# Activity 1.1.3 - Have YOU Been Pwned?

**Apply the Have I Been Pwned tool to check whether an email address has appeared in any data breaches and use the information to increase online security.**

**A. Inventory** - guesstimate how many of the following types of accounts you currently have:

1. Social Media how many? ____________ Ex: Facebook, Instagram, TIkTok
2. Gaming/Networking how many? ____________ Ex: Steam, Discord, forums
3. Shopping how many? ____________ Ex: Amazon, Etsy, coupon sites
4. Entertainment how many? ____________ Ex: Netflix, Hulu, AppleTV...
5. Other how many? ____________ Ex: Hobbies, Subscriptions...

**TOTAL** ________________

6. How many email addresses do you have? ________

B. Breaches - go to the Have I Been Pwned? website https://haveibeenpwned.com/ and enter each of your email addresses to see if it has been found in any data breaches.

1. For each email address, in the space below write down the number of times it was found in a data breach. Do NOT write down the email address, just the number.

2. Once you have looked up all your email addresses, add up all the numbers. What is the total number of data breaches in which your addresses were found? _____________
3. For those breached accounts, how many were using a unique password? __________ (unique = a password that is used only for one account)

Reflection: stolen user databases include both the username - usually an email address - and the password for that account. This means that any account using the same credentials will be vulnerable to a credential stuffing account.

For example, I log into Amazon with username: bgrad202@school.edu and password: qwerty5678. Then I create an account at Discord (and lots of other sites!) using the same email address and password. If the Discord user database is breached, then a credential stuffing account would be able to access my Amazon account even though Amazon is secure and hasn't been breached.

To protect against credential stuffing attacks use a unique password for every account. This is very difficult to do manually but easy with a password manager.