# Are You a Victim?

**Estimated Time:** 30 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.

**Reflection Assignment:** In your own words, analyze and reflect on the questions and write your thoughts. One or two words is not sufficient.

1. Open a web browser and enter the URL [**haveibeenpwned.com/**](https://www.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**.
3. Enter one of your email addresses in the box and click **pwned?**
4. **Paste a screenshot:**

Click or tap here to enter text.

1. 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.
2. Scroll down to **Breaches you were pwned in**.
3. 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?
4. 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.
5. **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.
6. Enter another email address and looked for **Compromised data** that shows any exposed passwords. Change the passwords for those accounts as well.
7. What are your feelings now that you know about your compromised data? Does this inspire you to take even greater security protections? Write a minimum 100 word reflection.

Click or tap here to enter text.

1. Close all windows.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.