



National Cyber  
Security Centre

a part of GCHQ



Mortimer

# Cyber Security Training For School Staff



# Cyber Security



National Cyber  
Security Centre  
a part of GCHQ



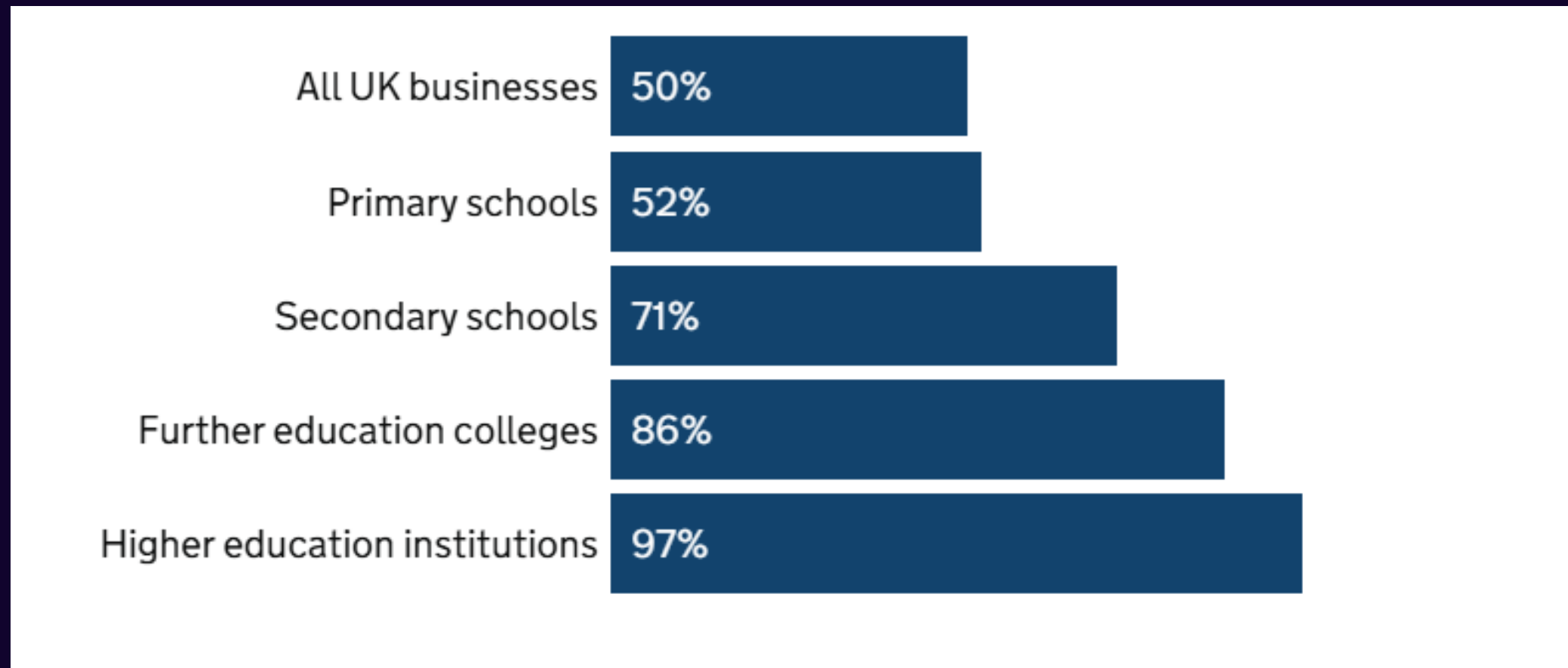
**The government have said that all schools need to meet the cyber security standard.**

**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**

# Percentage of organisations that have identified breaches or attacks in the last 12 months.





# Types of attack

Type of Attack	Primary	Secondary
Phishing	84%	86%
Others impersonating the organisation	23%	42%
Viruses, spyware, or malware	10%	16%
Unauthorised access of files or networks by students	6%	15%
Unauthorised access of files or networks by staff	2%	15%
Hacking or attempted hacking of online bank accounts	5%	4%
Ransomware	5%	3%
Denial of service attack	3%	8%

**Phishing** is generally  
the first stage in  
many cyber attacks

**89%** of schools have  
experienced a  
**phishing** attacks

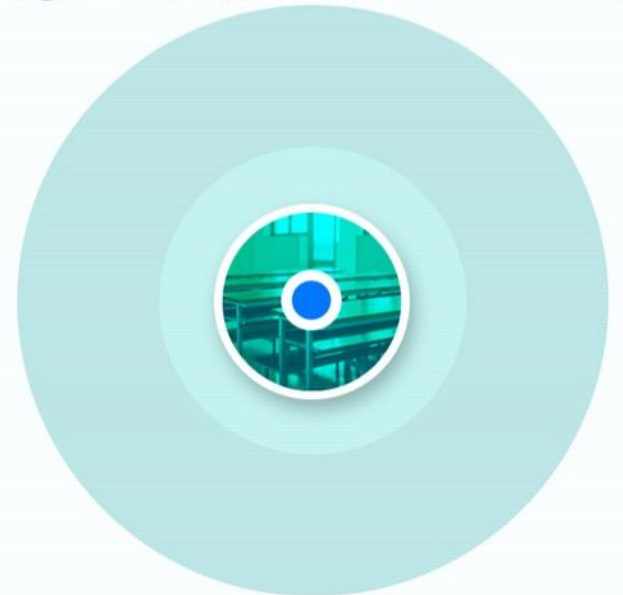
# Who is behind cyber attacks?

- 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



The image features a person in the foreground, seen from the side, working on a laptop. The background is a blurred office environment with other people. A teal overlay covers the entire image, and a white network diagram with nodes and connecting lines is visible in the lower half. The text "Online criminals" is prominently displayed in the center.

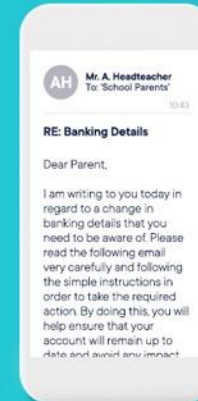
# Online criminals

## Case Study – Fraud and ransomware

# 'Payment fraud' and ransomware attacks in schools



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



Please click on the reference link below and enter your login information on the following page to access Billing Information. Failure to update your records will result in a delay to the fulfilment of your upcoming order.

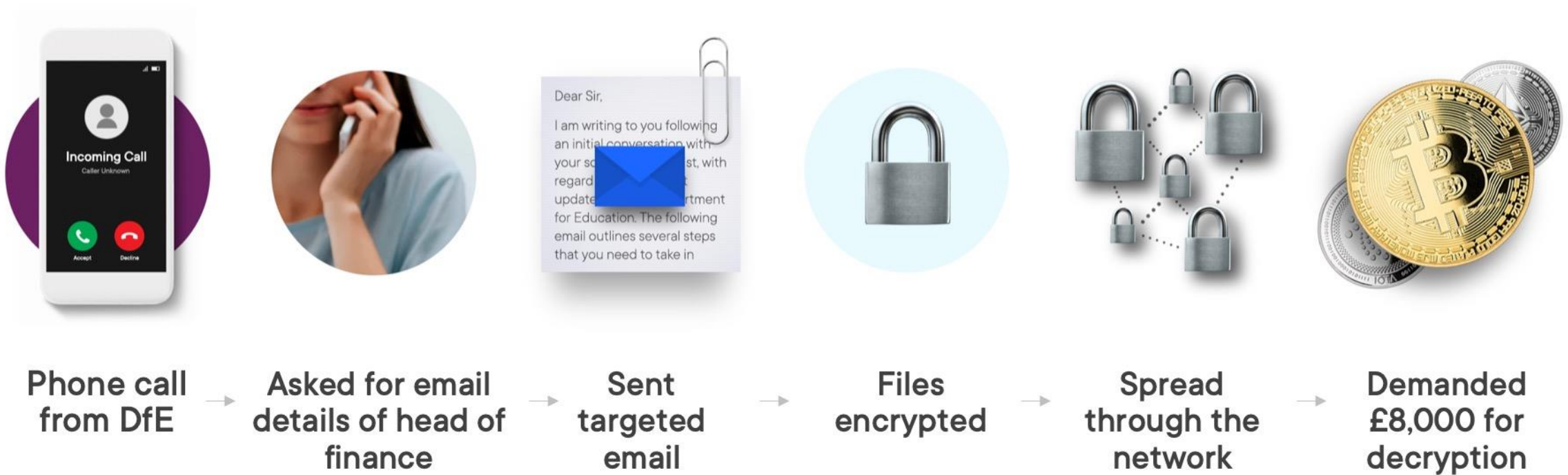






## Case Study – Ransomware

# Phone call from someone pretending to be from the DfE



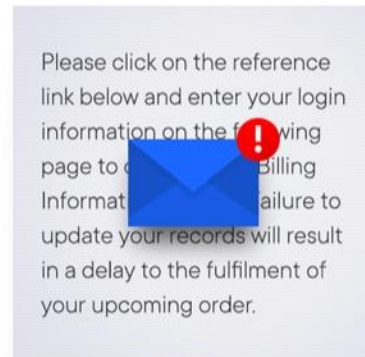


## Case Study – Fraud

# Independent school parents targeted by 'payment fraud' scam



Independent school targeted



Phishing attack led to the compromise of email



Email sent to parents informing of banking detail change



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



An aerial photograph of a dense urban landscape, likely Hong Kong, with a teal and blue color overlay. A network of white lines and dots is superimposed on the bottom half of the image, suggesting global connectivity or digital infrastructure. The text "Foreign government actors" is centered in a large, white, sans-serif font.

# Foreign government actors



The background of the image is a red double door with two small, rectangular windows on each leaf. The door is set within a wall of dark red bricks. A semi-transparent purple overlay covers the entire image. Overlaid on this purple background is a network diagram consisting of numerous small white dots connected by thin white lines, creating a web-like pattern that suggests digital connectivity or a network structure.

# **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

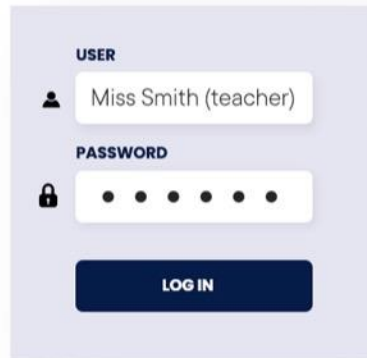






## Case Study – Password management

# School hacked by pupil Broke Data Protection Act



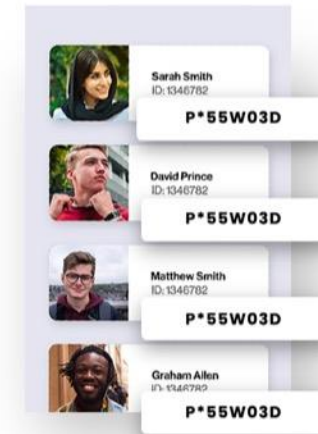
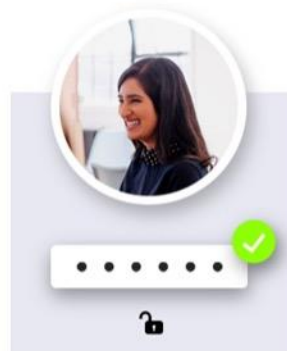
USER

Miss Smith (teacher)

PASSWORD

• • • • •

LOG IN



Accessed  
school MIS



Used teacher's  
password



20,000 records  
involved



Duplicate  
passwords used



Disciplined  
by ICO

A close-up photograph of a person's hands typing on a laptop keyboard. The person is wearing a black leather wristband with silver studs on their left wrist. The background is blurred, showing a laptop screen with some text and a mouse being used with the right hand. A semi-transparent purple and blue network overlay with white nodes and lines is visible across the bottom and right sides of the image.

# 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



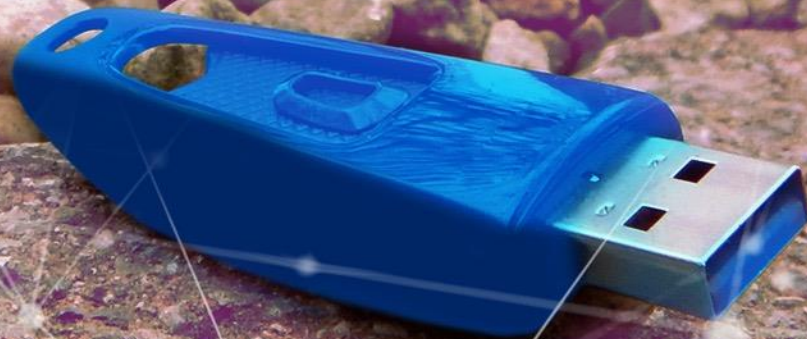
Access to CCTV systems



Wiped everything when caught



# Accidental cyber incidents



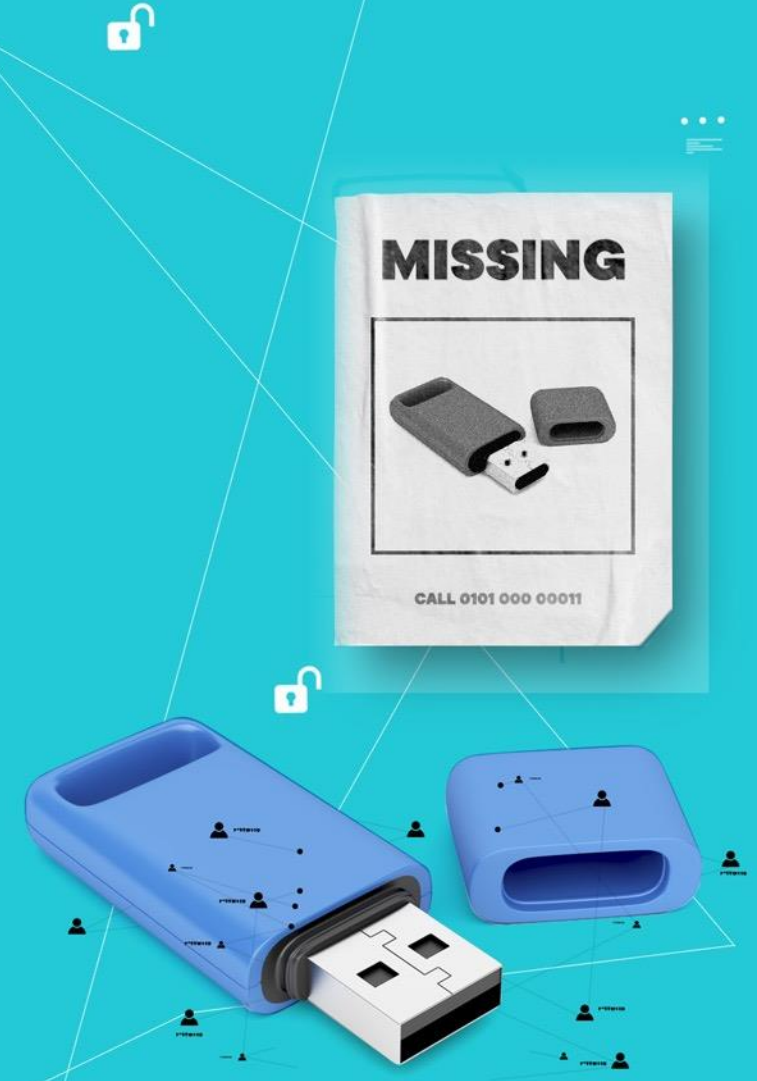


## Case Study – Secure storage

# School USB stick loss exposes pupil data



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

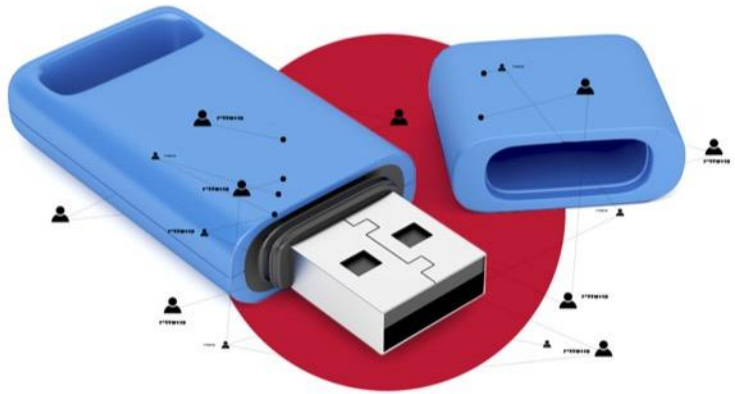






Case Study – Secure storage

# School USB stick loss exposes pupil data



Unencrypted USB  
stick with thousands  
of pupils details



Removed from  
school and lost



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](https://www.ncsc.gov.uk/glossary)





# Phishing example

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



[admin@m1cr0s0ftlogin.org](mailto:admin@m1cr0s0ftlogin.org)



Weds 05/02/2020 16:16

To: [businessmanager@theacademy.sch.uk](mailto: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](http://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!



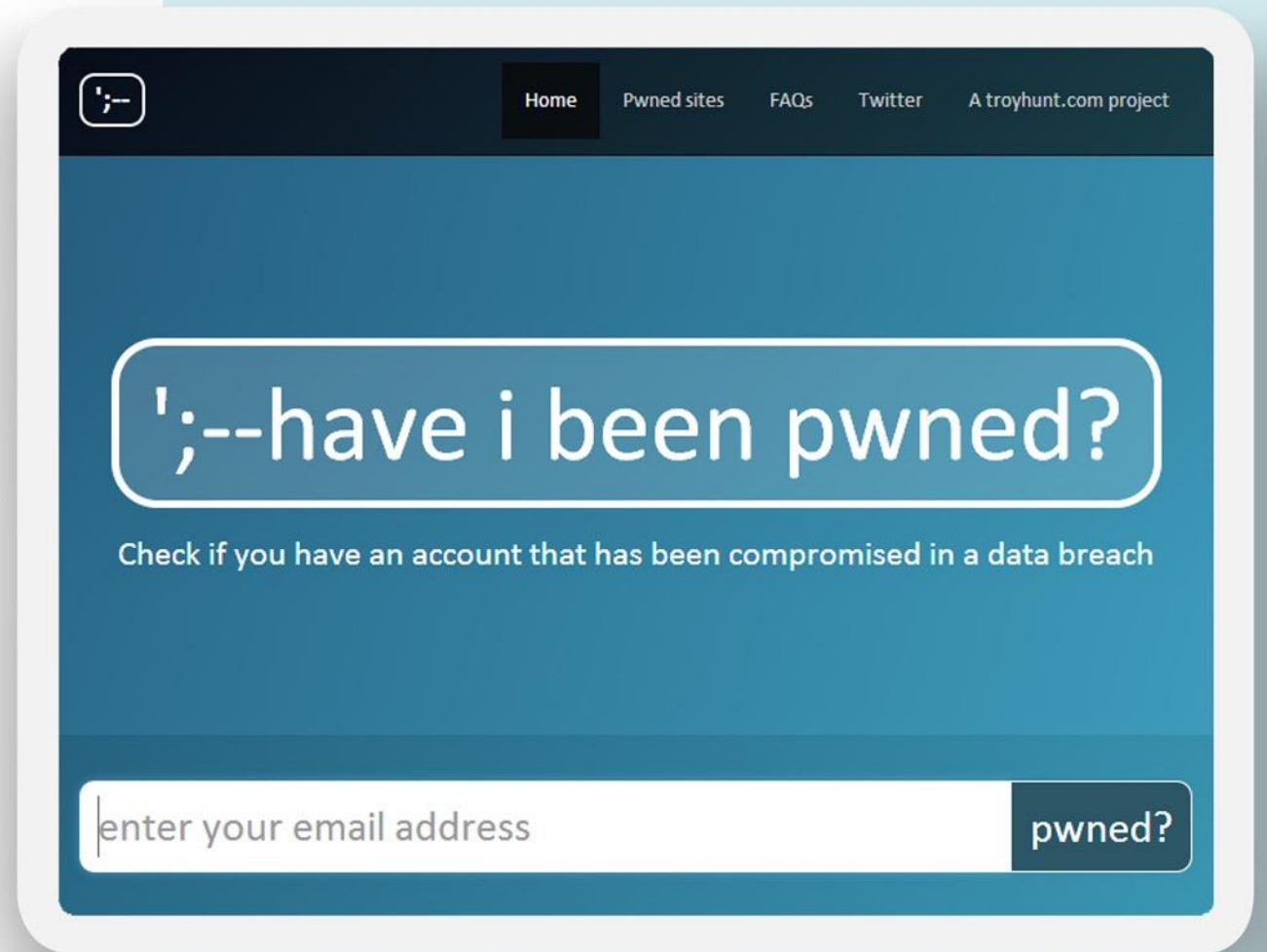
## 2. Use strong passwords





## 2. Using strong passwords

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



[www.haveibeenpwned.com](https://www.haveibeenpwned.com)

## 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.



# Safeguarding Training Register - Cyber Security Training - Wednesday 6th November 2024


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

\* Required

1. Please enter your surname: \* 

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>