Lancashire County Council

# Digital Security Guide

# Digital Security Guide

Lancashire County Council often faces security threats that could disrupt our services and compromise our data.

Each month we receive over 1,400 attempts via email. Keeping our data safe is a top priority, and it is everyone's responsibility to protect our systems.

Cyber-attacks can target any organisation. Nationally, there has been an increase in scams and phishing emails targeting sensitive information. Lancashire County Council has also seen a rise in such attempts.

We continually improve our digital security measures, but we need all employees to stay vigilant. To help with this, we regularly send test emails to teach staff how to identify phishing attempts. This is followed up with additional training for anyone who fails the test.

By staying alert and informed, we can protect our organisation from cyber threats and ensure the safety of our data.

## Tips for staying safe online

Watch this video to find out how to stay safe online:
https://www.youtube.com/watch?v=J9r_PqAHMuQ

and follow these tips:

- Your inbox is a gateway to our systems and data.
- When you get an email, stop and think before you click.
- Watch out for these phishing keywords: Urgent, Request, Important, Payment, Attention – they're designed to catch you off guard!
- Be cautious of emails with links or attachments - they are cyber-attackers most powerful weapons.
- Hover over links to check them before you click.
- Stay extra vigilant when working from home.
- Never share your password with anyone and avoid using the same password for all of your online accounts.
- Only approve your 2-factor authentication request if you're the one trying to login.
- Always lock your screen (ctrl+alt+del when you are away from your desk).

If you receive an unexpected email from an unknown source asking for personal details, to visit a website, or open an attachment, report it.

# How to report an issue

If you receive anything suspicious, please:

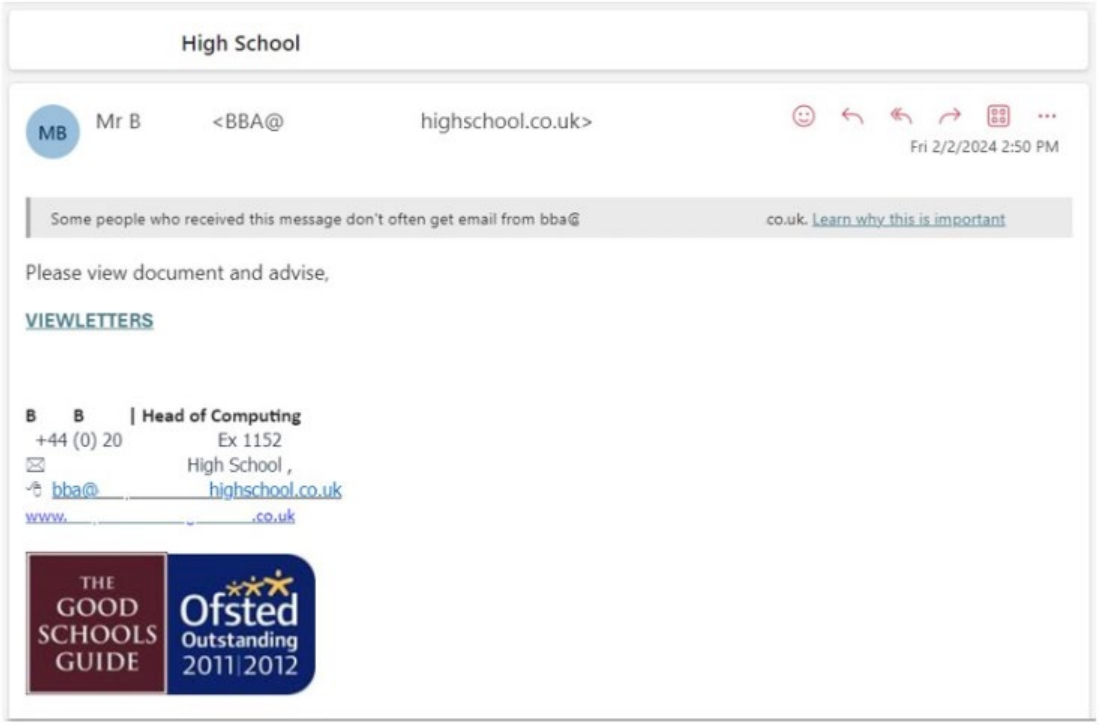
- **Use the "Report Message" button** in the top right corner of the email. This will alert Digital Services.
- Log an incident with Digital Services to report multiple SPAM emails.

If you suspect any security issues, threats or incidents with our systems, please report immediately using the Information Security Incident Reporting form.

For further guidance on what to do if you suspect a suspicious email, see

- Knowledge item KB0019521 - Email Hygiene Service - customer information (quarantined/spam emails)

# Example phishing email




**Hints that this is not a genuine email**

- no initial 'hello' greeting with receiver's name
- an alert to say that you don't normally receive mail from this sender
- poor formatting
- incorrect spellings
- hidden letters in link text
- no context as to why you are receiving the email

# Impact of cyber-attacks

All employees have a responsibility to protect our systems and data.

There are legal consequences for organisations that fail to ensure that appropriate technical and organisational measures are in place to protect data being handled.

## Recent action

The Information Commissioners Office has taken enforcement action against a number of organisations:

In July 2024, the Electoral Commission was reprimanded for a cyber-attack that occurred between August 2021 and October 2022. This breach allowed a threat actor to access personal data of approximately 40 million individuals.

Also in July 2024, the London Borough of Hackney were reprimanded following a cyber-attack that led to hackers encrypting 440,000 files, affecting 280,000 residents and staff.

# Training

## Awareness training

All employees are required to complete the mandatory Information Governance eLearning which includes a module on cyber security to help you identify potential phishing attacks.

The Information Governance course can be found on the MeLearning system.

This training will equip you with the knowledge and skills to identify and prevent potential threats and should be completed by everyone on an annual basis.

## Phishing tests

We continually improve our digital security measures, but we need all employees to stay vigilant. One of the measures we use to help staff remain vigilant is to carry out regular test emails to help staff learn how to spot phishing emails.

If you are requested to do any additional training as a result of failing a phishing test, please ensure you complete this. These regular tests and the associated training will help us all stay alert and prevent successful phishing attempts.

# Useful resources

## Further guidance from Digital Services

- Knowledge item KB0019521 - Email Hygiene Service - customer information (quarantined/spam emails)
- Knowledge item KB0019266 - What to do with a phishing email or unexpected email which you suspect is fraudulent

## Digital Champions

Our Digital Champions will have practical knowledge of using technology to support their services and the digital skills and aptitude to offer help to their colleagues. To find out who your digital champion is, speak to your line manager, or email Internal Communications.

## Further information

If you need further information for how to protect your systems and data, or want to access the Information Governance policies, please contact informationgovernance@lancashire.gov.uk.