Cyber Byte

September 2023

Data Breach – what should you do?

A data breach occurs when information held by an organisation is stolen or accessed without authorisation. Criminals can, using this information, create scam emails and text messages making them appear legitimate, even pretending to be from an organisation that has suffered a data breach. Their scam messages may even ask you to log in and confirm your identity because 'fraudulent activity has taken place'. They want their messaging to be as convincing as possible to trick you.

Actions to take following a data breach.

Find out if you've been affected - contact 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.

Be alert to suspicious messages following 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 • Being urged to act to confirm identity • Emails full of technical jargon.

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, change it there as well.

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 which you don't recognise.

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

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

Information stolen during a data breach often includes phone numbers so, if you are a victim of a data breach, you might receive a suspicious call commonly known as Vishing. The approach in this instance may be more direct where the criminal will ask you for banking details or passwords, or for access to your computer.

Reporting suspicious messages

If you receive a message (including SMS messages or nuisance calls) about a security breach that don't feel right, here's what to do if you have received;

• A suspicious email - forward it to the NCSC's Suspicious Email Reporting Service at report@phishing.gov.uk

• A suspicious text message - forward it to 7726 (a free service for reporting spam)

• A nuisance - suspicious or unwanted calls, hang up and contact your phone provider.

If you have been a victim of a sextortion scam Sextortion emails: how to protect yourself - NCSC.GOV.UK report this to your local police force by calling 101.

Information from Police Scotland Cybercrime Harm Prevention Team
PPCWCyberHarmPrevention@scotland.police.uk
All information correct at time of distribution. 01/09/2023