Ideation

In this activity you are expected to list the ideas (atleast 4 per each team member) by organizing the brainstorming session and prioritize the top 3 ideas based on the feasibility & importance.

1. Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer.

2. Anti-spyware and firewall settings should be used to prevent phishing attacks and users should Protect your mobile phone by setting software to update automatically. These updates could give you critical protection against security threats.

3. Protect your data by backing it up. Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage. Back up the data on your phone, too.

4.The website may be used to hack and misuse others' details so as to protect that Then kids nowadays are learning from online so to protect them from facing any unpleasant or bad activity. So create an extension in google which will detect the fake websites.

5. Every time you click on a link, look at the browser bar and see if it matches exactly the one you would type in to go to your account.

6. All members of your executive and management team are vulnerable. If a phishing scammer acquires the email credentials of high-profile leadership, it's likely they'll target anyone they can using that very email address.

7. Almost all spam messages are malicious emails sent by unknown sources. These sources could be hackers who aim to hack into the computers of their victims.

8. Never respond to spam messages because through this, the spammer will know that the email address is active and thus, it increases the chance of your email to be constantly targeted by the spammer.

9. Do not use your personal or business email address when registering in any online contest or service such as applications, deal updates, etc. Many spammers watch these groups or emailing lists to harvest new email addresses.
10. In fact, many unsuspecting users have been dumped via text message phishing (also known as smishing) and through social media.

11. The threat of malicious messages luring users to click on a link, open a malicious webpage, download malware or provide credentials on a spoofed site proves that threat actors are getting continuously creative in their methods to hijack your assets and steal your credentials.

12. While these attacks use electronic written words to lure a user into their scam and some of the messages may be hosted in social media, a new form of messaging attacks are emerging via other cloud and SaaS (software as a service) platforms that provide in-application messaging between users.

TOP 4:

1. We would create an interactive and responsive website that will be used to detect whether a website is legitimate or phishing. This website is made using different web designing languages which include HTML, CSS, Javascript and Python.

2. It must be noted that the website is created for all users, hence it must be easy to operate with and user-friendly.

3. The website will show information regarding the services provided by us. It also contains information regarding ill- practices occurring in today's technological world.

4. The website will be created with an opinion such that people are not only able to distinguish between legitimate and fraudulent websites, but also become aware of the mal-practices occurring in the current world. They can stay away from the people trying to exploit one's personal information, like email address, password, debit card numbers, credit card details, CVV, bank account numbers