FRAUD & CYBER PROTECT
EASTERN REGION

Account Hacked: escape challenge

Teacher guide

Setup, answer key, hints and debrief. Ages 11 to 14, about 65 to 70 minutes, teams of 3 to 5.

Teacher guide

Teams of 3 to 5 pupils help a friend, Jordan, recover a hacked social media account. They work out a lockbox code from Jordan's birthday, then find the answers to Jordan's security questions in Jordan's own posts. Next they spot the red flags in the phishing email that let the hacker in, and link it to a data breach. A twist shows the hacker used the account to recruit money mules. Finally, teams decide which Computer Misuse Act offence, if any, applies to three case cards, always including one about the game. The pack is written for ages 11 to 14 and runs in about 65 to 70 minutes. The same puzzle runs on the website version, so you can use either or mix them.

Learning aims. By the end, pupils can:

- explain how public posts give away security-question answers and passwords (digital footprint)
- spot the red flags in a phishing email
- explain what a data breach is, and why reusing a password makes it dangerous
- name four ways to protect an account: unique passwords, 2-step verification, made-up security answers and privacy or tagging settings
- explain what a money mule is, and why it counts as money laundering
- tell the difference between Section 1 and Section 2 offences under the Computer Misuse Act 1990, and know that logging in without permission is a crime even as a joke
- say how and where to report hacking and fraud, and where to use cyber skills legally (Cyber Choices)

Timings

Stage	What happens	Time
Hook	Read the mission brief (Handout A) aloud	3 min
Step 1	Find the birthday, open the lockbox	5 to 8 min
Step 2	Use the posts (Handout B) to fill in the reset form (Handout C)	15 min
Step 3	Circle the red flags in the phishing email (Handout D)	8 min
Twist	Team opens the sealed envelope (Handout E)	3 min
Step 4	Decide which law each case breaks (Handout F)	10 min
Debrief	Discussion questions and learning points (Handout G)	15 min

Before the lesson, for each team

1. Print Handout A (one copy) and leave it on the table, outside the box.

2. Print Handout B, cut out the twelve numbered posts, shuffle them and put them inside the lockbox. Set the lock to **228**. Keep the numbers on the cards, as the answer key and hints use them.
3. Print Handout C (one copy) and put it in the box.
4. Print Handout D (one copy) and give it out once the team's reset form is correct.
5. Print Handout E, fold it and seal it in an envelope marked "Do not open until your teacher says". Give it out once the team has found at least 5 red flags.
6. Print Handout F (one copy), cut out the 10 case cards and give them out after the twist. Each team draws one of the three game cards (A, B or E, marked ★) and two of the others.
7. Print Handout G (one per pupil) for the end. It finishes with the Stop! Think Fraud messages and a feedback slip. Collect the slips to count how many took part and how many are likely to change their behaviour. The website version saves these answers for you: open Teacher settings and choose "Show feedback results".
8. Optional: change "Slough" in post 9 and in the answer key to your own town to make it feel local.

Using the teacher's screen. You can show the website on the board as a timer and hint screen while teams work on paper. Click "We opened the real box" to skip the website's digital lock. The website shuffles the posts into a new order every time, so its post numbers won't match the paper cards. Use one version per team.

Sensitivity notes. All names, the Pixl app and the posts are made up. Do not set up real social media accounts for this activity. Some posts mention a pet that has died; check this is OK if a pupil has had a recent loss.

Answer key and hints

The lock code is **228**: Maya says Jordan and Sam share a birthday, and Sam's post is tagged #22ndAugust, so 22/8 gives 228.

Security question	Answer	Post	Also accept
Favourite colour	Green	3	Any spelling close to "green"
Favourite teacher	Miss Turner	10	Turner, Mrs/Ms Turner, small typos
First pet	Snowy	6	Snowy the gerbil, Snowey
Where born	Slough (or your own town)	9	In Slough, Slough Berkshire, small typos
Year Gran was born	1934	5	Exact year only (posted 5 Feb 2024 on her 90th: 2024 minus 90)
First school	St Michael's Primary	1	St Michaels, Saint Michael's, St Micheals, with or without "Primary"

Posts 2, 4, 7, 8, 11 and 12 are red herrings for the reset form, but they matter later. Post 11 is a phishing link and post 2 is a fake crypto investment (investment fraud). Post 4 reports the GameZone data breach, and in post 12 Jordan mentions using the same password for everything, as many people do. Post 8 shows Jordan uses the same name on every platform, and post 7 shows the hacker sending "is this u?" links to friends.

Hints to give, in order

Lockbox

1. Maya says Jordan and Sam share a birthday. When is Sam's?
2. Sam's hashtag gives the date: the 22nd of August.
3. Write it as day then month: 22 / 8. That makes three digits.

Password reset

1. Not every post helps. Posts 2, 4, 7, 8, 11 and 12 are red herrings, but remember them for later.
2. Each question has its own post: colour 3, teacher 10, pet 6, born 9, Gran 5, school 1.
3. Post 5 was posted on 5 Feb 2024, on Gran's 90th birthday. What is 2024 minus 90?

Phishing email (Handout D)

1. Look closely at the sender's email address, letter by letter.

2. Would a real company call you "Dear Customer", threaten you, or ask for your password?

3. The link should go to pixl.com. Where does it really go? And check the spelling in the subject line.

Phishing email: the six red flags. Teams need at least five.

Part of the email	Why it's a red flag
security@pixl-supp0rt.co	A zero instead of the letter o, and it doesn't end in pixl.com
URGENT: Unusual sign-in to your acount	Pressure to rush, and a spelling mistake
Dear Customer	Generic greeting; Pixl would use your name
Deleted within 24 hours	A threat and a deadline to make you panic
http://pixl-verify-login.co/secure	The link goes to a lookalike site, not pixl.com
Asks for password and security answers	Real companies never ask for these by email

The logo, the "new device" sentence, the To line and the sign-off are not red flags on their own. Logos are easy to copy, and real alerts mention new devices too.

How the hacker got in. Fraudsters sent Jordan a convincing phishing email. Its link led to a fake log-in page built to capture Jordan's password. Jordan was also at risk from the GameZone breach (post 4), because the same password was used everywhere (post 12), as many people's are. Stress that being hacked is never the victim's fault: the responsibility lies with the criminals.

Computer Misuse Act case cards (Handout F). Each team draws 3 of the 10, always including one game card (A, B or E).

Card	Answer	Why
A. You answered Jordan's security questions because Jordan asked you to	Not an offence	Jordan owns the account and gave permission. Without permission, the same steps would be Section 1.
B. The hacker logged in "just to have a look around"	Section 1	Unauthorised access, even if you only look
C. A friend saw your password and logged in to read your messages as a joke	Section 1	Knowing a password isn't permission, and a joke is no defence
D. A pupil uses a teacher's logged-in school system to look at other pupils' grades	Section 1	Using someone else's logged-in account without permission, even without changing anything
E. The hacker logged in and messaged 14 friends asking them to move money	Section 2	Access with intent to commit further offences (fraud, money laundering)

Card	Answer	Why
F. Someone logs in to a classmate's account planning to post a fake crypto investment to defraud people, but is caught first	Section 2	Intent at the time of access counts, even if the post was never made
G. Someone logs in to a friend's gaming account to sell their rare skins and keep the money	Section 2	Access with intent to commit theft or fraud
H. Someone gets in to an ex-friend's account, deletes their photos and changes the password	Section 3	Deleting data and locking the owner out impairs the account (getting in was also Section 1)
I. A gamer pays for a "booter" to knock a rival offline mid-match	Section 3	A DDoS attack impairs someone's computer or connection. Paying for the booter can also be Section 3A.
J. Someone builds a fake log-in page kit and sells it in a gaming Discord	Section 3A	Making or supplying tools for computer misuse, even if they never use it themselves

Debrief

Use these questions in order: how it happened, why, how to prevent it, and how to report it. Suggested answers are in brackets.

How did it happen?

1. How did the hacker find the security answers? (Jordan's public posts.)
2. How was the lock code found? (From a birthday in a tagged post. Codes based on dates are easy to guess or try one by one.)
3. How did the hacker get Jordan's password? (The phishing email: its fake log-in page captured Jordan's password. Post 11, the "free Pixl Gold" link, works the same way.)
4. What is a data breach, and why did the GameZone breach (post 4) put Jordan at risk? (A site is hacked and its users' details leak. Jordan uses the same password everywhere (post 12), as many people do, so a leaked GameZone password opens Pixl too. haveibeenpwned.com shows whether an email address has been in a breach.)
5. Post 8 shows Jordan uses the same name everywhere. Why does that help a hacker? (They can find and try every account.)

Why do it?

6. Why do hackers want ordinary people's accounts? (To commit fraud against friends, who trust messages from people they know; to sell things or run fake profiles; to spread phishing links like in post 10.)
7. What was the crypto post (post 2) for? (Investment fraud to take people's money, often run from hacked accounts so it looks trustworthy.)
8. What was the message in the envelope trying to do? (Recruit money mules.)

Money mules

A money mule lets criminals move money through their bank account, often for a small cut. The money usually comes from fraud. Passing it through other people's accounts hides where it came from, which is money laundering. Young people are often targeted with "easy money" offers on social media or in messages from friends' hacked accounts. Points to make:

- It is a crime, even if you only "helped a friend", kept a small amount or didn't know where the money came from.
- **Legal consequences for the mule:** money laundering can lead to prosecution and a criminal record, with a maximum sentence of 14 years in prison.
- **Financial consequences for the mule:** the bank can freeze or close the account, and it can be hard to open another. Banks can record a fraud marker on the national fraud database (Cifas), which lasts six years unless successfully challenged. Banks, phone companies and lenders check it, so the mule can be refused mobile phone contracts, credit cards, loans, student loans and, later, a mortgage.

- It can also put a college or university place and some jobs at risk.
- If anyone asks to use your account, say no, tell a trusted adult and contact your bank. Criminals deliberately target and pressure young people, so anyone already involved should tell a trusted adult and their bank as soon as possible, and they will be supported.

The Computer Misuse Act 1990 and Cyber Choices

The Computer Misuse Act makes it a crime to access a computer, account or data without permission. The maximum sentences are 2 years for Section 1, 5 years for Section 2 and 10 years for Section 3 (CPS guidance).

Section	Offence	Maximum sentence	Example from the activity
1	Unauthorised access to computer material	2 years	Logging in to Jordan's account with a stolen password, even just to look
2	Unauthorised access with intent to commit or facilitate further offences	5 years	Logging in to use Jordan's account to recruit money mules or post fake investments
3	Unauthorised acts with intent to impair, or reckless as to impairing, a computer	10 years	Deleting someone's data, locking them out, or a DDoS attack using a "booter"
3A	Making, supplying or obtaining articles for use in computer misuse offences	2 years	Making or selling a phishing kit, or buying stolen password lists

Section 3ZA (unauthorised acts causing serious damage, for example to national infrastructure) isn't covered in the activity. It carries up to 14 years, or life where it puts lives or national security at risk.

Points to make:

- The pupils' own actions were legal only because Jordan gave permission. The same steps without permission would be a Section 1 offence.
- "It was a joke", "I just wanted to see if I could" or "they told me their password once" are not defences.
- Section 2 depends on intent at the time of access, so it applies even if the further crime never happens.
- Cyber skills are in demand. Cyber Choices is a national programme coordinated by the National Crime Agency and delivered by teams in Regional Organised Crime Units and local police forces. It helps young people use their cyber skills legally, and schools can refer pupils who are at risk.

How could it have been prevented?

- A different strong password for every account (three random words is a good start), and checking haveibeenpwned.com for breaches
- 2-step verification turned on

- Made-up security answers that only you know, kept in a password manager
- Privacy settings that make posts friends-only, and tags that need your approval
- Not clicking log-in links in posts or messages

How to report it

- Tell a trusted adult (parent, carer or teacher) straight away.
- Report the hacked account to the app or website using its "hacked account" help pages.
- Report fraud and cyber crime to Report Fraud at reportfraud.police.uk or 0300 123 2040 (England, Wales and Northern Ireland). It replaced Action Fraud in December 2025. In Scotland, call Police Scotland on 101.
- Forward suspicious texts to 7726 for free.
- If you are worried or upset, contact Childline on 0800 1111 or at childline.org.uk.