LESSON 93

Data Protection, Viruses, Malware, Spam: Deep Dive

60 minutes | ICT Specialism 4: The internet and digital literacy | Outcome M4.U1.1 | Outcome M4.U2.3

WHAT THIS LESSON DOES

Explore the differences between data protection rules, viruses, malware, and spam. Identify how these threats operate and the common ways they reach you through email or downloads. Create glossary definitions and examples to support your future research projects.

CURRICULUM OUTCOMES

Outcome	What the specification asks for
M4.U1.1	Understand concepts and safety considerations relating to the effective and ethical uses of digital technologies and the internet.
M4.U2.3	Discuss the ethical implications of internet use and their digital footprint in relation to issues such as privacy and data protection.

WHAT STUDENTS SHOULD BE ABLE TO DO

- Explain GDPR at classroom level and how malware and spam operate
- Identify common infection and spam pathways
- Add definitions and examples for data protection, virus, malware, and spam to the glossary

BEFORE THE BELL

- Write the four key terms on the board: data protection, virus, malware, spam.
- Have both concept images ready (malware family; four doors).
- Optional: print threat_term_flashcards for a 2-minute support pair run before Glossary build.
- Plan one model spam glossary entry to write on the board before students type.
- Write the four terms on the board; open the drag-sort on the board for step 3; optional print of threat_term_flashcards for support pairs
- Have both concept images ready to display; four terms already on the board
- Have threat_term_flashcards ready for a 2-minute support pair run before glossary build
- Model one spam glossary entry on the board; confirm students can open or create sm4_digital_literacy_glossary in Project_Portfolio/09_specialism/sm4/

Data Protection, Viruses, Malware, Spam: Deep Dive

HOW THE LESSON RUNS

5 min	introduction	Start
8 min	content	Key concepts
14 min	activity	Sort the threat
4 min	content	Common issues
20 min	activity	Glossary build
4 min	content	Reflection
5 min	summary	Lesson summary

TEACHING MOVES

- Focus on clear distinctions between terms rather than dramatic examples during key concepts.
- Conduct whole-class discussion before students interact with the sorting activity; name pathways as "doors" during card talk only, there is no pathway card in the interactive.
- Model one full glossary entry live, then circulate during glossary build with paced checkpoints.
- Use the common issues table as a reference while students complete their glossary entries.

WHAT TO WATCH FOR

- Students call all threats viruses. Solution: Emphasise behaviour such as file copying for viruses versus locking for other malware.
- Students write vague or lengthy definitions. Solution: Encourage precise short sentences that capture the core idea; point at the sentence starters.
- Students confuse spam with malware pathways. Solution: Clarify spam as unsolicited messages that may lead to malware.
- Students look for a "door" or pathway card on the drag-sort. Solution: Re-state that pathways are talk labels applied to the eight scenario cards already on screen.

DIFFERENTIATION

- Support: Sentence starters on the glossary card; 2-minute flashcard pair before writing.
- Support: Pair students for the initial talk phase of the sorting activity.
- Extension: Ask early finishers to add infection pathways under each glossary term.