

Tips to secure your Internet of Things device



The Australian Cyber Security Centre has developed this information to help the community buy and use Internet of Things (IoT) devices securely. An IoT device is an everyday item that has had internet connectivity added to it. Examples of IoT devices include baby monitors, drones, security cameras, smart televisions and solar inverters. IoT devices within homes and businesses generally use Wi-Fi or cellular networks, such as 4G or 5G, to connect to the internet.

Many IoT devices commonly found in Australian homes and businesses have not been designed with security in mind. This has resulted in devices being vulnerable to compromise via the internet. Such incidents can allow cybercriminals unsolicited access to your device and personal data for malicious purposes.



Australian Government
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre

Before purchasing an IoT device

It is important to research devices before making a purchase, as manufacturers provide varying levels of security. Before purchasing a device, compare similar devices sold by different manufacturers.

Things to consider include:

1 **Is the device made by a well-known reputable company and sold by a well-known reputable store?** Well-known reputable companies are more likely to produce devices with security in mind. Well-known reputable stores are more likely to only sell devices from well-known reputable companies, and have a stricter supply-chain ensuring the device gets to you as intended by the manufacturer.

2 **Is it possible to change the password?** It is always good to change your password. However, if the device is shipped with a weak default password, this becomes more important. A device with good security should have unique, unpredictable, complex and hard to guess passwords, as weak default passwords are the easiest way to attack a device.

3 **Does the manufacturer provide updates?** It is important that companies offer updates to fix device vulnerabilities as they are discovered. For example, if software on the device contains known vulnerabilities or hackers develop new ways of compromising your device, updates are required to provide fixes.

4 **What data will the device collect and who will the data be shared with?** Information about what data will be collected and how it will be used should be readily available on the manufacturer's website or in their privacy policy. Always consider the information collected by the online app or mobile app.

5 **Does the device do only what you want it to do?** Buying a device that does more than what you need, including connecting to the internet, may reduce your security. Device capabilities that you will not use can increase the device's vulnerability to attacks without providing any benefit to you.

Setting up an IoT device

Keep in mind a few simple questions while setting up your device, to help you keep your network and data more secure.

1 **Does the device need to be connected to the internet?** Just because it can be connected doesn't mean that it should. Devices that are not connected to the internet are much less likely to be compromised. If you're not going to use the features that require internet connectivity, then you should consider whether it needs to be connected.

2 **Is the device in a secure location?** If the device does not need to be installed in an insecure area, installing it in a secure location can reduce the risk of physical compromise. Treat your IoT device like any other valuable and keep it behind locked doors if possible.

3 **Do I change the default username and password?** It is important that you [use a strong password or passphrase](#). If your device is not equipped with a unique, unpredictable, complex and hard to guess password, then you need to change the password. Default usernames and passwords are collected and posted online, leaving your device vulnerable.

4 **Is my Wi-Fi network set up securely, and does it have a secure password?** [Secure your Wi-Fi network and router](#) to make it harder for attackers to access your device and your network.

Go the extra mile

Set up an additional Wi-Fi network on your router for IoT devices only. This may be known on your Wi-Fi router as a 'guest' network. If your IoT devices do not require communication between each other, enable the 'client isolation' feature. Keeping your IoT devices isolated from your sensitive data helps ensure that a compromise of an IoT device does not grant access to your other devices or data.

5 **Are unnecessary device features turned off?** If your device has unwanted or unnecessary features (such as cameras or microphones), these should be disabled where possible.



Go the extra mile

Look for a configuration setting that mentions enabling remote access to the device's web administration interface from the local LAN or WAN/ internet. Ensure it is set to local LAN, unless you require remote access yourself.



Maintaining an IoT device

There are some important things to remember once your IoT device is set up and in use. These include:

-  **1 Reboot your devices regularly.** If the IoT device starts to become slow or inoperable, it may mean that viruses are present. Some malware is stored in memory and can be easily removed by a device reboot, that is, by turning the device off and on. If the device continues to be slow or inoperable after a reboot, try a factory reset. Be aware that implementing a factory reset may wipe your user data and personalised settings.
-  **2 Apply regular updates.** Some devices apply updates automatically. For those that don't, regularly check with the manufacturer and apply updates when they become available. When updates are no longer available for your device, consider upgrading to a newer device where updates are available. Devices that don't have access to security updates will not be protected if new vulnerabilities are discovered, and these devices may become a risk to your network, your privacy and your data.
-  **3 Turn off your device when it is not in use.** Leaving unused and unmonitored devices powered on and connected to your Wi-Fi network for extended periods can increase the likelihood of your devices being attacked. One option to achieve this automatically is to use a power outlet timer to only provide power to the device during the specified hours.
-  **4 Watch for a significant increase in your monthly internet usage or bill.** Significant increases in internet usage or billing charges can indicate that your device has been compromised. Implementing a factory reset and changing the password on your IoT device may assist (but remember that a factory reset may wipe your user data and personalised settings).

Disposing of an IoT device

Disposing of a device (by discarding or selling it) may give other people easy access to your personal information or data. Ways to prevent this include:

-  **1 Erase all data and personal information.** The manufacturer should provide a method for how to erase your data and personal information from both the device and associated applications. Erasing your personal information ensures that no one gains access to it after you have disposed of the device. Delete your online account if it is no longer needed without the IoT device.
-  **2 Perform a factory reset of the device.** A factory reset is designed to erase data kept in local storage and reset passwords, usernames and settings back to default. Check the device's user manual or the manufacturer's website for information on how to perform a factory reset.
-  **3 Disassociate the device from mobile phones and other devices.** Disposing of a device that still has access to your other devices, network or online accounts has the potential for others to gain access. Make sure you check your other devices and remove any pairing with the device you are disposing of. Remove any permissions granted to the mobile application that are no longer needed.
-  **4 Remove any removable media (e.g. USB flash drives, memory cards etc.) attached to the device.** Removable media may contain personal data that is not deleted in a factory reset and should be physically removed, physically destroyed and disposed of separately from the device.





Help

Contact the Australian Cyber Security Centre by emailing asd.assist@defence.gov.au or call the 24/7 Hotline for urgent assistance on 1300 CYBER1 (1300 292 371).

Report cybercrime to ReportCyber at www.cyber.gov.au/report

Contact IDCARE via their website www.idcare.org if you've experienced identity theft.

Visit www.cyber.gov.au for advice for you and your family. Sign up for the free ACSC Alert Service on recent online threats.

Let's make Australia the safest place to connect online.
For more cyber security advice, visit www.cyber.gov.au



Australian Government
Australian Signals Directorate

ACSC

Australian
Cyber Security
Centre