Data breaches: guidance for individuals and families

How to protect yourself from the impact of data breaches

As more aspects of our lives move online, data breaches are a fact of modern life. This guidance explains what data breaches are, how they can affect you, and what you should look out for following a data breach.

> **Note**
>
> If you think you've already responded to a scam message following a breach, read our guidance on dealing with suspicious messages.

What is a data breach?

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

Criminals can then use this information when creating phishing messages (such as emails and texts) so that they appear legitimate. The message has been designed to make it sound like you're being individually targeted, when in reality the criminals are sending out millions of these scam messages. Criminals may even send messages pretending to be from an organisation that has suffered a recent data breach.

Even if your details are not stolen in the data breach, the criminals will exploit high profile breaches (whilst they are still fresh in people's minds) to try and trick people into clicking on scam messages.

How might you be affected?

In a typical scam, you might receive a message claiming to be from an organisation that has suffered a recent data breach. The message could ask you to log in and verify your account 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.

Like many phishing scams, these scam messages are hard to spot, and are preying on real-world concerns (in this case, a data breach) to try and trick you into clicking.

And it's not just emails or texts. 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 sensitive information (such as banking details or passwords), or access to your computer.

Actions to take following a breach

If you're a customer of an organisation that has suffered a data breach you should take the following actions.

1. Find out if you've been affected by contacting the organisation using their **official** website or social media channels. Don't use the links or contact details in any messages you have been sent. The organisation should be able to confirm:

- if a breach actually occurred
- how you're affected
- what else you need to do

You can also phone the organisation directly, but be aware that many won’t have the capacity to respond to all calls during a major breach.

2. Be alert to suspicious messages (we've published guidance that can help you with this), which may be sent some time **after** the breach is made public. Remember, your bank (or any other official organisation) will never ask you to supply personal information. Things to look out for include:

- official-sounding messages about 'resetting passwords', 'receiving compensation', 'scanning devices' or 'missed deliveries'
- emails full of 'tech speak', designed to sound more convincing
- being urged to act immediately or within a limited timeframe

3. If you receive a suspicious message that includes a password you've used in the past, don't panic:

- if this is a password that you still use, you should change it as soon as you can
- if any of your other accounts use the same password, you should change them as well
- for advice on creating strong passwords, visit www.cyberaware.gov.uk

4. Check your online accounts to confirm there's been no unauthorised activity. Things to look out for include:

- being unable to log into your accounts
- changes to your security settings
- messages or notifications sent from your account that you don't recognise
- logins or attempted logins from strange locations or at unusual times

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 any other public data breaches, there are a number of online tools that you can use, such as https://haveibeenpwned.com. Similar services are often included in antivirus or password manager tools that you may already be using.

Reporting suspicious messages

If you receive a message or phone 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)
- 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**

If you've lost money

If you've lost money, tell your bank and report it as a crime to Action Fraud, the UK's reporting centre for cyber crime (in Scotland, contact the police by dialing 101). You'll be helping the NCSC and law enforcement to reduce criminal activity, and in the process, prevent others from becoming victims.

Further information

If you've received nuisance, suspicious or unwanted **calls**, please refer to this guidance from Ofcom (the regulator for UK communications services).

PUBLISHED

28 January 2021

REVIEWED

28 January 2021

VERSION

1.0

WRITTEN FOR

Individuals & families