Securing Your Digital Life

Think Your Personal Data Has Been Compromised?

Here's What to Do…

Cyber-attacks in the retail sector have been dominating the news just lately with M&S and The Co-Op constantly in the headlines. In today's digital world, data breaches and cyber-attacks are becoming increasingly common. Whether it's a phishing scam, a hacked account, or a leaked database, discovering that your personal information may have been exposed can be worrying.

Recent events may have raised some concerns with you as to whether your data may have been compromised or whether there's more you can do to further protect yourself.

There are a number of simple things you can do to check your own digital life:

Step 1: Confirm the Breach

Before taking action, try to verify whether your data has actually been compromised:

- **Check for official notifications** from companies or services you use.
- Use tools like Have I Been Pwned to see if your email or phone number appears in known data breaches.
- Look for unusual activity on your accounts (e.g. login attempts, password reset emails, or unfamiliar transactions).

Step 2: Change Your Passwords Immediately

If you suspect any account has been compromised:

- **Change the password right away**—especially if you have reused it elsewhere and if you have, make a real effort **not to reuse** passwords and make it as difficult as possible for cyber criminals to get what they want!
- Use **strong, unique passwords** for each account check the National Cyber Security Centre advice to use 3 random words.

- Enable **Multi-Factor Authentication (MFA)** wherever possible to add an extra layer of security.

Step 3: Secure Your Devices

- Run a **full antivirus or anti-malware scan** on your phone, tablet, or computer **at home.** At work, these are scheduled regularly – please allow these updates to take place and if for whatever reason that's not possible, ensure that you update as soon as you're able to ensure that your device remains protected.
- Make sure your operating system and apps are **fully updated**.
- Remove any suspicious apps or apps that you no longer use or need.

Step 4: Monitor Your Accounts and Credit

- Keep a close eye on your **bank accounts, credit cards, and online services** for unusual activity.
    - **DO NOT** click on any links in emails or Text messages.
    - **DO NOT** call the telephone number provided in the email or text
- Consider setting up **transaction alerts** with your bank.
- In the UK, you can check your credit report for free with agencies like **Experian** or **Equifax**.
- If needed, place a **fraud alert** or **credit freeze** to prevent new accounts being opened in your name.

Step 5: Report It

Depending on the nature of the breach:

- Report phishing emails or suspicious messages to:
    - Home: **report@phishing.gov.uk**.
- If money has been stolen, report it to your bank and **Action Fraud** (the UK's national reporting centre for fraud and cybercrime).
    - **Report** lost/stolen cards as soon as possible to your provider.
- If your identity has been stolen, contact **Cifas** for protective registration.

Step 6: Learn and Strengthen

- **DO NOT** use your work email address for personal matters.
- **DO NOT** use your home address for work related matters.
- Review your **digital footprint** and remove old or unused accounts.
- Be cautious about what personal information you share online.
- Stay informed about the latest cyber threats and scams.

Final Thought

Discovering that your personal data may have been compromised is unsettling—but acting quickly and calmly can make a big difference. By taking the right steps, you can reduce the risk of further harm and regain control of your digital life.