TEACHER GUIDE

Unit

Cybersecurity.

Unit Description

Recognising common online threats to data and knowing how to protect personal information.

Career

I'm a cyber security consultant.

Every unit is based on a career to help students see the relevance of what they are learning to the real world and to help schools achieve Gatsby benchmarks by linking curriculum learning to careers.

Career overview

As a cybersecurity consultant, I protect organisations from digital threats. This involves assessing security measures, identifying vulnerabilities, and implementing strategies to safeguard sensitive information. My goal is to ensure robust defences against cyberattacks, keeping data secure and businesses running smoothly.

Key question

How can we protect ourselves and others from online threats?

Every unit is designed to help students answer one over-arching key question relating to the units four knowledge statements.

Unit objectives: knowledge statements

1. Know how to recognise common online threats.
2. Know the importance of protecting personal information using human strategies.
3. Know the importance of protecting data using security software.
4. Know basic hacking techniques that are used.

Unit outcomes

1. Learn it workbooks evidencing the learning journey.
2. Make it workbook evidencing application of learning with an artefact.
    a) A cyber defence live simulation.
        i) Recognising threats.
        ii) Human strategies.
        iii) Software strategies.
        iv) Basic hacking techniques.
3. Review it workbook evidencing assessment and review.

Prior learning / spiral curriculum

No previous learning is necessary because all units have been developed in a modular way to allow you to plug them into your existing scheme of learning.

However, if you are following our recommended pathway for curriculum 2028 here is how this unit fits into the year 7 → 9 progression pathway.

The big picture: a three-year progression

Once the national curriculum programme of study has been released, we will update this section with how this unit fits into a progressive pathway across Key Stage 3.

How the three units connect

Once the national curriculum programme of study has been released, we will update this section with how this unit fits into a broader theme of units.

Contents

In addition to this teacher guide this unit also includes the following resources:

- Folder: Extension work. Use these activities to extend any lesson or for 7–8-week terms.
    - 1 teacher extension answers.
    - 1 student extension workbook.
- Folder: Homework. Use these activities for work outside of the lesson. They are independent of the lessons and can be set at any time.
    - 1 teacher presentation.
    - 3 videos.
    - 3 video scripts.
    - 3 worksheets.
- Folder: Lesson 1 – Learn it. This lesson addresses the key question and first knowledge statement.
    - 1 lesson plan.
    - 1 introduction video.
    - 1 teacher presentation.
    - 1 student workbook.
    - Any associated resources required for the lesson.
- Folder: Lesson 2 – Learn it. This lesson addresses the key question and second knowledge statement.
    - 1 lesson plan.
    - 1 teacher presentation.
    - 1 student workbook.
    - Any associated resources required for the lesson.
- Folder: Lesson 3 – Learn it. This lesson addresses the key question and third knowledge statement.
    - 1 lesson plan.
    - 1 teacher presentation.
    - 1 student workbook.
    - Any associated resources required for the lesson.
- Folder: Lesson 4 – Learn it. This lesson addresses the key question and fourth knowledge statement.
    - 1 lesson plan.
    - 1 teacher presentation.
    - 1 student workbook.
    - Any associated resources required for the lesson.
- Folder: Lesson 5 – Make it. This lesson provides an opportunity for students to evidence their learning.
    - 1 lesson plan.
    - 1 teacher presentation.
    - 1 student workbook.
    - Any associated resources required for the lesson.

- Folder: Lesson 6 – Review it. This lesson provides an opportunity for students to check their understanding of the key vocabulary and knowledge statements plus dedicated improvement and reflection time.
    - 1 lesson plan.
    - 1 teacher presentation.
    - 1 student workbook.
- Folder: Reading. Use these activities to support reading initiatives in your school.
    - 3+ two-page reading passages with 5 questions.

PowerPoint format is used for workbooks as it allows for easy sharing on displays, animations, simultaneous collaboration and pasting without disrupting content on other pages. All PowerPoints have been checked for compatibility with Google Slides.

Differentiation

Differentiation should be provided through “adaptive teaching”. This is defined as, “The opportunity for all pupils to experience success, by adapting lessons, whilst maintaining high expectations for all, so that all pupils have the opportunity to meet expectations”. This also meets the expectations of Deborah Eyre’s High Performance Learning strategy. Differentiation is provided by instruction and support rather than by task.

Vocabulary

Term	Definition
Antivirus	Software that scans your device for harmful files and removes them before they can cause damage.
Brute Force	Trying every possible password or PIN until one works.
Cyber security	Protecting computers, phones, and online information from being stolen, damaged, or accessed by people who shouldn't have it.
Cyber security consultant	Specialist who helps people and organisations stay safe online by finding weaknesses in their computer systems and advising them on how to fix those risks.
Cyber-attack / threats	Any attempt to break into computers, networks, or online accounts to steal information, cause damage, or disrupt how things work.
Firewall	A security tool that blocks unwanted connections to stop hackers getting into your device or network.
Hacker	Someone who uses technical skills to access, explore, or manipulate computer systems in ways not intended by their creators.
Malicious Website	A fake or dangerous website designed to steal information or install malware.
Password	A secret word, phrase, or code that proves your identity and lets you access an account or device.
Personal information	Any details that can identify you or describe you, such as your name, address, or date of birth.
Phishing	Online trick where someone pretends to be a trusted person or company to fool you into giving away personal information like passwords or bank details.
Scammer	Someone who deceives people to steal money, information, or resources through dishonest schemes.
Security software	Set of tools that protect your device and data from online threats like viruses, hackers, and unsafe websites.
Shouldering	Stealing information by watching someone type or write.
Social Engineering	Manipulating or tricking someone into revealing information.
System vulnerability	Weakness in a computer system that a hacker could use to break in or cause harm.

Lesson overview

Detailed lesson plans for each lesson are provided in the relevant lesson folder.

Lesson	Lesson Type	Phase 1	Phase 2	Phase 3
1	Learn it	Career overview	Understand common online threats such as phishing, malware, and social engineering.	Investigate real-world examples of cyberattacks to identify warning signs.
		Students consider what a cyber security consultant does and what skills / knowledge they need.	In groups of 4, students visit 8 stations around the room to identify threats and record their findings.	In groups of 4, students read and analyse 6 real-world case studies.
2	Learn it	Retrieval	Use human strategies such as strong passwords to protect personal information.	Understand how trust, judgement, and behaviour affect online safety.
		Students decode anagrams, identify 3 key words and write definitions of each key term.	Students make 5 passwords stronger. In pairs students decide how long it would take a computer to crack 5 more passwords.	In pairs students look at 20 images and must decide quickly if they can trust what they are seeing or whether it is a trap.

3	Learn it	Retrieval	Investigate how security tools (antivirus, firewalls, VPNs) protect data.	Use security software features (e.g., scans, settings, alerts) to evaluate digital safety.
		Students decode anagrams, identify 3 key words and write definitions of each key term.	In pairs students match 5 threats to 5 security tools.	Students consider 8 stimulus images and write what the software is saying, what action should be taken and how safe or dangerous it is.
4	Learn it	Retrieval	Understand basic hacking techniques such as brute force, keylogging, and packet sniffing.	Investigate how vulnerabilities are exploited and how cybersecurity consultants prevent attacks.
		Students decode anagrams, identify 3 key words and write definitions of each key term.	Students sort 8 hacking techniques into 4 groups: guessing passwords, watching people, fake messages and tricking people.	In pairs students examine 2 images
5	Make it	Retrieval	Make a cyber defence plan based on a scenario and budget.	
		Students decode anagrams, identify 3 key words and write definitions of each key term.	Students decide from costed human, software and system strategies how to spend a given budget justifying their choices.	

6	Review it	Assess	Self/Peer review.	Reflect and improve.
		Students complete a multiple-choice quiz.	Student's mark each other's answers to the quiz and self-assess or peer-review work from lesson 5.	Students RAG rate themselves against a series of "I can" statements. Students improve their work or undertake extension activities.

Homework

3 activities provided.

Students watch up to a 5-minute video about the hinterland (discovering), real-world application (exploring) or consolidation (revisiting) related to the unit. Students complete a simple sheet, with all the information required to complete it included within the video.

Homework is designed to require no parental support and is independent of any lesson.

Homework	Title
1	The hidden world of cyber threats.
2	How cyber security protects the real world.
3	Becoming your own cyber security consultant.

Extension activities in the student extension workbook could also be used for homework.

Assessment

Students are graded intern, junior, associate and senior to reflect the careers-oriented approach.

Artefact

It is recommended that the Learn it workbook is used for students to record their development in learning, new knowledge and skills. They may need help with these activities in order to make progress, and therefore it is not the best work for assessment.

Instead, assess the Make it artefact workbook. This should be the best work the student can produce and will allow you to judge their independence.

 Intern	• At least **one** knowledge statement is achieved. • Identifies at least one threat. • Gives simple defences. • Limited justification.
 Junior	• At least **two** knowledge statements are achieved. • Identifies multiple threats. • Uses human and software strategies. • Some justification.
 Associate	• At least **three** knowledge statements are achieved. • Recognises and understands all threats. • Explains why defences worked/failed. • Adds new ideas.
 Senior	• All **four** knowledge statements are achieved. • Fully considers all threats. • Uses human, software and system strategies. • Shows creativity and considers stakeholder needs.

Tick the statements that best apply to the student when making their artefact. Award a best-fit mark of intern, junior, associate or senior.

Multiple-choice quiz

A 24-question multiple-choice quiz assesses the 4 knowledge statements and vocabulary of the unit. Award intern for 0-9 marks, junior for 10-16 marks, associate for 17-21 marks and senior for 22-24 marks.

You may choose to put the quiz into Microsoft Forms or equivalent for automatic marking.

Students should not open their Learn it workbook or Make it artefact workbook when completing the quiz.

Reflection

Lesson 6 provides an opportunity for students to review the work of their peers, identify and carry out improvements to their own work. It may not be necessary for teachers to mark the artefact for every unit for every student. Instead, you could take a moderation approach instead, sampling just a few pieces of work.

It is suggested that peers highlight statements on the assessment grid in yellow and teachers highlight in green to distinguish the two markers.

Grading

Consider both the mark for the artefact and the mark for the quiz to award a best-fit judgement.

National curriculum links

These will be populated when the new National Curriculum is released.

Applications of AI

How the students can use AI to produce or enhance their work. Includes instructions for how use of AI can also be avoided.

1. Researching Online Threats & Real-World Cyberattacks

(Supports Knowledge Statement 1)

Using AI:

- Students can ask AI tools to summarise real cyberattacks, such as phishing campaigns, ransomware incidents, or data breaches.
- AI can help identify warning signs, patterns, and common attacker behaviours.
- Students can request simplified explanations of complex threats (e.g., “Explain malware like I’m 14”).
- AI can generate comparisons between threats (e.g., phishing vs. social engineering).

Without AI:

- Students manually research threats using trusted sources (e.g., BBC Tech, National Cyber Security Centre).
- They evaluate credibility by checking authorship, publication date, and domain.
- They identify warning signs by analysing screenshots, case studies, or teacher-provided examples.

2. Understanding Human Strategies for Protection

(Supports Knowledge Statement 2)

Using AI:

- Students can ask AI to generate examples of strong vs. weak passwords, or explain why certain passwords are vulnerable.
- AI can simulate social engineering scenarios, helping students practise identifying manipulation tactics.
- AI can help students explore privacy settings by describing what each setting does and why it matters.
- Students can ask AI to create role-play prompts for trust and judgement activities.

Without AI:

- Students create passwords manually and test them against password-strength checkers.
- They analyse real screenshots of privacy settings and decide which options are safest.

- They role-play social engineering scenarios with peers.
- They reflect on their own online behaviour and identify risks.

3. Investigating Security Software & Digital Protection Tools

(Supports Knowledge Statement 3)

Using AI:

- Students can ask AI to explain how antivirus, firewalls, and VPNs work in simple terms.
- AI can generate step-by-step guides for running scans, checking alerts, or interpreting warnings.
- AI can simulate "What if?" scenarios, such as:
    - "What happens if a firewall is turned off?"
    - "How would a VPN protect someone on public Wi-Fi?"
- Students can ask AI to compare different tools (e.g., antivirus vs. firewall).

Without AI:

- Students explore real or simulated security software interfaces.
- They run mock virus scans or examine example alerts.
- They evaluate suspicious downloads or websites using checklists.
- They complete teacher-guided investigations into how software protects data.

4. Learning About Hacking Techniques & Vulnerabilities

(Supports Knowledge Statement 4)

Using AI:

- Students can ask AI to explain brute force, keylogging, packet sniffing, and other techniques in age-appropriate language.
- AI can generate fictional case studies showing how vulnerabilities are exploited.
- Students can request step-by-step breakdowns of how an attack works (without technical danger).
- AI can help students design defence strategies, mirroring the role of a cybersecurity consultant.

Without AI:

- Students analyse teacher-provided diagrams of attacks.
- They match vulnerabilities to hacking techniques using scenario cards.
- They investigate how consultants prevent attacks through structured worksheets.
- They participate in simulations (e.g., Exploit & Defend, Live Threat Drops).

How to Avoid Using AI

To ensure students develop genuine cybersecurity understanding:

- Ask students to explain their reasoning in their own words.
- Require them to annotate screenshots, diagrams, or system maps manually.
- Use in-class simulations where AI cannot assist (e.g., live threat drops).
- Provide tasks that require personal judgement, such as evaluating trust or analysing behaviour.
- Encourage students to justify decisions rather than simply list defences.
- Use closed-book assessments or supervised tasks where AI is not permitted.

By using these approaches, students can learn to harness the power of AI when needed while also developing their own abilities and confidence in information literacy.

Software

PowerPoint or equivalent for students to complete the workbook and teachers to show class presentation.

Web browser to provide them with access to the online tools required for completion of this unit.

Online and unfiltered sites required

The following site is used to host our homework videos for this unit:

- https://www.tella.tv

Extension activities

These can be used as additional activities in 7–8-week terms, for alternative homework, or for additional activities in lessons.

Extension activities are included in a separate workbook for students “Student Extension workbook.pptx”

Extension answers are included in a separate presentation for teachers “Teacher Extension answers.pptx”

Extension 1	**Real world cyberattack summary**
Activity	Complete an incident report that outlines the Zoom credential stuffing attack in 2020 and the LinkedIn scraping & data exposure incident in 2021.
Extension 2	**What is Two Factor Authentication (2FA)?**
Activity	Researching what 2FA is, why it is helpful and where you should use it.
Extension 3	**Create a password recipe**

Activity	Write a simple mental algorithm that allows you to create hard to crack but easy to remember passwords.
Extension 4	**How secure is my password?**
Activity	Use an online password security checker to see how strong a range of passwords are.
Extension 5	**Trust or trap**
Activity	Exploring a phishing email.
Extension 6	**Build a security toolkit map**
Activity	Create a diagram that shows how different security tools protect you online. E.g. antivirus, firewall, VPN, password manager, 2FA, email filters.
Extension 7	**Exploit and defend | Defence pitch for BrightBrew Café**
Activity	Explaining one security vulnerability and how to fix it for a café.

Reading

This unit includes a folder titled, “Reading”. The files in this folder contain passages of text about scenarios related to the topic and each include five questions. These resources can be used in many ways. For example:

- Guided reading and oracy activities in terms of more than six weeks.
- Cover work.
- Work for students disapplied from the lesson.
- Alternative homework.

Guided reading is where the teacher reads the text to the students who follow along with a ruler on the line being read. To support literacy, it is important that students are both supported and challenged with text that is accessible and in places more demanding. The text has been checked that it meets these criteria and is suitable for a reading age of 11–14.

The associated questions go beyond simple comprehension using a framework that provides progression from basic understanding to deeper analytical thinking. Either moving students through increasingly demanding reading skills—retrieval, vocabulary, connection, inference and evaluation or encouraging students to identify and critique the structure of an argument or explanation.