BT Group

Cybersecurity: the low-down

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 on slide slide 4's 'Big Thinking' question: how can we use cybersecurity measures to effectively protect all online users as technology develops?

Resources

- PowerPoint presentation
- ‘Cyberthreat’ and ‘User group’ cards handouts
- Notebooks and pens (or a device where they can record answers e.g. PCs or laptops)

Icebreaker (15 mins)
Slides 9-13

Cybersecurity: keeping everyone protected

Safeguarding note: *please ensure that you have read this activity thoroughly before running it with students to identify any sensitivities or adaptations required as there is discussion of the impact of cybercrime on people with mental health issues and with disabilities.*

Test students’ knowledge of cybersecurity by discussing the questions on slide 10. Suggestions for answers are provided below:

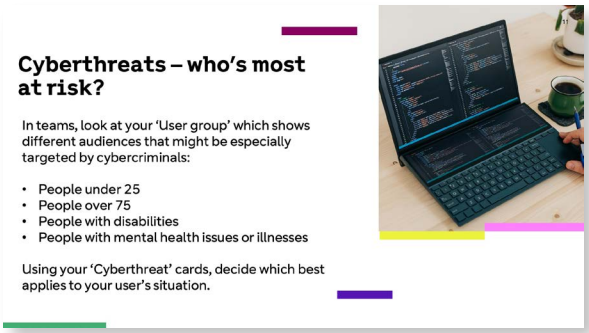
1. Name some different types of cyberthreat and how they work. For example:
    - **Malware** – software that is designed to disrupt, damage or gain access to someone’s computer system without their permission.
    - **Phishing** – a scam that involves sending emails which pretend to be from reputable companies. These emails will often ask recipients to send them personal details or click on unsecure which can download malware. Short for ‘malicious software’.
    - **Cyberbullying** – when someone uses technology to harass, threaten or embarrass another person.
    - **Ransomware** – a type of malicious software that blocks the user from getting onto their digital device until they have paid the criminal a sum of money.
    - **Botnets** – a network of devices infected with malicious software and controlled without the owner’s knowledge. These can be used to send spam, steal data or allow the attacker to command and control software within the network.
    - **Impersonation scams** – a scam often used on social media or emails where fraudsters impersonate trusted businesses, friends or family to steal their victims’ money or personal information.
    - **Corporate Account Takeover (CATO)** – a type of work-based identity theft where a user gets unauthorised access to a company’s bank account. They can then easily 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.
2. What are some human behaviours that can put us at risk from cyberthreats? For example:
    - Neglecting to report a potential threat to the correct department at work
    - Clicking on links or downloading files before researching the website to check that it’s legitimate
    - Failing to verify whether the sender of an email is definitely who they say they are

- Believing that a DM has come from a friend or family member without being able to provide evidence that it's definitely them

3. What is a cryptosystem and how does it work? For example:

- A cryptosystem is used to encrypt and decrypt messages that they can't be read be read by cybercriminals if they're intercepted
- It uses algorithms to turn plaintext messages into cyphertext (i.e. it takes a message everyone can read and uses a coding system – or 'key' – to scramble up the letters or replace them with different numbers or characters)

Highlight that cyberattacks can happen to anyone, especially as cyber criminals are becoming increasingly sophisticated, so it's important that we all stay vigilant. However, cybercriminals may also target particular groups of people who they consider more susceptible to these threats.
Show slide 11 and get students into small groups. Give each team a 'Cyberthreat' worksheet.



Ask students to work in their teams and decide which threats could apply to the different groups. Note that some groups may correspond to multiple threats. For example:

- Elderly people could be matched with most, and in some cases all of the points listed below
- People with disabilities can be matched with point 1, but potentially also points 3-5
- Some individuals may fit into more than one category (e.g. an older person with a disability) and therefore have more reasons to be targeted by cybercriminals

Ask students to reflect on how the impact of cybercrime on individuals in these categories might differ.

OPTIONAL EXTENSION: Show slide 12 to discuss how companies can be targeted by cybercriminals. Why do students think larger organisations can be susceptible to attacks? For example:

- They hold large amounts of personal data from employees, customers and suppliers, making it a more attractive target for fraudsters
- They have wide networks of email contacts – with scams like phishing, this can allow cybercriminals to harvest more data or spread messaging scams further
- They are likely to have more money in their company accounts and therefore present a bigger 'prize pot' to potential hackers

Companies like BT Group do a lot of work in cybersecurity research and innovation to keep people protected online and stay ahead of cyber criminals. Show students the video on slide 13 of a BT Group colleague talking about their job role and the importance of cybersecurity across the business.

Resources

Activity 2 (20 mins)
Slides 14-16

- PowerPoint presentation
- Notebooks and pens (or a device where they can record answers e.g. PCs or laptops)

Profiling cybersecurity risks

Assign each group a user group from the below options:

- People under 25
- People over 75
- People with disabilities
- People with mental health issues or illnesses

Show slide 15 and tell students that they're going to write a short pen portrait for the user group they've been assigned.

Explain that a pen portrait is essentially a profile of a possible target audience. This helps to give people an insight into a 'day in the lives' of the intended audience. Explain that this technique is used by professionals when developing ideas for products or services for a specific user. This enables designers and developers to understand how the product or service will answer their needs and make them more likely to use it.

Their pen portrait should cover:

- An overview of their user – what is their name, age, living situation, do they have any disabilities, illnesses or other issues (e.g. mental health challenges, financial worries) that impact their everyday lives?
- What day-to-day challenges could affect their ability to be aware of cyberthreats?
- What support do they need to keep their personal data safe?

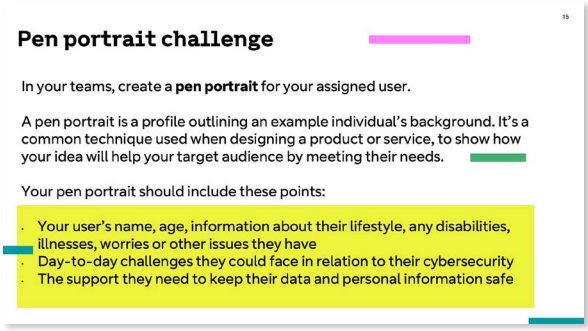
For an extra challenge, you could ask students to swap user groups, or come up with a pen portrait for someone who spans more than one user group (such as a young person with a mental health issue). How would this affect their needs and/or add to the challenges they face?

Give them a few minutes to write responses for their pen portraits, then ask a couple of groups to outline what they came up with.

Show slide 16 to reflect on the human skills students learned in this activity.

- Empathy and emotional intelligence are key to understanding which groups can be more affected and why – just thinking of their own experiences might not lead them to cybersecurity practices that work for everyone
- Critical and adaptive thinking are crucial to identifying the dangers for these groups and what additional measures may be needed to keep them safe
- Problem solving skills help developing ideas that meet specific needs of different people

Collect students' pen portraits in. Keep these to hand as they will need it again for lesson 3.



Resources

- PowerPoint presentation

Plenary (5 mins)
Slide 17

Reflect on learning

Use slide 17 to check students' learning by reflecting on the following questions:

- Who could be targeted by cybercriminals? Are some people or companies more at risk than others?
- What are the benefits of considering different audience needs when it comes to cybersecurity?

Explain that in the next session, students will explore how to use different digital tools to bring their ideas to life through a visually impactful campaign that raises awareness of the risks of cybercrime. They will use the pen portraits created in this activity to introduce the intended audience and set the scene for their campaign.