



# Practical Tips for Staying Secure in a Connected World

## Part Two: Staying safe at home

In light of recent high-profile data breaches, more of us are becoming aware of the risks of living in a digital, connected world. While we might be more aware of the risks at this moment, they didn't just appear; we've been living with things like data breaches, identity theft and scams for years.

In this series on personal security, we're discussing things you and your family can do to stay safe online. In this article, we'll cover a few things you can do to make your home more secure and provide you with some resources if you want to dig into these topics in more detail than we cover here.

### Update your network settings

Most of us use the WiFi router we got from our internet service provider ("ISP"), Telstra, Optus, Aussie Broadband etc.. While many ISPs are getting better at provisioning the hardware they send to us, there are still some thing you can do to improve the security of your network at home.

It might seem intimidating to meddle with the settings of your WiFi router, concerned you might accidentally change something and break the

internet. While this is possible, what we'll cover here should be fairly straightforward to complete and shouldn't impact your internet configuration. If you have any concerns or questions, you can contact your ISP and they should be able to walk you through these steps in more detail.

#### 1 Change the default administrator password on your WiFi router

It might come as a surprise, but many WiFi routers from ISPs still ship with administrator account 'admin' with a password set to something like 'password', 'admin' or 'telstra'. If you haven't updated your WiFi router recently, it's likely you still have some combination of these; generally, you can check by looking at the bottom of your WiFi router

where these details are typically printed. This combination of default settings makes it easy for an adversary to make changes to your WiFi router and interfere with your internet, like sending you to spam or malicious websites that can load malware onto your devices. Change your administrator password to something you will remember which isn't related to your personal circumstances.

## 2 Change the name and password of your WiFi network

Similar to point 1, most WiFi routers come with a default network name and password when you first turn them on. They typically carry the form 'telstra-12345' or 'aussie-broadband-a342f', but there's no need to have your ISP's name as your home WiFi network name.

Other than being free advertising for your ISP, you're giving away information about your network to a potential adversary. Information like this is useful to attackers because they can quickly narrow down their attacks to focus on a subset (e.g. just Telstra or Optus) of WiFi routers making it easier to target your network and break in.

When you change your network name, don't choose a name that exposes information about you. Network names like "smith house" if your name is Jordan Smith are not ideal. If you're looking for inspiration, names like 'Nacho WiFi' are always a fun place to start.

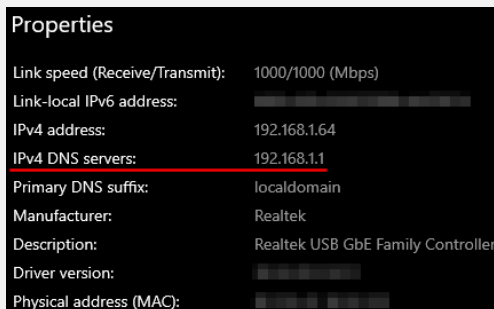
For the network password, a phrase is a good way to secure your network. A phrase of a few words will typically exceed 15 characters and be easy to remember. Spaces, punctuation and capital letters are also good additions that increase the complexity of the passphrase without making it harder to remember. As it happens, it's also just good grammar.

## 3 Advanced/Optional: Turn off UPnP

This one takes a little more work to find, but it's worth turning off if you don't need to access services (e.g. a camera system) remotely from outside your home. UPnP allows devices inside your network to tell the firewall in your WiFi router to open ports to the internet without telling you.

Opening a port in your firewall is like opening a door in your house, it can be good to let in people you know, but it's not a good idea to leave it open and unsupervised. Someone might invite themselves in and help themselves to your belongings. If you need to open a port, you can do it manually and limit how long it's open for. That way you have control over what is allowed into your network from the internet.

For all of these steps above, you will need to access your WiFi router's admin portal. Most home WiFi routers can be accessed via a web browser by navigating to the IP address 192.168.0.1 or 10.0.0.1 – it will depend on your device. If you're unsure what your IP address is, you can look up the address from your computer's settings, otherwise, some WiFi routers have the address on the bottom with the admin username and password.



Properties	
Link speed (Receive/Transmit):	1000/1000 (Mbps)
Link-local IPv6 address:	██████████
IPv4 address:	192.168.1.64
IPv4 DNS servers:	192.168.1.1
Primary DNS suffix:	localdomain
Manufacturer:	Realtek
Description:	Realtek USB GbE Family Controller
Driver version:	██████████
Physical address (MAC):	██████████

Before moving on, it's worth noting that there are lots of tools and products around that allow you to take more control of your network, from firewalls to advanced home networking solutions. We're not going to cover them here, but if you're interested in trying some of this kit, make sure you do your homework first.

## Content management

Monitoring what happens on your home network isn't always easy, but there are some steps you can take to make browsing activities more transparent and controlled. We'll talk about two tools here:

### 1 DNS filters and blockers

Much like your phone number, servers on the internet use an IP address to be contacted. The Domain Name Service ("DNS") does a few things, but the main one for us to know is that it turns a domain name (e.g. 'google.com.au') into an IP address (e.g. 192.168.0.1). This is great, because it means we don't need to remember all the IP addresses of sites we like to visit, we can just enter 'google.com.au' and our web browser takes us to the website without us knowing what the server address is.

DNS filters act as a middleman that checks to see if a website you request is safe, and returns the IP address to your browser if the site is safe, or blocks the request if the site is not safe. Cloud-based services like OpenDNS and Cloudflare provide DNS filtering services that can prevent access to sites from adult content and black markets to malicious websites serving malware or scams. They're not perfect and they don't catch everything, but they do stop a lot of things. You can also look into software like pi-hole if you don't want to rely on a cloud service.

Blocking different types of content is a conversation you need to have with the people you share a house with, but blocking malicious sites is highly recommended. Doing so can help save you if you accidentally click on a phishing link or a link to malware by stopping the request before you get to the malicious site.

### 2 Time limits for devices at home

A hot topic for many parents of pre-teen and teenage children is time limits for internet connected devices, but it's also something that we may want to consider for ourselves. Switching off for a bit is good for maintaining balance and setting yourself a hard cut off can help with managing the endless scrolling of social media feeds before bed.

Time limits allow you to turn on/off internet connectivity for specific devices at different times of the day (e.g. allowing access from 6am – 8pm). That means, you can limit access on phones, tablets and laptops, while still allowing access to things like smart TVs so you can put your phone down and finish watching the end of that movie on your favourite streaming service.

Time limits can play a role in supporting families managing things like cyber bullying; but, like with the DNS filtering above, a conversation with the people you share a house with is generally a good idea before you start limiting internet access.

Both of these options can be managed from your home WiFi router, but there are also software products and apps you can use to manage access if you prefer not to navigate through the settings in your WiFi router.

## More resources

To close this conversation, it's important to note that we have only touched briefly on some complex topics. There are lots of great resources available online that continue this conversation and can help you and your family work through these topics.

### E-Safety (<https://www.esafety.gov.au/>)

Many of us may already be familiar with the e-Safety commission, they were the world's first commissions tasked with maintaining a safe internet. Amongst their many activities, the commission investigates cyber harassment and performs many child protection activities.

They also have lots of resources to help you work through the topics we've covered here and many more.

### Scam Watch (<https://www.scamwatch.gov.au/>)

We only touched on scams briefly, but with the recent high-profile cyber attacks and heading into the holiday season, there are going to be more (and increasingly sophisticated) scams doing the rounds in the coming months.

Scam watch provides information about the recent scams, provides information about how you can spot and prepare yourself against a scam, and what to do if you or someone you know has fallen victim to a scammer.

## Closing

In this article we've covered a few ways you can improve the security at home, and some steps you can take to help protect you and your family while browsing the internet. The e-safety commission and scam watch are both useful resources for preparing your home.

## CONTACT US

---



### Ed Little

[elittle@amstelveen.com](mailto:elittle@amstelveen.com)

Ed is a Senior Manager at Amstelveen, specialising in cybersecurity and data governance. Ed also oversees Amstelveen's product offerings including Amstelveen Risk Culture platform 'Amstelveen iQ'