



HAVE YOUR DETAILS BEEN EXPOSED?

Follow Authlogics simple 5 step guide to recovering from a data breach



STEP 1: FOCUS AND DOUBLE CHECK

Having your details exposed can be alarming and it is important to stay calm. When a company alerts of a data breach, it is crucial you check which of your details have been compromised – personal? passwords? financial? Talk to those that have raised the alarm to find out more.



STEP 2: ACT IMMEDIATELY

Change the password of the affected account immediately to mitigate any risks of further cybersecurity incidents. Protect your digital identity and learn how to identify scams like BEC (Business Email Compromise), Account Takeover and Phishing Attacks.



STEP 3: SECURE EVERYTHING

If you have used the same password for multiple accounts, these will need to be changed. With people having so many online accounts nowadays to manage, it is easy (and the lazy way) to set the same password across all. Make sure that your email, bank, work and social media passwords are different.



STEP 4: ALERT THE AUTHORITIES

Monitor bank accounts to ensure there is no unusual activity and alert your bank of the incident to keep them informed. If you use the same passwords for both personal and business accounts, your workplace is now vulnerable to a cyberattack. Advise your IT support team of the incident and request to change your work password.



STEP 5: TALK TO THE EXPERTS

Authlogics are experts in identifying data breaches within organisations. We witness many cybersecurity incidents through the management of our Password Breach Database which holds over 4 billion compromised credentials.

Find out how Authlogics is helping businesses manage existing password problems and offering passwordless and deviceless authentication solutions.



[Learn More](#)

Authlogics