Prevention

- Ensure that the devices are up-to-date. This includes smart devices such as printers, laptop, smart watches, cars, refrigerators, etc.

- Use a strong PSK password when configuring the WPA-PSK encryption on the router
  - Setting a strong password means:
    - password is not the default password
    - password used is not notoriously weak
    - password that is a common phrase or word
    - passwords that does not include your birthday.
  - Other aspect to avoid
    - use of password hints
    - adding the season or month or year at the end or front of the website name.
    - using the same password for more than one account
    - sharing of password with others

- Turn off public network sharing when connected to an unsecured network

- Turn off auto connection to prevent the devices from connecting to an unknown network

- Avoid connecting to public Wi-Fi network as an attacker could capture your network traffic should you connect to the attacker's router or in the same network as the attacker

- Ensure that firewall and anti-virus is turned on at all times

- Do not browse website that are suspicious in nature or unsecured website