Andy Graybeal CYBR-1100 Week 1 – 24, August 2025

Project 1-4: Are You a Victim?

My answers are interlaced and colored orange.

Even though all states require some type of notification sent to victims of a data breach, there are several loopholes in the requirements and not all users pay strict attention to these notification emails. In this activity, you will test your email addresses to determine if they are contained in a database of known breaches.
Caution

This website is considered highly reputable. However, other websites may actually capture your email address that you enter and then sell it to marketers as a valid email address. You should be cautious about entering your email address in a site that does not have a strong reputation.

Open a web browser and enter the URL https://haveibeenpwned.com/. (If you are no longer able to access the site through this web address, open a search engine and enter "Have I been pwned.")

Scroll down and note the Largest breaches. Also, note the total number of pwned accounts.

https://haveibeenpwned.com/ says there are 901 breached websites with 15,097,848,140 owned accounts.

Enter one of your email addresses in the box and click pwned?

If this email address has been stolen and listed in the database, you will receive a Oh no – pwned! message. If this email address has not been stolen, enter another of your email addresses.

Scroll down to Breaches you were pwned in.

I've entered in andy@knivesandchives.com. My email has been involved in two breaches. One from Advanced Auto and the other from Open Subtitles.

Read the information about the breach, and particularly note the Compromised data of each breach. Do you remember being alerted to these data breaches with a notification letter?

For any breaches that list Passwords in the Compromised data, this serves as a red flag that your password for this account was also stolen. Although the stolen password should be "scrambled" in such a way that an attacker would not be able to view it, that may not always be the case. You should stop immeditely and change your password at once for that website.
Note 17

Other information listed as compromised data, while important, may be difficult or impossible to change, such as a phone number or physical address. The most critical item that can be changed and should be changed are any passwords.

Enter another email address and looked for Compromised data that shows any exposed passwords. Change the passwords for those accounts as well.

Here is what the Advanced Auto summary says:
In June 2024, Advance Auto Parts confirmed they had suffered a data breach which was posted for sale to a popular hacking forum. Linked to unauthorised access to Snowflake cloud services, the breach exposed a large number of records related to both customers and employees. In total, 79M unique email addresses were included in the breach, alongside names, phone numbers, addresses and further data attributes related to company employees.

Here is what the Open Subtitles summary says:
In August 2021, the subtitling website Open Subtitles suffered a data breach and subsequent ransom demand. The breach exposed almost 7M subscribers' personal data including email and IP addresses, usernames, the country of the user and passwords stored as unsalted MD5 hashes.

I was using opensubtitles when this happened! It went down and eventually came back up. I had no idea at the time it was hacked.

I entered several other of my email addresses into the site, but none of them had breaches. I assume that they are too old to be recorded onto the haveibeenpwned website.

I never received any notification of these breaches from these companies.

What are your feelings now that you know about your compromised data? Does this inspire you to take even greater security protections?

My feelings about this are that I’m not surprised really. I remember when Heartland and Equifax were hacked and that was a huge deal!! Did they change their ways, we can only hope.

But yes, seeing does help reinforce my usage of secure passwords.

Close all windows.