National Cyber Security Centre
a part of GCHQ

Mortimer

Cyber Security Training For School Staff

2025/26

Cyber Security

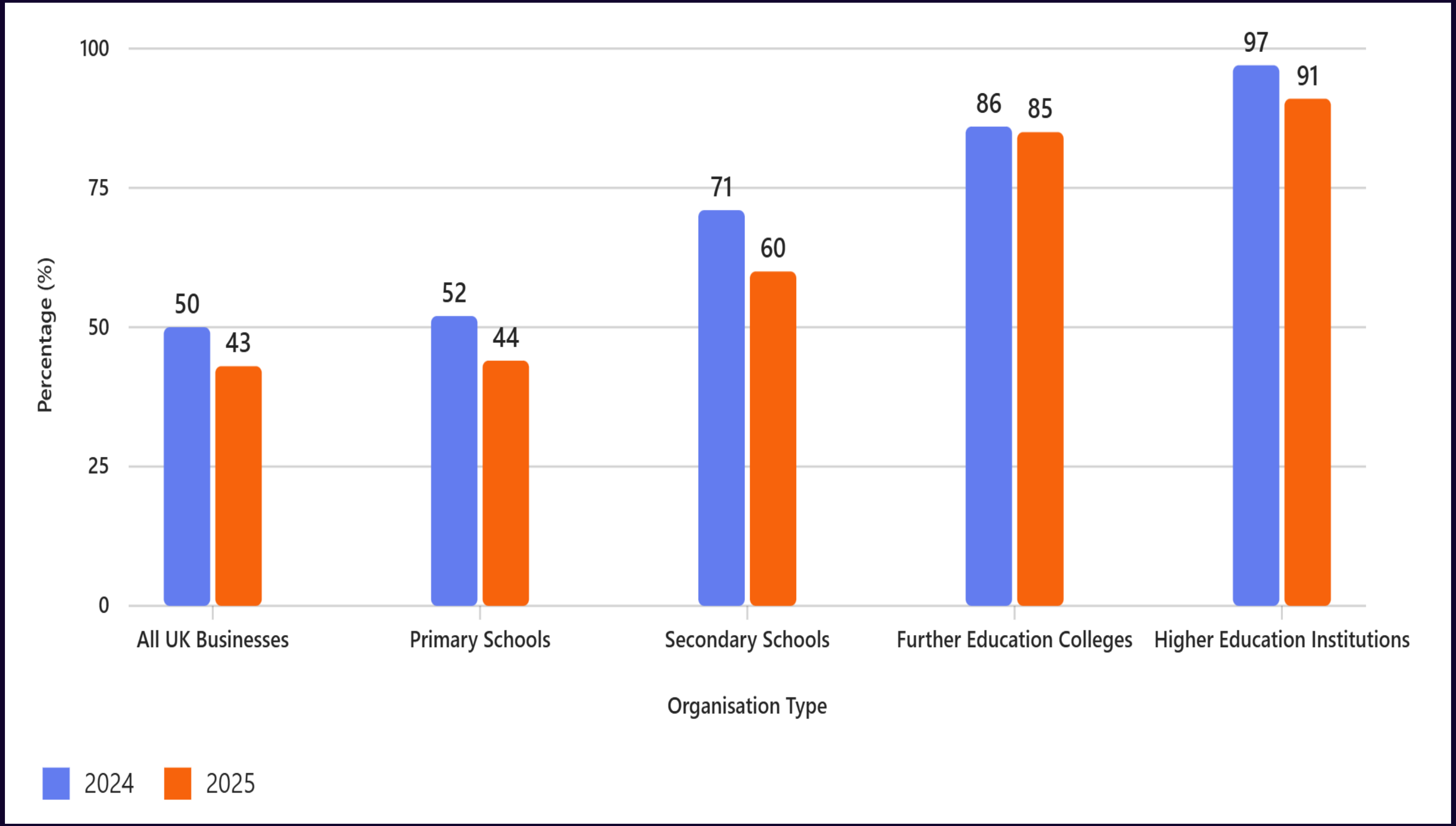
The government have said that all schools need to meet the cyber security standard.

All staff should have annual cyber security training.

Agenda

- School cyber resilience in numbers.
- Who is behind school cyber attacks?
- Cyber threats from outside the school.
- Cyber threats from inside the school.
- 4 key ways to keep yourself safe.

Cyber Security Breaches: Percentage of Organisations Identifying Attacks (2024 vs 2025)



Types of attack - 2025

Type of Attack	Primary	Secondary
Phishing	89% ↑	89% ↑
Others impersonating the organisation or staff	32% ↑	50% ↑
Viruses, spyware, or malware	9% ↑	22% ↑
Unauthorised access of files or networks by students	5% ↓	17% ↑
Unauthorised access of files or networks by staff	6% ↑	10% ↓
Hacking or attempted hacking of online bank accounts	6% ↑	3% ↓
Ransomware	7% ↓	3% ↓
Denial of service attack	2% ↓	10% ↑

Phishing is generally the first stage in many cyber attacks

89% of schools have experienced a phishing attacks

What is cyber phishing?

Question: What is cyber phishing?

A. A method of encrypting data to keep it secure online

B. A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source

C. A technique used to speed up internet connections

D. A process for backing up files to cloud storage

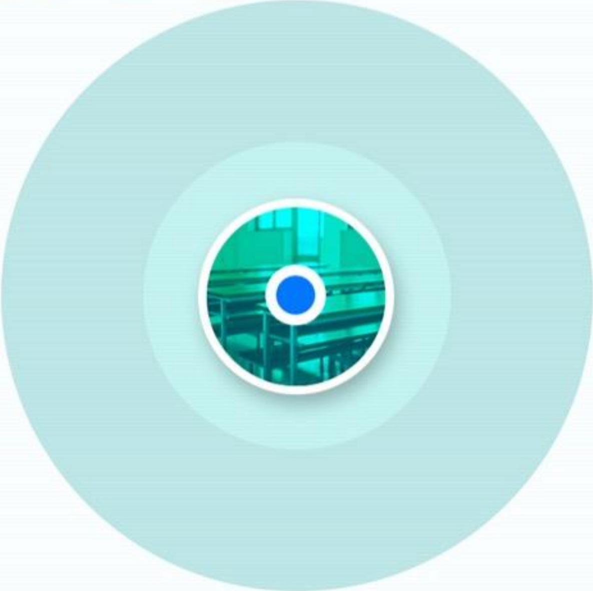
✅ **Correct Answer: B** – A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source.

Who is behind cyber attacks?

- Criminals that might wish to target your school for financial gain.
- Criminals that have identified a potential weakness in the school's technology or processes.
- Staff or pupils that could be responsible for attacks either intentionally or accidentally.

Why would they target my school?

- Schools hold lots of sensitive data that can be very valuable.
- Lots of financial transactions signed off by one person.
- May be seen as a soft target.
- Don’t have dedicated security and fraud teams.
- IT may be older and therefore more vulnerable.



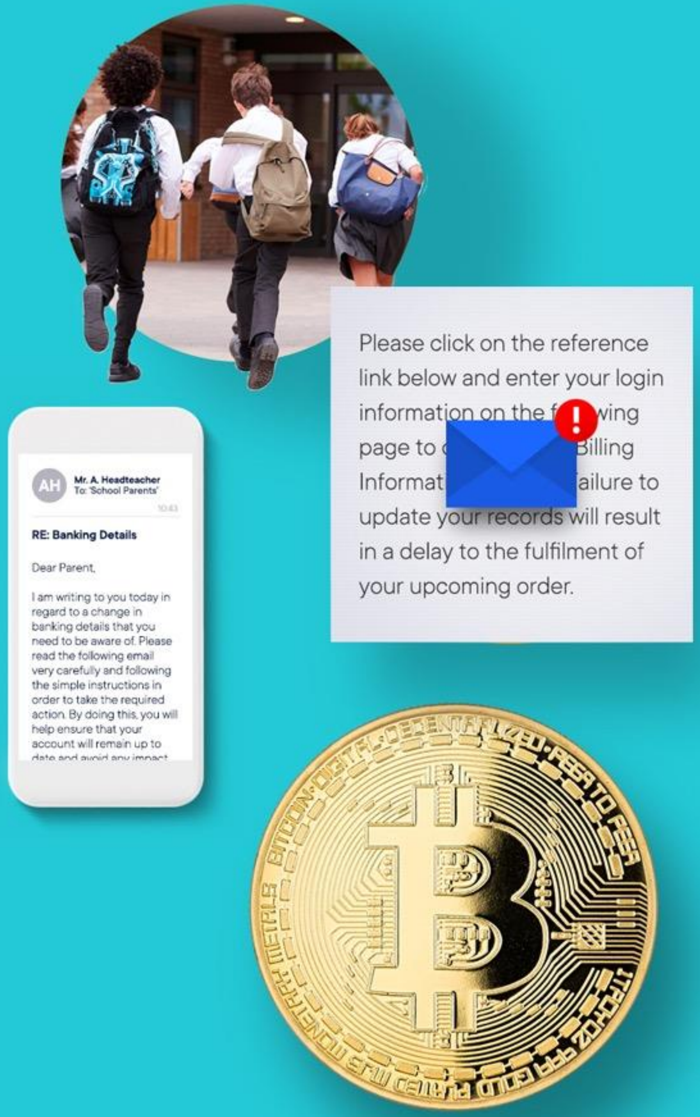
Cyber threats from outside the school

Online criminals

Case Study – Fraud and ransomware

‘Payment fraud’ and ransomware attacks in schools

The case study will automatically play when progressing to the next slide



Mr. A. Headteacher
To: 'School Parents'
10:43

RE: Banking Details

Dear Parent,

I am writing to you today in regard to a change in banking details that you need to be aware of. Please read the following email very carefully and following the simple instructions in order to take the required action. By doing this, you will help ensure that your account will remain up to date and avoid any impact

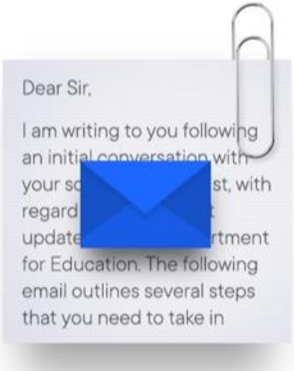
Please click on the reference link below and enter your login information on the f wing page to c Billing Informati ailure to update your records will result in a delay to the fulfilment of your upcoming order.

Case Study – Ransomware

Phone call from someone pretending to be from the DfE

Phone call from DfE →

Asked for email details of head of finance →



Dear Sir,

I am writing to you following an initial conversation with your sc st, with regard update rtment for Education. The following email outlines several steps that you need to take in

Sent targeted email →

Files encrypted →

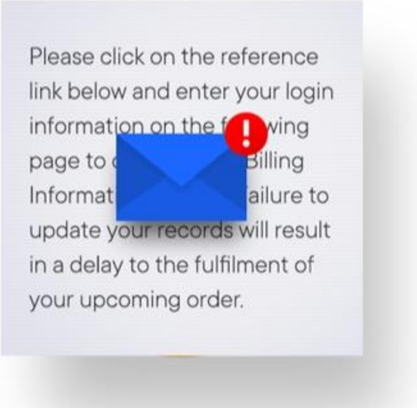
Spread through the network →

Demanded £8,000 for decryption

Case Study – Fraud

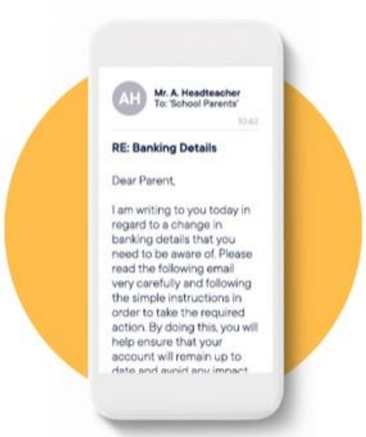
Independent school parents targeted by ‘payment fraud’ scam

Independent school targeted →



Please click on the reference link below and enter your login information on the f wing page to c Billing Informat ailure to update your records will result in a delay to the fulfilment of your upcoming order.

Phishing attack led to the compromise of email →



Mr. A. Headteacher
To: 'School Parents'
10:43

RE: Banking Details

Dear Parent,

I am writing to you today in regard to a change in banking details that you need to be aware of. Please read the following email very carefully and following the simple instructions in order to take the required action. By doing this, you will help ensure that your account will remain up to date and avoid any impact

Email sent to parents informing of banking detail change →

Parent’s school fees stolen and details sold on for identity fraud

Threat to critical national infrastructure

Foreign government actors

Target: defence industries | governments | academia

Cyber threats from inside the school

Pupils

Case Study – Password management

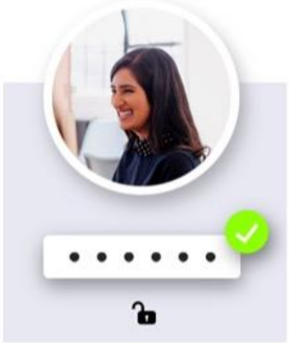
School hacked by pupil broke Data Protection Act

The case study will automatically play when progressing to the next slide

Case Study – Password management

School hacked by pupil
Broke Data Protection Act

Accessed school MIS →



Used teacher’s password →

20,000 records involved →

Duplicate passwords used →

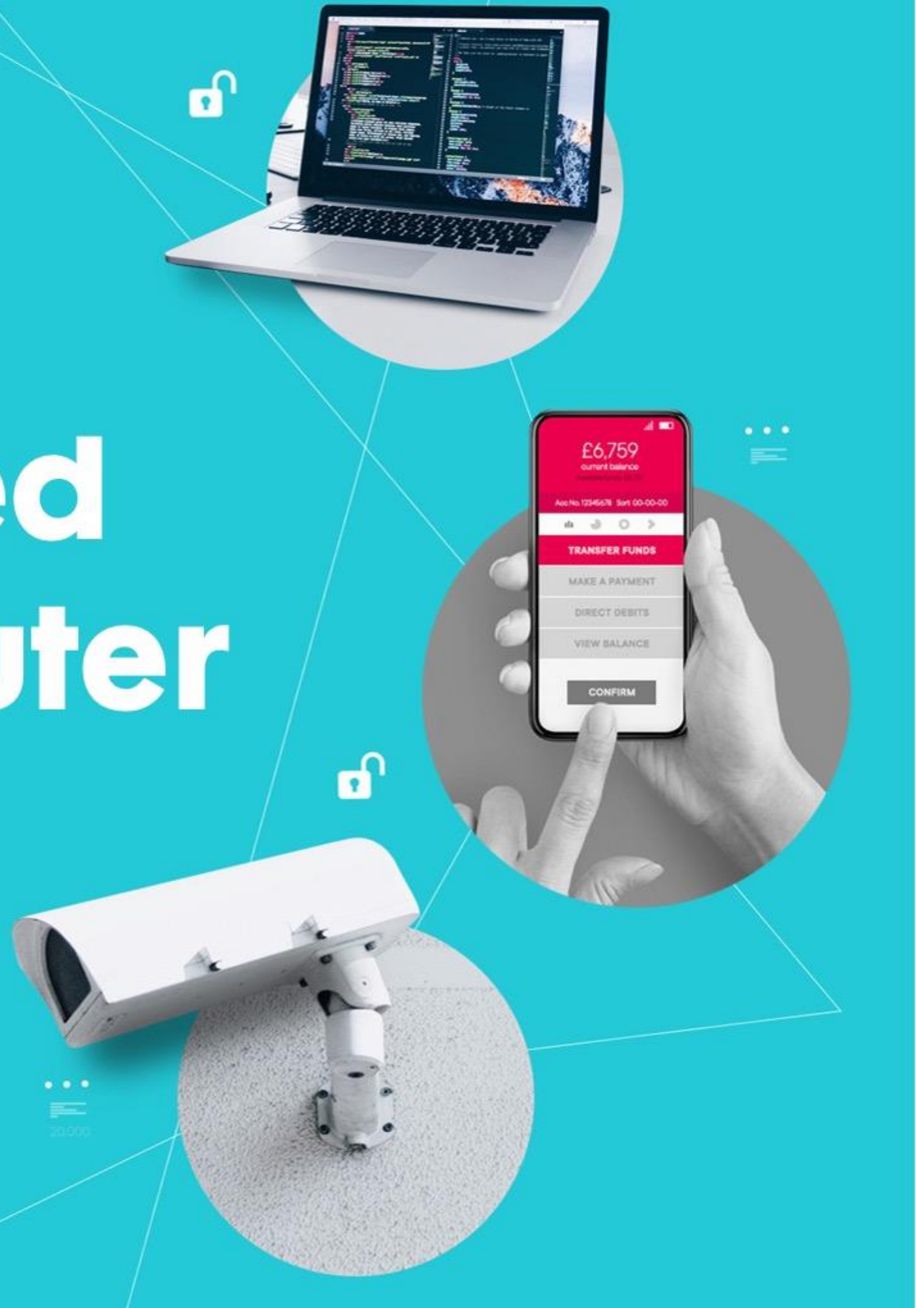
ico.
Information Commissioner's Office

Disciplined by ICO

Staff

Case Study – Access control

IT manager convicted after school's computer network hacked



Case Study – Access control

IT manager arrested after school's computer network hacked

School IT manager

→

Taking school money

→

Access to CCTV systems

→

Wiped everything when caught

What is the average age of a cyber criminal?

Question: What is the average age of a cyber criminal in the UK?

A. 24 years old

B. 17 years old

C. 30 years old

D. 12 years old

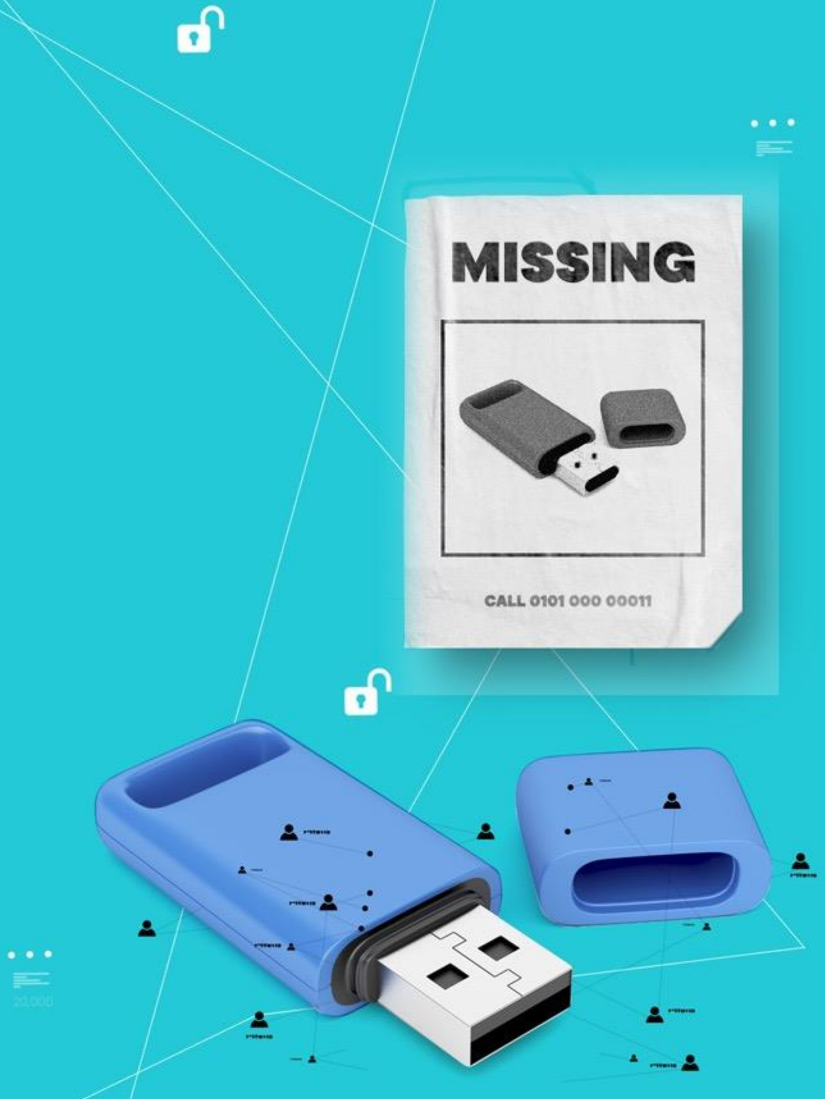
✅ **Correct Answer: B. 17 years old – Source National Crime Agency**

Accidental cyber incidents

Case Study – Secure storage

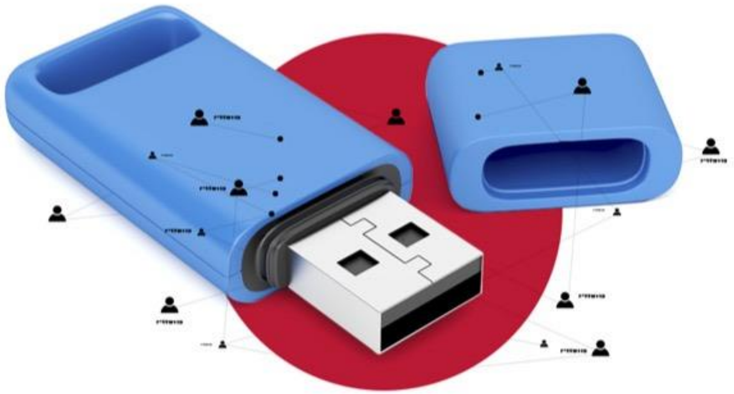
School USB stick loss exposes pupil data

The case study will automatically play when progressing to the next slide



Case Study – Secure storage

School USB stick loss exposes pupil data



Unencrypted USB stick with thousands of pupils details

→

Removed from school and lost

→

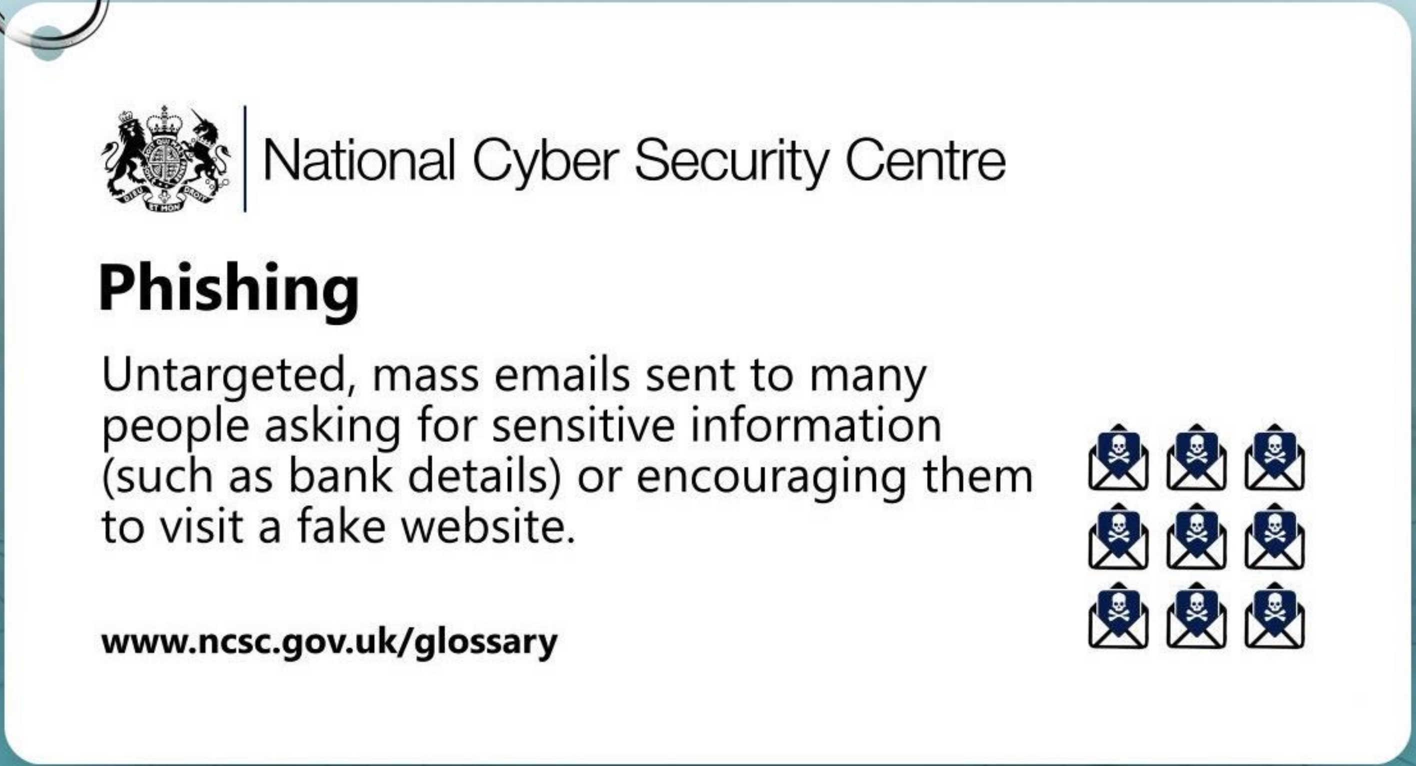
ico.
Information Commissioner's Office

Handed back in and reported to ICO

4 key ways to defend yourself

- Defend against phishing attempts.
- Use strong passwords.
- Secure your devices.
- If in doubt call it out.

1. Defend against phishing attempts



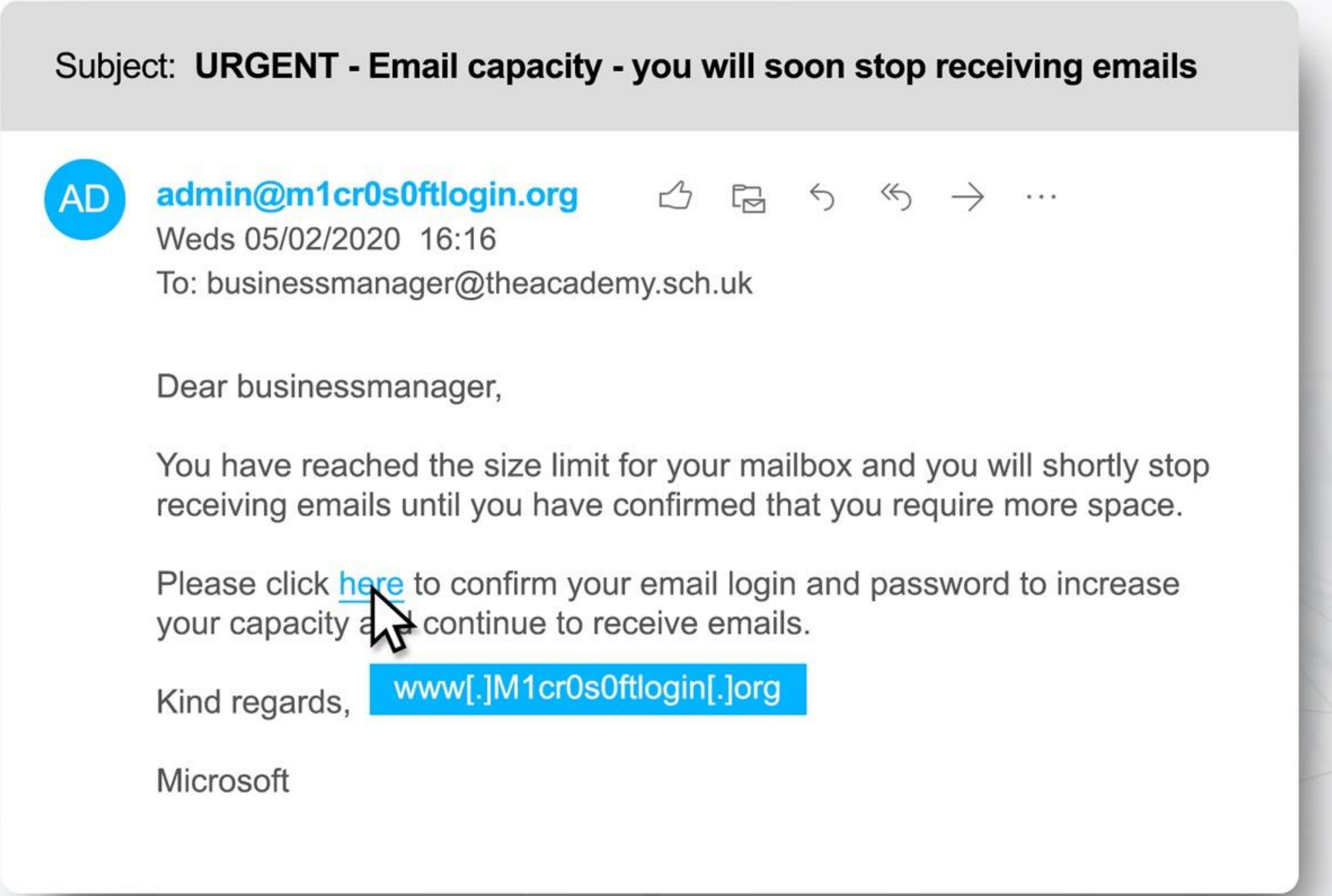
National Cyber Security Centre

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

www.ncsc.gov.uk/glossary

Phishing example



Subject: **URGENT - Email capacity - you will soon stop receiving emails**

admin@m1cr0s0ftlogin.org

Weds 05/02/2020 16:16

To: businessmanager@theacademy.sch.uk

Dear businessmanager,

You have reached the size limit for your mailbox and you will shortly stop receiving emails until you have confirmed that you require more space.

Please click here to confirm your email login and password to increase your capacity and continue to receive emails.

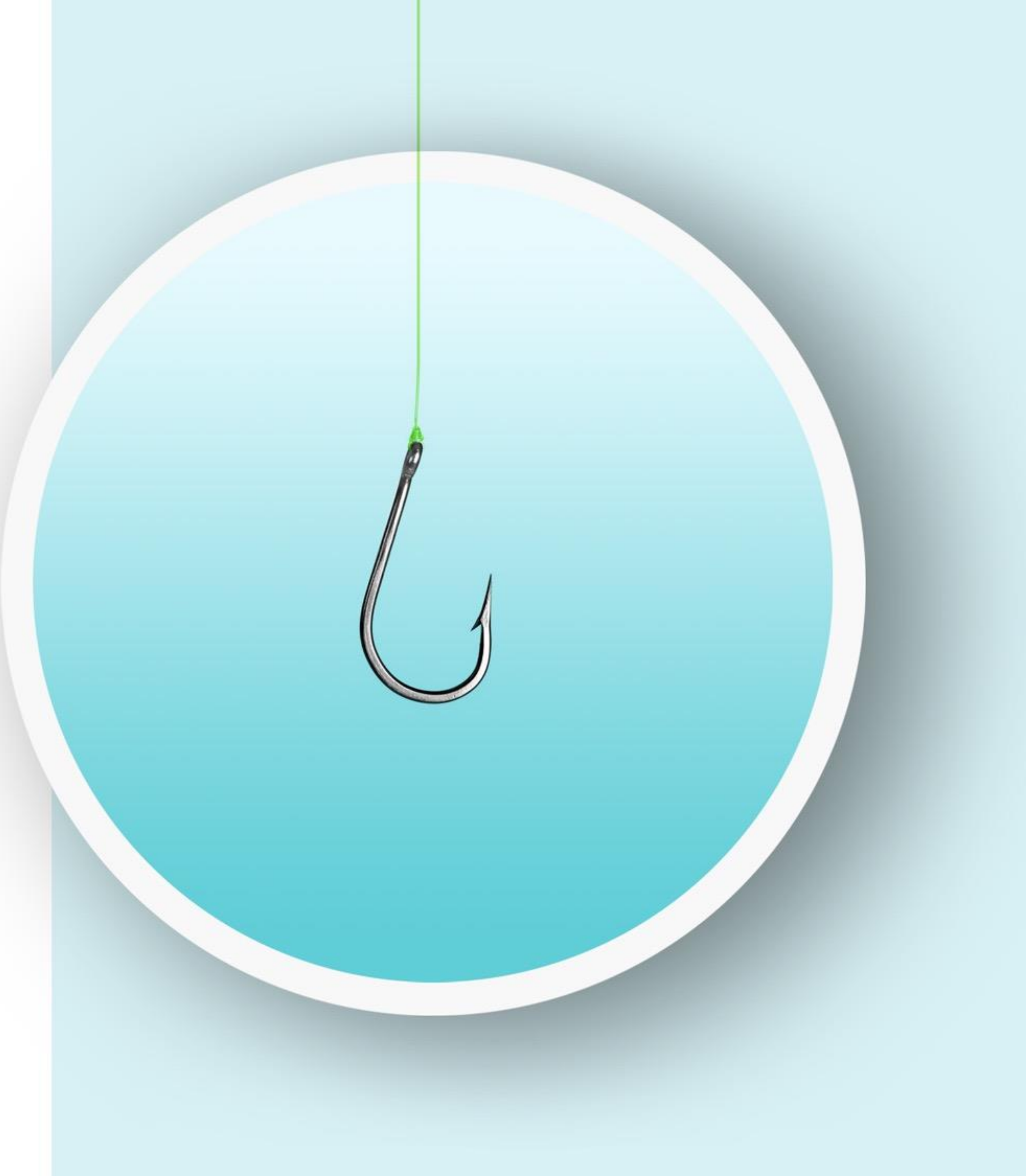
Kind regards,

www[.]M1cr0s0ftlogin[.]org

Microsoft

1. How do I defend myself against phishing attempts?

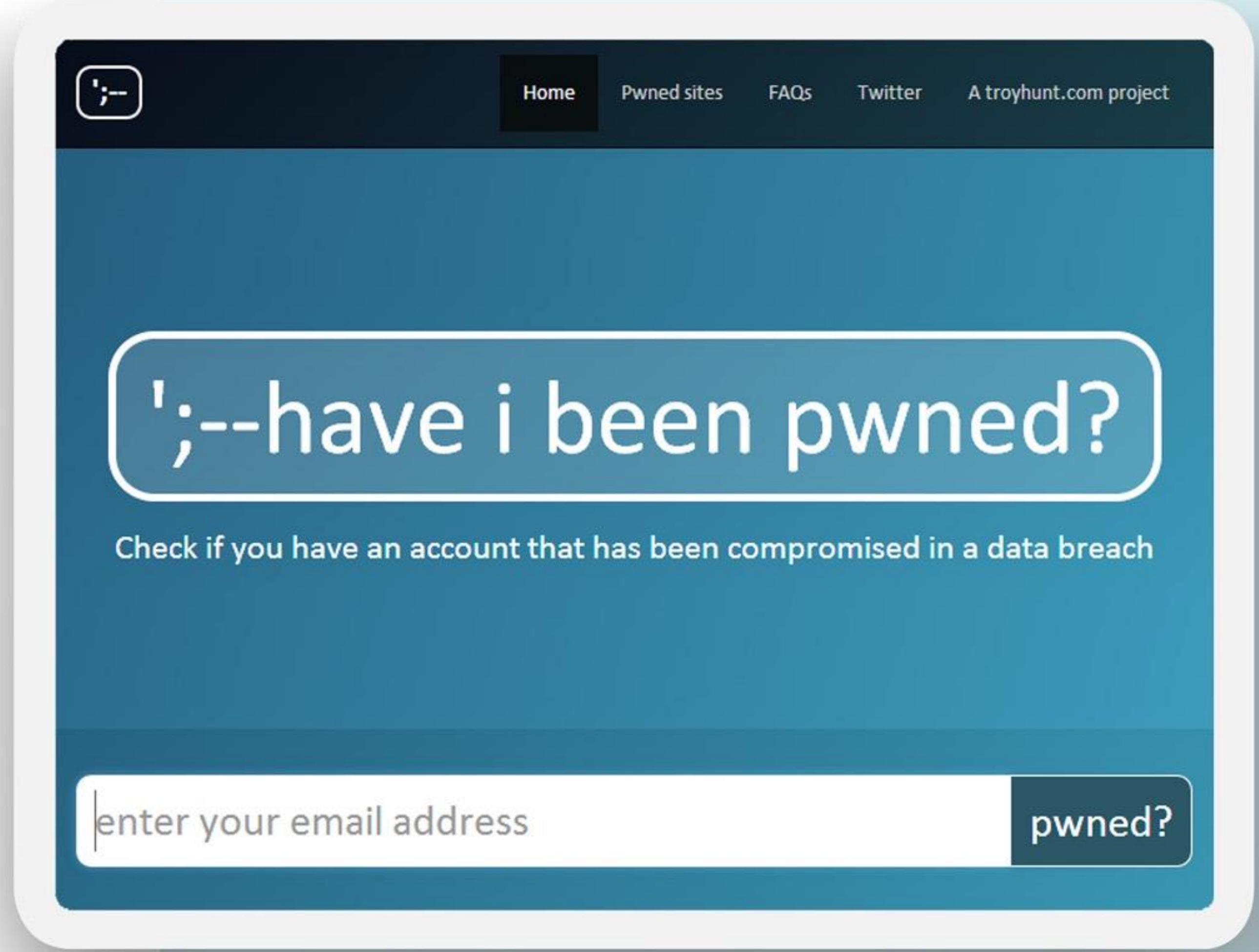
1. Reduce the information available to attackers.
2. Know the influence techniques.
3. Know what 'normal' looks like.
4. Don't be embarrassed to ask for help.
5. Report if you click!



2. Use strong passwords

2. Using strong passwords

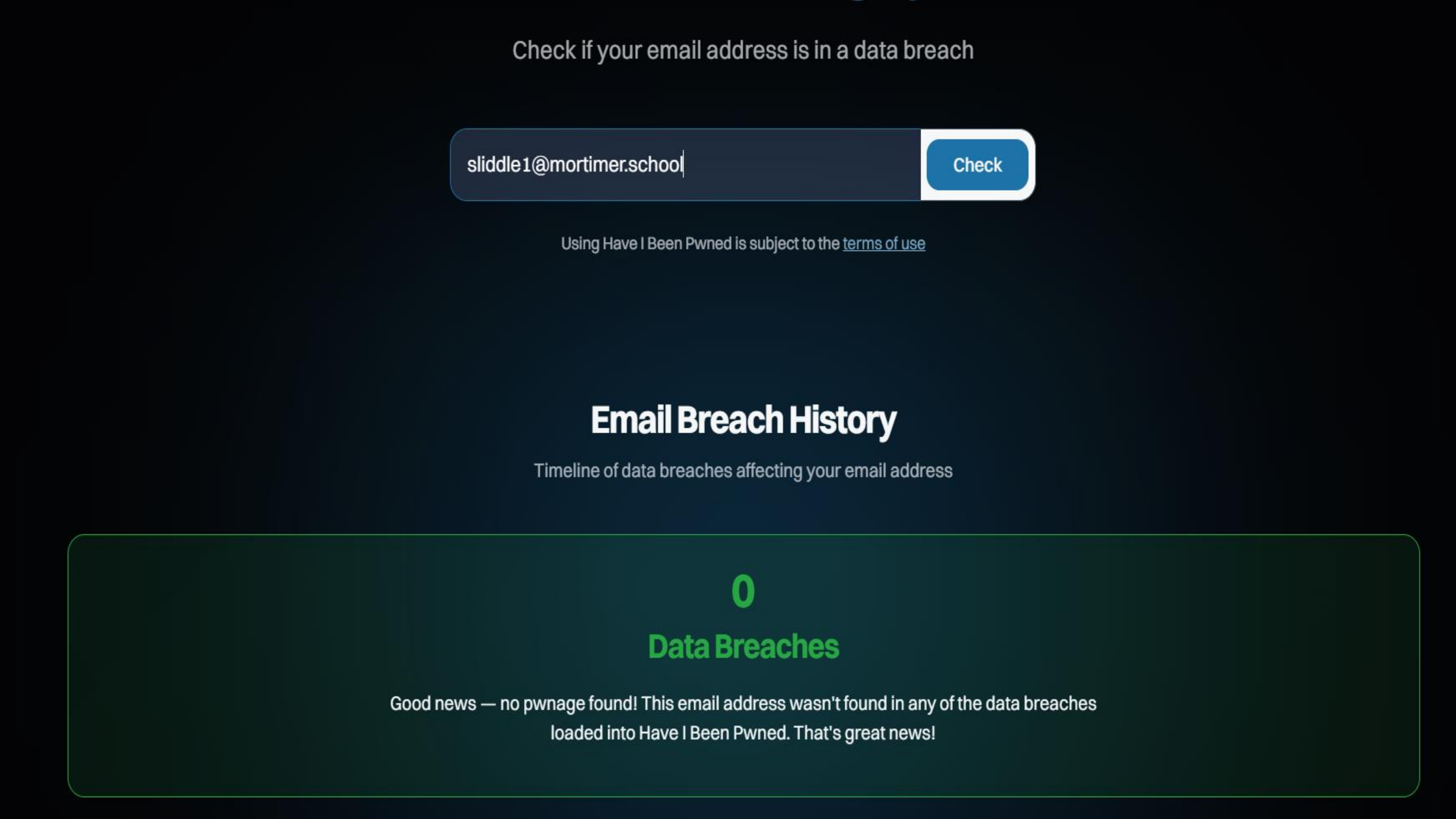
- Avoid commonly used passwords.
- Avoid passwords relating to personal information.
- Avoid passwords that have been breached previously.



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

www.haveIbeenpwned.com



Check if your email address is in a data breach

sliddle1@mortimer.school

Using Have I Been Pwned is subject to the terms of use

Email Breach History

Timeline of data breaches affecting your email address

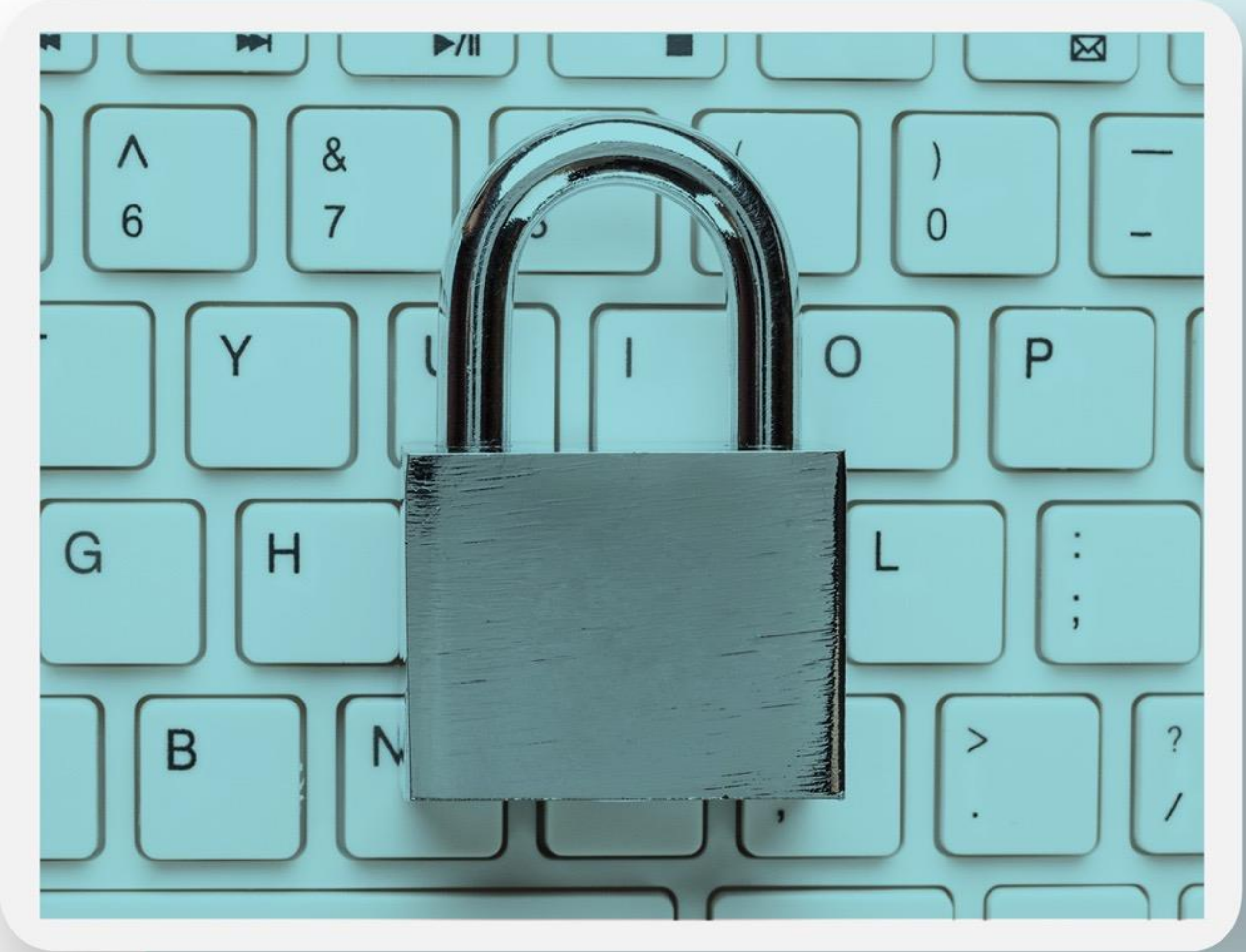
0

Data Breaches

Good news — no pwnage found! This email address wasn't found in any of the data breaches loaded into Have I Been Pwned. That's great news!

2. Using strong passwords

1. Create a strong password for important accounts.
2. Use a separate password for your work account.
3. Where available, switch on two-factor authentication for important accounts.
4. Store passwords securely.



3. Secure your devices

3. Secure your devices

1. School owned devices.
2. Your own devices.
3. Removable storage.

3. Secure your devices

1. Do not ignore updates.
2. Only download apps from trustworthy sources.
3. Physically protect your device.
4. If you need to use USB storage, ensure it is encrypted.

4. If in doubt call it out

4. If in doubt call it out

1. Report any suspicious activity.
2. Report as soon as possible.
3. Don’t be afraid to challenge.

Summary

Your checklist

Review

Review the privacy settings for your social media, professional networking sites and app accounts.

Know

Know who to report any unusual activity to. If you're not sure, ask your line manager or IT team.

Check

Check your device is set to receive updates automatically.

Set

Set a strong password and switch on two-factor authentication, if available, for your most important accounts.

Remove

Remove any apps that have not been downloaded from official stores.

Check

Check that the password for your work account is unique.

Flag it

If it's not possible to follow security advice, process or policy - flag it to your IT team.

Staff Code of Conduct – Sept 2025

11 Core Principles

Duty of Care: Protect pupils from harm; act with integrity and good judgment.

Confidentiality: Share sensitive info only on a need-to-know basis; follow safeguarding protocols.

Professional Boundaries: Avoid favouritism, inappropriate relationships, or misuse of authority.

Behaviour & Appearance: Maintain high standards; dress appropriately; avoid compromising conduct.

Whistleblowing & Reporting: Report concerns promptly; maintain accurate records; use CPOMS

Transport & Visits: Follow risk assessments; avoid lone situations; inform senior staff.

Physical Contact: Follow "no touch" culture unless necessary for safety or SEN; always transparent.

Technology & Communication: Use only school systems; no personal contact details or social media links.

Images & Internet: Use school devices only; obtain consent; never access inappropriate material.

Gifts & Rewards: Only within agreed school policy; avoid perception of bribery or grooming.

Social Contact: No secret or inappropriate social relationships with pupils or parents.

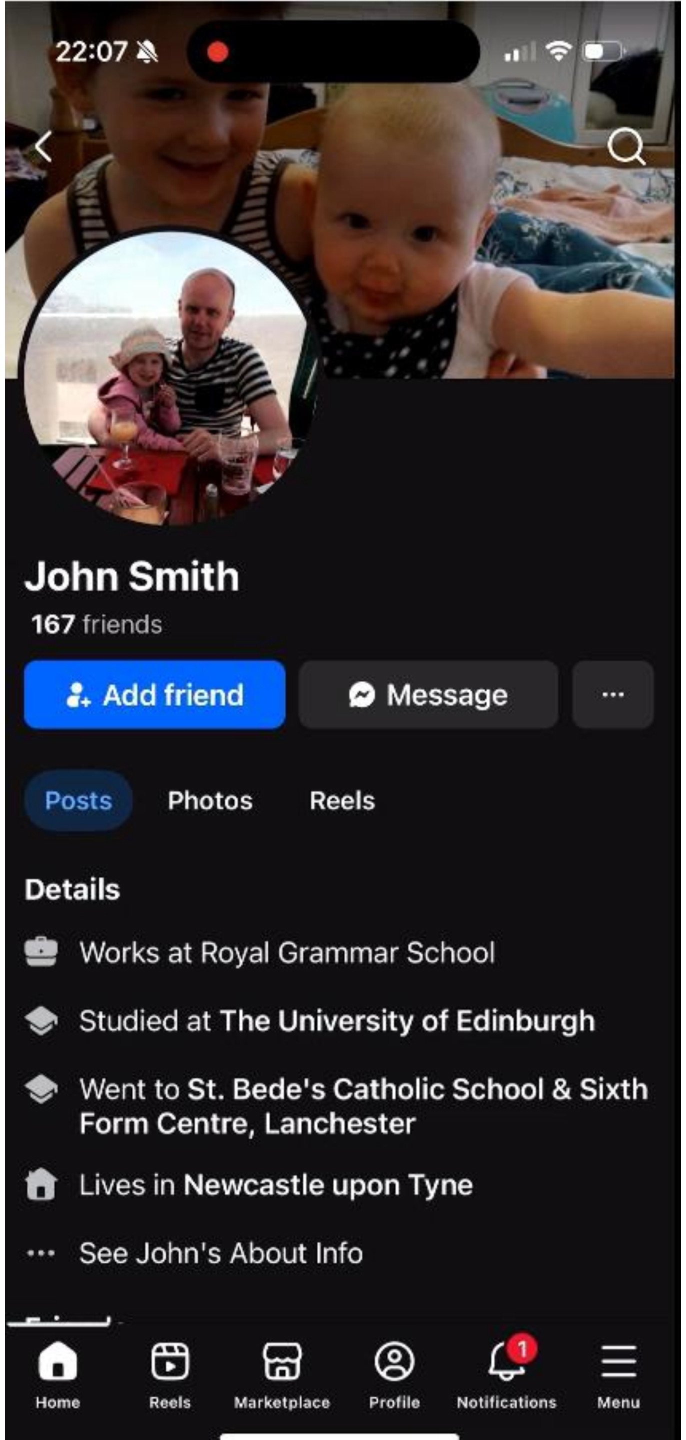
STAFF USE OF SOCIAL MEDIA

No personal social media links or contact details with pupils or parents.

Use only school approved communications.

No secret or inappropriate relationships with pupils of parents.

Avoid posting content that compromises professional standards or school reputation.



John Smith

167 friends

Details

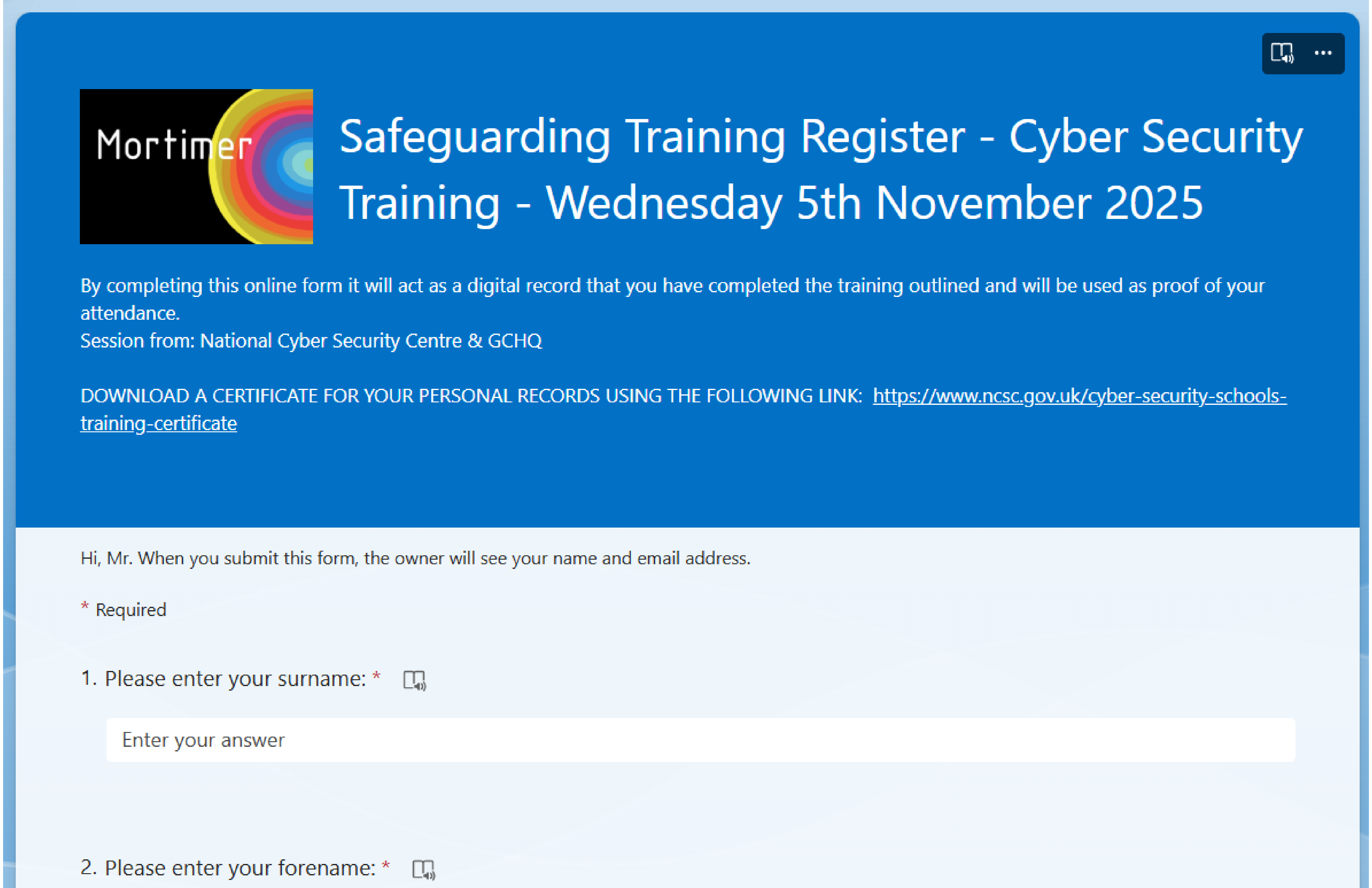
Works at Royal Grammar School

Studied at **The University of Edinburgh**

Went to **St. Bede's Catholic School & Sixth Form Centre, Lanchester**

Lives in **Newcastle upon Tyne**

See John's About Info



Safeguarding Training Register - Cyber Security Training - Wednesday 5th November 2025

By completing this online form it will act as a digital record that you have completed the training outlined and will be used as proof of your attendance.
Session from: National Cyber Security Centre & GCHQ

DOWNLOAD A CERTIFICATE FOR YOUR PERSONAL RECORDS USING THE FOLLOWING LINK: https://www.ncsc.gov.uk/cyber-security-schools-training-certificate

Hi, Mr. When you submit this form, the owner will see your name and email address.

* Required

1. Please enter your surname: *

Enter your answer

2. Please enter your forename: *

National Cyber
Security Centre
a part of GCHQ

Thank you

To download your cyber security training certificate please click on this link:
https://www.ncsc.gov.uk/cyber-security-schools-training-certificate

For other useful school cyber security resources please visit:
https://www.ncsc.gov.uk/cyber-security-schools