Cyber Safety

Based on CBSE Curriculum

Class -11

Introduction

- Now a days we can not even think our lives without internet. Internet has not only provided so many facilities to us but also made tasks really easy.
- At the other hand, if it is not used carefully then it may be dangerous too.
- Therefore, it is required to know that what are the risks of using internet and what are the ethics of using internet.
- In this chapter we will learn all this in detail.

What is Cyber Safety ?

- Using internet with care and responsibility is called Cyber Safety so that we can keep our personal information safe.

Browsing the Web securely

- Now a days working on web has become necessary therefore we should be aware about the risks we can face on web. We should be take care for the following facts-

–What are the Possible Dangers?

- How to avoid these?

–How to behave while using web?

-Additionally we should always remember that–

- Every site is not safe.
- Whatever you are doing online can be viewed by others.
- Whatever you see online is not necessarily true.
- Before going online you should make arrangements for your computer's safety.

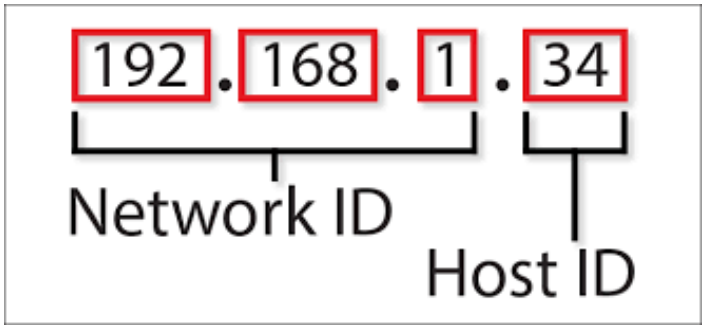
Identity Protection using Internet

- Identity Theft is a kind of fraud which involves using someone else's identity to steal money or gain other benefits.
- Online identity theft refers to an act of stealing someone's personal information such as name, login details etc. and then posing as that person online.
- Most common solution to this is- Private browsing or Anonymous browsing.
- Before talk about it, lets talk about what happens when you normally browse the internet.

Many ways Websites track you

- Whenever you visit a website, your web browser may reveal your location via your device's IP address.
- It can also provide your search and browsing history etc. which may be used by third parties, like advertisers or criminals.
- This way website track you. Tracking is generally used by advertising networks to build up details profiles for pinpoint ad-targeting.
- This information is compiled through your web usage patterns, and which websites generally use for tracking you. This generally includes-

(a) IP Address: IP address is a unique address of your device when you connect to the internet. 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. Cookies can be-

1. *First Party Cookies-* These are the cookies that store your own log in id, password, auto fill information etc.
2. *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.

(c) HTTP Referrer : when you click a link, your browser loads the web page linked to it and tells the website here you came from, it is called HTTP referrer.

(b) Super Cookies : these are also cookies but these are persistent cookies. i.e. they come back even after you delete them. They store data in multiple places like in flash cookies, Silverlight storage, your browsing history and HTML local storage etc.

(c) 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.

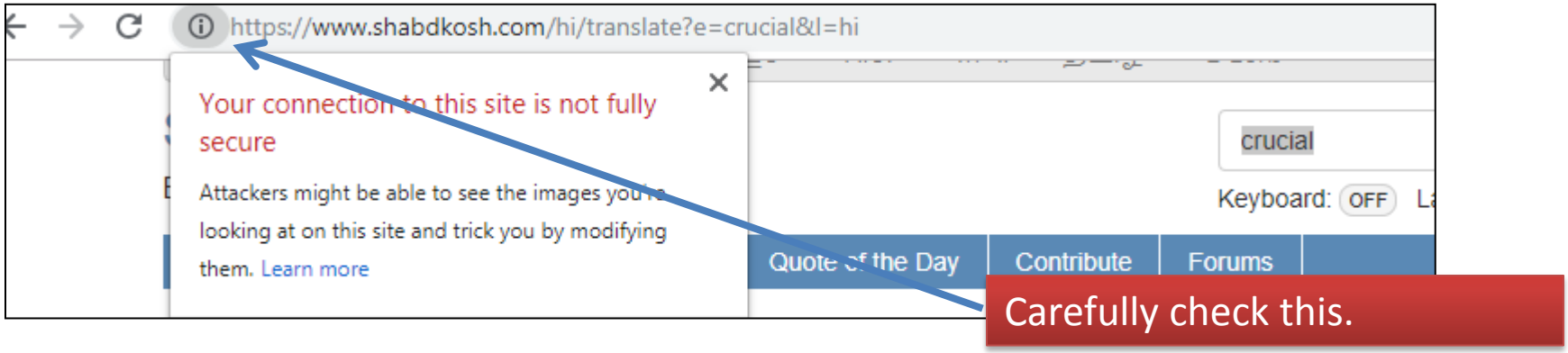
All the above things leak your identity information to websites and it may be used against you. Solution to this is Private browsing and Anonymous browsing.

Private Browsing And Anonymous Browsing

- Anonymous browsers allow users to view websites without revealing personal information of user.
- It can be sued as a tool for governments, journalists and every security conscious surfers.
- A popular solution to this is- Private Browsing.
- **Incognito browsing open up a version of the browser that will not track your activity.it is particularly useful if you are entering sensitive data like bank details into your browser.**
- **Proxy** works as a middleman between your computer and the website you want to access. Now the tracking website will get the IP address of proxy site.
- **Virtual Private Network (VPN)** this is a method to add security and privacy to private and public networks, like WiFi hotspots and Internet. It is originally meant for business employees working offsite to gain access to shared drives or networks.

Confidentiality of Information

- Confidentiality of Information ensures that only authorized users get access to sensitive and protected data. Best practices used to ensure confidentiality are-
  1. Use of Firewall.
  2. Control browser settings to block Tracking.
  3. Browse Privately.
  4. Be careful while posting on Internet.
  5. Ensure safe sites while entering crucial information.



Confidentiality of Information

6. Carefully handle emails.
7. Do not give sensitive information on Wireless.
8. Avoid using Public computers.
9. While using public computers don’t forget to delete history and cookies.
10. Use Virtual keyboards to input login and Passwords.
11. Don’t save your personal information.
12. Don’t leave your computer unattended.
13. Disable the feature that stores passwords.

CYBERCRIME

- Any criminal offense that is facilitated by, or involves the use of, electronic communication or information systems, including any electronic device, computer, or the internet is referred to as **Cybercrime**.
- Some common Cybercrimes are-
    1. Cyber Trolls and Bullying:
    2. Cyber Bullying
    3. Cyber Stalking (Online Harassment)
    4. Spreading Rumours Online
    5. Unethical hacking
    6. Stealing information etc.
- ***Reporting Cybercrime :*** One must report it firstly to parents, school authorities and then to police.
- The procedure for reporting cybercrime is more or less the same as for reporting any other kind of offence.
- The local police stations can be approached for filling complaints.
- Mot of the states have facility of E-FIR.
- Ministry of Home Affairs is also launching a website for registering crime against women and children online including Cybercrime.

COMMON **SOCIAL NETWORKING** SITES

- A Social networking site is a web application or online platform where people can setup their public profile and make connections with other online people called **online friends**.
- Some popular social networking sites are-
- *Facebook*: it is a platform where you can share your ideas in the form of posts, photos, videos etc.
- *Twitter*: it is a micro blogging site which allows to post very small messages. Earlier limit was 140 characters now extended to 280 characters.
- *LinkedIn*: it is a social networking site for professional. It provides features to make profiles like resumes.
- *Instagram*: it is one of the most popular site for online photo sharing.

APPROPRIATE USAGE OF SOCIAL NETWORKING SITES

- Social media is everywhere these days, from personal to professional front. Social media has made it too difficult to remain entirely anonymous these days.
- Whatever you do online, leaves a permanent foot print, called digital foot print.
- Once posted these becomes part of public domain and hence are visible to anyone who looks for it.
- Thus appropriate usage of Social media is very important and you must be aware that it may pose problems later if not used appropriately.

What you should do on SOCIAL NETWORKING SITES-
Usage rules

- You should conduct yourself in a responsible way so that you can enjoy using it.
- Be Authentic.
- Use a Disclaimer.
- Don’t pick fights Online.
- Don’t use fake names or pseudonyms.
- Protect your identity.
- Always take publicity test when post something.
- Respect your audience.
- Respect other's sentiments.
- Monitor comments.