Edition Two

Stop! Think Fraud.

The Big Con

Data Breach

A data breach happens when information held by a company or organisation is accessed or stolen without permission.

Recent reports involving Manchester Airport Group highlighted how a breach can expose personal information such as email addresses, phone numbers, home addresses and purchase history. Criminals can use this information to make scams more convincing and targeted.

What should you do?

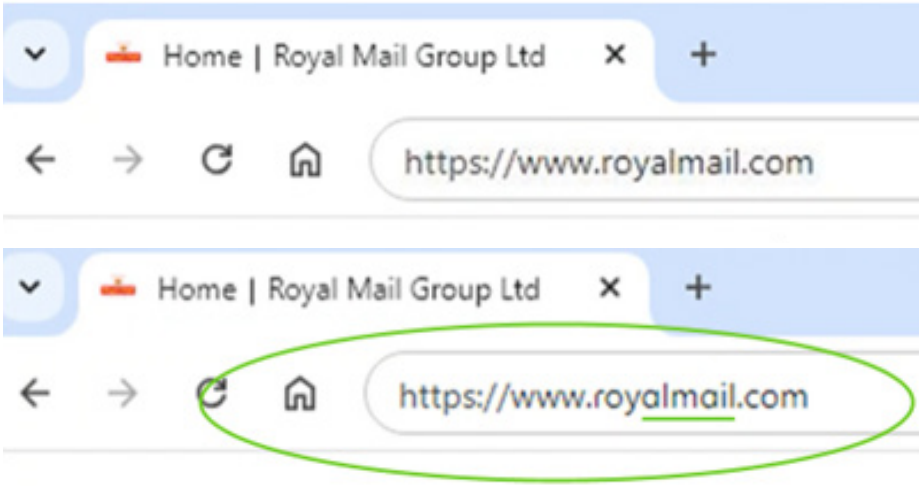
- Report stolen documents, including passports, bank cards and driving licences.
- Check bank statements and direct debits for unusual activity.
- Review your credit report for unfamiliar accounts.
- Use strong passwords and enable multi-factor authentication.

Stay alert

- Be cautious of unexpected emails, texts and phone calls.
- Verify requests using a trusted contact method.
- Avoid clicking links in unsolicited messages.
- If someone is pressuring you to act urgently, share information or send money, it could be a scam.

For more information about data breaches and your rights, visit the Information Commissioner's Office (ICO). **https:/ico.org.uk**

Spot the scam - The answer



If you remember our Spot the Scam challenge from Edition One, here's the answer - Visual spoofing.

This example uses a technique called visual spoofing, where criminals replace or combine letters with similar-looking characters (for example, using 'rn' instead of 'm' to create web addresses that appear legitimate at first glance.

Genuine: royalmail.com *(Aptos font)*

Fake: royalmail.com *(Berlin Sans FB font)*

By switching between uppercase and lowercase letters, criminals can create web addresses that look almost identical to genuine websites. In the fake address, the lowercase "**L**" has been replaced with a capital "**i**", making it look almost identical to the genuine website.

Without seeing both addresses side by side, it would be extremely difficult to spot the difference.

The page also uses Royal Mail's name and logo to appear legitimate, a common tactic used to impersonate trusted organisations. If entered, your personal or payment details could be stolen.

Remember: A convincing website can still be a scam. Always check the web address carefully before sharing any information.

Did you know?

Have I Been Pwned is a FREE website where you can check if your email address or passwords have been exposed in a data breach and sign up for alerts about future breaches: **https://haveibeenpwned.com**

Send your story for a future issue: TheBigCon@derbyshire.police.uk

Case study: **When my identity was stolen**

Written by our fraud officer, using details from the many victims she has helped. If you suspect identity fraud, contact Report Fraud: **www.reportfraud.police.uk** or **call 0300 123 2040**

It started with a phone call from someone claiming to be my mobile phone provider, offering me an upgrade. They knew my name, address and phone details, so I had no reason to suspect anything was wrong.

As part of the upgrade, I was asked to confirm personal information, including my date of birth and bank details. Everything appeared genuine, and I agreed to the new contract.

When my new phone arrived, I realised I had been sent the wrong handset. After calling the number provided, I was given an address to return it to and assured a replacement would arrive within two working days. However, the following day another phone arrived, along with two smartwatches I had never ordered. It was at this point that alarm bells started ringing.

When I contacted my mobile phone provider directly, I discovered I had been the victim of identity fraud. Criminals had used my details to obtain phones, smart devices, open credit accounts and even apply for a personal loan.

Two years later, the victim is still dealing with the consequences, receiving fraud-related calls and credit file alerts.

Red flags

- Unexpected contact offering an upgrade or deal.
- Requests for personal or banking information.
- Being asked to return items to an unverified address.
- Receiving products or account notifications you did not authorise.



Myth vs Fact

Myth: You can spot a scam because it looks fake or has poor grammar.

Fact: Modern scams are highly convincing. Criminals use stolen branding, personal information and professional - looking emails, texts and websites to mimic trusted organisations, often with perfect spelling and grammar. Always verify requests before responding.

The takeaway

The scam worked because it was personal, appeared genuine, and a phone was delivered. This helped build trust, lowering suspicion, making the fraud seem legitimate.

Remember:

Someone knowing your personal details doesn't make them genuine. Always verify unexpected contact.

Stop! Think Fraud.

Thank You

Thank you for the fantastic feedback on The Big Con. If we help protect even one person from becoming a victim of fraud, then the newsletter has done its job. A special thank you to everyone who has shared their stories and scam updates. Your contributions help us keep Derbyshire residents informed and protected.

Editor's note: This newsletter has been written by officers and staff from Derbyshire Constabulary to highlight the signs of fraud and how to protect against it. This inbox is not monitored 24/7, so please do not report crime to this email.

If you've got any feedback, or stories you'd like to be included in future editions please email TheBigCon@derbyshire.police.uk.