Handout A: Mission brief (on the table, outside the box)

SECURITY ALERT: your friend Jordan has been hacked.

Jordan has just messaged you in a panic. Someone has taken over their Pixl account and changed the password. To get it back, you need to answer Jordan's security questions. Jordan can't remember the answers, but the hacker found them easily. Can you?

Step 1: Crack the 3-digit lock. Hackers often guess codes from birthdays. These two posts give away Jordan's birthday. Use it to open the box.

Clue post
Maya @maya.k · Today: @jordz_r and @sam_t I literally can't believe you two have the SAME birthday! You both out tonight??
Sam @sam_t · Today: Another year older! Thanks for all the messages everyone! #22ndAugust

Step 2: Inside the box you'll find Jordan's posts and the password reset form. Use the posts to answer the questions. When you think you have all six, show your teacher.

Handout B: Jordan's posts (cut out, inside the box)

Cut along the lines. Not every post is useful.

No.	Post
1	**Jordan** @jordz_r · 12 Nov 2023: Still hanging out with @suzi_b, St Michael's Primary crew forever [Photo: Jordan and Suzi]
2	**Kai** @kai.trades · 28 Feb 2025: Turned £50 into £2,000 in ONE week with CoinRocket! DM me "ROCKET" and I'll show you how. Only taking 5 more people!!
3	**Jordan** @jordz_r · 14 Feb 2025: Green is 100% my favourite colour, new hoodie day [Photo: Jordan in a green hoodie]
4	**Tech News Daily** @technews.daily · 1 Mar 2025: BREAKING: Gaming site GameZone has been hacked. The usernames, email addresses and passwords of 2.3 million players have been leaked online. Change your password now!
5	**Jordan** @jordz_r · 5 Feb 2024: Happy 90th birthday to the best gran in the world! #90today
6	**Jordan** @jordz_r · 3 Dec 2024: Dog walking is so tiring. Honestly still miss my first ever pet… Snowy the gerbil #SnowyForever
7	**Alfie** @alfie.j · Today: @jordz_r just sent me a message saying "is this u??" with a link… was that actually you??
8	**Jordan** @jordz_r · 20 Feb 2025: New phone who dis. Add me everywhere, same name on everything: Insta @jordz_r · TikTok @jordz_r · Steam jordzR
9	**Jordan** @jordz_r · 22 Aug 2024: 15 years since I arrived in this world, right here in my home town #Slough #HomeTown
10	**Jordan** @jordz_r · 9 Jan 2025: Saw Miss Turner in town with her new baby. Still the best PE teacher EVER
11	**Pixl Rewards** @pixl.rewardz · Sponsored · 2 Mar 2025: Get PIXL GOLD free for 30 days! Just log in with your username and password here: pixl-gold-free.co
12	**Jordan** @jordz_r · 1 Mar 2025: lol I had a GameZone account years ago, not changing anything, I use the same password for literally everything anyway

Handout C: Pixl password reset form

Team name: _____

To prove you are Jordan, answer all six security questions. Use the numbered posts. When you're done, show this form to your teacher.

Security question	Your answer	Post no.
1. What is your favourite colour?		
2. Which teacher did you like most at school?		
3. What was the name of your first pet?		
4. Where were you born?		
5. What year was your gran born?		
6. What was the name of your first school?		

Teacher check: ____ / 6 correct Time: _____

Handout D: How did the hacker get in?

ACCOUNT RECOVERED! Jordan is back in. But how did the hacker get in? The day before the hack, fraudsters sent Jordan this convincing email, and Jordan followed the link.

Circle every red flag you can find. You need at least 5.

Inbox · 1 unread
From: Pixl Security security@pixl-supp0rt.co
To: jordz_r@mailbox.com
Subject: URGENT: Unusual sign-in to your acount
Pixl
Dear Customer,
We noticed a sign-in to your account from a new device.
If you do not verify within 24 hours, your account will be permanently deleted.
Verify now: http://pixl-verify-login.co/secure
You will need your password and the answers to your security questions.
Thanks, The Pixl Team

Red flags we found: _____

Bonus: look back at the posts. Which two posts show another way the hacker could have got Jordan's password? Posts ____ and ____

Handout E: The twist (sealed envelope)

ONE MORE THING…

When you check Jordan's messages, you find this. The hacker sent it to 14 of Jordan's friends while they had the account:

> **Jordan @jordz_r · sent to 14 friends**
>
> Heyy need a quick favour, can I send £500 into your bank account? Just send it straight on to my cousin's account and keep £50 for yourself. Easy money, nobody will know

Talk about it as a team:

1. What was the hacker trying to do?
2. Why send it from Jordan's account instead of their own?
3. What could happen to a friend who said yes?

Write your answer to question 1 here, then show your teacher:

Check your answer: what could happen to the mule?

- **A criminal record.** Money laundering can mean prosecution, with a maximum sentence of 14 years in prison.
- **No bank account.** The bank can freeze or close your account, and it can be hard to open another one.
- **A fraud marker for up to six years.** Banks, phone companies and lenders check it.
- **Refused phone contracts and credit.** You can be turned down for a mobile phone contract, credit card, loan, student loan or, later, a mortgage.

Criminals deliberately target young people and can pressure or threaten them. If you've been asked, or already got involved, it's not too late: tell a trusted adult and your bank as soon as you can, and you'll be helped.

Handout F: Cyber Choices: what does the law say?

The **Computer Misuse Act 1990** makes it a crime to get into someone else's account or device without permission. What happens next decides how serious it is.

Section	What it means	Maximum sentence
Section 1	Unauthorised access: getting into an account or computer without permission, even "just to look"	2 years
Section 2	Unauthorised access **with intent** to commit another crime, such as fraud or money laundering	5 years
Section 3	Doing something without permission to damage or disrupt, such as deleting files, knocking someone offline or locking the owner out	10 years
Section 3A	Making, supplying or getting hold of hacking tools, such as phishing kits, password-stealers or lists of stolen passwords	2 years

Cut out the 10 case cards. Put the three game cards (marked ★) in one pile and the rest in another. Shuffle both face down, then draw 1 game card and 2 other cards. For each card you draw, decide which box to tick, then check with your teacher.

Case card	Not an offence	S1	S2	S3	S3A
A ★. You answered Jordan's security questions because Jordan asked you to help get the account back.	☐	☐	☐	☐	☐
B ★. The hacker logged in to Jordan's account with the stolen password, "just to have a look around".	☐	☐	☐	☐	☐
C. Your friend saw you type your password, then logged in to your account to read your messages as a joke.	☐	☐	☐	☐	☐
D. A pupil spots that a teacher left the school system logged in, and looks through other pupils' grades without changing anything.	☐	☐	☐	☐	☐
E ★. The hacker logged in to Jordan's account and used it to message 14 friends asking them to move money.	☐	☐	☐	☐	☐

Case card	Not an offence	S1	S2	S3	S3A
F. Someone guesses a classmate's password and logs in, planning to post a fake crypto investment from their account to defraud people. They get caught before posting it.	☐	☐	☐	☐	☐
G. Someone logs in to a friend's gaming account to sell their rare skins and keep the money.	☐	☐	☐	☐	☐
H. After getting in to an ex-friend's account, someone deletes all their photos and changes the password so they can't get back in.	☐	☐	☐	☐	☐
I. A gamer pays for a "booter" service to flood a rival's internet connection and knock them offline in the middle of a match.	☐	☐	☐	☐	☐
J. Someone builds a fake log-in page kit for stealing passwords and sells it in a gaming Discord.	☐	☐	☐	☐	☐

Talk about it: what would have made your own actions in this challenge illegal?

Good with tech? Use your skills legally. Find clubs, competitions and careers at cyberchoices.uk.

Handout G: Congratulations!

Well done, Team _____! You recovered Jordan's account, tracked down how the hacker got in, uncovered the money mule fraud and know where the law draws the line.

Time taken: _____ Hints used: _____

Six things to remember

1. **Your posts can unlock your accounts.** Every security answer was in Jordan's public posts, and the lock code came from a birthday. Use made-up security answers that only you know, and think before posting personal details.
2. **One password per account, plus 2SV.** Use a different strong password for every account (three random words is a good start) and turn on 2-step verification, so a stolen password isn't enough.
3. **Spot the phish.** Check the sender's address letter by letter. Watch for "Dear Customer", threats, deadlines, odd links and anyone asking for your password. Instead of using the link, go to the app or website yourself.
4. **Data breaches happen.** Sites you've used can be hacked and their passwords leaked. Check your email at haveibeenpwned.com, and change any password you've used on more than one site.
5. **Never lend your bank account.** Letting someone move money through your account is money laundering, even for a friend. You can get a criminal record, lose your bank account and get a fraud marker that stops you getting a phone contract, credit or a student loan for up to six years.
6. **No permission? No access.** Logging in to someone else's account without permission is a crime under the Computer Misuse Act, even as a joke (Section 1, up to 2 years). Doing it to commit another crime is Section 2 (up to 5 years).

Need help? Tell a trusted adult. Report hacked accounts to the app. Report fraud at reportfraud.police.uk or 0300 123 2040 (in Scotland, call 101). Forward suspicious texts to 7726. Childline: 0800 1111. Use your cyber skills legally: cyberchoices.uk.

Stop! Think Fraud

The national campaign against fraud. Fraudsters aren't fussy: they'll pick on anyone, so take a moment every time something feels off.

Stop	Think	Check	Protect	Report
Take a moment before you click, reply, pay or share anything. Fraudsters rush you so you don't have time to think.	Could this be fraud? Pressure, deadlines, offers that are too good to be true, and requests for passwords, codes or money are all warning signs.	Is it genuine? Go to the app or website yourself, or contact the person another way. Never use the link or number in the message.	Use passkeys instead of passwords where you can, and turn on 2-step verification everywhere else.	Been targeted? Tell a trusted adult and report it at reportfraud.police.uk.

Find out more at stopthinkfraud.campaign.gov.uk.

Before you go: tell us what you think

Team name: _____

How many people were in your team? _____

After playing, how likely are you to change how you stay safe online? Tick one.

☐ Very likely ☐ Quite likely ☐ Not sure ☐ Not very likely ☐ Not at all likely

What will you do first? Tick any.

- ☐ Turn on 2-step verification
- ☐ Use a different password for each account
- ☐ Make my posts private and check tagging
- ☐ Use made-up security answers
- ☐ Check haveibeenpwned.com
- ☐ Stop and check before clicking links
- ☐ Never lend my bank account