
Network Security Checklist

The following checklist contains the configurations that should be put into place after the correct network device is purchased. It is possible that some of the steps below are not applicable to your situation.

Register your device with the manufacturer

Change the default administrative password of all routers and modems to something unique

Use a unique password to access your ISP's web portal

Enable two-factor authentication wherever possible. This may include accessing the ISP web portal, the router/modem, or a mobile app

Change the WiFi network name (i.e., SSID) password to something unique

Ensure the WiFi network (i.e., SSID) name does not provide any identifying information

Carefully guard who has knowledge of the WiFi network password

Turn off the 2.4 GHz or 5GHz network if you're not using one of them

Move all routers and modems to a location not accessible by the general public or passersby

Enable automatic updates for all routers and modems

Turn on WPA2 or WPA3

Disable WPS if possible

Enable the router and modem firewall

Enable network address translation (NAT)

Enable DNS filtering on the router and/or modem

Disable UPnP