BT Group

Cybersecurity: the low-down

Lesson 1

Resources

- PowerPoint presentation

Intro (10 mins)
Slides 2-8

Introduction

Start by asking students if they know what cybersecurity is. Gather some answers from the class before showing slide 2. Check students' understanding of the Internet of Things – a network of devices that are connected to the internet and can therefore 'talk to each other' to automate tasks, share information and innovate how different devices work together (e.g. Siri, Alexa). If you completed the IoT module in this series, you may want to recap key learnings from this.

Make sure to highlight the 'Big Thinking' question on slide 4 which will be revisited throughout the module - using their creative and analytical skills to challenge ideas and develop opinions, key capabilities for the tech and digital future. They don't have to have all the answers by the end but should be able to share an opinion on the key questions.

Use slides 4-8 to introduce the module overview and learning objectives of this lesson.

Resources

- PowerPoint presentation
- Internet connected device (tablets, computer/laptop or smartboard)

Icebreaker (15 mins)
Slides 9-13

Cyberthreats: what's out there?

Show slide 10 and give students a couple of minutes to complete this quick-fire task to match the term to the definition. Once finished, go through the answers on slide 11. These have also been included below:

- Malware – software that is designed to disrupt, damage or gain access to someone's computer system without their permission. Short for 'malicious software'.
- Phishing – scam emails pretending to be sent from reputable companies, often requesting personal details or including links which can download malware.
- Cyberbullying – when someone uses technology to harass, threaten or embarrass another person.
- Ransomware – a type of malicious software that blocks the user from accessing their digital device until they have paid the criminal a sum of money.
- Botnets – a network of devices infected with malicious software which can then be controlled without the owner's knowledge and used to send spam or steal data.
- Impersonation scams – a scam often used on social media where fraudsters impersonate trusted businesses, friends or family to steal victims' money or personal information.
- Corporate Account Takeover (CATO) – a work-based identity theft where a criminal gets unauthorised access to a company's bank account to steal money and/or customers' sensitive data.
- Denial-of-Service (DoS) attack – a cyberattack where the criminal disrupts or shuts down a server, service or network so that it can't be accessed by the lawful owners.

Lead a brief discussion about which terms students were or weren't aware of.

Cyberthreat detectives

Explain that students are now going to look at how scams can occur. They will also be working in teams to do some of their own cyberthreat detective work.

Get students into groups and give each team one of the three 'Scam scenario' cards. Ask students to spend a few minutes considering and writing down answers to the below questions. Keep slide 11 on screen to remind students of the different types of cyberthreats.

1. Which type of cyberthreat is shown?
2. What risky behaviour is demonstrated?
3. What are the possible consequences of this behaviour? (think about who is at risk and why)
4. How could this issue have been avoided? (think about what the victim could have done differently)

Below you'll find a summary of each scenario and suggested responses.

Scam scenario 1: An office worker is going through their emails and sees a message from an organisation claiming to have worked with the company on a project. It says the organisation has not yet been paid and provides a link where they can go online and pay the outstanding amount from there. The employee clicks the link and proceeds to make the payment using the company's bank details.

1. **Type of cyberthreat:** phishing scam
2. **Risky behaviour demonstrated:** the employee clicks a link in an email and makes a payment online without verifying the source or whether the email is legit
3. **Possible consequences:** The company has its money stolen by a cybercriminal. As their bank details are now compromised, the cybercriminal may take more money from the company in the future and/or pass the information on to other criminal networks. The employee may also face disciplinary action for not being vigilant enough.
4. **How the issue could have been avoided:** the employee should have questioned the validity of the email, checking things like the sender (is it from a supplier they know?) and the link address (does it go to a secure and recognisable site from a reputable company?). Additionally, they should have reported the email to their security team or manager to tell them before taking any action. They could also have checked with the finance department to see whether there was really an outstanding invoice.

Scam scenario 2: A family member is browsing the internet on their home computer to find a cheaper alternative to their household's security software. They find a site which is offering a much more affordable package. They haven't come across the software company before, but the reviews on the website all seem very positive. They're in a rush to get this sorted before a busy day, so go ahead and start the download.

1. **Type of cyberthreat:** malware
2. **Risky behaviour demonstrates:** the family member goes ahead and downloads the software without doing any proper research on the company, and doesn't check whether the link is secure
3. **Possible consequences:** the family member will probably lose the money they have paid and are at risk of more cyberattacks as the cybercriminals now have their bank details and personal information. The household's computer network could also be infected with the malware, putting everyone connected at risk of viruses, spam and other cyberattacks designed to get their personal details or steal their money.
4. **How the issue could have been avoided:** the family member should have researched the software provider and product further before deciding to download or pay for anything. Often, fraudulent websites will use bots or fake reviews to make the product seem more legitimate than it is.

Scam scenario 3: A young person is on TikTok late one evening and sees a DM pop up from a friend. The message doesn't come from the friend's usual account, but they explain that this is because their phone has been stolen, so they've created a new account. The friend says that the thief has also got into their bank account, taken all their money and changed the passwords. The friend is staying at a relative's quite far from home and needs to catch a train that night. They ask if the young person can transfer them some money just so they can get back safely. The message seems urgent so the young person logs onto their online banking app and sends the friend their train fare using some bank details they have sent.

1. **Type of cyberthreat:** impersonation scam
2. **Risky behaviour demonstrates:** the young person decides to believe the story and transfer their own money to the friend, even though they don't have any real way of proving that it's them.
3. **Possible consequences:** the young person loses the money they have transferred and may be asked for more money to be sent once the cybercriminal knows that they have bought into the scam. There is a good chance they will not be able to get the money back unless their bank agrees

to reimburse them. If the friend still doesn't know that the scam is happening, the criminal could continue to go around and scam other people in their follower list.

4. **How the issue could have been avoided:** the young person should have verified whether this was really their friend – for example they could have messaged the friend's original account to see if any of these details were true. They could have also looked at the fake account, looked online to see if similar situations had happened before, or spoken to an adult. They should also have looked at their own account to see if the scammer was able to see any of their personal details such as a nickname or location to make the story seem more real.

After a few minutes ask for volunteers to share their answers and discuss.

Show slide 13 to encourage a discussion on why it's so important to know how to identify different types of cybersecurity threats and how to avoid them. You can also start exploring how critical thinking is crucial when trying to avoid online scams and threats.

For example:

- If we know how cybercriminals operate, we're more likely to recognise a threat when we come across it
- It's key to know which steps to take once we've identified a cyberattack taking place. It's usually important to take the right action as quickly as possible to stop the criminal from getting any further and causing more damage
- Critical thinking is crucial to detecting fraud because it helps us to question the validity of the information we've been given. Cybercriminals will often use very sophisticated schemes that exploit our fears, use persuasive language and find personal information to build very believable impersonations and cover stories. All of these things can be used to convince us that we're not being scammed. Critical thinking helps us to deconstruct and detect misinformation.

If students need more guidance on what 'critical thinking' is, explain that it is when you use all the facts and information about a topic to consider if there are any deeper meanings or different ways of thinking about the topic.

Resources

- PowerPoint presentation
- Treasure hunt clue cards printable handouts

Activity 2 (20 mins)
Slides 14-19

Decoding cryptosystems

Recap that in the previous activity, students looked at how cybercriminals can gain access to computer systems and therefore steal private data or personal information.

Show slide 15 and introduce encryption and decryption. Ask students if they can name examples of where they've heard about it. (E.g. social networks like WhatsApp and Snapchat use encryption on their private messaging platforms; websites use the "https" at the start of URLs to show information is encrypted and secure).

Use slides 16-17 to talk through what the encryption/decryption process is and how it works. To help further their understanding, ask students to imagine how a front door, security box, bike lock or locker works. When we turn the key, this moves the mechanisms within the lock (i.e. encrypting), making it impossible for anyone to enter. When the key is inserted again, its specific shape allows it to make the mechanisms align and unlock (i.e. decrypting).

Explain that there are two main types of encryption, outlined on slide 17:

- **Symmetric encryption** is where we use the same key for encryption and decryption. This relies on both the sender and recipient having the key. It's the simpler method for encryption, but not as secure. This is because if the key is found by an unauthorised person, they can easily gain access.
- **Asymmetric encryption** is where a different key is used to encrypt and decrypt. This makes it more secure, as the data cannot be decrypted unless the users has access to both keys.

Show slide 18 and explain that you are now going to play a treasure hunt activity which mirrors the process of decryption. Students will need to use their best decoding skills and cybersecurity knowledge to find a clue to a secret treasure.

1. Before the game starts, make sure you have hidden the following things around the room:
    - Hide 'Clue card 2' under your desk
    - Hide 'Clue card 3' next to a window
    - Hide a key behind a bookshelf
    - For extra competitivity, you can use the key to a box which contains a special 'treasure' that will be awarded to the first team to find it
2. Get students into small groups and give each team 'Clue card 1'. Hand them the cards facing down and tell them they are not allowed to turn them over until you say so.
3. Once everyone is sat in their teams with a downturned clue card, start the clock and let everyone start the treasure hunt.
4. Give students a few minutes to complete the treasure hunt around the classroom. The clues and answers are below for reference:

Clue 1: decode this sentence if:

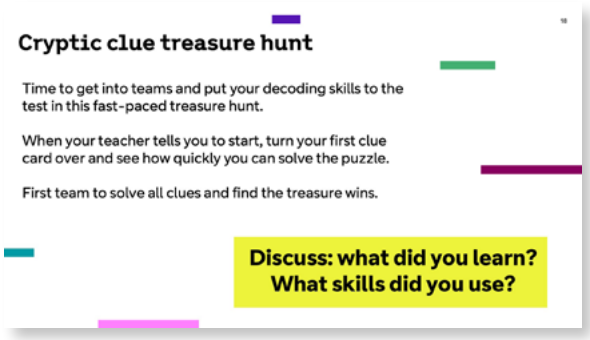
Z = A
A = B
B = C
C = D
Etc. The rule being moving one letter forward in the alphabet

T M C D Q S I D C D R J

Answer: UNDER THE DESK

Clue 2: Answer these questions to find the secret word.

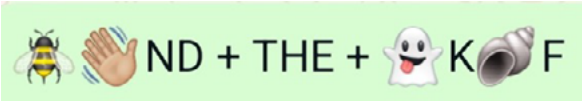
1. Malicious software that is designed to disrupt, damage or gain access to someone's computer system without their permission. (Take the fourth letter of your answer).
- **Answer:** Malware
2. A type of scam that involves sending fraudulent emails to spread a virus or steal personal details (Take the sixth and seventh letters of your answer).
- **Answer:** Phishing



3. A cyberattack where the criminal disrupts or shuts down a server, service or network so that it can't be accessed by the lawful owners. (Take the first letter of your answer).
- **Answer:** Denial-of-Service
4. The acronym used to refer to a network of internet-connected devices. (Take the second letter of your answer)
- **Answer:** IoT
5. The same letter as your first answer.
- **Answer:** W

Final answer: WINDOW

Clue 3: Decode these emojis to figure out the answer:



Answer: BEHIND THE BOOK SHELF

Ask students to discuss the skills they used when completing the clues as a team. For example: problem solving, critical and adaptive thinking, communication, deductive thought process etc.

Ask students to consider what this activity taught them about encryption and decryption and how these processes work. Highlight that in this activity, the clues that students solved were similar to the key in a cryptosystem – the key (or puzzle clue) is the information which can be used to either decode the words or hide their meaning. This is an example of **symmetric encryption.**

Resources

- PowerPoint presentation

Plenary (5 mins)
Slide 19

Reflect on learning

Ask students to answer the following questions to recap their learning from the lesson:

- What are some examples of cybersecurity threats?
- Why is cybersecurity so important for our personal privacy and online safety?
- What are some ways that we can prevent or avoid breaches to our online data security?
- How do encryption and decryption work?
- What is the difference between symmetric and asymmetric encryption?
- What is a key in relation to a cryptosystem?