पुणा International School

Shree Swaminarayan Gurukul, Zundal

Term – II Class – XI Computer Science

Society, Law and Ethics

Q1. What is cyber safety? Why is it important ?

Cyber Safety refers to the safe and responsible use of Internet so as to **ensure safety** and security of personal information and not posing threat to anyone else's information.
It is **important** because it involves gaining knowledge about possible threats to personal safety and security risks for the information along with measures to prevent and counter them.

Q2. What should you do to protect your identity on Internet?
You can protect your identity on Internet by using private browsing or anonymous browsing.

Q3. How do websites track you online ?
(a) **IP Address :-**
IP address is a unique address of your device when you connect to the Internet. It's likely that your computer shares your IP address with the other networked devices in your house or office. From your IP address, a website can determine your rough geographical location.

(b) **Cookies and Tracking Scripts :-**
Cookies are small pieces of information websites can store in your browser. They have plenty of legitimate uses - for example, when you sign into your online-banking website, a cookie remembers your login information. When you change a setting on a website, a cookie stores that setting so it can persist across page loads and sessions e.g., you change the zoom percentage of your webpage, then this setting will reflect on all opened webpages - because this was stored in a cookie. Cookies can also identify you and track your browsing activity across a website.

Cookies can be :-
(i) First party cookies. These are the cookies that store your own login id, passwords, auto fill information etc. for some websites that you frequently visit.
(ii) Third party cookies. These are the cookies that websites store to know about your search history and web browsing history so as to place advertisements as per your interests.
Third party cookies may result in many unwanted advertisements on your webpages.

(c) **HTTP Referrer :-**
When you click a link, your browser loads the web page linked to it and tells the website where you came from.
For example, if you clicked a link to an outside website on a webpage then the linked website will get opened and internally information about you such as your IP address, location, your web browser, machine type etc. will also be provided to the linked website - it is known as the HTTP

referrer.

(d) **Super Cookies :-**
Super cookies are also cookies but these are persistent cookies, i.e., they come back even after you delete them. Super cookies (like ever cookie) store cookie data in multiple places - for example, in Flash cookies, Silver-light storage, your browsing history, and HTML 5 local storage etc.
When a website notices that you've deleted part of the super cookie, the information is repopulated from the other location. For example, you might clear your browser cookies and not your Flash cookies, so the website will copy the value of the Flash cookies to your browser cookies.

(e) **User Agent :-**
Your browser also sends a user agent every time you connect to a website. This tells websites your browser and operating system, providing another piece of data that can be stored and used to target ads.

Q4. What are cookies? How are they used by websites to track you ?
Cookies are *small text files* stored on a user's computer and created and used by websites to *remember basic information* or *to record the user's browsing activity*.

Q5. What is Private browsing? Why is it considered a better way of browsing the Internet?
Private browsing :-

A type of browsing wherein browser opens in incognito mode or through proxy or VPN, and does not store cookies about your online activity, is called Private browsing.

Q6. What is confidentiality of information? How do you ensure it?

Best practices used to ensure confidentiality are as follows:

1. Use firewall wherever possible.
2. Control browser settings to block tracking.
3. Browse privately wherever possible.
4. Be careful while posting on Internet.
5. Ensure Safe sites while entering crucial information.
6. Carefully handle emails.
7. Do not give sensitive information on wireless networks.
8. Avoid using public computers.

Q7. What is cyber crime? How can you report it ?

Cyber crime :-

Cyber crime is any criminal offense that is facilitated by, or involves the use of, electronic communications or information systems, including any electronic device, computer, or the Internet.

The term, cyber crime, is a general term that covers crimes like *phishing, credit card frauds, illegal downloading, industrial espionage, child pornography, cyber bullying, cyber stalking, cyber terrorism, creation and/or distribution of viruses, spam* and so on.

That is, to report a cyber crime:-

- The local police stations can be approached for filing complaints just as the cyber crime cells specially designated with the jurisdiction to register complaint.
- In addition, provisions have now been made for filing of 'E-FIR' in most of the states.
- In addition, the Ministry of Home Affairs is also launching a website for registering crimes against women and children online including cyber crimes.

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.

Q8. What is cyber bullying and cyber stalking ?

(a) **Cyber bullying :-**

Cyber bullying refers to act of online harassment of someone by using online tools such as Internet, email, instant messages, chat rooms or social networking sites etc. Cyber trolling, which means posting of sarcastic-, demeaning- or insulting- comments about someone, is also considered form of cyber bullying.

(b) **Cyber stalking :-**

Cyber Stalking refers to online stalking where someone uses Internet, chat rooms, social networking sites, emails etc. to stalk his/her victim. Cyber stalker follows the victim online everywhere and keeps posting/sending something which are unsolicited.

Q9. What is identity fraud ?

Online **identity theft** is the theft of personal information in order to commit fraud.

Or

Identity theft occurs when someone uses another person's personal information such as *name, Adhaar number, driver's license number, credit card number, or other identifying information* to take on that person's identity in order to commit fraud or other crimes.

Q10. What is digital footprint? Why is it so important ?

Digital Footprint: - A **digital footprint** is the record or trail left by the things one does online. The social media activity, the information on personal website, the **browsing activities**, online **subscriptions**, any photo galleries and videos uploaded by a user - essentially, any activity carried out on the Internet makes the digital footprint of a user.

It is important because mistakes aren't as easy as they used to be because once we post anything online, it stays forever and cannot be undone, Digital Footprints last forever, and colleges and jobs will look back at them to see if you are what you portray and how you conduct yourself actually.

- In short, you should always set-up or read privacy settings for all types of sites yourself.

Q11. Why are privacy settings of a social networking site so important ?

Privacy settings of a social networking site is so important because you should know

- Who all can see what you have posted.
- Who all can send requests to you.
- What all information about you is visible to others, even to your contacts etc.

Q12. What are the usage rules for effective use of social networking sites ?

The usage rules for effective use of social networking sites are as follows :-

- Be Authentic
- Don't Pick Fights Online
- Use a Disclaimer
- Protect Your Identity
- Does Your Information/Post Pass the Publicity Test?
- Don't Use Fake Names or Pseudonyms
- Monitor Comments
- Respect Your Audience
- Respect other's Sentiments