Continued…

NORTH-EX PUBLIC SCHOOL (Session 2020-21)
Class - XI
Subject: Computer Science
Unit 3: Society Law & Ethics
Topic: Cyber Safety
Worksheet: 2

***Note- Before reading about the topic you must check this link which will help you in understanding the topics.**

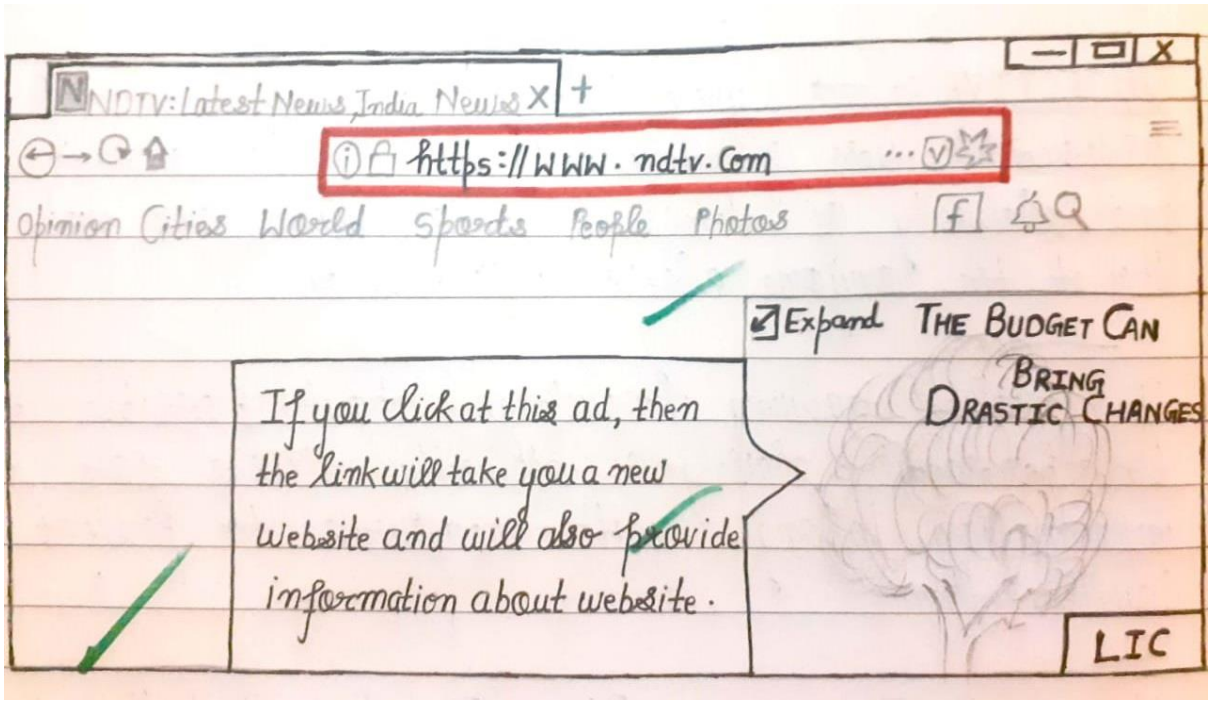
You can download this or if you do not have facility to get printout then you can ask your ward to copy it in a simple notebook and must do exercise in the notebook.

NOTES

Many ways websites track you.

4.1. (C) HTTP Referrer:

When we click a link, our browser loads the web page linked to it and tells the website where we came from. For example. If we clicked a link to an outside website on a webpage then the linked website will get opened and internally information about us such as our IP address, location, our 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 we delete them**. When a website notices that we have deleted part of the super cookie, the information is repopulated from the other location. For example, we might clear our web browser cookies and not our flash cookies, so the website will copy the value of the Flash cookies to our browser cookies.

4.2. Private Browsing and Anonymous Browsing:

4.2.1. Anonymous browsers allow users to view websites without revealing any personal information of the user like their IP address, machine type, location etc. An anonymous browser lets users access websites anonymously. It can be used as a tool for governments, journalists, and everyday security-conscious surfers.

There is another type of browsing- **Private browsing.**

4.2.2. Private Browsing: A type of browsing wherein browser opens in incognito mode or through proxy or VPN, and does not store cookies about our online activity, is called **private browsing.**

There are other ways to use the internet without revealing our search history and sharing our data. These are:

a. **Incognito browsing:** opens version of the browser that will not track our activity. It is particularly useful if we are entering sensitive data like bank details into the browser, as it can minimize the risk of our information being saved to that computer. It can also be used for purpose like- to look at surprise gifts for the family without leaving clues, filling examination forms etc. But this information is still visible to our school, university, or organization. We may also use private browsers and search engines like **DuckDuckgo.**
b. **Proxy:** works by acting as a middleman between our computer and the website we want to access. Now the tracking website will get the IP address and information that belongs to the proxy site, so we are effectively getting the same content from another source without it getting to know our browsing details.
c. **Virtual private network:** or a VPN is a method used to add security and privacy to private and public networks, like WiFi hotspots and the internet. VPN are most often used by corporations to protect sensitive data. Virtual Private Networks (VPN) were originally meant for business employees working offsite to gain access to shared drives or networks. Now a days, we can set up a VPN at home to protect yourself from hackers trying to access our sensitive information.

5. Confidentiality of information:

Internet is a public platform, mostly. The sites we visit, the things we search on it, the posts that we put on social networking sites are all visible to public. But there must be some information like our credit history or bank details, our mails etc., which we do not want to make public, i.e., we want to keep this information confidential.

Confidentiality of information ensures that only authorized users get access to sensitive and protected data.

5.1 Practice to ensure confidentiality of information:

We can follow certain practices to safeguard our data and ensure its confidentiality. Best practices used to ensure confidentiality are as follows:

a. **Use firewall wherever possible:** Our system must be secured such that only authentic users can connect to it. Firewall is one very good solution for this. Firewall is a program that monitors all communications and traps all illicit packets. Most operating systems now come with a firewall preinstalled. However, some, such as the windows Firewall, only block suspect incoming communication, leaving completely open access to the internet from our machine.
b. **Browse Privately wherever possible:** To avoid the tracking by websites, we should try to browse Internet privately wherever possible. This way websites would not be able to store cookies on your computer, which give information about our search pattern and surf history.
c. **Be careful while posting on Internet:** When we post anything to a public Internet such as social networking sites like Instagram or Facebook etc. At that time ensure that we never post our crucial information like our personal details such as address, mobile phone number, bank details, credit details etc. on public Internet sites.
d. **Ensure safe sites while entering crucial information:** Sometimes we have a need to provide our crucial information such as our personal details or bank details etc. For example, we might be applying online to register for an entrance exam through a legitimate site that asks for our personal details.
   In such cases, ensure these things:
   - Type the URL of the website in the address bar of the browser on our own. Do not click on a link that takes to this website; or do not cut/copy the link of this website and paste it. TYPE THE URL ON OUR OWN in the address bar of the web browser.
   - **Ensure that the address contains HTTP and a pad lock sign.** When this website gets loaded, before we start typing any information, ensure that the website address. A safe site's URL starts with http:// and not with http://. Also, it shows a closed pad lock.

https:// in a URL means it is a secure connection and no one can see our private information. When there is no https, or the URL contain only http, then it is an insecure connection, which means our private information may get leaked.

e. **Carefully handle emails:** While opening an email, make sure that we know the sender. Even if we open the email message by accident, make sure not to open attachment in an email from unrecognized source and never click on any link inside an email to open it. The link might look legit, but it may take us to a fraudulent site.
f. **Do not give sensitive information on wireless networks:** Sometimes we get access to some wireless connections such as the Wi-Fi connections available on Airports or

Railway Stations. While using such Wi-Fi connections, make sure not to open any personal email or provide any sensitive information on a website. The reason for this is that **most wireless networks are not encrypted and hence information on it can be tapped and used for fraudulent purposes.**

g. **Avoid using public computers:** Always try not to use the public computer especially if we have to deal with our crucial data. But of we need to work on a public computer, then make sure following things:
    - Browse privately, first of all.
    - Do not save your login information.
    - Never save passwords while working on a public computer.
    - Avoid entering sensitive information onto a public computer.
    - Do not leave the computer unattended with sensitive information on the screen.
    - Disable the feature that stores passwords.
    - Properly log out before we leave the computer.
    - Erase history and traces of your work, i.e., clear history and cookies.

Worksheet 5

Attempt all questions in your notebook.

1. What is Private browsing?
2. What is super cookies?
3. What do you mean by Http Referrer?
4. What is the difference between https and http in URL?
5. What do you mean by Virtual Private Network?
6. What is the confidentiality of information? How do you ensure it?
7. What measures should one take to avoid and maintain confidentiality of personal information, when we use public computers?

Answers

1. ***Refer Section 4.2.2 of this PDF.***
2. ***Refer Section 4.1 (d) of this PDF.***
3. ***Refer Section 4.1 (c) of this PDF.***
4. ***Refer Section 5.1(d) of this PDF.***
5. ***Refer Section 4.2.2 (c) of this PDF.***
6. ***Refer Section 5.0 of this PDF.***
7. ***Refer Section 5.1 (g) of this PDF.***