# A logo for a college AI-generated content may be incorrect.T-Level Cybersecurity

## Pre-course Preparation Activity (Summer 2025)

Welcome to the Pearson T-level in Digital: Cybersecurity, a course that’s all about understanding and protecting the digital world we live in.

From your smartphone and social media accounts, to hospitals, banks, and even national defence systems – everything relies on digital systems. And that means everything is also at risk from cyber threats. Cybersecurity is how we protect our data, our devices, and even our identities. It's one of the fastest-growing areas in tech, and it affects everyone – not just big companies or governments.

On this course you will explore topics such as:

* How networks and systems work (and how attackers try to break into them),
* Different types of cyber threats, like phishing, ransomware, and malware,
* How we can prevent attacks and respond when they happen,
* Laws and ethics around cybersecurity,
* And the role of cybersecurity professionals in keeping society safe.

To get you off to a great start, this summer activity is about researching current cyber threats and solutions. We will be discussing your findings in the first few lessons in September, so please remember to bring this with you.

## TASK 1

Using the Internet (search engines rather than AI chat bots, please) make a list of what you believe are the **top three** cybersecurity threats to businesses and large organisations – these will be slightly different from the threats to private individuals.

Research each of these threats to find out how they work, including how they might be triggered. Also, see if you can find out what the cybercriminals aim to get from it – money, information or just the satisfaction of causing disruption. Summarise this information in three to five bullet points.

*Continues the next page…*

## TASK 2

Choose just **one** of your top three (perhaps the number one) and find a recent news story (from the last year) which involves a large organisation being hit by that threat. Try to find out what happened, how it affected them both initially and, in the aftermath, and see if you can find out how they recovered afterwards.

Summarise this into one or two paragraphs, avoid the use of technical jargon (or explain the jargon) so that it makes sense to a non-technical person.

## TASK 3

Based on your findings from tasks 1 & 2, find out what the recommended approach is to deal with an attack of that type. Then create a short guide, aimed at supporting non-technical people, using the following headings:

**What is a <name\_of\_threat>**

*Briefly describe the type of cyber-attack you researched in task 2*

**How to avoid a <name\_of\_threat>**

*Give some simple tips to avoid this type of attack, for example do not open attachments in emails from unknown senders.*

**What to do if you are hit by a <name\_of\_threat> attack**

*Give some advice on what to do if hit by this sort of attack, for example immediately change your passwords.*

To avoid writing too much text, just use bullet points or a numbered list under each f the headings, aim for between three and five points for each section. It should be no more than a page of A4.

## Submission Procedure

Put everything together into a single document, either in Microsoft Word (doc/docx) format, Office Libre (odt) format or export as Adobe (pdf).

Email your submission to [rhind@yorkcollege.ac.uk](mailto:rhind@yorkcollege.ac.uk) before the start of term i.e. no later than Sunday 7th September 2025.

You should bring a copy of your work to the first lesson, either printed or electronically on your smartphone/laptop, or email a copy to your student email account at the college (see enrolment information for details).