**🔐 Have I Been Pwned? (HIBP)**

**Level:** Beginner  
**Category:** OSINT / Account Safety / Data Breaches

**🧠 What Is "Have I Been Pwned"?**

**HIBP** is a **free online service** that tells you if your **email, phone number, or password** has been exposed in a **data breach**.

* Website: 🌐 [https://haveibeenpwned.com](https://haveibeenpwned.com/)
* Created by cybersecurity expert **Troy Hunt**

**❓ What is a Data Breach?**

A **data breach** is when a website or company is hacked, and user data is stolen. This may include:

* Email addresses
* Passwords
* Phone numbers
* Credit card info
* Location, birthdate, etc.

If a website you used got breached, **your info might be floating around on the dark web**.

**🔎 What Can You Check on HIBP?**

**✅ 1. Check Email Address**

* Go to: [https://haveibeenpwned.com](https://haveibeenpwned.com/)
* Type your email (e.g., ahmad@gmail.com)
* Click **“pwned?”**

🔴 If your email appears in red, it means it **has been found in one or more breaches.**

**✅ 2. Check Phone Number**

* Works for numbers in international format, e.g., +923001234567
* Shows if your number was leaked in any breach.

**✅ 3. Check Password (safely)**

* Go to: <https://haveibeenpwned.com/Passwords>
* Type in a password **(doesn’t get saved!)**
* It tells you how many times that password appeared in leaks.

🔒 If it says "This password has been seen 10,000 times", never use it again.

**🧩 What Is a “Pwned Website”?**

These are websites that have suffered a data breach, and whose user data is now publicly leaked or for sale.

Examples:

| **Website** | **Breach Year** | **What Was Leaked** |
| --- | --- | --- |
| LinkedIn | 2021 | Emails, passwords |
| Dropbox | 2012 | Emails, hashed passwords |
| MyFitnessPal | 2018 | Emails, usernames, passwords |
| Wattpad | 2020 | Emails, passwords, birth dates |
| Nitro PDF | 2020 | Emails, names, document titles |

You can view the full list here:  
🔗 <https://haveibeenpwned.com/PwnedWebsites>

**🔐 How to Protect Yourself**

| **Action** | **Why It Helps** |
| --- | --- |
| 🧠 Use Unique Passwords | Never reuse same password across websites |
| 🔐 Use a Password Manager | Tools like Bitwarden, 1Password, or LastPass can help |
| 🛡️ Enable 2FA | Even if your password is leaked, attacker can’t log in |
| 🔄 Change Passwords Often | Especially for old accounts |
| 📥 Use Email Aliases | Helps track who leaked your email |

**🧠 Summary**

| **Feature** | **What It Does** |
| --- | --- |
| Email/Phone Check | Finds if your data was leaked |
| Password Check | Verifies if a password has appeared in breaches |
| Pwned Websites List | Shows which companies were hacked |
| Awareness Tool | Great for personal and professional OSINT use |