POLICE SCOTLAND
POILEAS ALBA

Data Breach Guidance

Personal Information

Police Scotland Cybercrime Harm Prevention Team
04.03.2025

What if my information has been stolen in a data breach?

A data breach occurs when information held by an organisation is stolen or accessed without authorisation. *NCSC guidance explains what data breaches are, how they can affect you, and what you should look out for following a data breach.*

Criminals can then use this data when creating phishing messages (such as emails and texts) so that they appear legitimate. If you think you've already responded to a scam message, please read NCSC guidance on dealing with suspicious messages.

What if my username and password have been stolen?

Personal credentials, such as usernames and passwords, can be stolen by criminals using tactics such as phishing emails. They can also be stolen by hackers from the online services you use, if these services suffer a data breach.

If you suspect either has happened you should change your password as soon as possible. If you have used the same password on any other accounts, you should change it there also.

Services such as www.haveibeenpwned.com can tell you if your information has ever been made public in a major data breach, and even alert you if it happens in the future.

I'm worried my banking details may be stolen

Contact your bank or building society and speak to their fraud department. Your bank will not ask you to reply to an e-mail with personal information, or details about your account. If you contact them, use a phone number/email address you have found yourself, rather than one sent to you in the email – it may be false. You can check your credit reference file online. You should follow up on any unexpected or suspicious results.

For more guidance on protecting yourself from cyber-enabled fraud, please visit Take Five.

What signs should I look for?

There are a number of signs to look out for that may mean you are or may become a victim of identity theft:

- Mail from your bank or utility provider doesn't arrive.
- Items that you don't recognise appear on your bank or credit card statement.
- You apply for state benefits, but are told you are already claiming.
- You receive bills or receipts for goods or services you haven't ordered.
- You are refused financial services, credit cards or a loan, despite having a good credit rating.
- You receive letters in your name from solicitors or debt collectors for debts that aren't yours.

What can I do if I am the victim of identity theft?

If you think you are a victim of identity theft or fraud, act quickly to ensure you are not liable for any financial losses.

Report all lost or stolen documents, such as passports, driving licences, credit cards and cheque books to the organisation that issued them.

Inform your bank, building society and credit card company of any unusual transactions on your accounts.

Request a copy of your credit file to check for any suspicious credit applications. This can be accessed online from a variety of providers.

Contact CIFAS (the UK's Fraud Prevention Service) to apply for protective registration. Once you have registered you should be aware that CIFAS members will carry out extra checks to see when anyone, including you, applies for a financial service, such as a loan, using your address.

CIFAS – The UK's Fraud Prevention Service
www.cifas.org.uk

Call 101 for advice and support (or call 999 in an emergency)
Police Scotland

If in England, Northern Ireland or Wales, you can report to Action Fraud Contact us | Action Fraud / Adroddiad yn gymraeg | Action Fraud

Recovering a hacked account

Whether it's your email, social media or some other type of online service, there are many things which can alert you to the fact that someone else is accessing your account.

Being locked out of the account is an obvious indication that something has gone wrong, but the signs can be more subtle. Things to look out for include logins or attempted logins from strange locations or at unusual times. Changes to your security settings and messages sent from your account that you don't recognise are also give aways.

However you discover the problem, once you know your account has been hacked, this is what you should do;

1. Update the software apps on your devices.
2. Check your email settings
3. Use the service support page
4. Change passwords on relevant accounts
5. Protect your accounts using 2-Step Verification (2SV)
6. Notify your friends followers and contacts
7. If you can’t recover your account, create a new one
8. Report online crime to Police Scotland on 101

Useful Links

Recovering a hacked account - NCSC.GOV.UK

Individuals & families - NCSC.GOV.UK

Self employed & sole traders - NCSC.GOV.UK

Small Charity Guide - NCSC.GOV.UK

Cyberaware

NCSC Data Breaches Infographic

10 Steps to Cyber Security - NCSC.GOV.UK

Cyber Essentials - Iasme

Stay protected online with a Cyber Action Plan - NCSC.GOV.UK

Check Your Cyber Security (ncsc.gov.uk)

Top tips for staff - Overview (ncsc.gov.uk)