

This is an beta website by [Inclusive Bytes CIC](#), The aim is to create one location for digital resources in Oldham.



- [Home](#)
- [Events](#)
- [Tutorials](#)
- [Resources](#)
- [Hubs](#)

How to check if your email has been leaked in a data breach.



A Simple Guide to Using “Have I Been Pwned” to Check if Your Data Has Been Breached

What is “Have I Been Pwned”?

“Have I Been Pwned” (HIBP) is a free and trusted website that helps you find out if your **email address** or **password** has been exposed in a data breach.

A **data breach** happens when hackers break into websites and steal user information, such as email addresses, passwords, and other personal data.

□ Step 1: Visit the Website

Go to <https://haveibeenpwned.com>.

- You can access the site on a computer, tablet, or smartphone.
- The website is safe and easy to use.

□ Step 2: Enter Your Email Address

In the search bar on the homepage, type the **email address** you want to check.

- Example: myemail@example.com

Then click the **“pwned?”** button.

□ Step 3: Understand Your Results

□ Green Screen = Good News!

If you see a green message that says **“Good news – no pwnage found!”**, your email address has not been found in any known data breaches.

□ Red Screen = Uh-Oh!

If you see a red message that says **“Oh no – pwned!”**, your email address has been found in one or more data breaches.

Don't panic! This doesn't necessarily mean someone has access to your account right now, but it does mean your information was exposed in the past.

□ Step 4: View the Details

Scroll down to see:

- **Which websites were breached**

- **What types of data were exposed** (such as passwords, names, or addresses)
 - **The date of the breach**
-

□ **Step 5: Protect Yourself**

If your email was found in a breach:

- 1□□ **Change your password immediately** for any affected accounts.
 - 2□□ Use **unique passwords** for different websites. A **password manager** can help you create and remember strong passwords.
 - 3□□ Enable **two-factor authentication (2FA)** where possible for extra protection.
 - 4□□ Watch out for **phishing emails or scams** that might target you after a breach. (Tutorials are available for this.)
-

□ **Step 6: Sign Up for Alerts (Optional)**

Click **“Notify Me”** at the top of the page to receive **free alerts** if your email address appears in future data breaches.

□ **Extra Tip: Check Your Passwords**

HIBP also has a **“Password” tool** where you can check if a password has been exposed in a breach.

△□ **Important:** Never enter a password you currently use. This tool is only for testing old or weak passwords.

□ Frequently Asked Questions

Is “Have I Been Pwned” safe?

Yes! The site is trusted by cybersecurity experts worldwide and was created by security expert **Troy Hunt**.

Does the website save my email or password?

No. Your information is not stored or shared when you search.

What should I do if I’m unsure what to do next?

Ask a trusted friend, family member, or IT support for help.

□ Final Thoughts

Regularly checking “**Have I Been Pwned**” is a simple and powerful way to protect your online accounts. By staying informed and updating your passwords, you can reduce the risk of identity theft and hacking.

Made with the help and support of [Inclusive Bytes CIC](#)

[Training](#) | [Reporting](#)