










How to Secure Your Home Network Against Cyber Threats




Computers, tablets, smartphones, TVs, thermostats, cameras, doorbells, and coffee pots. What do all these things have in common? They are all devices that connect to your home network and the internet. We rely on our home internet connections more than ever before, so it is critical that we keep it cybersafe.

Use this information as a checklist to improve the security of your home network and protect you and your family from potential cyber threats.


Secure Your Modem and Router

-  **Use current hardware.**
Consider replacing modems/routers at least every five years so your devices receive the support and updates you need to keep your home network safe.
-  **Enable automatic updates and install the latest firmware.**
Keep your modem and router up to date with the latest firmware. These updates help protect them as new vulnerabilities emerge and are patched.
-  **Disable remote management.**
Disable remote management by default, and if you absolutely need it, be sure to enable multi-factor authentication (MFA), like Duo, to use this feature.
-  **Change your modem and router passwords.**
Changing default passwords will prevent others from getting into your network.
-  **Enable the router's firewall.**
The firewall helps prevent the devices on your network from accessing malicious sites as well as keeping outsiders on the outside of your network.
-  **Enable website filtering.**
Some routers have website filtering and parental controls to prevent users from accessing malicious or inappropriate websites while on your network.
-  **Reboot your modem and router once a month.**
Rebooting your modem and router keeps your internet connection healthy and fast.

Secure Your Wi-Fi

-  **Change the Wi-Fi network name (SSID).**
Using the default settings allows outsiders to know the brand of your router and exploit any vulnerabilities. Change the Wi-Fi name, but don't use personal information.
-  **Enable Wi-Fi encryption.**
Use Wi-Fi Protected Access 3 (WPA3) if supported by your device and choose a strong passphrase to connect devices to your network.
-  **Enable a Wi-Fi guest network.**
Keep your computers, mobile devices, printers, and other trusted devices on your primary wireless network, and have visitors and your web-enabled appliances connect to a guest network.

Monitor Your Network

-  According to [Deloitte's 2022 Connectivity and Mobile Trends Survey](#), the average U.S. household has 22 connected devices. Do you know what devices are connecting to your network? Periodically review the devices that are connected to your network and block the ones that you don't recognize.