

Aware and Safe

Be aware. Stay safe.

Home Wi-Fi Safety Checklist

Seven simple fixes that make your home network dramatically safer. Most take five minutes each - do them in order, tick each box, and you're done.



1. Change your router's default admin password

The password printed on the router's sticker (often 'admin' / 'password') is public knowledge. Log in at the address on the sticker (usually 192.168.1.1) and set a new admin password only you know.



2. Set a strong, unique Wi-Fi password

Use WPA2 or WPA3 security (check the router's wireless settings) and a long passphrase - four or five random words beat a short jumble of characters, and they're easier to remember.



3. Update your router's firmware

In the router settings, look for Administration / Firmware Update and install any available update. Manufacturers patch security holes this way - an old router is an open door.



4. Turn off features you don't use

Disable WPS (the push-button connect feature - it's insecure) and Remote Management / Remote Access unless you specifically need them. Fewer open features means fewer ways in.



5. Put guests and gadgets on a separate network

Most routers can create a Guest network. Put visitors - and smart-home gadgets - on it, so a compromised device can't reach your computers and phones.



6. Check which devices are connected

Your router shows a list of connected devices. If you see one you don't recognize, change your Wi-Fi password immediately - that boots every device off, and you reconnect your own.



7. Restart your router regularly

Reboot it once a month, and any time you hear about a major security scare. It clears temporary glitches and forces a fresh, clean connection.

From Aware and Safe - plain-language security guides for everyday people. Learn more at awareandsafe.com