

The first hour

Speed matters more than certainty. It is always better to raise it and be wrong.

DO THIS FIRST

1 Disconnect, do not switch off

Unplug the network cable or turn off the Wi-Fi on the affected device. Leave it powered on, because switching it off destroys evidence.

2 Tell someone now

Use the list below. Do it even if you are not sure yet. Nobody is in trouble for raising something early.

3 Write down what happened

What was clicked or sent, roughly what time, and what appeared on screen. Memory fades fast and this is what everyone will ask for.

4 Change the password from a clean device

Use a different computer or phone, change the password on the affected account, and sign out of all sessions.

5 If money has moved, ring the bank

Immediately, and ask them to attempt a recall. The first hour is when a payment can still be stopped.

DO NOT

- ✗ Delete the email, file or messages. They are the evidence.
- ✗ Wipe or factory reset the machine before someone has looked at it.
- ✗ Reply to the sender, or click anything else in the message.
- ✗ Pay a ransom before taking advice.
- ✗ Post about it publicly until you know what actually happened.

WHO TO CALL

Fill these in now, while nothing is wrong.

First point of contact here

IT support

Bank fraud line

Cyber insurance, and policy number

REPORTING IT

- **Action Fraud** England, Wales and NI. 0300 123 2040, actionfraud.police.uk
- **ICO** Within 72 hours if personal data is at risk. 0303 123 1113, ico.org.uk