



Your Guide to the Internet of Things (IoT)



An information security eBook by TSC

Inspire. Engage. Protect.



Your Guide to the Internet of Things

If you own a smart speaker, fitness tracker, smart meter or games console, you're an Internet of Things (IoT) user.

Most of us don't consider ourselves as IoT users with IoT devices. We only think of these gadgets as 'smart' devices that help make our lives easier.

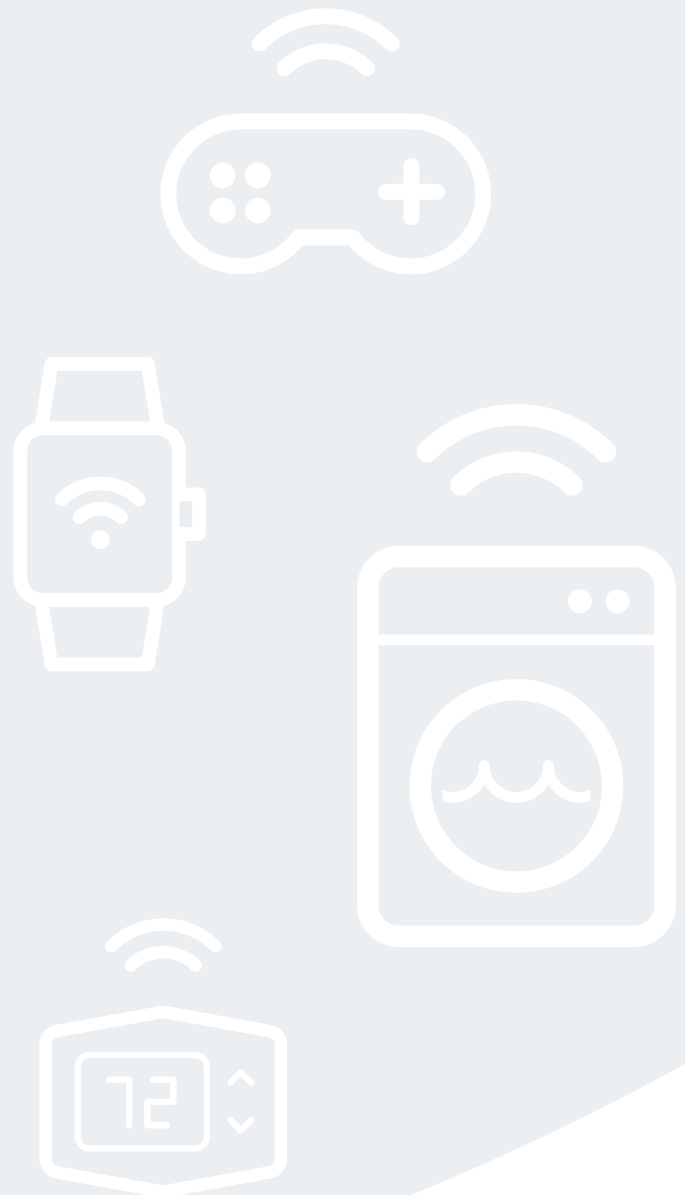
But the Internet of Things is growing. And as technology continues to evolve, these devices are becoming more integrated into our lives with more access to our personal information.

FACT

There were 9 billion IoT devices in 2017 and 10 billion in 2018. IoT is predicted to grow to more than 64 billion devices by 2025.

FACT

Cisco researchers predict 50 billion devices will be wirelessly connected worldwide by 2020.





What is the Internet of Things?

The Internet of Things (IoT) is the network of connected devices that can collect and exchange data via an internet connection.

It is made up of billions of smart products that incorporate everyday devices, sensors and systems. These products range from tiny sensors that track things like calories and humidity, to connected devices that span entire cities.

Kevin Ashton, co-founder of AutoID at MIT, is credited as first using the term. He said that the Internet of Things has 'the potential to change the world, just as the internet did. Maybe even more so'.



Today's information technology is so dependent on data originated by people that our computers know more about ideas than things.

If we had computers that knew everything there was to know about things – using data they gathered without any help from us – we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best.

We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory.

(Kevin Ashton)



IoT devices

Phones and computers are only a small part of IoT.

If a device has an internet connection and integrated technology to collect and share data, it's an IoT device. Along with communicating data, some IoT devices also allow us to access or control them remotely.

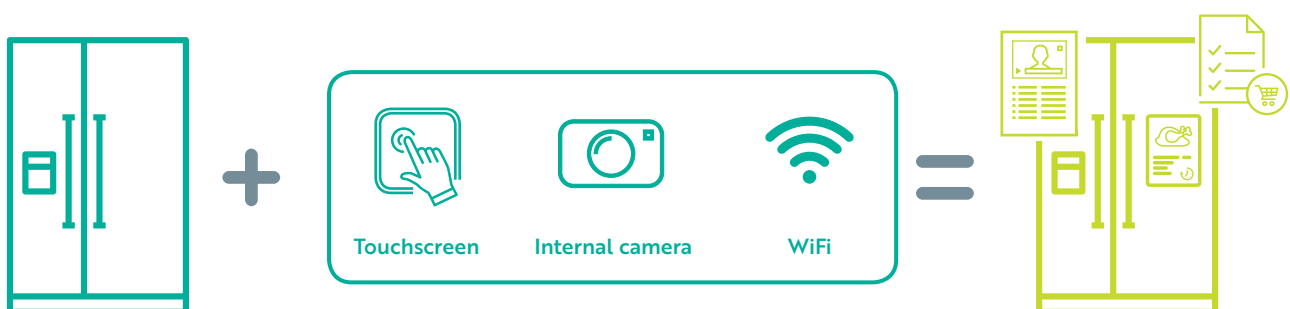
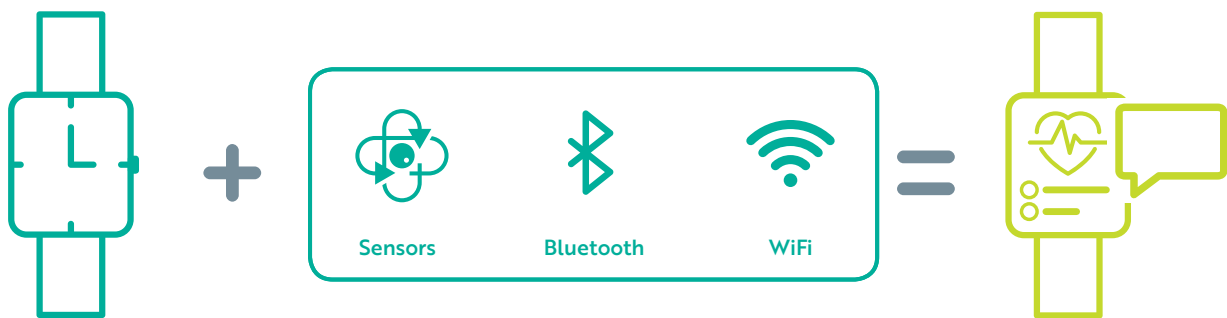
The popularity of IoT devices is perhaps most noticeable in our homes, from appliances we can control with our phones to smart refrigerators that allow us to order food.

IoT has become more accessible and convenient because devices can easily be integrated into a home network, potentially allowing us to control all our devices over a single interface.

Smart energy appliances allow us to monitor and control our lighting, temperature and energy consumption remotely.



These IoT devices can help us save on energy costs by automatically turning off lights and adjusting the temperature in our homes, or just making us more aware of our usage.


Home automation is made easier by platforms such as Google Home and Amazon Alexa, which allow IoT devices – such as thermostats, plugs, lamps, locks, appliances and sensors – to communicate over a unified network.

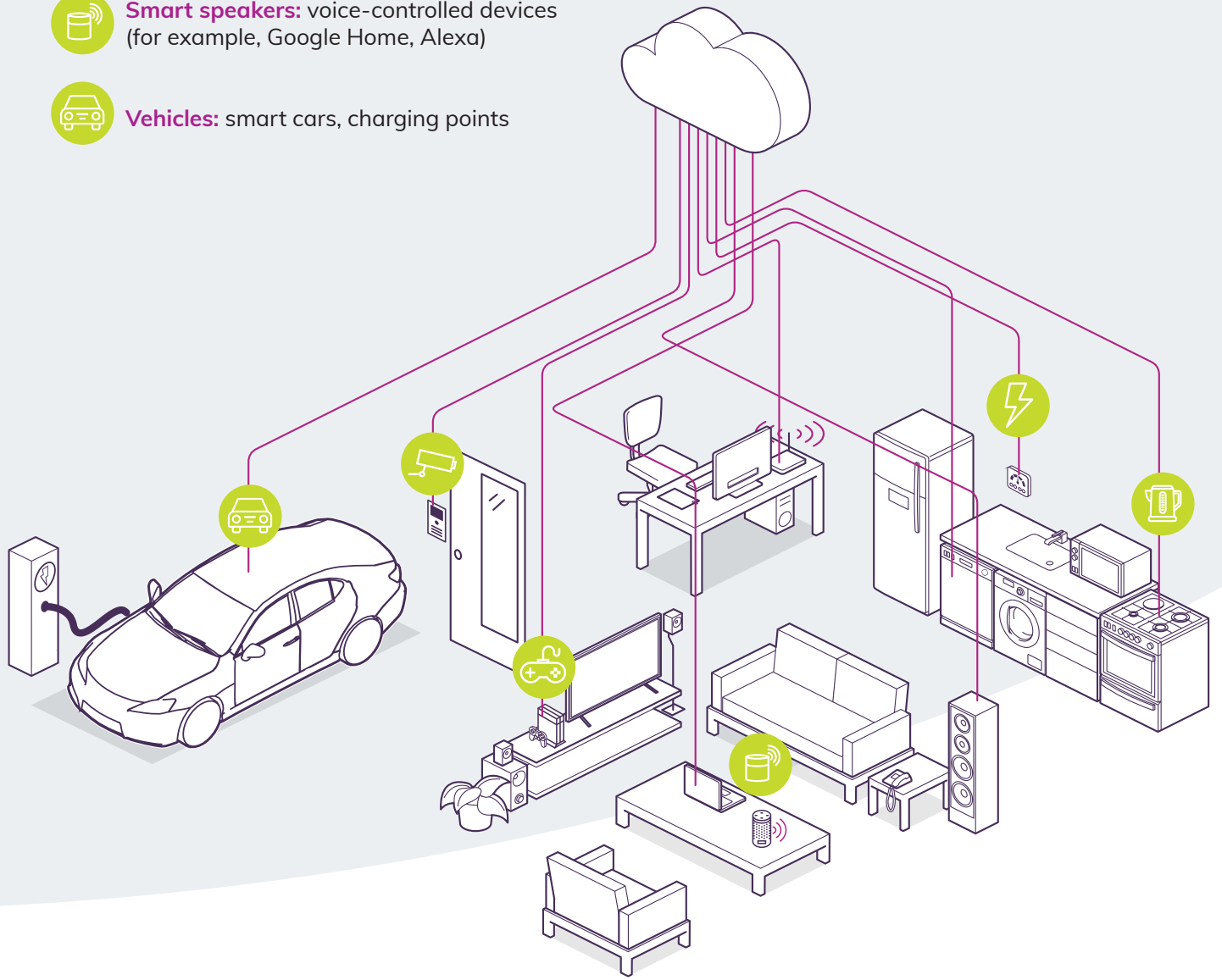




Examples of IoT devices in the home include:

-  **Security:** cameras, doorbells
-  **Energy:** smart meters, smart plugs
-  **Entertainment:** televisions, games consoles
-  **Appliances:** coffee machines, refrigerators, ovens
-  **Smart speakers:** voice-controlled devices (for example, Google Home, Alexa)
-  **Vehicles:** smart cars, charging points

 **FACT**
The number of IoT devices is predicted to increase to 500 per household by 2022.





IoT sectors

IoT devices can also be found in a range of industry sectors where they are used in a variety of ways.



Healthcare

IoT has played a part in healthcare advancements and given us more control over our health, fitness and medical treatments.

Those with medical conditions can use IoT devices and sensors, such as heart monitors and insulin pens, to track their health and medication, generate reports for doctors and collect data about their condition. This real-time monitoring increases the chance that any issues will be identified and responded to instantly, helping both patients and doctors take preventative measures.



Fitness

Fitness trackers can monitor a range of health data including exercise, distances travelled, heart rate, sleeping patterns, calories and personal fitness targets.

Fitness trackers are increasingly being promoted by insurance companies who encourage their customers to wear and use them. By tracking health and fitness, the hope is to encourage users to lead healthier lives and, thus, reduce insurance claims and premiums.



Urban development

IoT is increasingly influencing the development of our towns and cities to turn our urban areas into 'smart cities'.

Sensors can be used in roads to detect the amount of traffic and adjust speed limits accordingly. They can also adjust street lighting levels, indicate available parking spaces and monitor the structural integrity of bridges, tunnels and buildings. We can also receive live updates for public transport, incidents, delays and diversions straight to our mobile devices.



Manufacturing

Manufacturers can now use IoT to track their merchandise and revenues.

They can use GPS and radio-frequency identification (RFID) to precisely track products in transit and collect data on its condition, arrival times and storage temperatures. This makes it easier for manufacturers to ensure their products are delivered on schedule and without damage.

The data also allows companies to monitor their inventory and ensure supplies don't run out.

FACT

178 million wearable devices were shipped in 2018 – this is expected to grow to 453 million by 2022.



Pros and cons of IoT devices

IoT allows us to connect our devices and create home networks for efficiency and convenience, however, there are benefits and challenges related to its use.

Advantages of IoT devices include:

- They allow us to access information and devices in real time from anywhere.
- They can automate daily tasks and give us more control.
- They increase efficiency and save time, making our lives easier.
- They help save money by monitoring energy usage, reducing manual tasks, and transferring data quickly.

Disadvantages of IoT devices include:

- They are prime targets for hackers and cybercriminals. The more devices we connect, the greater the risk of a data breach.
- They do not always have strong security features and may come with weak default passwords.
- Software updates may be discontinued, leaving devices unsupported and vulnerable.
- Automated tasks can impact employment levels as they can reduce the need for human actions.
- Legislation around IoT is not keeping up with the rate of growth.
- We are becoming more dependent on technology for the smallest of tasks and losing the ability to do these things for ourselves.



FACT

95% of all new devices will incorporate an internet connection by 2020.



How secure are IoT devices?

The more we rely on connected technology, the more we are at risk from cyber threats tailored to exploit IoT flaws and vulnerabilities.

IoT devices are prime targets for hackers because they collect and share data about us, our homes and businesses. Devices and their connections present opportunities for cybercriminals to enter a network and steal information.

The rapid growth of IoT means people do not always know how devices connect, access and share data or how to keep them updated and secure. IoT connectivity may also be bundled into products whether consumers realise it or not. As a result, many are unaware of the risks these devices can pose to data security.

While the data collected by IoT devices is useful for businesses, customers and governments, it's also a target for malicious actors. As more sector and consumer devices become connected to the internet, IoT becomes more vulnerable to ever-evolving cyber attacks.



FACT

There were an average 5,200 IoT attacks per month in 2018 – 90% came from routers and connected cameras. (Symantec, 2019)



How secure are IoT devices?

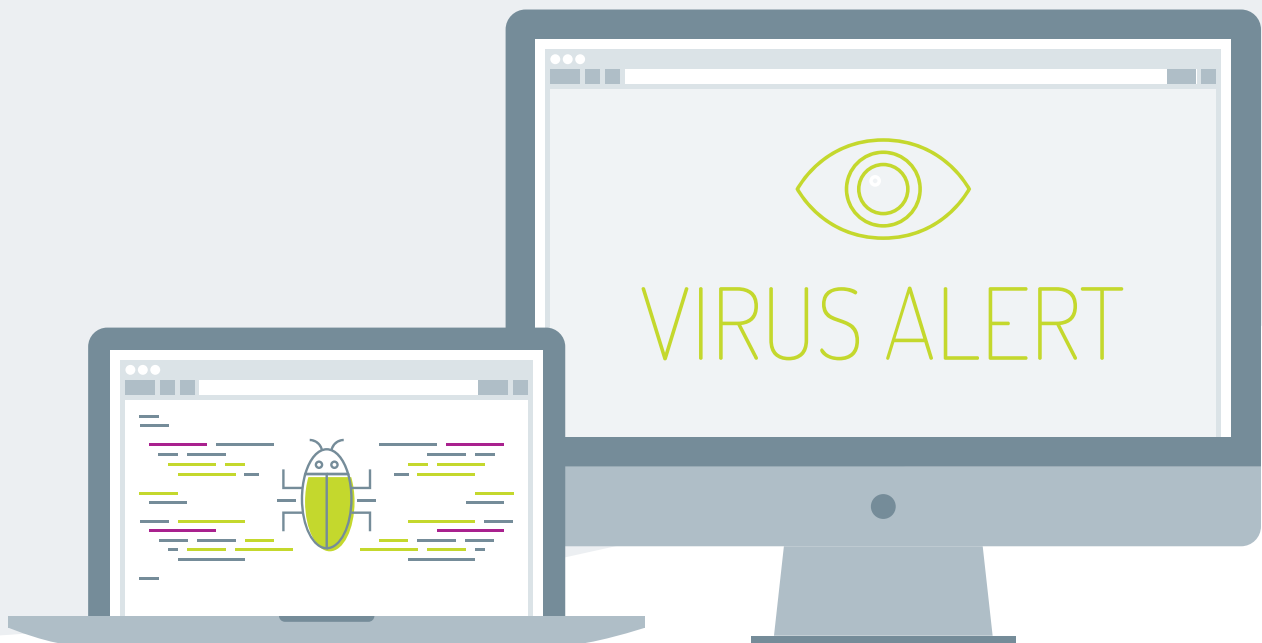
Unsecure devices

Hackers will target anything from routers to refrigerators – just one weak device can compromise an entire network and grant them access our data. Devices can also be used to track our locations, online activity, or to spy or eavesdrop on us.

IoT devices, even with only basic security, can connect to home WiFi networks and then link to other devices such as computers and mobile phones. Cybercriminals can exploit these weak security settings to gain access to home networks and steal personal information – they could even access biometric data, such as fingerprints or facial recognition images.

Some IoT devices, such as smart meters and cameras, monitor which appliances are being used, learning their owners' schedule and habits. If hacked, criminals could use this information to find out when our homes are empty and vulnerable.

Then there is the potential for eavesdropping and spying. There have already been instances of webcams and baby monitors being hacked and used to spy on the victims and their homes.





How secure are IoT devices?

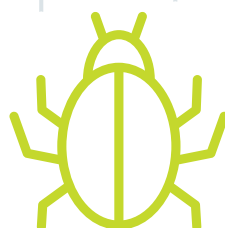
IoT threats

- **Malware:** Malicious software can use known vulnerabilities and weak passwords to access devices and run tasks.
- **Botnets:** Unsecure IoT devices can easily become part of a botnet – potentially thousands of devices controlled from a central device – and launch DDoS attacks.
- **Cryptomining:** Cybercriminals can install miners onto compromised devices without the victim's knowledge and use the devices to mine cryptocurrency.

Attacks like the Mirai botnet continue to evolve and exploit new vulnerabilities. New malware campaigns continue to be launched; notably the VPNfilter strain that targets home and office routers and network storage devices, rendering them unusable.

FACT

The Mirai malware created a botnet of webcams, CCTV cameras and routers to carry out attacks on internet service providers and businesses.





In the news

Doll toy hacking fears

In 2017, the Federal Network Agency in Germany advised parents to destroy a talking doll toy, My Friend Cayla, because the device could reveal personal data.

Researchers claimed hackers could use an unsecure Bluetooth device in the toy to eavesdrop and talk to children. But the UK's Toy Retailers Association said the doll 'offers no special risk'. The toy is now banned in Germany.



Vulnerable home security camera

A wireless security camera vulnerability meant audio and video recordings could be hijacked by tweaking the Swann Security app.

The flaw affected Swann Smart security cameras and resulted in one customer being sent another person's recordings. The user described the incident as a 'gross breach of privacy'. The issue was resolved by Swann in 2018.



Oven control app vulnerable to hackers

An Aga oven app that allows users to control their cookers remotely could have been vulnerable to hackers.

In 2017, cybersecurity researcher Ken Munro of Pen Test Partners discovered vulnerabilities in the iTototal Control system that could allow hackers to turn ovens on or off. Mr Munro also criticised issues relating to unauthenticated SMS messages used to control the system, weak passwords and emails sent as plaintext.



Health apps pose privacy risk

In 2019, researchers warned that popular health apps may not be keeping data about medical conditions confidential.

Medical journal BMJ studied 24 health apps and found that 19 shared user data with other companies including Google, Facebook and Amazon. The report also found that data was shared even if developers claimed they did not collect personally identifiable information. The journal concluded that patients need to be warned about privacy threats relating to these apps.



Child smartwatches easy to hack

In 2018, a security researcher warned that a children's smartwatch could be easy to hack because of unsecured accounts and unencrypted data.

The researcher said he could use the MiSafes Kid's Watcher Plus to track children's locations, make spoof phone calls pretending to be from parents, and eavesdrop on activities.



Smart devices and domestic abuse

Smart home devices can be used to control and harass victims of domestic abuse, the New York Times reported.

It identified that devices could be used to monitor, scare and confuse victims by locking doors or altering thermostats, for example.

A resource [list offering guidance](#) to those affected was published online.





How aware are IoT users?

The continuing growth of IoT and smart device usage means information security is an essential cornerstone in the threat landscape.

All devices, both large and small, are significant because each one is a gateway for hackers to infiltrate other devices on a connected network.

But many users are unaware that the majority of IoT devices are sold without basic security features.

Manufacturers do not always add adequate security features (such as data encryption) or tell users how to change default passwords. Software may not be updated, or it may not be clear how users can ensure their devices are up to date.

Many consumers and businesses still use older operating systems: only 20% of Android devices were running the newest major version in 2018, a Symantec report found.

FACT

The average smart home has 20 smart devices, including the home router.





How aware are IoT users?

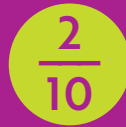
A Bitdefender report identified weak passwords, lack of firmware updates and unsafe browsing were the most prevalent IoT vulnerabilities.

Of the users surveyed:

Passwords



use the same password for all smart devices



have several passwords that they randomly use, but are still shared by some devices



smart TV owners have never changed their device password

The weakest passwords were found in phones (44.8%), printers (16.6%), and computers (10.3%).

Firmware



do not install updates on their wireless router throughout its lifetime



do not run updates on their smartphones or tablets



do not run updates on their smart TVs





How aware are IoT users?

Unsafe browsing

50%

store personal information on their phones

61%

store private files on their personal computer

11%

keep information on dedicated storage solutions attached to their home network

$\frac{6}{10}$

worry their identity could be stolen, their information accessed, or their devices infected by malware

$\frac{7}{10}$

have a vulnerable router connected to a least one internet-enabled camera

$\frac{5}{10}$

smart TV users have not updated software apps in over a month

The most vulnerable connected devices were routers (59.5%), computers (9.5%) and network-attached storage (NAS) (9.3%).

IoT users are also concerned about how connected devices collect data and how their privacy is protected. A recent study by Ipsos Mori found that:

63%

of global consumers consider their IoT devices 'creepy'

48%

of British consumers do not trust devices to handle information responsibly

73%

worried about eavesdropping

The report also found that a variety of products are 'rushed to market' with little thought about basic data and privacy protection.

Many of those surveyed believed that accountability for connected devices should sit with manufacturers, retailers and regulators:

88%

said regulators should enforce IoT privacy and security standards

80%

said retailers need to address security and privacy

60%

think consumers are mainly responsible for the security and privacy of their devices



IoT regulation

Data security is a crucial part of IoT, but there are currently no official security requirements in place (at time of writing), meaning users need to be more aware of their responsibilities to keep data and devices secure.

Attacks such as botnets and strains of malware continue to evolve and exploit new vulnerabilities. But despite high-profile attacks highlighting IoT weaknesses, the first regulatory steps for security countermeasures have been tentative.

Regulators are still catching up with the rapid growth of IoT, meaning some new products are not entirely secure.

Manufacturers and services providers may have reviewed how they collect and process users' data since the introduction of the General Data Protection Regulation (GDPR), but security-related processes still need to be addressed.

But implementing effective regulation comes with many challenges. For regulation to be effective on the internet, it needs to be coordinated on an international scale – a process that is both complicated and time-consuming.

The rapidly evolving threat landscape of IoT is also a challenge as regulation races to keep up and implement relevant and effective guidelines.





IoT regulation

IoT Code of Practice

The UK government released its voluntary Code of Practice for consumer IoT security in 2018 as part of the Secure by Design report.

The Code of Practice sets out thirteen guidelines for manufacturers, service providers and retailers to ensure IoT devices are secure to use by design.

The Code guidelines are:

- 1 Do not use default passwords
- 2 Implement a vulnerability disclosure policy
- 3 Keep software updated
- 4 Securely store credentials and sensitive data
- 5 Communicate securely
- 6 Minimise exposed attack points
- 7 Ensure software integrity
- 8 Ensure that personal data is protected
- 9 Make systems resilient to outages
- 10 Monitor system telemetry data
- 11 Make it easy for consumers to delete personal data
- 12 Make installation and maintenance of devices easy
- 13 Validate input data



For more information, visit: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security>

Next steps

Following the introduction of the IoT Code of Practice, new laws have been proposed that aim to secure IoT devices.

The proposed legislation would introduce a security labelling system to show customers how secure an IoT device is.

To gain a security label, a device must:

- Use unique passwords by default.
- Clearly state how long security updates would be available.
- Offer a public point of contact for cybersecurity vulnerabilities.

The new law could mean that retailers would eventually be barred from selling IoT devices without security labels.



How to use IoT devices securely

Before you buy

- Research the device's security features and check reviews of the manufacturer and the product.
- Check for manufacturer's documentation, such as a manual or 'getting started' guide – this may be with the device, on the manufacturer's website or within a mobile app.
- Check if the device needs an internet connection or smart phone app, or if you will need to create an account to use it.
- Always buy IoT devices from trusted manufacturers and retailers.

Default settings

Some IoT devices may not be secure when first switched on. You will need to take steps to protect yourself and your information:

- Immediately change the default password. Default passwords, such as 0000 or 1234, are easy to guess and can be cracked by cybercriminals. Many passwords used by manufacturers are available online.
- Ensure all device passwords are unique.
- Create strong passwords that are a minimum of 10 characters long and use a mixture of upper- and lower-case letters, numbers and special characters.
- Use a password manager, such as LastPass, to help you remember and generate secure passwords.
- Activate two- or multi-factor authentication (2FA or MFA) if available.
- Enable automatic updates if available and install manual updates when prompted.
- Never allow devices to automatically connect to public or unsecure WiFi networks.
- Review all privacy settings to limit what data your device collects.





How to use IoT devices securely

Getting rid of your device

If you decide to sell or dispose of your device, you should:

- Perform a factory reset – this will return the device to its original settings. Check the manufacturer’s website for details.
- Remove all personal information from the device.
- Log out of and uninstall all apps you may have added to the device.

Compromised devices

If you suspect your device is compromised:

- Disconnect your device from your network, to prevent other devices becoming compromised.
- Visit the manufacturer’s website to check for news or updates on what to do next.
- Check the [Information Commissioner’s Office](#) website and the [National Cyber Security Centre](#) website for advice.
- Install any available updates or security patches released to fix the vulnerability.





Conclusion

IoT is here to stay and has the potential to change the world as we know it.

But as IoT continues to evolve, so do the security threats users face.

We must be proactive and take steps to stay ahead of criminals looking for new ways to exploit IoT devices.

Information security depends on us as individuals being more security conscious and making information security a regular feature of our lives.

Checking for updates, installing firmware and using strong passwords are some of the ways we can prevent unauthorised access to our data.

While steps are being taken to implement laws to govern IoT, these regulations need to catch up to ensure ongoing information security and data protection.

Without adequate protection, our data, homes, businesses and families are at risk.



Contact TSC for more information about Internet of Things resources and other information security support.

www.thesecuritycompany.com

 @thesecuritycompany

 @thesecurityco

 @thesecurityco



Inspire. Engage. Protect.