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 Another small advice is that you should always keep your software update since usually the outdated protect protocol do not help and get easily hacked.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.

Source :: <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>

Focus = 3 (techniques)