

The IoT: a world of connectivity



Lesson 2

Resources

- PowerPoint presentation

Intro (10 mins)
Slides 2-8

Introduction

Use the slides to introduce the lesson, the module overview, and learning objective for today. Make sure to recap the 'Big Thinking' question on slide 4: should smart devices be allowed to make decisions for us without our consent?

Big Thinking...

In this module, we will consider:

*What are the **risks and benefits** of the IoT?*

*Should smart **devices** be **allowed to make decisions** for us without our **consent**?*



Resources

- PowerPoint presentation

Activity 2 (15 mins)

Slides 9-11

The IoT: a risky business?

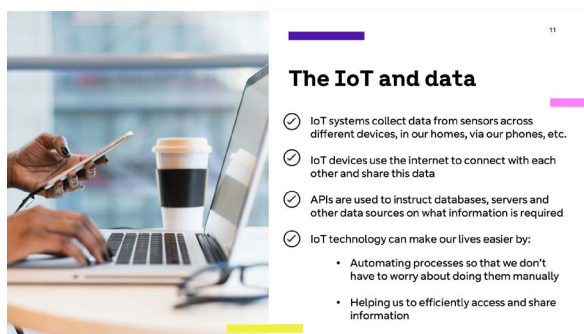
Ask students if they know how the IoT uses data and the benefits this can have. Use slide 10 to go over some of the key concepts:

- Devices in the IoT systems collect data from different sources such as sensors in our homes, microphones or cameras on our phones, etc.
- Devices within the IoT system use the internet to connect with each other and share this data.
- To make sure the right data is found and sent to the correct location, an API is used as a 'middleman' to instruct databases, servers and other data sources on what information is required - for example, if someone asks their smart speaker, for the weather in their area, the smart speaker will use an API to request a search of local forecasts from a weather database; this data is then sent back to the smart speaker so that it can answer the user's question.
- The IoT technology can benefit us by making our lives easier. It can automate processes so that we don't have to worry about doing them manually, and help us to efficiently access and share information across large distances.

Ask students to think about how their own data may have been collected. Show slide 11 to encourage a discussion around a few key questions:

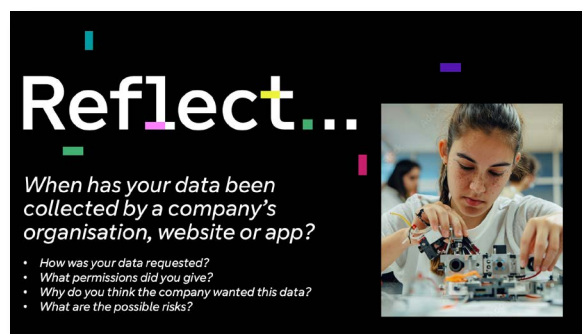
- How was your data requested?
- What permissions did you give?
- Why do you think the company wanted this data?
- What are the possible risks?

For example, when signing up to apps or social media accounts, they will probably have been asked to agree to the company's terms and conditions around data and privacy. This is often accompanied by a request to allow access to features such as their phone's camera, microphone or contacts list. Some risks might include: not reading or understanding how your data will be used or who else it might be shared with, data can be used to promote certain products or companies to someone based on their preferences, and any data shared online is vulnerable to cyber attack or scams.



Slide 10: The IoT and data

- ✓ IoT systems collect data from sensors across different devices, in our homes, via our phones, etc.
- ✓ IoT devices use the internet to connect with each other and share this data
- ✓ APIs are used to instruct databases, servers and other data sources on what information is required
- ✓ IoT technology can make our lives easier by:
 - Automating processes so that we don't have to worry about doing them manually
 - Helping us to efficiently access and share information



Slide 11: Reflect...

When has your data been collected by a company's organisation, website or app?

- How was your data requested?
- What permissions did you give?
- Why do you think the company wanted this data?
- What are the possible risks?

Resources

- PowerPoint presentation

Activity 2 (25 mins) Slides 12-16

The IoT and the dangers of data-sharing

Explain that by sending our data over the internet, there is the risk that it will fall into the wrong hands. However, the good news is that there are measures we can put in place to better protect our personal information.

Show slide 13 and read through the data disasters shown. Put 60 seconds on a timer and get students matching the topic areas to the descriptions as quickly as they can. The answers are below:

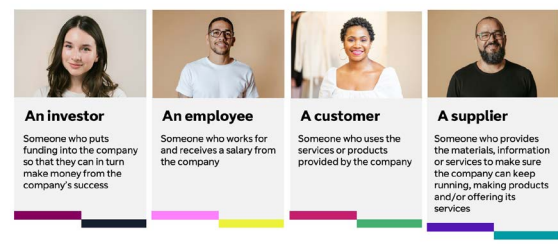
Data breaches: Cybercriminals may intercept communications between personal IoT devices or target businesses' servers to access company, employee and customer information. They will look to take advantage of private information such as bank details or login credentials.

Third party sellers: Some companies will sell personal data to other organisations to make more profit. Victims may then be exposed to more fraudulent activity if the data is sold on to cybercriminals looking for scam opportunities. The data's original owners may not know for many years, or ever, that their personal information is being used by other businesses.

Botnets: This is a network of private computers that have been infected by malicious software. They can be controlled by cybercriminals to spread malware and steal data without requiring human interaction. This means they can be extremely damaging to companies with large databases of personal information which are connected via the internet.

In their shoes

Put yourself in the role of these different company stakeholders:



Now tell students that they are going to look at these data privacy issues from the perspective of different stakeholders. Explain that a stakeholder is someone who has an interest – usually financial – in the success of a company.

Show slide 14 which lists the different stakeholders students are going to consider:

- **An investor** – someone who puts funding into the company so that they can in turn make money from the company's success
- **An employee** – someone who works for and receives a salary from the company
- **A customer** – someone who uses the services or products provided by the company
- **A supplier** – someone who provides the materials, information or services to make sure the company can keep running, making products and/or offering its services

Get students into small groups and assign each team one of the above stakeholders. Hand out the stakeholder cards. Show slide 15 and give them a few minutes to think about the following questions from that stakeholder's perspective:

- **What would be their biggest concerns or priorities for this stakeholder in relation to the company?** (E.g. that the company can still make a profit; that they are able to be paid by the company; that their data is handled in a safe and secure way; that they have enough funding and resources available to continue providing the company with what it needs to run, so that they stay in business)
- **What are the potential consequences for this stakeholder if the company's IoT system experiences a data breach?** (E.g. the company makes a loss and they therefore lose all their profits; the company closes down and they have to find employment elsewhere; their data is compromised and used by cybercriminals to commit fraud; the other organisations they use to source the materials for the company's products are also hacked by the cybercriminals)

Regroup and ask each team to share their thoughts. Encourage everyone to listen actively, make notes and suggest any other ideas they come up with as they hear what the other teams have come up with.

Show the discussion question on slide 16 and ask students what advice they might give to someone around protecting their personal data when using the IoT systems. Run through the following examples:

- Carefully read a company's terms and conditions to see how they will use people's information.
- If in doubt, do not agree to any terms or share personal data with an organisation, especially if the reasons for needing this information feel unclear.
- Check what permissions are requested – for example, apps that want to use cameras and microphones – and read the T&Cs to check how companies plan to use these permissions.
- Change your passwords regularly and don't share login details with anyone else.

In their shoes

Consider these questions:

- ❓ What would their biggest concerns or priorities be?
- ❓ What are the potential consequences for them if the company's IoT system experiences a data breach?



Resources

- PowerPoint Presentation
- Timer
- Stakeholder cards

Activity 2 (30 mins) Slides 17-18

Real risks of the IoT

Get students into small groups and hand out the following 'Real risk' scenario cards which are based on real incidents of data breaches related to the IoT:

Doorbell disaster

A leading retailer launched smart doorbell product which features a motion-sensor security camera, allowing homeowners to see visitors, passersby and potential burglars by viewing a live camera feed via a password-protected app. Cybercriminals were able to break into accounts by exploiting weak password credentials. The attackers could then view live feeds to know when houses are empty or gain access to the property.

Healthcare havoc

An innovative medical device was developed to be installed in people's pacemakers*. The device was created to send data about the patient's heart rate back to healthcare professionals. If they could see any issues, doctors could also use the device to send pulses to the patient's heart. Cyber-attackers found a way to intercept the transmissions from the device, meaning they could change how well the pacemaker worked by depleting the battery and accessing confidential patient information.

*A pacemaker is a medical implant that sends electrical pulses to the heart to help it beat at a normal rate and rhythm

Four-wheel fraud

A well-known car company created software which could monitor safety issues, for example if the driver was travelling at dangerous speeds or going towards a collision. The software allowed users to take control of the car's

steering and speed as a way to keep drivers out of danger. Cybercriminals were able to hack into this system through its IoT network, meaning they could slow the car down, cause it to stop or even turn the wheel to make it veer off the road. They could also access GPS history and phone contacts connected through the entertainment system.

In their groups, ask students to discuss the following questions:

- What were the possible consequences of these scenarios? (Be sure to think about how it affects the different people involved e.g. the patients, their families, the developers of the devices)
- Why is consent so important in these situations?
- What steps could be taken in to avoid the same thing happening in the future?

OPTIONAL EXTENSION: Ask students if they can think of other risks that the IoT can present. Examples could include the following:

- **Human agency:** letting devices make decisions for us reduces our autonomy and our ability to make decisions based on our critical thinking or moral values
- **Socioeconomic equality:** The IoT costs money to have, meaning it can create a 'digital divide' by only giving some people access to technology which can improve their lives
- **Environmental issues:** The IoT requires a lot of electrical infrastructure (meaning they need lots of resources and energy to run). Many smart devices also have short lifespans and are made of materials that aren't recyclable. This can therefore increase our environmental footprint

Resources

- PowerPoint presentation

Plenary (5 mins)

Reflect on learning

Conclude that there are certainly risks when it comes to using IoT systems. However, as they saw in the previous lesson, there are also many benefits.

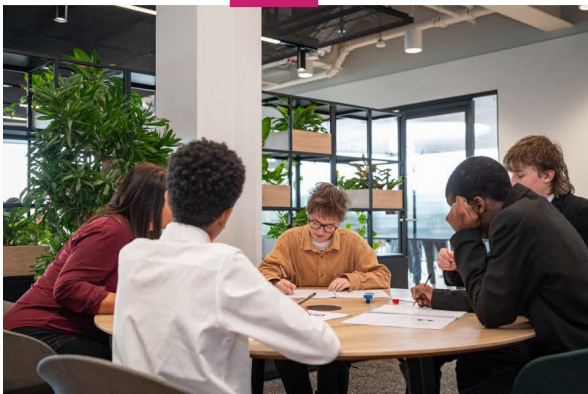
Ask for examples of the positive impact the IoT can have. For example:

- Making our lives easier and reducing human error by automating processes we would otherwise have to do manually
- Helping us to find innovative solutions that help our communities and environment, such as apps to help us monitor and manage our household energy use
- Providing opportunities to connect and share information over huge distances
- Advancing technology in important areas like healthcare

Ask students if they can imagine a future where we have a healthy balance between using IoT and using our critical thinking and autonomy to make decisions.

Finish by explaining that in the next lesson, they'll be having a go at designing visuals for their own innovative IoT product using a 3D modelling programme called TinkerCAD. You may also want to set a brief homework to start researching TinkerCAD, using this tutorial to get an idea of how it works: https://www.youtube.com/watch?v=LrU2zm_g7IE.

19



Recap

What have you learnt today?

- ✓ What are some of the potential risks of using IoT products?
- ✓ Why is it so important that products are designed with security and safety in mind?
- ✓ Is it possible to use IoT products whilst maintaining our personal data, privacy and decision-making?