**ACTIVITY -1**

**Discover your own risky online behaviour**

**Scenario 1: posting private information on your social media**

* A lot of information is leaked through the social network in public such as photos, videos, etc. that can be missused.
* Cyberbulling cases has been increased.
* It could be aserver distruction for many people and become on addiction to them.
* It can causes health issues such as sleeping disorder.
* It includes a lot of privacy concerns related to your personal data.
* Virus attacks and fraud can be commited as a result of this vulnerability.
* Identity theft.

**Scenario 2: what password you choose when creating new account for social service**

* **Make sure your password is strong**: It should be atleast 8-10 characters long, and longer password are even more secure. Some sites or applications may limit the password length however . Example:Wh01292014etV
* **Use atleast one capital letter and one lower case letter in your password**: The capital and lower case letters should not be grouped together. Mixing them up makes the password more difficult to predict. Example: JeCaMiJe.
* **Use space in your password**: many password systems don’t allow actual space, but it can be useful to insert on into the middle of the password with system that do. Alternatively, on under score “\_” or two can serve a similar functions.
* **Generate similar but distinct passwords for separate accounts**: You can use similar base words to help you remember your password easily without making them too easy to crack. So “JeCaMiJe\_” might be modified as “my kids JeCaMiJe” “HouseOnSpooner#1500” might become”1500\* my first House on spooner.
* **Use more complex obfuscation**: Instead of using the password “prOd@dmin” (A password compromised during theDigiNoter attack), use an anagram such as “0@imdndpr”.

**Scenario 3: Using public WiFi**

* **Theft of Personal Information:** One of the common threats of using public WiFi is the theft of personal information such as login credentials, pictures, personal data, and financial information. In case a hacker gains access to your PC or any other personal device, they may have free reign over everything you’ve stored.
* **Man-In-The-Middle (MITM) Attacks:** These attacks occur when an individual impersonates a credible public WiFi service to dupe you into connecting. For instance, you’re staying in the Hilton Hotel for the night. The hotel offers free WiFi to its guests, so you decide to switch on your laptop, turn on the WiFi, and see a network called Hilton. If you’re not keen, you might miss the slight misspelling.
* **Cyberattacks on Businesses:** Business travelers who are always on the road throughout the day may connect to public WiFi to download files, check their emails, review customer information, among other tasks that require network connectivity.
* **Unencrypted Connections:** Not every public WiFi network provides encryption. You can determine this by looking at the HTTP prefix that’s stated just before a domain name. Suppose it begins with HTTPS, then it’s an encrypted site. However, if the web address contains HTTP, it’s unencrypted.
* **Session Hijacking:** This is another public WiFi security risk. Here, a threat actor intercepts information about your device and its connections to websites and other services. Upon accessing this information, they can configure their own computer to match yours and hijack the connection.
* **Malware Distribution:** Implementation of malware such as viruses, worms, ransomware, and Trojans on PCs and other personal devices is another threat that can occur when using public WiFi. If someone on the same public network as you has malicious intentions, they could plant malware on your computer if it doesn’t have proper protection.

**Scenario 4: Using trail version of the software**

Offering a free trail is a common stratergy of software vender,which has been stualied by many researches fowsing on impact of positive network effects .However the software is not perfectly security, security vulnerability may be exploited and incure negative security externalities among software users.

\*\*\*\*\*\*\*\*\*