Which among the following is not a social networking site?

a. Facebook
b. Gmail
c. Twitter
d. LinkedIn

Ans. b. Gmail

9. _____ monitors user activity and transmit that information in the background to someone else.

a. Malware
b. Spyware
c. Adware
d. None of these

Ans. b. Spyware

10. Viruses are_____.

a. Man made
b. Naturally occurring
c. Machine made
d. All of these

Ans. a. Man made

II. Fill in the blanks with the given words.

1. Unsolicited commercial email is called **Spam**.
2. **Protect** your computer and smartphone with strong, up-to-date security/anti-malware software.
3. A **Virus** is a piece of code which is capable of replicating itself and typically has a detrimental effect, such as corrupting the system or destroying data.
4. **Biographical** Information is submitted voluntarily in social networking sites.
5. The default privacy settings in social networking site is **Public**.
6. **Tagging** refers to assigning a keyword or phrase that describes the theme of a group of articles, photos, videos, or other types of media files in social networking sites.
7. **Confidentiality** of information is defined as information to which the public does not have general access.

8. **Cyberstalking** is a crime in which the attacker harasses a victim using electronic communication.
9. An **authentication** process, ensures that authorized users are assigned confidential user identification and passwords.
10. A **malware** is a broad term used to describe all sorts of unwanted or malicious code.

III. State whether the following statements are True (T) or False (F).

1. Computer "virus" is a program which is developed by humans whose malicious intents is to disrupt the normal activity that can be done using a computer. **T**
2. A virus can spread if you are using an infected media like Pen drives, CD, DVD, etc, which may have itself got infected from some other computer. **T**
3. Worms are usually parasitic in nature. **F**
4. Macro viruses infects files with .exe extension. **F**
5. Privacy is used to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply. **F**
6. Identity protection refers to the protection of personally identifiable information. **T**
7. Confidentiality of information is is defined as information to which you do not have general access. **T**
8. Cyber safety refers to safe and responsible use of Information and Communication Technologies (ICT). **T**
9. Facebook is a malware. **F**
10. Polymorphic viruses have the capability of changing itself after infecting a computer. **T**

IV. Short Answer Type Questions (SA-I)

1. What are blogs?

Ans. A blog is a regularly updated website or web page, typically one run by an individual or small group, that is written in an informal or conversational style.

2. What does https stand for?

Ans. Hyper Text Transfer Protocol Secured.

3. What is the feature of private browsing called in Chrome browser?

Ans. Incognito

4. What is Log off in Social Networking?

Ans. Log off refers to closing the current session in the social networking site.

5. What is Cyberstalking?

Ans. Cyberstalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a social networking site and chat site. A cyberstalker, using anonymity allow them to stalk their victim without being detected.

V. Short Answer Type Questions (SA-II)

1. State two methods by which you can detect a virus.

Ans. Following are some of the ways your computer reacts to viruses:

- The speed of your computer may go down to a considerable extent.
- Certain software may require more time to start than it does usually.
- Certain software may not start at all.
- Some software may start normally but closes down abruptly.

2. Name the three type of information collected by a social networking site.

Ans. They are

- **Required Information**: Name, E-Mail, Date of Birth, Location. (Essential for the account.)
- **Secret Information**: Alternate e-mail, mobile phone number, security question and answer. (In case the account is compromised or you have lost your password.)
- **Biographical Information**: Information about yourself submitted voluntarily. (For advertisement content offered to you and to aid in advertisement targeting.) .

3. State three points that you should remember while selecting a password.

Ans. While selecting passwords the following points are to be remembered:

- The longer the password, the harder it is to crack. Consider a 12-character password or longer.
- Avoid names, places, and dictionary words.
- Mix it up. Use variations on capitalization, spelling, numbers, and punctuation.
- You may also use a specialized Password Manager package; as ultimately the number of passwords that you need to remember will grow.

4. What is Pharming?

Ans. Pharming refers to the fraudulent practice of directing Internet users to a bogus website that mimics the appearance of a legitimate one, in order to obtain personal information such as passwords, account numbers, etc.

5. List two methods by which you will be able to identify malicious websites.

Ans. The following are the list of malicious, criminal or inappropriate websites:

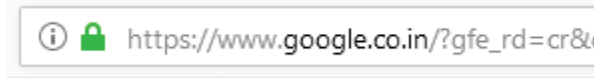
- Check for presence of an address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity.
- Check that the website's address seems to be genuine by looking for subtle misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser. Beware if this is different from what is displayed in the text of the link from either another website or an email.

VI. Long Answer Type Questions (LA)

1. Give four methods of identifying malicious sites.

Ans. The following are the list of malicious, criminal or inappropriate websites:

- Check for presence of an address, phone number and/or email contact – often indications that the website is genuine. If in doubt, send an email or call to establish authenticity.
- Check that the website's address seems to be genuine by looking for subtle misspellings, extra words, characters or numbers or a completely different name from that you would expect the business to have.
- Roll your mouse pointer over a link to reveal its true destination, displayed in the bottom left corner of your browser. Beware if this is different from what is displayed in the text of the link from either another website or an email.
- If there is no padlock in the browser window or 'https://' at the beginning of the web address to signify that it is using a secure link, do not enter personal information on the site.



- Websites which request more personal information than you would normally expect to give, such as user name, password or other security details IN full, are probably malicious.

2. Give four methods by which you will be able to safely use a social networking site.

Ans. The following list should be followed for using the social networking safely:

- Use a strong password. The longer it is, the more secure it will be.
- Use a different password for each of your social networking accounts and try changing it frequently.
- Set up your security answers which available with social networking sites.
- If you have social networking app on your phone, be sure to password protect your device.

3. What do you understand by Identity protection? Give three steps you should take to protect from theft.

Ans. Identity protection refers to the protection of personally identifiable information, such as Aadhar Card Number, Credit/Debit Card Number, bank account number, username or password by an imposter in order to impersonate someone else. Identity fraud can be used to obtain credit, merchandise and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, in rare cases, an imposter might provide false identification to police, creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen.

Some of the steps you should take to protect your identity from theft are:

1. Protect your computer and smartphone with strong, up-to-date security/anti-malware software. This is because if your computer or phone is infected with malicious software, other safeguards will be of little help.
2. The Operating System should also be regularly updated with different security patches and service packs as this will decrease the possibility of the security breach.

You should be able to spot spam and scams. Although some phishing scams are easy to identify, other phishing attempts in email, Instant Messaging, on social networking sites, or websites can look very legitimate. You should never click on a link that has been sent to you, if you have no idea about the source.

4. What is the method of selecting a strong password?

Ans. While selecting passwords the following points are to be remembered:

- The longer the password, the harder it is to crack. Consider a 12-character password or longer.
- Avoid names, places, and dictionary words.
- Mix it up. Use variations on capitalization, spelling, numbers, and punctuation.
- You may also use a specialized Password Manager package; as ultimately the number of passwords that you need to remember will grow.

5. What do you understand by confidentiality of information? State the best practices to ensure confidentiality.

Ans. Confidentiality of information is defined as information to which the public does not have general access. This policy governs the use or further disclosure of such information.

Best practices used to ensure confidentiality are as follows:

- An authentication process, which ensures that authorized users are assigned confidential user identification and passwords. Another type of authentication is biometrics.
- Role-based security methods may be employed to ensure user or viewer authorization. For example, data access levels may be assigned to specified department staff.
- Access controls ensure that user actions remain within their roles. For example, if a user is authorized to read but not write data, defined system controls may be integrated.

Application based Questions

1. To use the internet safely, Suresh has been given a questionnaire consisting of 5 questions. Help him with the questionnaire.

a. When you are making up a user name for email and instant messaging, you should:

i. Always use your real name.

ii. Use a name that does NOT reveal your true identity.

iii. Use a name that gives good clues about who you really are.

Ans. ii. Use a name that does NOT reveal your true identity.

b. With your secret codes and passwords, you should:

i. Give them out to only your best friends.

ii. Give them out to strangers.

iii. Never give out your passwords, except to your parents.

Ans. iii. Never give out your passwords, except to your parents.

c. When someone asks for personal information like phone numbers or addresses online, you should:

i. Give the information to anyone who asks because it's the polite thing to do.

ii. Post the information on any public Web site like MySpace, so anyone can find it.

iii. Never give out personal information online in emails or instant messages because you never know who you are really communicating with.

Ans. iii. Never give out personal information online in emails or instant messages because you never know who you are really communicating with.

d. When you are filling out forms or surveys online, you should:

i. Answer all the questions truthfully.

ii. Before you answer any questions, you should get your parents' approval.

iii. Make up funny answers to all the questions.

Ans. ii. Before you answer any questions, you should get your parents' approval.

2. Shobhit felt that he had been a victim of cyberstalking for a long period of time. Give 4 steps you should take for reporting cybercrimes.

Ans. Here are few steps you should keep in mind for reporting cybercrimes:

- The first step is to register a written complaint to the immediate cyber cell in the city. The Information Technology Act categorically provides that a cyber crime has global jurisdiction, meaning that the crime may be reported in the Cyber Crime Units of any city, irrespective of the place where the act was committed. At the time of filing of the complaint, the person reporting the crime may also be required to provide their name, contact details and mailing address along with the application, which is to be addressed to the Head of the Cyber Crime Cell of the city.
- In case of non-availability of cyber-cells in the city, one can file a F.I.R. in the local police station, commissioner or judicial magistrate of the city.
- Offences covered by the Indian Penal Code may also be reported at a local police station by lodging a First Information Report (FIR) irrespective of the jurisdiction in which the offence was committed.
- A report should also be send to the administration of the website for them to take immediate steps. Most social networking websites have a procedure in place for reporting any abusive activity or other such alleged offence.

3. Mr Swapan wants to secure his profile in a Social Networking site. To do this, he needs to change some privacy settings of his profile in the social Networking site. Suggest some privacy settings that will safe guard his identity.

Ans. Some of the common privacy settings associated with social networking sites are:

- The default privacy settings is "Public" , which may also be "Friends" or "Custom. The first two options are good for someone who has a small group of friends they don't mind sharing everything with or who has no personal identifying information on their profile and doesn't

mind it all being public. But for those of us who want a little more control over exactly who sees what on our profiles, it's time to familiarize yourself with the "Custom" option.

- How You Connect– This section allows you to change how people find you, who can post to your wall and who sees what information on your wall.
- How Tags Work– This option controls who can tag you in pictures, you can see the pictures you're tagged in and who can tag people in the pictures that you post. By default, Facebook shows the pictures you are tagged in publicly, even if you do not have a public wall.
- Apps and Websites– This section controls the third party apps that are allowed to access and interact with your profile without compromising it.
- Privacy of each post- This option is for convenience where each time you make a post, you can choose if that post is public, only to friends, only to you and more. You can even set it to show only to certain lists that you have.

4. Indranil always finds his password is being compromised in his social networking account. Suggest him suitable ways by which, he will be able create a strong password.

Ans. While selecting passwords the following points are to be remembered:

- The longer the password, the harder it is to crack. Consider a 12-character password or longer.
- Avoid names, places, and dictionary words.
- Mix it up. Use variations on capitalization, spelling, numbers, and punctuation.
- You may also use a specialized Password Manager package; as ultimately the number of passwords that you need to remember will grow.