Contents

Router Security

For the majority of homes with internet access the main method of communicating with these devices will be through your home Wi-Fi network. Therefore it is important that this network is as secure as possible. This starts with the Wi-Fi router, which is the device that connects your home devices to the internet wirelessly.

If your router has security weaknesses this means that hackers could be able to access your internet connection by gaining control of your router. This could be done remotely, so you would not know that it had happened. If hackers gain control of your router they would then be able to gain access to your devices and view your web activity; e.g., if you were undertaking online banking then they could acquire your login details, with all of the potential damage that could ensue.

There are some security areas that should be considered when using a router.

- **Firewall**. A Wi-Fi router that uses a recognized firewall should be used, as this will help to prevent malicious software and programs infecting your system.

- **Encryption**. This should be used by your router, to ensure that all communication is encrypted to make it much harder to be hacked or intercepted.

- **Auto-updating**. Routers sometimes have software updates that are designed to improve security or patch any flaws that have been identified. Look for a router that does this automatically whenever an update is available.

- **Change the default router password**. See Tip 7.

Check the specifications of the router before you buy it to see its security features.

Changing a Router Password

One area of security weakness for Wi-Fi routers can be their admin password. This is set when the router is manufactured and is generally very basic, along the lines of “admin” or “password”. It is therefore important to change this password as soon as possible, to make it more secure. To do this:

1. Open a web browser and type the router’s address in the address bar. (This is usually in the form of 192.168.1.1 or similar. Check with the documentation that came with the router, or search on the web using your router’s model name)

2. Enter the **Username** and **Password**. If these have never been changed they should be along the lines of **Admin** and **Password**. Check the router’s documentation if you are unsure about the default login details

3. Access the section for changing the password, and update the router with a secure password

16 Two-Factor Authentication

Also known as multi-factor authentication, two-factor authentication (2FA) is a security feature that requires a user logging in to an account on a website or an app to present two pieces of unique information in order to gain access to the account. One piece of information is the combination of username and password. The second piece of information is something that is generated at random once the first piece of information has been entered correctly.

Two-factor authentication is frequently used in conjunction with smartphones: when the user wants to log in to an account, a one-time passcode is generated once they have entered their username and password. This is sent to their smartphone and once the passcode has been entered successfully, the user will have access to their online account.

If an online account supports two-factor authentication you will be asked if you want to use this when you log in to the account. A smartphone number will need to be linked to the account, so that the one-time passcode can be sent to it. If an account has two-factor authentication, then it should be used, to make the account much more secure.

When you log in to a two-factor authentication account, a passcode field will appear. The passcode will be sent to your smartphone and can be entered from here.

About Password Managers

One way to create strong passwords automatically is to use a password manager. This is an app that performs a number of security options relating to secure passwords. All you need to do is remember one password, for your password manager (this makes it even more important to ensure that your password for the password manager is stored securely).

Password managers can be downloaded from app stores connected to desktop PCs or laptops, and also the app stores connected to smartphones and tablets. If you use a password manager, ensure that it is downloaded to all of your digital devices, so that if a strong password is automatically generated on one device, it will be recognized by the password manager on all of your other devices. Some of the features of a password manager to look for are:

- **Password generator**. This is used by the manager to create very complex and secure passwords, which it duly remembers for you.

- **Encryption**. Make sure that the password manager encrypts your passwords and saves them securely, so that even if the password manager site was hacked, your passwords will be safely encrypted.

- **Cross-device compatibility**. Some password managers are specific to a single operating system; e.g., iOS on the iPhone or iPad. Others can be used across devices using different operating systems.

- **In-app purchases**. A lot of password managers are free to download, but have a paid-for version that can involve an annual subscription. This does not have to be used, but it does add extra functionality.