BT Group

Cybersecurity

Cybersecurity: the low-down

We live in a world of **digital connectivity**; and thanks to advancements in areas like the Internet of Things, this world is **evolving rapidly**. Being more connected has many positives, improving how we live, how we connect with others and supports the health and wellbeing of our communities. However, it has also resulted in an increase in **criminal activity**.

To protect ourselves and our devices from these threats, we need **cybersecurity**. This refers to **techniques and approaches** which **secure our digital networks** against **cyberattacks** and **cybercriminals**.

Companies like BT Group do a lot of work in **cybersecurity research and innovation**, finding new ways to protect their **staff**, **customers**, **suppliers** and wider **communities** from cybercriminal activity.

Effective cybersecurity boils down to two core elements: **finding any problems quickly (detection)** and **fixing them fast (response).**

Big Thinking…

In this module, we will consider:

What is the ***impact of cybercrime*** *on those* ***most at risk****?*

How can ***we use cybersecurity measures*** *to effectively* ***protect all online users*** *as technology develops?*

Module overview

01

Cybersecurity: the low-down

Learn about different types of cyber threat, how these threats can occur and the different techniques we can employ to stop them from happening.

02

Taking cybersecurity to the next level

Debate how cybersecurity can impact people who may be more at risk of attacks.

03

Cybersecurity campaign challenge

Use digital tools to devise an impactful visual campaign that raises awareness of cyberthreats.

04

Presentations and reflections

Module objectives

Today's lesson is one part of a module of four lessons.

By the end of the module, you will be able to demonstrate different technical and human skills that will help you succeed in a future transformed by technology.

Module objectives

This module will focus on the following skills:

- Technical skills: using and managing digital devices, platforms and apps
- Human skills: critical-thinking and problem solving

Lesson objectives

By the end of this lesson, you will be able to:

- Be able to name and define different types of cyber threat
- Understand how encryption and decryption work
- Employ detection and prevention techniques to identify and suggest solutions to different threats

Cyberthreats: what’s out there?

Speedy match-making

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.

Software that is designed to disrupt, damage or gain access to someone's computer system without their permission. Short for 'malicious software'.

When someone uses technology to harass, threaten or embarrass another person.

Scam emails pretending to be sent from reputable companies, often requesting personal details or including links which can download malware.

A type of malicious software that blocks the user from accessing their digital device until they have paid the criminal a sum of money.

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.

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.

A scam often used on social media where fraudsters impersonate trusted businesses, friends or family to steal victims' money or personal information.

Impersonation scams

Denial-of-Service (DoS) attacks

Corporate Account Takeover (CATO)

Botnets

Malware

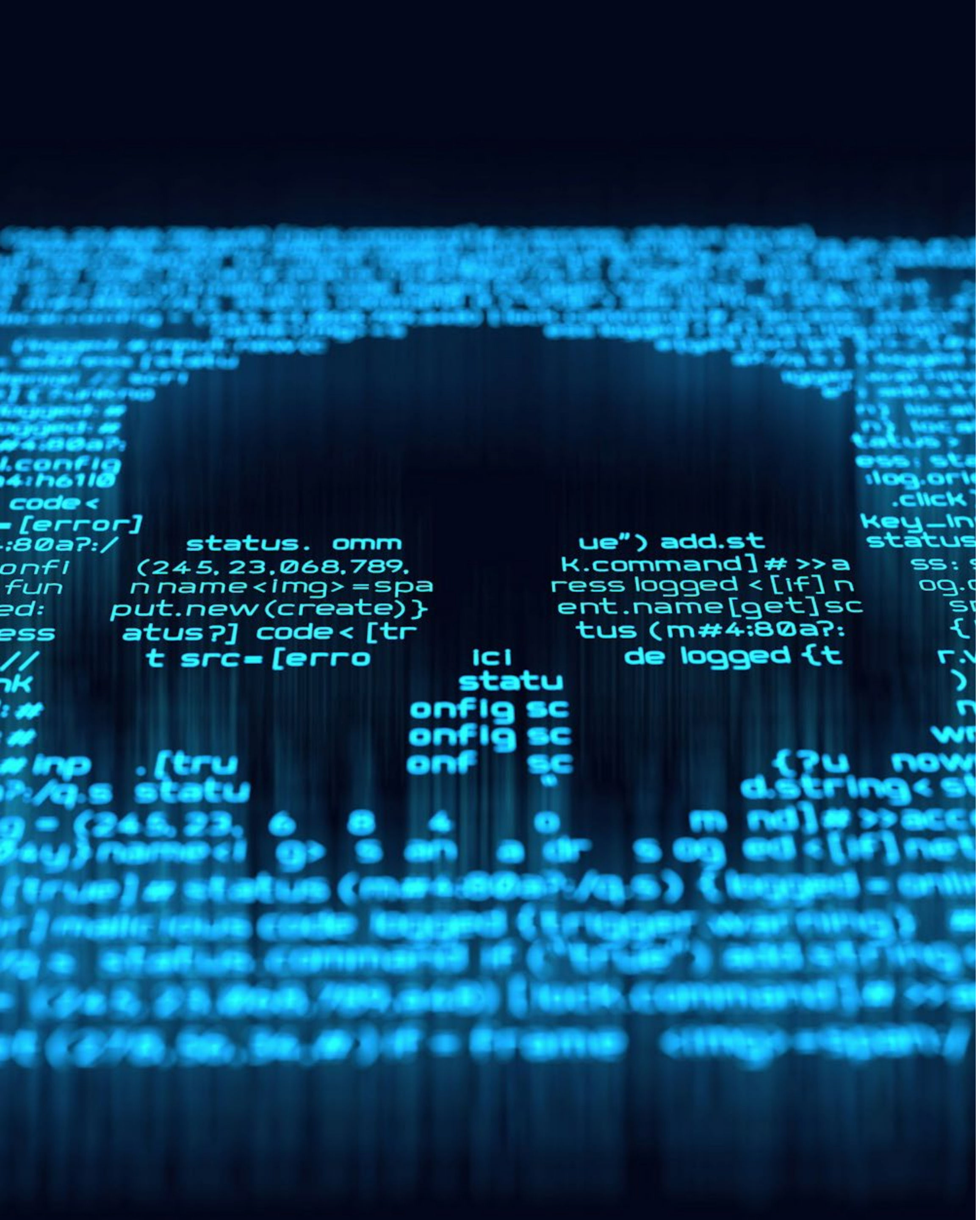
Cyberbullying

Ransomware

Phishing

Speedy match-making - answers

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)	• 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.



Cyberthreat detectives

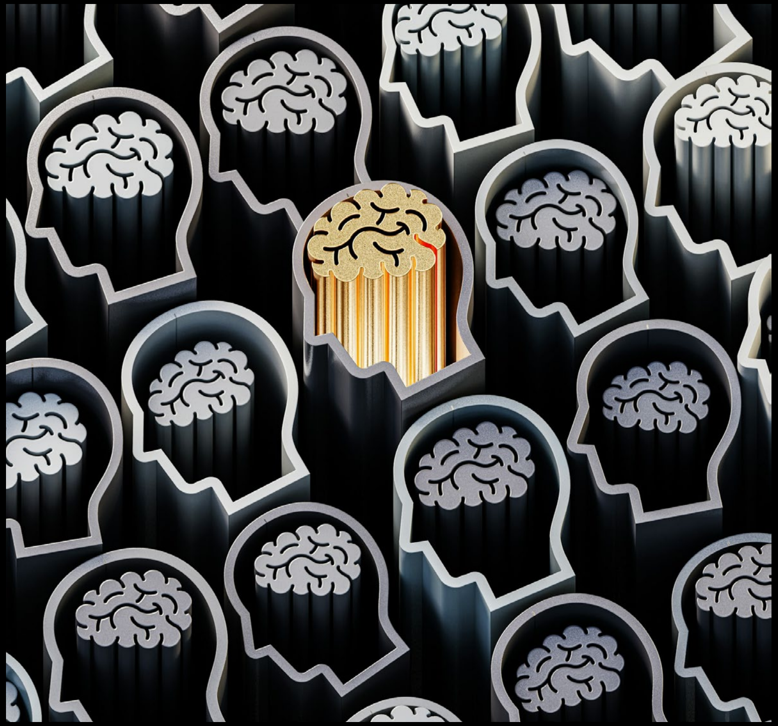
Read your scenario card and write down responses to the following questions:

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)

Discuss...

Why is it important that we understand different cybersecurity threats and how to avoid them?

What role does critical thinking play?



Decoding cryptosystems

What is encryption and decryption?

Encryption is a way of concealing a message so it can be sent secretly. It can be used to protect sensitive information from cybercriminals who may steal or gain unauthorised access to our data.

Decryption is the process of transforming this data back into a readable form.

What is encryption and decryption?

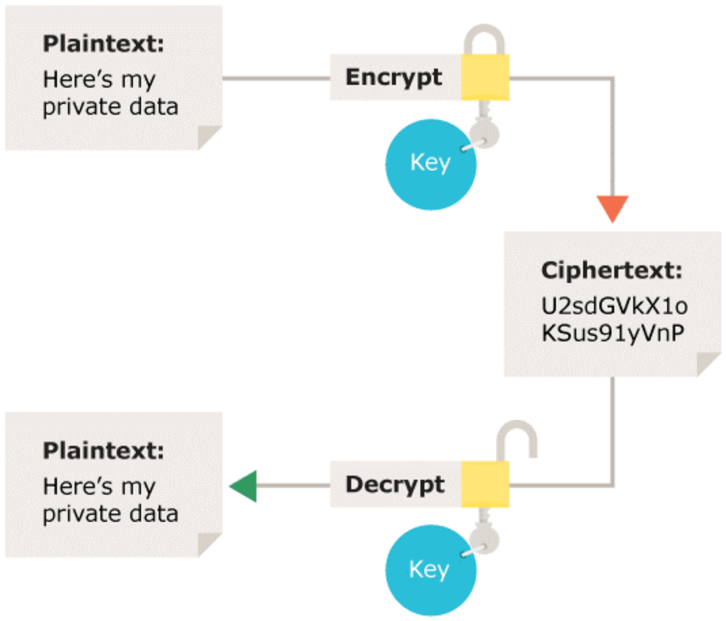
The system used to encrypt and decrypt messages is called a **cryptosystem**.

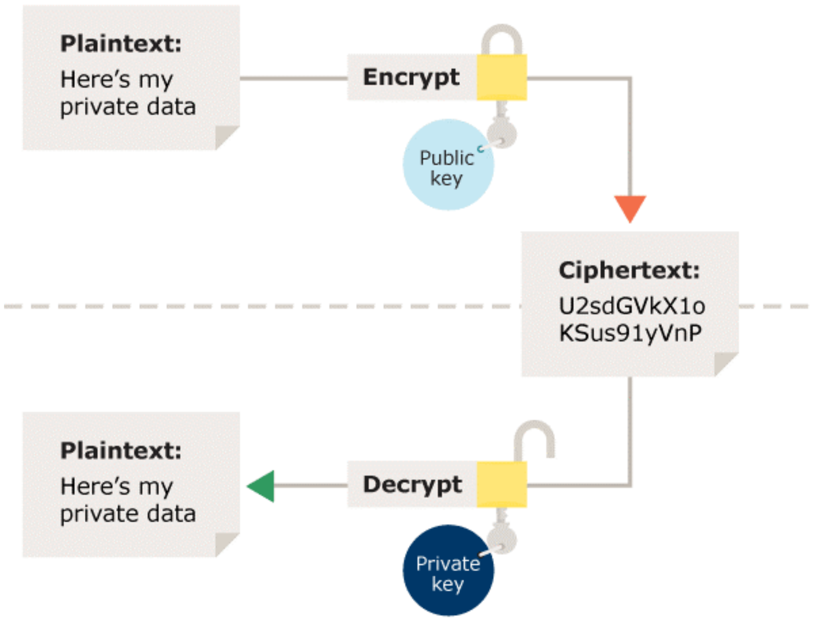
Cryptosystems use **algorithms** (instructions that are followed by a computer to complete an action).

Algorithms turn **plaintext** (a message everyone can see) into **cyphertext** (text that’s been replaced with a system of seemingly random characters or numbers).

To scramble and decode a message, cryptosystems need a ‘**key**’. This is a piece of information which, when passed through an algorithm, can encrypt or decrypt the data – converting that ‘random’ sequence of characters into the original message, or vice versa.

Different types of encryption





Symmetric encryption is where we use the same key for encryption and decryption. This relies on both the sender and recipient having the key.

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.

Cryptic clue treasure hunt

Time to get into teams and put your decoding skills to the test in this fast-paced treasure hunt.

When your teacher tells you to start, turn your first clue card over and see how quickly you can solve the puzzle.

First team to solve all clues and find the treasure wins.

Discuss: what did you learn? What skills did you use?

Recap

What have you learnt today?

- 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?