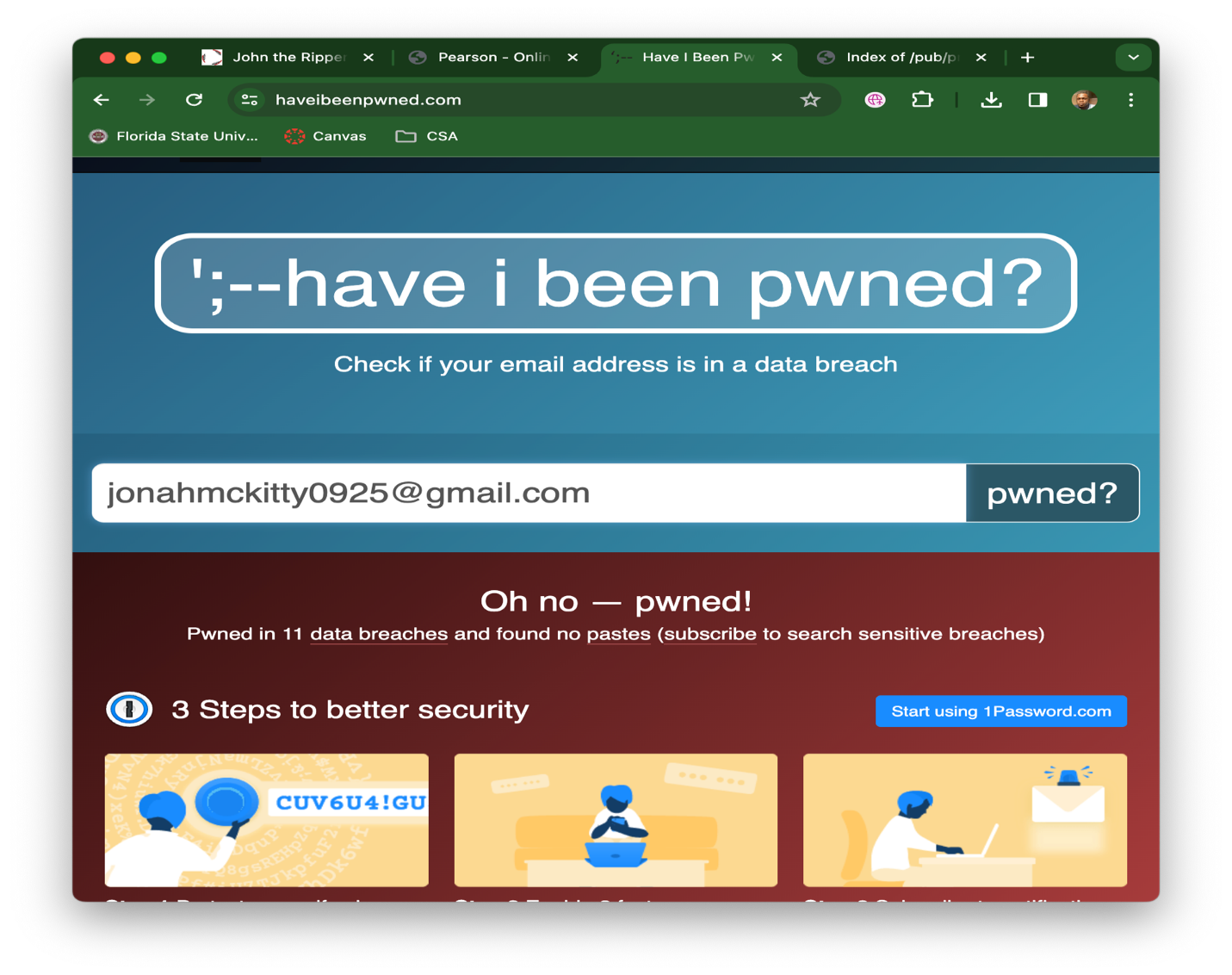


1. Time of my system

2. System running John the Ripper

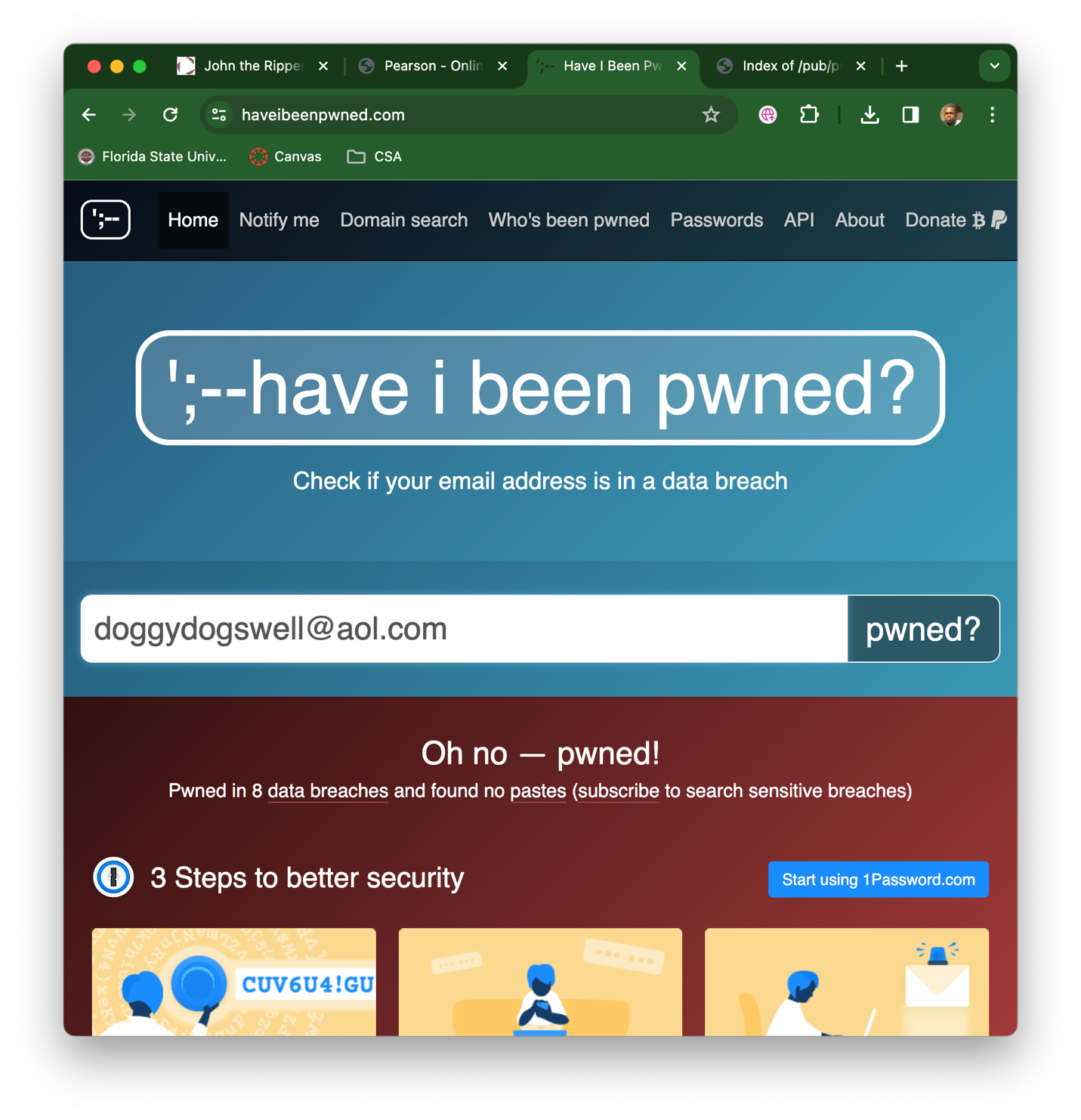
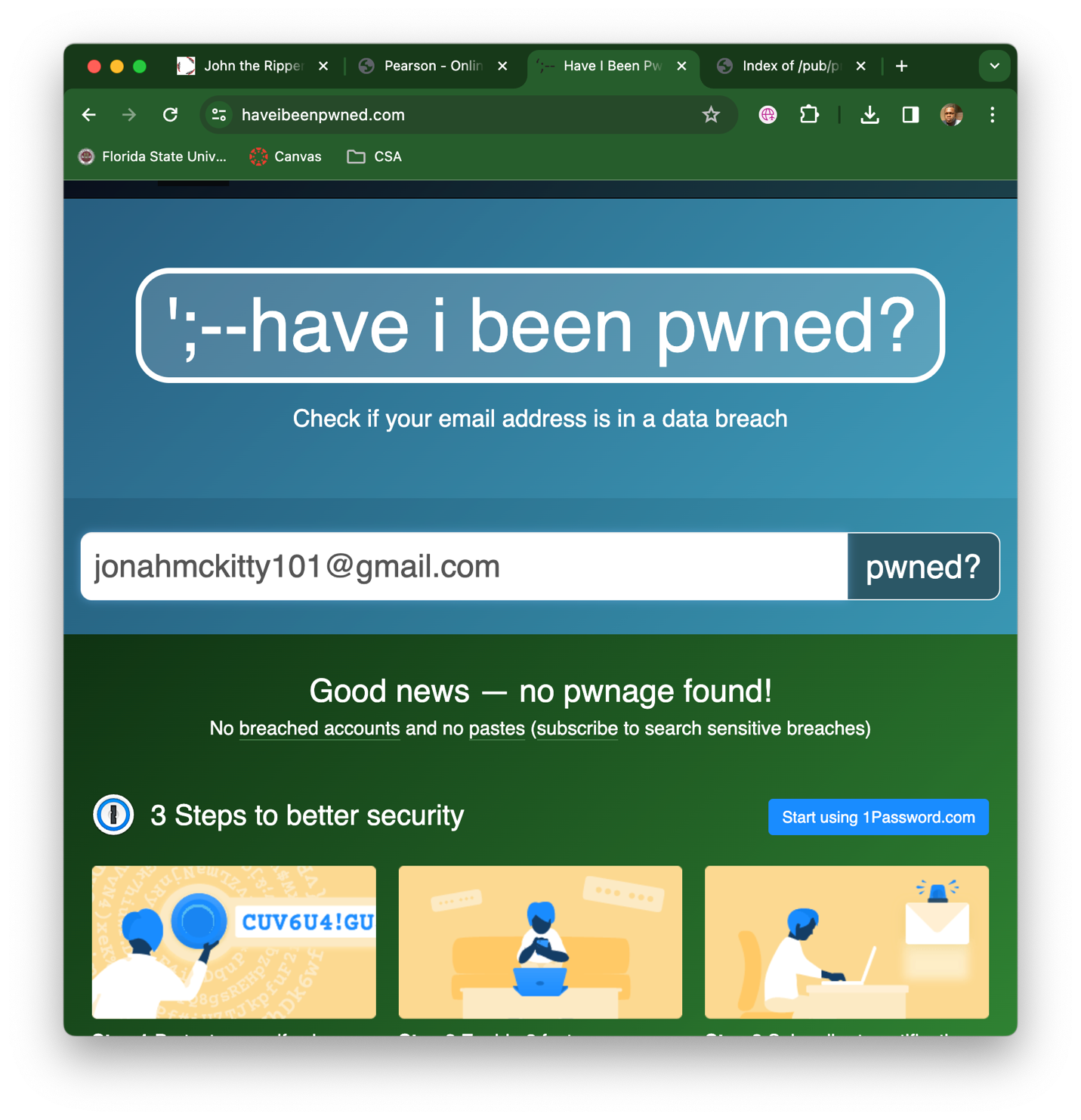
.

A screenshot of a computer

Description automatically generated

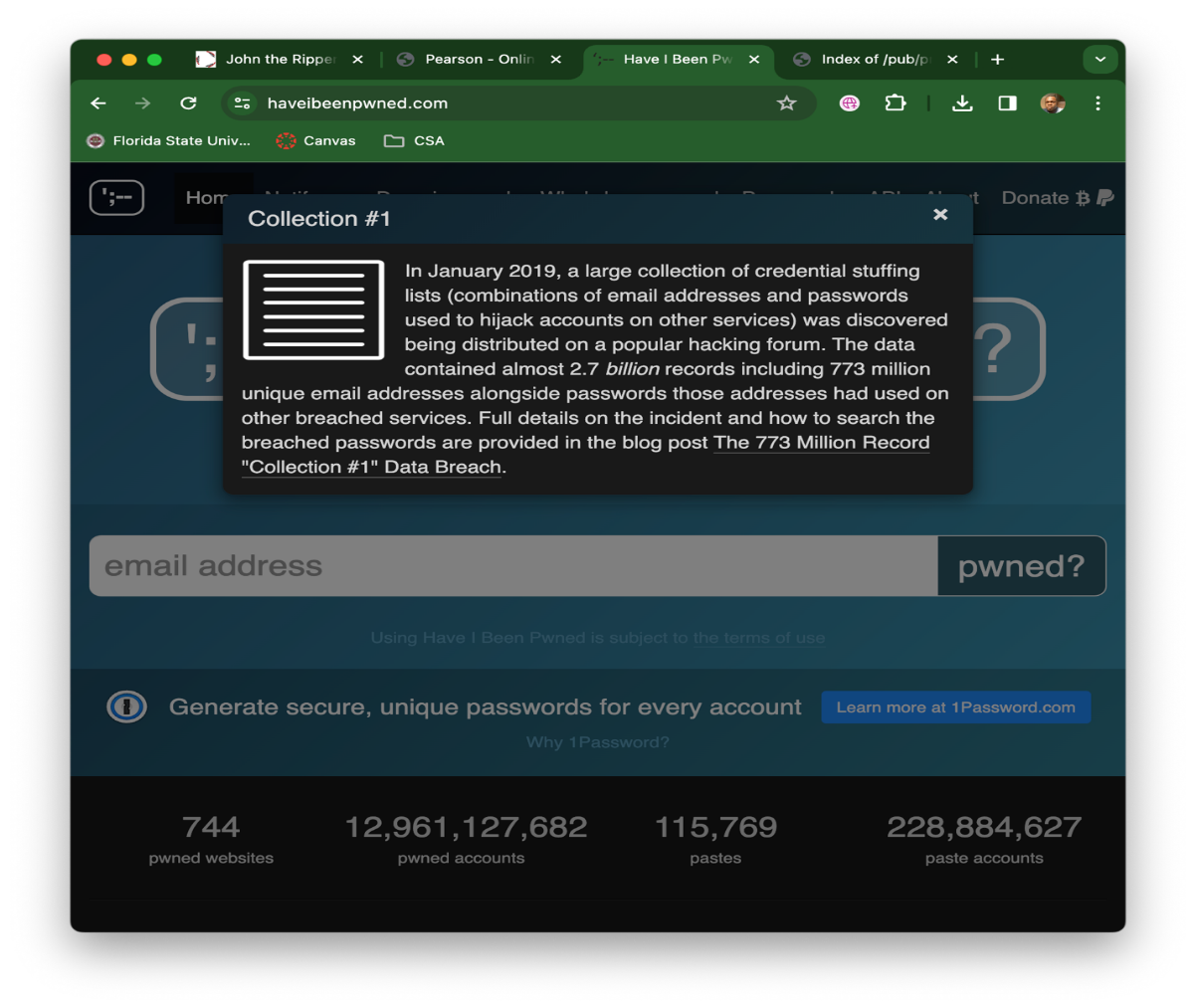
3. Passwords cracked by John the Ripper

4. Checking if my email has been pwned :(



5. Checking if an alternate email has been pwned.

6. Checking if a friends email has been pwned

A screenshot of a computer

Description automatically generated

7. Recent data breach

8. Large data breach

1. How does the cracking program actually “crack” the password?

John the Ripper, like other password cracking tools, typically uses methods like brute force attacks, dictionary attacks, or hybrid attacks to systematically try different combinations of characters until it finds the correct password.

1. If you used a larger wordlist, would it crack the passwords faster?

Yes, using a larger wordlist in a dictionary attack could increase the chances of cracking passwords, as it expands the range of possible combinations that the cracking program will try.

1. Can you use foreign language wordlists?

Yes, using foreign language wordlists can be effective in password cracking, especially if the target user might use words or phrases in a language other than the default language of the cracking tool.

1. Why do special characters (e.g., @#$%^&\*) make passwords difficult to crack?

Special characters increase the complexity of passwords by expanding the character set. This makes it harder for attackers because they have to consider a larger range of possible combinations.

1. Why does a change of case help make a stronger password?

Changing the case of letters in a password increases its complexity by introducing both uppercase and lowercase characters, making it more resistant to simple dictionary attacks and brute force attempts.

1. Were you in any data breaches? Which ones?

Yes, I was in a Wattpad, Dubsmash, Zynga and Chegg data breach to name a few.

1. Were any of your other e-mail addresses or e-mail addresses of friends listed in data breaches?

My other email address was not in any breach, my friends however was included in several breaches.

1. How could the delay in data breach notification hurt users?

A delay in data breach notification could give attackers more time to exploit stolen information, increasing the risk of identity theft, financial fraud, or other malicious activities against the affected users.

1. Why would you want to avoid using your name in your e-mail address? (i.e., Could you be identified in a data breach of an embarrassing site?)

Avoiding the use of your name in an email address can enhance privacy. It reduces the risk of being directly identified in the event of a data breach, especially on sites that some may find or considet embarrassing or sensitive.

1. Do you use the same password for multiple accounts? Why would this be a security risk?

I try not to, but there has been instances where I’ve used the same password for multiple accounts. This is a security risk because if one account is compromised, all linked accounts become vulnerable.