Data breaches

Protecting yourself from the impact of data breaches

National Cyber Security Centre
a part of GCHQ

This guidance explains what data breaches are, how they can affect individuals and families, and what you should look out for following a data breach.

What is a data breach, and how might it affect you?

A data breach occurs when information held by an organisation is stolen or accessed without authorisation.

Criminals use this information within scam emails and text messages, so that they appear legitimate. They may even send emails pretending to be from an organisation that has suffered a recent data breach, asking you to log in and confirm your identity because 'fraudulent activity has taken place', or similar.

These scam messages will typically contain links to websites that look genuine, but which store your real details once you've typed them in. Or these websites could install viruses onto your computer, or steal any passwords you enter.

If the information stolen during the breach includes phone numbers, you might receive a suspicious call. The approach may be more direct, asking you for banking details or passwords, or for access to your computer.

Reporting suspicious messages

If you receive a message or call about a security breach that doesn't feel right, here's what to do:

- if you've received a suspicious email, forward it to the NCSC's Suspicious Email Reporting Service at **report@phishing.gov.uk**
- if you've received a suspicious text message, forward it to 7726(a free service for reporting spam)
- if you've received nuisance, suspicious or unwanted calls, hang up and contact your phone provider
- if you have been a victim of a sextortion scam, then report it to your local police force by calling 101

Actions you should take following a data breach

If an organisation experiences a data breach and they have your personal data.

1. Find out if you've been affected by contacting the organisation directly by checking their official website or social media accounts. They should be able to confirm:
- if a breach actually occurred
- how you're affected
- what else you need to do

2. Be alert to suspicious messages which may follow a breach. Your bank (or any other official organisation) will never ask for personal information by email, so look out for:
- official-sounding emails about 'resetting passwords',
- 'receiving compensation' or 'confirming identity'
- emails full of 'tech speak'
- being urged to act immediately

3. If you receive a message that includes a password you've used in the past, don't panic:
- if you still use the password, change it as soon as you can
- if any of your other accounts use the same password, you should change them as well

4. Check your online accounts to see if there's been unusual activity. Things to look out for include:
- being unable to log into accounts
- changes to your settings
- messages or notifications from your accounts that you don't recognise

5. If you suspect an account of yours has been accessed, refer to the NCSC guidance on recovering a hacked account.

6. To check if your details have appeared in public data breaches, you can use online tools such as haveibeenpwned.com. Similar services are often included in antivirus or password manager tools that you may already be using.

If you've lost money

If you've lost money, tell your bank and report it as a crime to Action Fraud (actionfraud.police.uk), the UK's reporting centre for cyber crime (in Scotland, contact the police by dialling 101).

You'll be helping the NCSC and law enforcement to reduce criminal activity, and in the process, prevent others from becoming victims.