7 steps to take after your personal data is compromised online

If you have been made aware that your personal data has been breached there are a few steps to take that will help prevent fraud:

1. **Report it**

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

You should also inform your bank, building society and credit card company of any unusual transactions on your statement.

2. **Change your passwords.**

It is no longer advised to keep changing your password on a regular basis, instead NCSC advice use Three Random Words to develop a strong password.

However, it is important to change your passwords after a data breach to something strong, secure, and unique, ideally using the Three Random Words guidance.

Another tip is to use password manger, such as 1Password, which incorporate monitoring services and that will help avoid falling victim to scams, as the service will alert you if you try to enter your password on a fake website.

3. **Sign up for two-factor authentication**

In addition to changing your passwords, sign up for two-factor authentication (also known as “2FA" or “two-step verification") wherever possible. This is an added layer of security for your account logins, and many services such as Gmail and Facebook now offer it. With two-factor authentication, your online account will require you to enter an additional level of identification to access your account – such as a code texted to your phone. This means that even if hackers get your email and password, they cannot get into your account without that second factor of identity verification.

4. **Check for updates from the company.**

If your data is involved in a major data breach, the company will likely post ongoing updates and disclosures about which customers were affected. For example, after a recent Facebook data breach, the company automatically logged out the users whose accounts were affected and sent them messages via the platform about what had happened and what to do next.

5. **Watch your accounts, check your credit reports**

After a data breach, it is essential to be vigilant and pay extra attention to your account activity – that includes your account at the company that suffered the breach, as well as your bank account and other financial accounts. Read your bank or credit card statements and

watch for suspicious transactions. Also, sign up for your free annual credit report from Equifax and Experian.

6. Consider identity theft protection services

If you want additional peace of mind, you can consider signing up for identity theft protection services. These are paid for service, that emulate free services such as credit checks, however they provide an automated one stop service that may be appealing to some colleagues.

Often when there is a significant data breach, the company involved will give affected customers a free year of credit monitoring.

7. Freeze your credit

Another step you can take, whether you are affected by a data breach or not, is to ask for Credit Freeze. This is a free service from Experian and Equifax where your credit file will be placed on hold to prevent fraudsters claiming your identity.

Freezing your credit should not be done lightly, as this adds additional checks when credit is being taken out in your name. Hence, credit freezing can impact your ability to make legitimate applications for loans and mortgages and mobile phone contracts for example.

Steps to take if have concerns about your personal security

General Advice

1. Change your passwords.

It is no longer advised to keep changing your password on a regular basis, instead NCSC advice use Three Random Words to develop a strong password. However, it is important to change your passwords after a data breach using the Three Random Words guidance.

Another tip is to use password manger, such as 1Password or LastPass which incorporate monitoring services and that will help avoid falling victim to scams, as the service will alert you if you try to enter your password on a fake website.

2. Sign up for two-factor authentication.

Sign up for two-factor authentication (also known as “2FA" or “two-step verification") wherever possible. This is an added layer of security for your account logins, and many services such as Gmail and Facebook now offer it as standard. With two-factor authentication, your online account will require you to enter an additional level of identification to access your account – such as a code texted to your phone. This means that even if hackers get your email and password, they cannot get into your account without that second factor of identity verification.

3. Secure your internet traffic.

Using a virtual private network (VPN), is not necessary for everyone, but can offer greater privacy online if you believe your details have been breached. If you frequently connect to public Wi-Fi, a VPN is useful because it adds a layer of security to your browsing. It can also provide some privacy from your Internet service provider and help minimise tracking based on your IP address. But all your Internet activity still flows through the VPN provider’s servers, so use a well-known VPN provider like Guardian or NordVPN.

4. Privacy settings on your social media should

It is recommended that you routinely check the privacy and security settings in your social media and online accounts. Most organisations provide easy to use settings to restrict the visibility of your profile. Privacy settings should generally be set to the highest possible level. If you at particular risk, you may wish to restrict your social media usage altogether, or limit contact to friends only.

5. Opt out of the Electoral Roll

The electoral register (sometimes called the ‘electoral roll’) lists the names and addresses of everyone who is registered to vote. This is an open register which means your name and address can be searched by anyone. You can ‘opt out’ of the register by following the online guidance here https://www.gov.uk/electoral-register/opt-out-of-the-open-register

6. Block nuisance calls

Your telephone provider will be able to advise on the best protections against nuisance callers, however, most include optional caller ID services to screen calls and block unknown numbers. You can also register your number with the Telephone Preference Service (tpsonline.org.uk) and install truecall.co.uk to help screen calls on your mobile device.

Higher-Risk Individuals

If you believe you are at significant risk from an organised criminal gang or hostile/fixated individual(s), you must report your concerns to the Police immediately. They will be able to advise on appropriate measures, such as:

Home Security

- At home, your security can be enhanced based on the assessment of risk. Some measures may include the installation of 3rd party Monitored Alarms, where an alarm notification will result in emergency responders being alerted. Added delay measures could also be considered, such as the installation of Security Rated Doors and glazing, which will make it harder for attackers to enter your property.

On the Move

- Making your travel patterns unpredictable is the best way protect yourself against hostile reconnaissance. Sophisticated reconnaissance teams will be very hard to spot, but you can make the job harder by taking different routes wherever possible. The Police may also provide additional measures such as tailing your vehicle occasionally to deter criminals.

Children and Spouses

- The Police will also be able to advise on the best precautions for your loved ones. This may include alerting your child's educational setting or partner's workplace to the risks and advising them on proper security protocols.

In addition to the police response, high risk individuals may wish to consider:

Land Registry

If you own your home your Title Deeds will be stored in Land Register for England and Wales or the Register of Scotland depending on where you live. Both registers are open and accessible to anyone for a small fee, hence, it possible to track an individual address.

Neither HM Land Registry nor Register of Scotland offer a closed register service, hence you should seek legal advice about the best way to obscure your details on these registers.

Device security

If you believe you are likely to be the target of organised criminal gangs or foreign intelligence services, it is advised that you use hardware authentication devices such as YubiKey which are supported by Apple and Android. The use of hardware authentication removes the ability to by-pass 'soft' tokens such as those sent as text messages or digital code generators, which can be vulnerable if your sim card is cloned, or phone is stolen.

Apple and Android devices also provide a Lockdown Mode, which is an optional protection designed for the most sophisticated digital threats. The mode will make your devices less susceptible to highly targeted mercenary spyware. However, certain apps, websites and device features will be strictly limited for security.

If you suspect your device has been hacked, performing a hard restart can neutralise most hacks, although a factor reset and restore from the last known secure back-up is the best course of action.