

Project 1-3: Are You a Victim?

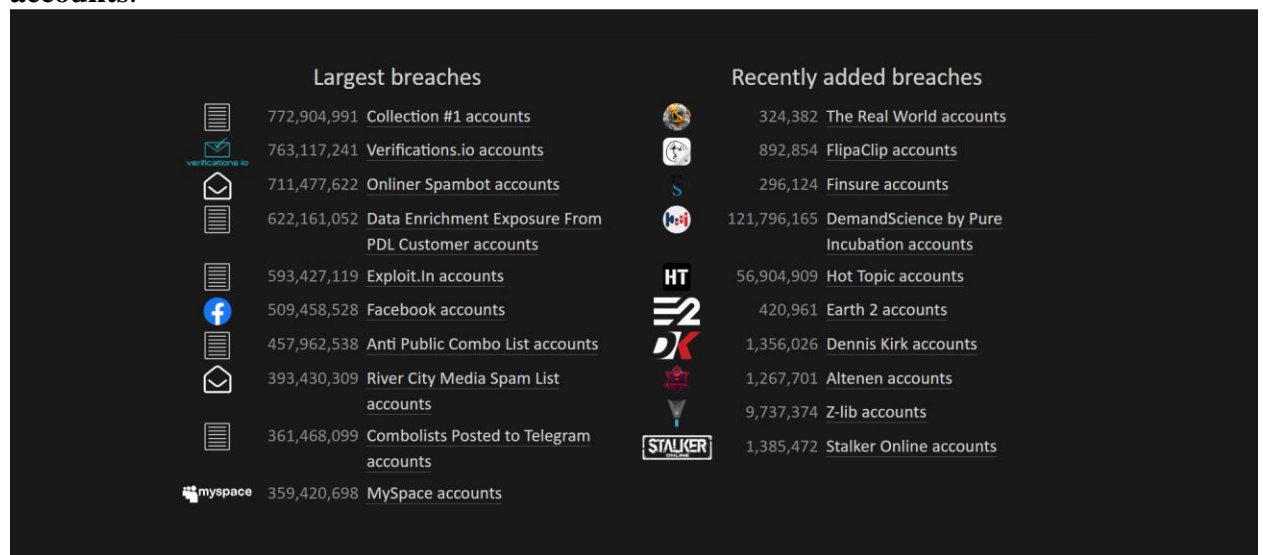
Estimated Time: 20 minutes





















Objective: Assess the personal impact of cyberattacks.

Description: 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.

1. Open a web browser and enter the URL 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”.)
2. Scroll down and note the **Largest breaches**. Also, note the total number of **pwned accounts**.



Largest breaches		Recently added breaches	
	772,904,991 Collection #1 accounts		324,382 The Real World accounts
	763,117,241 Verifications.io accounts		892,854 FlipaClip accounts
	711,477,622 Onliner Spambot accounts		296,124 Finsure accounts
	622,161,052 Data Enrichment Exposure From PDL Customer accounts		121,796,165 DemandScience by Pure Incubation accounts
	593,427,119 Exploit.In accounts		56,904,909 Hot Topic accounts
	509,458,528 Facebook accounts		420,961 Earth 2 accounts
	457,962,538 Anti Public Combo List accounts		1,356,026 Dennis Kirk accounts
	393,430,309 River City Media Spam List accounts		1,267,701 Altenen accounts
	361,468,099 Combolist Posted to Telegram accounts		9,737,374 Z-lib accounts
	359,420,698 MySpace accounts		1,385,472 Stalker Online accounts


3. Enter one of your email addresses in the box and click **pwned?**
4. 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.

jones_9315@yahoo.com **pwned?**


Oh no — pwned!

Pwned in 17 data breaches and found 1 paste (subscribe to search sensitive breaches)


3 Steps to better security [Start using 1Password.com](#)



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.




Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.

[Why 1Password?](#)


5. Scroll down to **Breaches you were pwned in**.
6. 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?
Absolutely not, some of the compromised data are still applications I have on my iPhone currently.
7. 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 immediately and change your password at once for that website.

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




MyHeritage: In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, Passwords



MyFitnessPal: In February 2018, the diet and exercise service MyFitnessPal suffered a data breach. The incident exposed 144 million unique email addresses alongside usernames, IP addresses and passwords stored as SHA-1 and bcrypt hashes (the former for earlier accounts, the latter for newer accounts). In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".

Compromised data: Email addresses, IP addresses, Passwords, Usernames



Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".

Compromised data: Email addresses, Geographic locations, Names, Passwords, Usernames

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

Discovering that my data has been compromised is very concerning, especially when considering the timeline of these breaches. It's unsettling to realize how little control we truly have over our personal information once it's entrusted to third parties. While frustrating, this experience serves as a crucial reminder of the importance of adopting stronger cybersecurity habits. This lab reminds me to avoiding weak or reused passwords, ensuring each account has a unique, strong password, and enabling multi-factor authentication whenever possible. It's a lot but necessary wake-up call to take proactive steps to safeguard my digital security.

10. Close all windows.

Criteria	Meets Requirements	Needs Improvement	Incomplete
Content	The assignment clearly and comprehensively addresses all questions in the assignment. 15 points	The assignment partially addresses some or all questions in the assignment. 8 points	The assignment does not address the questions in the assignment. 0 points
Organization and Clarity	The assignment presents ideas in a clear manner and with strong organizational structure. The assignment includes appropriate content, coverage of facts, arguments, and conclusions. 10 points	The assignment presents ideas in a mostly clear manner and with some organizational structure. The assignment includes appropriate content, coverage of facts, arguments, and conclusions. 7 points	The assignment does not present ideas in a clear manner or with a strong organizational structure. The assignment includes some appropriate content, but coverage of facts, arguments, and conclusions are not logically related and consistent. 0 points
Research	The assignment is based upon appropriate and adequate data collection and analysis of results from the activity or	The assignment is based upon adequate data collection and includes some analysis of results from the activity or	The assignment is not based upon appropriate data collection and includes no analysis of results from the

	research from academically reliable sources. 5 points	research from academically reliable sources. 3 points	activity or research from academically reliable sources. 0 points
Grammar and Spelling	The assignment has two or fewer grammatical and spelling errors. 5 points	The assignment has three to five grammatical and spelling errors. 3 points	The assignment has more than five grammatical and spelling errors, is incomplete, or is unintelligible. 0 points