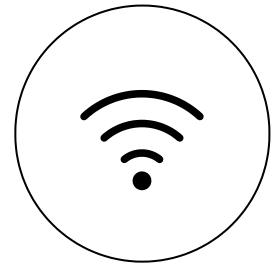




Home network check

Your router, your Wi-Fi and what is connected

Walk round your home network with a pen and your router's app or settings page. Tick what is done; note what to fix.



Never write a password on this sheet. Keep your passwords to yourself, or in a password manager.



The router

- | | |
|---|--|
| <p>☐ The router's settings password is changed from the one on the sticker, and is different from the Wi-Fi password.
On some routers (eir's F3000, for one) it starts out the same as the Wi-Fi password on the sticker, so anyone with your Wi-Fi password could log in to the router's settings.</p> <hr/> <p>☐ The Wi-Fi password is changed from the short one on the sticker: at least 12 characters, ideally four or more random words that are not about you.</p> <hr/> <p>☐ Security is set to WPA3, or WPA2 (AES) if a device can't use WPA3. Never Open, WEP, WPA, TKIP or a "WPA/WPA2" mix.
Your router only offers WEP or WPA? Ask your provider for a newer one.</p> <hr/> | <p>☐ WPS is turned off, if your router lets you. NCSC Ireland says its PIN can easily be guessed by brute force.</p> <hr/> <p>☐ Remote management (changing the router's settings from the internet) is turned off, if your router lets you.</p> <hr/> <p>☐ UPnP is off if nothing needs it. If a game or gadget stops working, it may need it back on.</p> <hr/> <p>☐ Automatic updates are on, if the router offers them. Not sure? Ask your provider.</p> <hr/> <p>☐ The network name doesn't say who you are or where you live, and isn't the router's default name.
No names, address or Eircode. A default name can tell an attacker the router's make and model.</p> <hr/> |
|---|--|



One thing to do this week

Change your router's settings password from the one on the sticker, to one that is different from your Wi-Fi password. Your provider's help pages show how.



What's connected

Open your router's app or settings page and find the list of connected devices. Write each one down. Don't recognise one? Find out what it is, and remove it if you can't.

Device its name in the list	Where it is	Whose	Recognised?
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐
			☐



Visitors and smart devices

☐

Visitors use the guest network, with its own password, not your main Wi-Fi.

Anyone on your main Wi-Fi can cast to your TV, and may reach your printer and shared folders.

☐

Smart plugs, bulbs, speakers and cameras are on the guest network, where they only need the internet.

Then they can't find the other devices on your home network.

☐

The guest network has a password. If it is open, with no password, turn it off.

☐

Your Wi-Fi password goes only to people you trust.



What others on your Wi-Fi can reach

Anyone on your Wi-Fi may be able to reach these. Check each one.

☐

The printer's settings page has its own admin password, changed from the default.

Printer makers ask you to change it: the default may be on a label, or even the printer's serial number.

☐

Smart TVs and cameras have their own passwords, not the default ones.

Some cameras come with a well-known default, like admin or 000000.

☐

Smart devices install updates automatically, where they offer it.

☐

You know what your computer shares, and nothing private is shared with "Everyone".

In Windows, type \\localhost into File Explorer's address bar to see what is shared.

☐

Cheap Android TV boxes, tablets and photo frames: buy from makers and shops you trust.

NCSC Ireland found harmful software already installed on some low-cost devices; a factory reset often doesn't remove it.



Notes: what to fix, and when