NORTH-EX PUBLIC SCHOOL (Session 2020-21)
CLASS - IX
Subject: Computer Applications
Unit 2: Cyber Safety
Topic: Cyber Safety
Worksheet: 6

*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

1.0. THREATS IN CYBER WORLD

These days internet related crimes are growing at an alarming rate. In order to understand Cyber safety, we need to understand threats available in online world. Some of the threats are mentioned below:

1.1. **Unauthorized Access or Hacking:** Hacking means that your online accounts, computer, or network is being accessed without authorization. It is done with intension to get access to sensitive data, committing financial frauds, causing loss or troubling the person. Cases of people breaking into email, social media, and bank accounts are frequently reported.

1.2. **Spamming:** Spam refers to unsolicited messages sent by e-mail, text message and so on without recipient consent. It's also refereed to as electronic junk mail. Spam messages often contains commercial advertisement.

1.3. **Phishing and E-Mail Frauds**: Phishing refers to the activity of sending mails and fraudulently gaining access to sensitive information by posing to be a trustworthy source. Mail contains malicious file attachment that contain phishing software or contains link to malicious websites. The mail may have deceptive URL that take you to fake website that looks the same as original website.

These emails compel the users to click on the link. For example:

i. The message creates a sense of urgency by having text like: "If you do not click on link, your subscription or account may get deactivated".
ii. The message claim that you have won a reward or prize and you can claim it only when you click on the link.

1.4. **Online Predators:** There are many users on internet who want to exploit children and are on outlook for easy prey. These people take advantage of the anonymity of the internet. They trap children, forces them into meeting in person, and exploit them.

1.5. **Cyberterrorism:** People try to break into Government Websites to gain access to confidential information of national importance.

2.0. SECURITY ON SOCIAL NETWORKS

People use social networks like LinkedIn, Facebook, Twitter etc to connect with others and share messages, photos and videos. With growing popularity of these sites, the misuse is also on rise. It is essential that we are aware of some safety measures to be followed:

i. Use a strong password. Use different passwords for different accounts.

ii. Use privacy and security setting on your social network profile to control who all access your posts. Think before messaging or posting any pics/videos on Social media.

iii. Limit the amount of personal information shared online. The more information you post, the easier it is for others to use that information to break into your accounts, access your data, and commit crimes. A common way to get access to somebody else's account is to use "Forgot your password" option. The security question should be carefully chosen such that the answers to the security questions are not available online.

iv. Be selective in choosing your friends online. Do not accept every friend request you get. Peoples often creates fake profile, befriend you, and gain access to personal information. You may consider restricting or blocking your profile accessibility via public search.

v. Be wary of clicking on links and following the instructions in message. You could receive message that looks as if your friends have sent you but actually, they are fraud.

vi. Protect your social media app on your phone with a strong password.

vii. Remember to log off after every session.

3.0. IDENTITY PROTECTION

If you do not exercise caution while surfing the net or using social networks, people can access your information, impersonate you, and commit various crimes in your name. This is known as identity theft.

Identity theft occurs when someone uses another's information , such as credit card number or Aadhar card number without their permission, to commit frauds or other crimes. Identity thieves can use your identity when they commit crimes such as laundering money, drug trafficking etc.

3.1. Causes of Identity Theft:

i. Fraudsters may access your information through lost or stolen personal documents. There have been instances where documents thrown in the trash have led fraudsters to access important information about others (dumpster diving).

ii. Lots of people store data online on cloud storage. Insecure online data could also lead to easy access to it.

iii. Posting your personal details on Social network with no proper security setting also make you susceptible to online theft.

iv. There have been instances of companywide data breaches. A security breach of the database of a social network or a financial institution could lead to hackers having access to information of millions of customers. Recently a software data breach was in news , which you can read here https://securityboulevard.com/2020/04/zoom-recordings-exposed/ .

v. You can fall prey to hackers if you are using unsafe connections in public areas or using Internet without firewall.

vi. Using easy-to-guess passwords, visiting insecure websites when shopping, clicking on unknown links & opening unknown attachments make you vulnerable to identity theft.

Worksheet 6

Attempt all questions in your notebook.

Q1) What do you mean by identity theft? ***(Ans: Refer Section 3.0)***

Q2) Mention some causes of identity theft. ***(Ans: Refer Section 3.1)***

Q3) Mention some safety measures that can be followed for security on Social Networks. ***(Ans: Refer Section 2.0)***

Q4) What do you understand by Phishing. Explain with example. ***(Ans: Refer Section 1.3)***

Q5) Mention any three threats in Cyber World & explain them. ***(Ans: Refer Section 1.0)***

Q6) Mention any two social networking sites. ***(Ans: Refer Section 2.0)***