techskills

TEACHERS

Cyber in the classroom: the teacher pack

Activities, answers and the evidence behind every claim

Every figure was checked against its source on 1 November 2026. Free to use in your classroom.

About this pack

This is the printable companion to the Cyber in the Classroom page on techskills.org. It holds everything you need at the front of a class: how to run each activity, the questions to ask, the answers, and the evidence behind every claim, with its source.

Everything below works in a normal lesson. Most of it needs one projector. Two activities can be run with no devices at all: the starter, and the cipher workshop, which works with pencil and paper. Timings are our suggestions from how long each takes to run, so adjust them to your group, and every activity has teacher notes, answers and discussion questions in the downloadable pack.

Every message, name and address in these activities is made up. Web addresses in the examples end in .example, a reserved ending that can never be a real website, and nothing in the interactive activities collects or stores anything a student types.

For	Teachers, from about key stage 3 upwards. Written for England; see the curriculum section
Activities	7
Sources	14, each opened and read on 1 November 2026
Produced by	TechSkills, techskills.org

Ask your class to draw a hacker

Before you say a single word about cyber security, hand out paper and ask everyone to draw a hacker, and then compare notes. You already know what you will get: a hoodie, a dark room, green letters raining down a screen and possibly a mask, none of which has much to do with what the work actually looks like, which is at least as likely to involve a policy, a spreadsheet and a long meeting about why a supplier's invoice looks slightly off.

That gap between the picture in our heads and the reality is the whole opportunity. Cyber security is full of jobs that never make it into a film, and the latest labour market report shows how different the real mix is, with governance and risk management employing people in far more cyber businesses than security testing does. Once students see that, the subject stops being a thing for a particular type of person and becomes a thing for a lot of types of person, which is a much better place to teach it from.

The evidence

Fact	Condition	Source
Among UK cyber security businesses, 45% employ people in governance and risk management, the most common specialism, 27% in security testing, 23% in incident response and 10% in digital forensics.	Based on 230 cyber security businesses, using the 15 specialisms in the Cyber Career Framework.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)

The honest case for teaching it

We could just say there is a huge skills shortage and leave it there, and plenty of people do. But you are the one standing in front of fifteen year olds who will check, so here is what the evidence really says, including the awkward bits.

The need is genuine. Businesses lack basic cyber skills, the sector has to find thousands of new people every year, and it is a real industry worth billions with thousands of firms. But the entry door is narrower than the headlines suggest: employers mostly ask for experience and for a degree, and the share of roles open to beginners has fallen. What the numbers do not say is that cyber is closed. A good proportion of firms have hired through routes that are not degrees, and people arrive from many subjects. So the message for your students is not 'this is easy' and it is not 'this is impossible', it is that real, demonstrable skill gets noticed, and you can start building it years before anyone asks for a CV.

The evidence

Fact	Condition	Source
57% of UK businesses (about 808,000) had a basic technical cyber skills gap in the latest survey, up from 49% the year before.	Businesses were asked about basic technical skills, the everyday things like setting up and managing protection.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
About 145,900 people work in UK cyber security, only 2% more than the year before, so the report describes growth as slowing.	The report calls this an experimental estimate.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
The report estimates the sector needs about 10,200 people in 2026: about 4,400 to meet new demand plus about 5,800 to replace people who leave.		Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
The UK has 2,603 active cyber security firms providing about 69,600 full-time equivalent jobs and £14.7 billion of revenue.	The firm count is an estimate for December 2025. Revenue and jobs are for the most recent financial year, most often 2024/25.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security sectoral analysis 2026 (Published 12 May 2026)
In 2025 there were 66,964 job postings that asked for cyber skills, 34,932 of them in core cyber roles (up 7% on 2024).	Core cyber roles are jobs whose main purpose is cyber security. The rest are jobs in other fields that ask for cyber skills.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)

Fact	Condition	Source
Only 16% of core cyber job postings in 2025 were open to someone with under a year of experience, down from 25% in 2022.	The most common request, in 64% of postings, was for 2 to 6 years of experience.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
77% of employers required at least a bachelor's degree (or equivalent) for a core cyber role, and 12% of roles were open to people with GCSEs, A levels or equivalent.		Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
Among cyber firms that had been recruiting since the start of 2024 and described steps to widen who applies, 65% said they had hired through non-degree routes.	This is the share of those firms, not of all hires.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
Enrolments in cyber security apprenticeships fell 15% between 2023/24 and 2024/25, while cyber security graduates rose 14% to 7,950 in 2023/24.		Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)
Of 670 graduates working in cyber professional roles within fifteen months of graduating, 59% had studied a cyber security course, 18% computing, 7% another STEM subject, 9% humanities or social sciences and 6% accounting, business, economics or finance.	These are graduates of the 2022/23 academic year. Figures add to 99% because of rounding.	Department for Science, Innovation and Technology (research by Ipsos and Perspective Economics), Cyber security skills in the UK labour market 2026 (Published 29 September 2026)

Your school is in the figures too

This is the part that makes a class sit up. The government's annual survey asks organisations whether they have had a cyber breach or attack, and it includes schools, colleges and universities. A good lesson hook is that the thing you are about to teach is not abstract: it is happening to institutions very like this one. Treat the numbers as indicative, because the samples are small and only count what organisations noticed themselves, but the pattern is clear and so is the most common type of attack.

The evidence

Fact	Condition	Source
In the 12 months before the survey, 60% of secondary schools and 44% of primary schools identified a cyber breach or attack, as did 85% of further education colleges and 91% of higher education institutions.	Samples are small (240 secondary and 250 primary schools) and the survey only counts what institutions noticed themselves.	Department for Science, Innovation and Technology and the Home Office, Cyber security breaches survey 2025: education institutions findings (Updated 19 June 2025)
Phishing was the most common type of attack, reported by 89% of the primary and secondary schools that identified any breach or attack.		Department for Science, Innovation and Technology and the Home Office, Cyber security breaches survey 2025: education institutions findings (Updated 19 June 2025)

Starter: draw a hacker

A five minute starter that shows a class what they already believe, before you show them what the industry actually looks like.

Time	5 to 10 minutes
You need	Paper and pens. No devices.
Where	Can be done with no devices.

Students will be able to

- Describe how cyber security people are shown in films and games.
- Name at least three kinds of cyber job that look nothing like that picture.

Running it

- Give each student a sheet of paper and two minutes to draw a hacker. No talking and no looking at each other's.
- Put the drawings up, or hold them up, and ask what the same things are.
- Then open the attack diagram and the hard hat map and ask what is missing from the drawings.

Questions to ask

- Where does our picture of a hacker come from?
- Which jobs in the attack diagram would never appear in a film?
- Who in this room could do one of them?

Watch for

- Some students will draw an attacker and others a defender. Ask which they drew, because it is a good way into red team and blue team.

Game: spot the phish

Eight made-up messages, two of them genuine. Can your class tell which? Built on the NCSC's five signs of a scam.

Time	20 to 30 minutes
You need	A projector for the whole class, or one device per pair.
Where	Interactive on the page. Needs a screen.

Students will be able to

- Name the five tell-tale signs of a scam message.
- Explain why a genuine message can still have a deadline.
- Say what to do, and who to report to, when one arrives.

Running it

- Project the page. Read message 1 aloud and give the class 30 seconds to vote with hands up: scam or genuine.
- Press the answer, then ask which of the five signs they noticed before you read the clues.
- Repeat for all eight. After the last one, point out that two were genuine and ask what made them safe.
- Finish with how to report: texts to 7726, emails to the NCSC, and who to tell in your own school.

Questions to ask

- Which message would have fooled you, and why?
- A genuine message can have a deadline. What else did the sign-in code email do to show it was safe?
- Why do scammers try to make us feel panic or excitement?

Watch for

- Students who decide everything is a scam. The aim is knowing what to check, not trusting nothing.
- The headteacher gift voucher message may be recognised from real life. That is useful, and a good moment to remind everyone how to report.

The five signs, from the NCSC

Sign	What it means
Authority	It claims to come from someone official or important, like a bank, a courier, a teacher or the government.
Urgency	It sets a deadline or threatens a consequence so you act before you think.
Emotion	It tries to make you panic, hope, worry or feel curious.
Scarcity	It offers something in short supply, so you feel you might miss out.
Current events	It uses the news or the time of year, like results season or tax deadlines, to seem relevant.

Answer key

Six of the eight are scams and two are genuine. Every name and address is made up, and web addresses end in .example, which can never be a real website.

No.	Message	Answer	Signs it uses	What gives it away, or makes it safe
1	Text message from +44 7700 900123	Scam	Authority, Urgency	It says it is a courier, but you were never told the name of a courier or a parcel number. A 12 hour deadline and a threat to send it back, to rush you. The link is not a courier's own website, and the 'fee' is really a request for your card details.
2	Email from Mrs Okafor <headteacher.okafor@mailbox-free.example>: Quick favour	Scam	Authority, Urgency, Emotion	It is from the headteacher, but the address is a free mailbox, not the school's own. She cannot be called, it is needed today and it must stay secret, all of which stop you checking. Asking for gift voucher codes is a payment method that is very hard to undo.
3	Email from Ravenscroft Academy IT <it-helpdesk@ravenscroft-verify.example>: Your account will be deleted tomorrow	Scam	Authority, Urgency, Emotion	It is addressed to 'Dear user', not your name, which a real school system would know. Deletion tomorrow is a scare tactic. Losing your work is exactly what it wants you to worry about. No genuine IT team asks you to type your password into a link in an email.
4	Email from Ravenscroft Academy Office <office@ravenscroft.example>: Parents' evening: bookings open on Monday	Genuine	None	It asks for nothing: no password, no payment, no personal details. There is no pressure and no threat, and it tells you to use the website you already know. It gives you a way to check it independently, by ringing the number on the real website.
5	Text message from Unknown number	Scam	Emotion, Urgency	It pretends to be someone you love, which makes you want to help before you check. A new number and a locked banking app, so you cannot call or verify the usual way. It wants money today, to a bank account you have never seen.
6	Email from Prize Desk <winners@kickz-giveaway.example>: You have been picked! Limited edition trainers, only 3 pairs left	Scam	Emotion, Scarcity, Urgency	You never entered a competition, so how did you win? Only 3 pairs and 15 minutes: scarcity and a countdown, working together. Winning something exciting is designed to switch off the part of you that asks questions.
7	Email from Ravenscroft Learn <no-reply@learn.ravenscroft.example>: Your sign-in code	Genuine	None	It has a deadline, but you can tell it is expected: you have just asked to sign in. It asks you to do nothing except use a code you requested, and it contains no link. It tells you to ignore it if you did not ask, which is exactly what a safe service says.
8	Email from National Exams Portal <results@national-exams-portal.example>: Results day: your predicted grades are ready	Scam	Authority, Urgency, Current events	It rides on a real moment in the year, when students are nervous and checking their phones all the time. It sounds official but gives no name, no reference and no way to check it another way. A threat that a place might be withdrawn is there only to hurry you.

What to do with a real one

- Suspicious text messages can be forwarded to 7726.
- Suspicious emails can be forwarded to the NCSC, which says it acts on every message but cannot tell you the outcome. Reporting to the NCSC is not the same as reporting a crime.
- In England, Wales and Northern Ireland, fraud and cyber crime are reported to Report Fraud at reportfraud.police.uk or on 0300 123 2040. In Scotland, call Police Scotland on 101.

The evidence

Fact	Condition	Source
The NCSC lists five tell-tale signs of a scam message: authority, urgency, emotion, scarcity and current events.		National Cyber Security Centre (NCSC), Phishing scams: how to spot and report them (Published 26 November 2021, reviewed 5 September 2022)

Your notes

Lab: password maths

Change one thing and watch the number of possibilities explode. Why length beats cleverness, shown with real arithmetic.

Time	15 to 20 minutes
You need	A projector or one device per pair.
Where	Interactive on the page. Needs a screen.

Students will be able to

- Explain how the number of possible passwords grows with length.
- Say why three random words works and why swapping letters for numbers does not.

Running it

- Start with the random characters panel at 8 characters with every type ticked, at the fastest speed. Ask students to guess how long it will last.
- Move the length slider by one and ask what happens to the number. Establish that each extra character multiplies it.
- Switch to random words. Compare 3 words with 8 mixed characters in the side by side table.
- Ask why the NCSC suggests words rather than symbols, and which is easier to remember at the same strength.

Questions to ask

- Why does one extra character make such a difference?
- What is wrong with using your pet's name, even if you add a number?
- Where would a password manager help?

Watch for

- The figures flatter whoever chose the password, because real choices are less random. Make sure students leave with long and random, not with one particular number.

Worked answers

These are the numbers the lab shows, so you can check them in advance. They are for a truly random choice, so they flatter the person choosing. The speeds are illustrations, not measurements.

Password	Possible passwords	Bits	At 1 million guesses a second	At 100 billion a second
8 random characters, every type (94 possible each)	about 6.1 quadrillion	52	97 years	8 hours
12 random lower case letters	about 95.4 quadrillion	56	about 1.51 thousand years	6 days

Password	Possible passwords	Bits	At 1 million guesses a second	At 100 billion a second
3 random words (7,776 word list)	about 470 billion	39	3 days	2 seconds
4 random words (7,776 word list)	about 3.66 quadrillion	52	58 years	5 hours

The evidence

Fact	Condition	Source
The NCSC recommends combining three random words to make a password that is strong enough for most uses and easier to remember, and warns that swapping letters for numbers does not meaningfully help.		National Cyber Security Centre (NCSC), Three random words (Published and reviewed 21 December 2021, version 2.0)
The NCSC advises avoiding common passwords and anything based on significant dates, sports teams or family and pet names, because that information is often found on social media.		National Cyber Security Centre (NCSC), Three random words (Published and reviewed 21 December 2021, version 2.0)

Your notes

Workshop: crack the cipher

Send a secret message with the oldest trick in the book, then break it by counting letters. Then see why nobody uses it any more.

Time	30 to 40 minutes
You need	A device per pair, or paper cipher wheels. Pencil and paper also works.
Where	Interactive on the page. Can be done with no devices.

Students will be able to

- Encrypt and decrypt with a Caesar cipher.
- Break one using frequency analysis.
- Explain why a key that can only be one of 25 values is not secure.

Running it

- Pair students. Each writes a short message and encrypts it with a shift only they know, using the first panel or a paper cipher wheel.
- Swap messages and try to read each other's using the letter count in the second panel.
- Show the list of all 25 readings and ask how long a computer would take.
- Finish with the modern encryption box: why 25 keys is nothing and 2 to the power 128 is out of reach.

Questions to ask

- Why did counting letters work so well on the long message and so badly on a short one?
- If an attacker can try every key, what makes a cipher strong?
- Where do you rely on encryption without noticing?

Watch for

- Ciphers are not named in the DfE content we read, so present this as enrichment, and check how your exam board's specification covers encryption.

Worked answer

With a shift of 3, "Meet me at the library at noon" becomes "Phhw ph dw wkh oleudub dw qrrq". The sample message on the page is encrypted with a shift of 7, and the letter count finds it because the most common letter in English is E.

Paper version: write the alphabet twice on strips of card, one above the other, and slide the lower strip along by the key.

Your notes

Diagram: an attack, step by step

An interactive diagram that walks through how an attack unfolds, what defenders can do at each stage, and which job does it.

Time	15 to 25 minutes
You need	A projector. Best as a whole class discussion.
Where	Interactive on the page. Needs a screen.

Students will be able to

- Describe the stages of an attack in order.
- Suggest a defence for each stage.
- Match a cyber job to the stage it works on.

Running it

- Project the diagram at stage 1. Read the plain description and the example, then ask the class what a defender could do.
- Reveal the ways to make it harder and compare them with the class's ideas. Use the Ask the class question at each stage.
- At every stage, point to the jobs that work there, and ask which stage a student would like to work on.

Questions to ask

- Which stage is easiest to stop, and which is hardest?
- If a defender could stop only one stage, which would you pick?
- Where do people, rather than computers, matter most?

Watch for

- Real attacks do not always follow the order, skip stages and repeat others. Say so when a student points it out, because they are right.

The worked example follows Marlow & Finch, a made-up accountancy practice with 40 staff.

Stage	MITRE ATT&CK tactics	What happens	Ways to make it harder	Jobs
1. Find out about the target	Reconnaissance, Resource Development	Before anything happens to a computer, an attacker gathers information to plan, and sets up what they will need. Often this means reading what people have put online. The attacker reads the Marlow & Finch website and staff social media, learns who runs the finance team and which software they use, and sets up an email address that looks almost like the managing director's.	Be thoughtful about what is public about staff and systems. Teach everyone that information about them can be used against them. Watch for look-alike addresses and websites.	Threat Intel, Penetration Tester
2. Get in	Initial Access	The attacker finds a way in. Very often this is a person tricked into helping, or a weakness that was never fixed. A member of the finance team gets an email that appears to come from the managing director asking for an urgent invoice to be paid, and clicks the link.	Train people to spot and report scam messages. Use two-step verification so a stolen password is not enough. Install software updates promptly.	SOC Analyst, Vulnerability Analyst
3. Get settled	Execution, Persistence, Privilege Escalation, Stealth, Defense Impairment	Once in, the attacker runs their own code, makes sure they can get back in, tries to gain more power on the system, and tries to avoid being noticed or to switch off the alarms. Hidden software installs itself on the finance computer, creates a second way in, and quietly turns off the usual warnings.	Give people only the access they need for their job. Keep security tools running and protected from being switched off. Keep a record of what happens on systems, so odd behaviour can be spotted.	Security Engineer, Malware Analyst
4. Look around and spread	Credential Access, Discovery, Lateral Movement	The attacker steals more logins, explores the network to learn what is where, and moves from computer to computer towards what they want. From the finance computer, the attacker finds saved passwords, discovers the file server holding client records, and logs into it.	Separate systems so one problem cannot reach everything. Use different strong passwords for different things. Monitor for unusual logins, like a finance login at 3am.	SOC Analyst, Security Architect
5. Take what they came for	Collection, Command and Control, Exfiltration	The attacker gathers the data or access they want, keeps in touch with the compromised systems, and sends the stolen information out. Client records are copied into a single hidden file and sent out of the firm over several nights.	Watch for large or unusual amounts of data leaving. Protect the most sensitive data with extra controls. Keep clear records of what data is held, so a loss can be understood quickly.	Incident Responder, GRC Analyst

Stage	MITRE ATT&CK tactics	What happens	Ways to make it harder	Jobs
6. Cause the damage	Impact	The attacker disrupts, destroys, locks or manipulates systems or data, or demands money. This is the stage most people notice. The firm's files are locked and a message demands payment. Staff cannot work and clients cannot be reached.	Keep backups that are separate from the main systems and test that they work. Have a written plan for what to do, and practise it. Know who to tell, inside and outside the organisation.	Incident Response Lead, Digital Forensics Analyst

A deliberate simplification of the tactics in MITRE ATT&CK (version 20). Real attacks skip, repeat and reorder stages.

Your notes

Gamers and cyber: what we know, and what we do not

Everyone says gamers make brilliant cyber professionals, and it is a lovely story, so we went looking for the evidence. We did not find a published study that measures whether gaming experience predicts how well someone does in a cyber job, so we are not going to tell you it does. We would rather give you a claim that survives a sceptical student, and there is a more practical truth underneath it.

Capture the flag competitions and cyber practice platforms are games in their own right, with puzzles and scoreboards. If you have gamers in your class, and you almost certainly do, the useful thing you can do is point their energy at places where it is legal, and tell them why that matters. The National Crime Agency lists several, and it is blunt about the risks: knocking an opponent offline with a booter in a game is, in its own example, an offence.

So the line we would give a gamer is this: the instincts you already have are worth something, there are real, legal, free places to use them, and the same skill used on someone else's system without permission can lead to a criminal record and damage your education and career, which is the NCA's own list of consequences. Both halves of that sentence are true and both are worth hearing.

The evidence

Fact	Condition	Source
The NCA's Cyber Choices page points young people to legal places to practise, including CyberLand, OverTheWire, Cyber Explorers, Hack The Box, Vulnhub and Cybrary, and to British Esports.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
The NCA gives knocking an opponent offline in a game with a 'booter' tool as an example of an offence, and says many young people commit cyber crime without realising it is illegal.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
The NCA lists the possible consequences as a visit and warning, seized devices and internet restrictions, arrest, a fine, a criminal record, damage to education and career prospects, travel restrictions and, for the most serious offences, up to life imprisonment.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
CyberFirst, the NCSC's programme, offers courses for 11 to 17 year olds, competitions and student bursaries, and CyberSprinters offers online security games for 7 to 11 year olds.		National Cyber Security Centre (NCSC), Schools (education and skills) (Page shows no date)

Hard hats, drones and the physical world

Here is something that surprises almost every student, and quite a few teachers: some genuine technology careers involve a hard hat and steel toecaps. Our Career Matrix has a name for the genuinely physical, on-site routes, Hard Hat Tech: fibre engineering, data centres, industrial automation, smart buildings, utilities and surveying with drones. Five of our eight career families have one.

And cyber itself has one. Operational Technology security is about protecting the control systems of physical equipment, such as pumps, power switches and factory machines, and its roles, OT Security Engineer and ICS Security Analyst among them, are listed in the Matrix as a genuinely hands-on route. Equipment like that is controlled by digital systems, which is why it is also a cyber question, and why the hard hat world is worth a look for a student who likes both the practical and the digital.

Drones are the perfect doorway, because students already find them thrilling. They turn up on the hands-on side, with surveyors piloting mapping drones, and on the cyber side, where the Matrix gives the example of securing a fleet of autonomous drones from signal hijacking. If your school wants a drone club, the rules changed on 1 January 2026, and the box below says exactly how.

An interactive map of the physical world cyber has to protect, and the hands-on careers, including drone work, that keep it running.

Time	10 to 20 minutes
You need	A projector or a device per pair.
Where	Interactive on the page. Needs a screen.

Students will be able to

- Name three hands-on technology careers and what each looks after.
- Explain why a power switch or a drone is also a cyber question.

Running it

- Ask the class to name a job that involves a hard hat and a computer. Collect the answers.
- Open the map and look at three routes together: read the jobs, then why it is a cyber question too.
- If you have a drone club, or want one, read the CAA box together.

Questions to ask

- Which of these jobs did you not know existed?
- Why would a power switch or a drone need cyber security?
- Which would you try?

Watch for

- Pay figures are medians or ranges from different sources, so always read the source line and the date.

Route	Family	Jobs	Pay, with its source
Construction Technology & Geospatial Surveying: Capturing the data that describes the physical world, on site rather than in an office.	Data & AI	Surveying Technician, Engineering Design Technician (BIM/CAD), Geospatial Survey Technician	£32,905 to £47,519 (median, surveying technician to chartered surveyor)
Non-Destructive Testing (NDT): Hands-on inspection of real components and structures, through a paid apprenticeship rather than an engineering degree.	Data & AI	NDT Operator Apprentice, NDT Engineering Technician, Inspection Engineer	£22,000 to £45,000+ (Level 2 operator apprentice to Level 3 engineering technician, Glassdoor/Indeed UK benchmarks)
Operational Technology (OT) Security: Protecting the industrial control systems that run power stations, water plants and factories, not just office networks.	Cyber Security	OT Security Engineer, ICS Security Analyst, Industrial Cyber Security Consultant	£36,000 to £100,000+ (range across real UK OT security job postings, analyst to consultant level)
Data Centre Operations: Keeping the internet physically running: servers, cooling, backup power and cabling.	Cloud & Infrastructure	Data Centre Support Technician, Electrical Service & Maintenance Technician, Information Communications Technician	£34,073 to £41,111 (median, equipment installer to electrical maintenance technician)
Telecoms & Fibre Field Engineering: Building and maintaining the UK's physical fibre and mobile network, on-site rather than at a desk.	Networks & Connectivity	Network Cable Installer, Telecoms Field Operative, Fibre Jointer, Cellular Network Field Engineer	£23,000 to £60,000 (ITP range for Cellular Network Field Engineer; ONS ASHE median £39,652 for the wider occupation)
Smart Buildings: Installing and commissioning the connected systems that make a building intelligent.	Networks & Connectivity	Fire & Security Systems Technician, BEMS Controls Engineer, Building Automation Installer	£37,991+ (median, Security System Installers and Repairers)
Industrial Automation: Keeping factories and production lines running: PLCs, robots, sensors, conveyors.	Emerging Technologies	Automation & Controls Engineering Technician, Mechatronics Maintenance Technician, Aircraft Maintenance Technician	£40,002+ (median, Automation Maintenance Technicians)
Utilities Technology: Modernising the UK's energy, water and metering networks, on-site and in the field.	Emerging Technologies	Water Industry Network Technician, Dual Fuel Smart Meter Installer, Overhead Linesperson / Substation Fitter, Battery Manufacturing Technician	£39,057 to £48,171 (median, water network operative to electrical trades)

Route	Family	Jobs	Pay, with its source
Manufacturing & Production Engineering: Hands-on entry into keeping factories and production lines running, through a paid apprenticeship rather than an engineering degree.	Emerging Technologies	Engineering Manufacturing Technician Apprentice, Process Industry Technician Apprentice, Production Support Technician	£24,000 to £55,000+ (technician apprentice to experienced production/process technician)

The evidence

Fact	Condition	Source
From 1 January 2026 anyone flying a drone that weighs over 100g needs a Flyer ID, which comes from a free theory test on the CAA website (the old threshold was 250g).		Civil Aviation Authority (CAA), Regulator calls on new and existing drone users to learn new rules before taking off (Published 29 December 2025)
Under-18s need a Flyer ID and can take the test themselves, but a parent or guardian must hold the Operator ID. Children under 13 need a parent or guardian with them for the online test, and children under 12 must be supervised by someone aged 16 or over when flying.		Civil Aviation Authority (CAA), Regulator calls on new and existing drone users to learn new rules before taking off (Published 29 December 2025)

The law, in plain English, and how to play legally

A cyber lesson will, sooner or later, produce a student who asks whether they could try it on something real. It is far better to have answered that before it is asked. The Computer Misuse Act 1990 is the law that matters, and the National Crime Agency explains it clearly for young people, parents and teachers, and names all three as audiences.

The practical rules for your classroom are short. Only practise on systems built to be practised on, or ones you have clear, written permission to test. Never let students point tools at the school network, a website or another person's account, however friendly the intention. Use the activities here and the legal platforms the NCA lists. And if you ever worry about a student, the NCA's Cyber Choices programme is aimed at helping young people make better choices, and it names teachers as one of its audiences.

This is general information to help you teach, not legal advice, and the NCA's page is the place to read the detail.

A lunchtime or club session built on the legal places to practise, with the law explained first so nobody gets caught out.

Time	A club session
You need	Devices with internet access, and a teacher who has read the law section.
Where	Needs a screen.

Students will be able to

- Explain what the Computer Misuse Act 1990 means for them.
- Name at least three legal places to practise.

Running it

- Read the law section aloud first, so nobody can say they were not told.
- Choose one legal platform from the NCA's list that suits the group's age, and try it yourself before the session.
- Make the rule clear: only on systems built for practice, never the school network or anyone else's accounts.

Questions to ask

- What is the difference between a capture the flag game and breaking into a real website?
- Why does permission matter?
- Who could you talk to if you were unsure?

Watch for

- Check each platform's own age rules and terms before using it with a class.

The evidence

Fact	Condition	Source
The Computer Misuse Act 1990 makes it an offence to access computer material without permission, to make unauthorised changes that impair a computer, and to make, supply or obtain tools to do either, even if the tool has not been used yet.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
The NCA gives knocking an opponent offline in a game with a 'booter' tool as an example of an offence, and says many young people commit cyber crime without realising it is illegal.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
The NCA lists the possible consequences as a visit and warning, seized devices and internet restrictions, arrest, a fine, a criminal record, damage to education and career prospects, travel restrictions and, for the most serious offences, up to life imprisonment.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
The NCA's Cyber Choices page points young people to legal places to practise, including CyberLand, OverTheWire, Cyber Explorers, Hack The Box, Vulnhub and Cybrary, and to British Esports.		National Crime Agency (NCA), Cyber Choices (Page shows no date)
Teachers and safeguarding staff are among the audiences the NCA's Cyber Choices programme is aimed at.		National Crime Agency (NCA), Cyber Choices (Page shows no date)

The Translator

Jargon in plain English, with a comparison from school life. Where the comparison stops working, it says so.

Term	In plain English	Think of it like this
Botnet	A network of infected devices controlled by an attacker, often without their owners knowing, used to send spam or carry out denial of service attacks.	Thousands of classroom clocks secretly set to chime on the same signal, from one hidden remote.
Capture the flag	A cyber competition where teams solve puzzles and challenges, on systems built for the purpose, to find hidden 'flags' that score points.	A very nerdy treasure hunt, with a leaderboard.
Denial of service	Flooding a website, game server or network with so much traffic that real users cannot get through. 'Booter' or 'stresser' tools sell this as a service.	Everyone in the school blocking one doorway at the same time so nobody can get to lessons. Where that stops working: Using a booter, even on a gaming opponent, is an offence under the Computer Misuse Act. The NCA uses this exact example.
Digital forensics	Finding, preserving and examining digital evidence, for example to work out how an attack happened or to support an investigation.	Working out who left the tap running by looking carefully at what was left behind, without touching anything that might spoil it.
Encryption	Scrambling information with a key so only someone with the right key can read it.	A note written in a code that only you and your friend know how to read. Where that stops working: Real encryption is far stronger than a pass-a-note code. Try the Cipher Workshop to see why the simple ones fail.
Firewall	A control that decides which network traffic is allowed in and out of a device or network.	The front office: everyone coming in is checked against a list, and some people are simply not let past. Where that stops working: A firewall does not stop someone you have already let in, or a user who clicks a bad link.
Governance, risk and compliance	The side of cyber about decisions, rules and evidence: deciding what risks matter, writing policies, checking they are followed and proving it.	Safeguarding policy and the checks, records and training that show it is real, not just a document in a drawer.
Incident response	What an organisation does when something has gone wrong: working out what happened, stopping it spreading, fixing it and learning from it.	The plan for a fire: raise the alarm, get everyone out, find the cause, and change something so it does not happen again.
Malware	Software designed to cause harm: to steal information, spy on you, lock your files or give someone else control of your device.	A game that says it is free but quietly copies your contacts while you play. Where that stops working: Not all malware announces itself. Much of it is built to stay quiet.
Operational technology	The technology that controls physical equipment: pumps, power switches, factory machines, building systems. Securing it is its own specialism.	The boiler controls and the fire alarm panel, as opposed to the school's admin computers. Where that stops working: OT often runs for many years, so it can be harder to update than ordinary IT.

Term	In plain English	Think of it like this
Password manager	An app that creates strong, different passwords for every account and remembers them for you.	A very trustworthy friend with a perfect memory and a locked diary. Where that stops working: You still need one strong password to protect the manager itself. The NCSC suggests a password manager as an alternative to remembering lots of passwords.
Patch	A fix released by a software maker that closes a vulnerability. Installing updates is how you get the fix.	The caretaker mending the door latch. Where that stops working: A patch only helps once it is actually installed.
Penetration test	An authorised, agreed attempt to break into a system, carried out to find weaknesses so they can be fixed. The permission is the whole point.	The school asking an outside expert to try every door and window one weekend, then write a report on which ones opened. Where that stops working: Without written permission it is not a test, it is a crime. See the section on the law.
Phishing	A message that pretends to come from someone you trust, sent to trick you into clicking a harmful link or handing over passwords or bank details.	Someone in a school jumper who is not from your school walking up and saying the head sent them to collect everyone's locker keys. Where that stops working: A phishing message can be much more convincing than a stranger, because it can copy a real logo and a real name.
Ransomware	A kind of malware that locks or scrambles a victim's files and demands payment to give them back.	Someone swapping the padlock on your locker, then selling you the key. Where that stops working: Paying does not guarantee you get anything back, which is why backups matter so much.
Red team and blue team	In an exercise, the red team plays the attacker and the blue team plays the defender, so an organisation finds out how well it really copes.	A fire drill where somebody secretly hides a blocked exit and watches how the building copes.
Security operations centre	A team, often working in shifts, that watches an organisation's systems for signs of trouble and responds when something looks wrong.	The control room in a hospital or an airport, with everyone watching screens and ready to act.
Social engineering	Getting people, rather than computers, to do the wrong thing: using trust, pressure or curiosity to get past security without any clever technology.	Saying 'Mr Patel said I could borrow the sports cupboard key' when he said nothing of the kind.
Threat intelligence	Information about who is attacking, how and why, collected and explained so defenders can prepare.	A teacher on duty knowing which corridors tend to get crowded, and when, so she is standing in the right place.
Two-step verification	Proving who you are in two ways, usually a password plus something else such as a code sent to your phone.	A locker that needs both a key and a combination, so a stolen key alone is no use.
Vulnerability	A weak spot in software, a system or a process that an attacker could use.	A fire door that does not quite latch. It is not a break-in, but it is how one could happen.
Zero trust	A way of designing security on the idea that nobody and no device is trusted just because they are inside the network. Every request is checked each time.	Being asked to show your pass at every door, not only the front gate.

The Curriculum Translator

Stage	What the curriculum says	Activities that support it
Key stage 3	"use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy"	Spot the phish, Password maths lab
Key stage 3	"recognise inappropriate content, contact and conduct, and know how to report concerns"	Spot the phish
Key stage 4	"understand how changes in technology affect safety, including new ways to protect their online privacy and identity"	Password maths lab, An attack, step by step, Where hard hats meet hackers
Key stage 4	"how to report a range of concerns"	Spot the phish
GCSE computer science	"forms of attack (based on technical weaknesses and behaviour)"	Spot the phish, An attack, step by step
GCSE computer science	"methods of identifying vulnerabilities"	An attack, step by step
GCSE computer science	"ways to protect software systems (during design, creation, testing, and use)"	An attack, step by step
GCSE computer science	"issues of privacy and cyber security"	Password maths lab, Play it legally
GCSE computer science	"use appropriate security techniques, including validation and authentication"	Password maths lab

Be aware of the limits

- The key stage 3 and 4 programmes of study (published in 2013) do not use the words cyber security. The links above are to the statements on safe and secure use of technology and on privacy and identity.
- The GCSE content names cyber security only generally, under forms of attack, identifying vulnerabilities, protecting software and the ethical and legal impacts of technology.
- Encryption and ciphers are not named in either of the pages we read, so treat the Cipher Workshop as enrichment, and check your own exam board's specification for how it covers encryption.
- All of this is for England. Scotland, Wales and Northern Ireland have their own curricula, and curriculum documents are reviewed from time to time, so check the current version for your school.

Questions students, parents and colleagues ask

Do students have to be brilliant at maths or coding to work in cyber?

No, and the latest labour market report is quite clear about it. The most common specialism among UK cyber security businesses is governance and risk management, which is about decisions, policies and evidence, and a much smaller share employ people in security testing, the part most people think of as hacking.

People also arrive from all sorts of subjects. Among graduates working in cyber roles, 59% had studied a cyber security course and 18% computing, but 9% came from humanities or social sciences and 6% from business, accounting or economics. Coding helps in some roles and is irrelevant in others, so the honest answer is that it depends which part of cyber you mean.

Do you need a degree to get in?

Two things are true at once, and a student deserves to hear both. In the latest figures, 77% of employers required at least a bachelor's degree for a core cyber role and only 12% of roles were open to people with GCSEs or A levels.

At the same time, 65% of the cyber firms that had been recruiting and described steps to widen who applies said they had hired through non-degree routes. Apprenticeships are one of the routes we list in the career guides, though cyber apprenticeship enrolments fell by 15% in the latest year. So a degree is the most common requirement on a job advert, it is not the only way in, and the routes that avoid one are narrower.

Is it easy to get a first job in cyber?

It is worth being straight about this, because students will hear lots of excited headlines about skills shortages. Demand is real: 57% of UK businesses have a basic skills gap and the report estimates the sector needs about 10,200 people a year. But only 16% of core cyber postings in 2025 were open to someone with under a year of experience, down from 25% in 2022.

The useful message for a student is not 'cyber is easy' or 'cyber is closed', it is that early evidence of real skill matters: competitions, projects, work experience, an apprenticeship, a placement. That is a very teachable thing.

Are gamers better at cyber?

People say so a lot, and we went looking for the proof. We did not find a published study that measures whether gaming experience predicts how well someone does in a cyber job, so we are not going to claim it. What we can say is more practical: capture the flag competitions and practice platforms are games in their own right, and there are plenty of them.

The practical point for a teacher is the legal one. The NCA lists places where students can practise legally, including CyberLand, OverTheWire, Cyber Explorers, Hack The Box and British Esports. And it gives knocking an opponent offline with a booter as an example of an offence.

Is it legal for students to try hacking?

Only on a system built to be practised on, or one they have clear permission to test. Under the Computer Misuse Act 1990 it is an offence to access a computer without permission, and downloading hacking tools can

be an offence even if they are never used. The NCA says many young people commit cyber crime without realising it.

That is not meant to frighten anyone. It is why we point students at legal platforms and competitions, and why the NCA runs Cyber Choices, which names teachers as one of its audiences. If you are ever worried about a student, that is who to talk to.

Is it all sitting at a desk looking at screens?

No. Our Career Matrix separates desk-based routes from genuinely physical, on-site ones, which we call Hard Hat routes, and one of them sits inside cyber itself: Operational Technology security, with roles such as OT Security Engineer and ICS Security Analyst. These protect the control systems for physical equipment like pumps, switches and factory machines.

Beyond cyber, five of our eight career families have a hands-on route, from fibre engineering and data centres to industrial automation and, in Data & AI, surveying with mapping drones. Digital systems all sit on physical equipment, and someone has to install and look after it.

What about drones?

Drones show up in two places. On the hands-on side, our Data & AI family includes a geospatial surveying route where people pilot mapping drones. On the cyber side, the Career Matrix gives the example of securing a fleet of autonomous drones from signal hijacking.

If a school wants to start a drone club, the rules changed on 1 January 2026: a Flyer ID, from a free theory test, is now needed for any drone over 100g, and there are specific rules for under-18s and under-13s.

Is our own school really a target?

Schools are in the data. In the most recent survey, 60% of secondary schools and 44% of primary schools had identified a breach or attack in the previous 12 months, and the most common type was phishing. The sample is small and counts only what schools noticed themselves, so treat the numbers as indicative.

It makes a good opening for a class: this is not something that happens to other people.

What should someone do with a scam message?

Stop, break contact and think about what the message is trying to make you feel. Then check with the organisation using details you find yourself, not the ones in the message.

Suspicious texts can be forwarded to 7726 and suspicious emails to the NCSC. Reporting to the NCSC is not reporting a crime, so if money has been lost, report it to Report Fraud, or to Police Scotland on 101 in Scotland.

What is the best way to choose a password?

The NCSC recommends three random words. The word random matters: avoid dates, teams, names of family and pets, because that kind of information is often easy to find online. And swapping an 'o' for a zero does not make a password meaningfully stronger. Try the Password Maths lab to see why length does most of the work.

Sources and how we checked them

Each source was opened and read on 1 November 2026. Where we looked for evidence and did not find it, as with gamers and cyber performance, we say so.