POLICE
SCOTLAND
Keeping people safe
POILEAS ALBA

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. 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.

Social media is a fantastic tool for keeping up with friends and family however, it can be exploited by criminals therefore please be careful what you put online. Please refer to the NCSC guide on how to use Social Media safely to setup privacy settings and manage your digital footprint.

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.

Actions to take following a data 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.
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. The National Cyber Security Centre (NCSC) publishes guidance on how to spot suspicious communications and what to do if you're worried you have fallen victim to a phishing attack.
3. If you receive a suspicious message that includes a password you've used in the past you should change it as soon as you can.
4. Check your online accounts to confirm there's been no unauthorised activity.
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.

Refer to the NCSC's guidance on data breaches if you have any concerns.

Useful links and advice

- **Take Five** – Advice to help prevent email, phone based and online fraud particularly where criminals impersonate trusted organisations.
  https://takefive-stopfraud.org.uk/

- **Police Scotland** – Internet Safety advice on a range of different online topics including romance fraud, sextortion, social media, internet dating, cybercrime, online shopping and keeping safe online.
  https://www.scotland.police.uk/advice-and-information/internet-safety/

- **Cyber Aware –** Cyber Aware is the government's advice on how to stay secure online.
  www.cyberaware.gov.uk

- **Cyber Action Plan Tool:** NCSC have launched the free of use Cyber Action Plan tool for individuals and small business to receive advice on improving their cyber security in an increasingly digital world. https://www.ncsc.gov.uk/cyberaware/actionplan

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** which spells SPAM on your phone keypad.
- If you've received nuisance, suspicious or unwanted **calls**, hang up and contact your phone provider for further advice on how to stop nuisance calls.
- If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

This alert was sent out for your information by Police Scotland
Cybercrime Harm Prevention Unit - PPCWCyberHarmPrevention@scotland.pnn.police.uk
All information was correct at time of distribution. 06/04/2021