There are various ways to protect yourself when connecting to public Wifi. Firstly, you should check that whether your URL starting with https:// which have already been encrypted or not and avoid other URL that is not started with https://. Website that started with other maybe the phishing website although there user interface are may look as like as the official webpage. Beside, you should stick in your mind that whenever connecting to public Wifi, avoid using personally private identifiable information (PII) such as bank account, visa card number, phone number and home address… Another mostly used method is using VPN. VPN (Virtual Private Network), which creating a private network or a tunnel that you can transfer data and information in private and safe way. VPN (Virtual Private Network) can be considered as an encrypted cooperated network that connect device and network.

There are some simple steps that people who have lack of IT knowledge can applied such as setting up your phone again before joining the public Wifi. By doing such tasks: turn off the automatically connect, share of the phone, you can avoid your data is accidentally leaked or being collected by attackers. Another small advice is that you should always keep your software update since usually the outdated protect protocol do not help and get easily hacked. Finally remember to log out and disable connection to Wifi by “Forgot this network”. You may still have been connected for a period of time after you turn off the devices which may contain risks.

Focus = 3 (techniques)

Topic = 5

Reference:

https://us.norton.com/internetsecurity-wifi-public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-to-attack-and-how-to-stay-safe.html

Cookies, more properly called HTTP cookies, can be understood as small bits of data stored as text files on a browser. Websites use those small bits of data to keep track of users and enable user-specific features. They normally just contain information that allows the server to remember who you are between page requests. The main security risk is really that different sites might gain access to the content of that cookie, which may have different type of attacks. Cross Site Scripting (XSS) happens in application levels when user visit a malicious website, the attacker place the exploit in cookie and being retrieved by users’ computers. Then, the exploit will fetch the payload from the cookie and continue executing exploitation. Thus, when users visited other website, the script payload contained in cookie is sent to the host sever. Another Cross Site attack type would be Cross Site Request Forgery Attack. Cross Site Request Forgery Attack (XSRF) happens when attackers make the victims’ browser execute unwanted actions on web application (which the user have been authenticated before). The script which have been injected by attacker when he/she visited the trusted website can be through social engineering (via link or email). Through a legal website and receive the legitimate cookie. Thus, the victim is forced to transferring fund, changed email or maybe compromise the whole entire web application if the victim is administrative. Session fixation, another common attack, happens in application level, when attacker impel users to use the attackers’ or another session ID instead of users’ ID by directive path. Thus, attackers can urge user to log in as the attacker on various websites.

[Focus = 1] (Attack)

[Topic = 10]

Ref:

https://resources.infosecinstitute.com/risk-associated-cookies/

https://www.whoishostingthis.com/resources/cookies-guide/