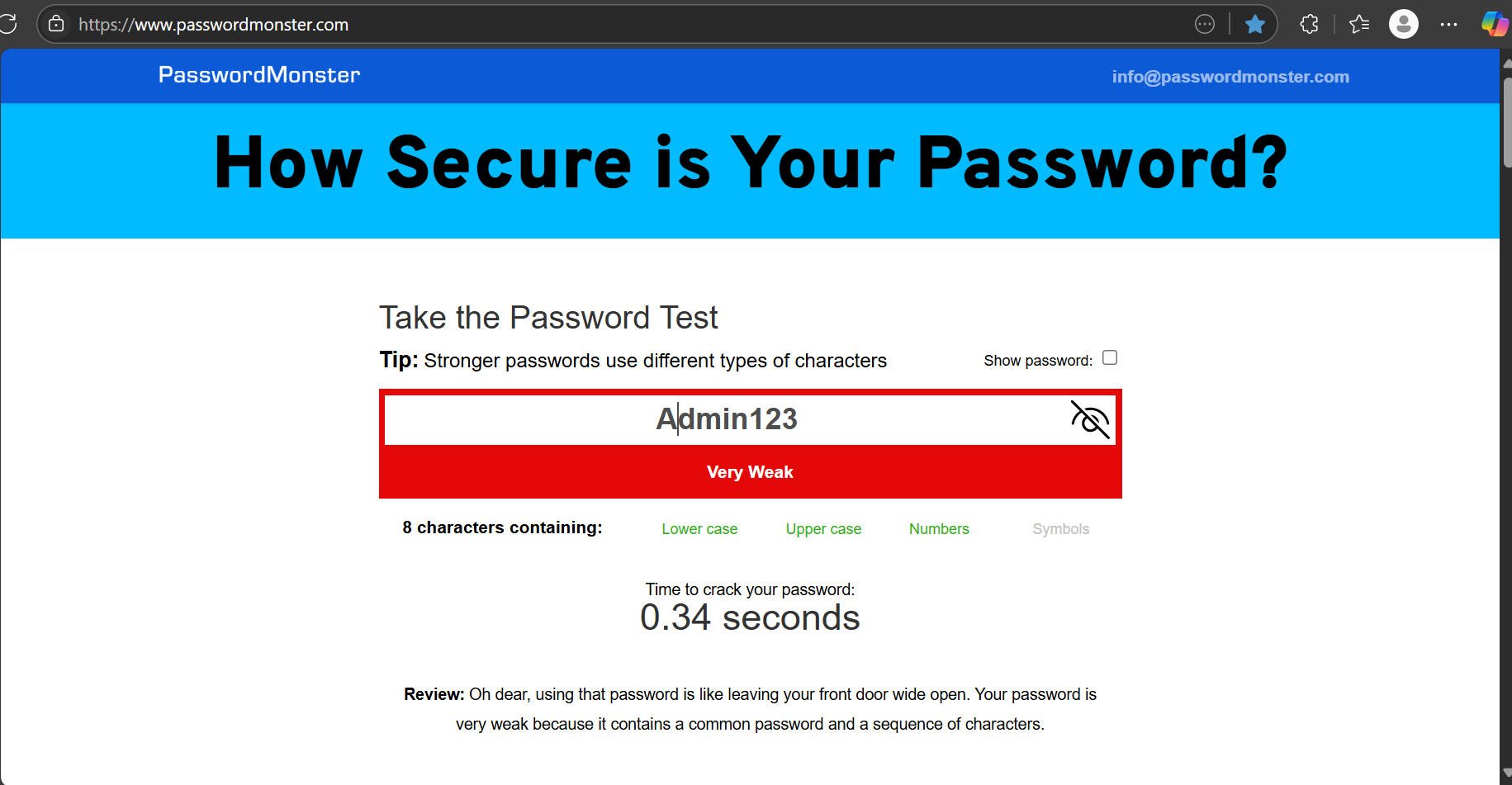
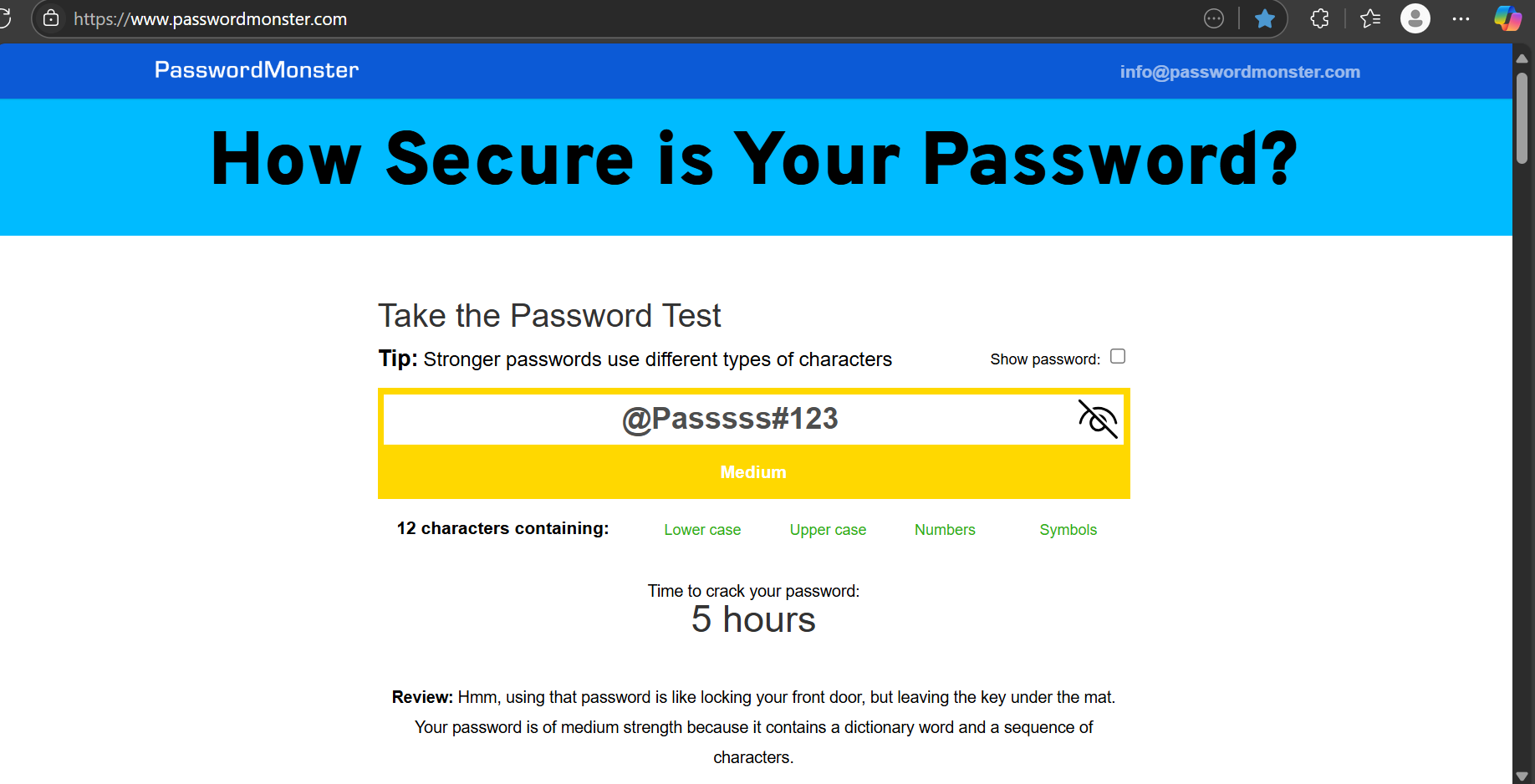
**Evaluating Password Strength**

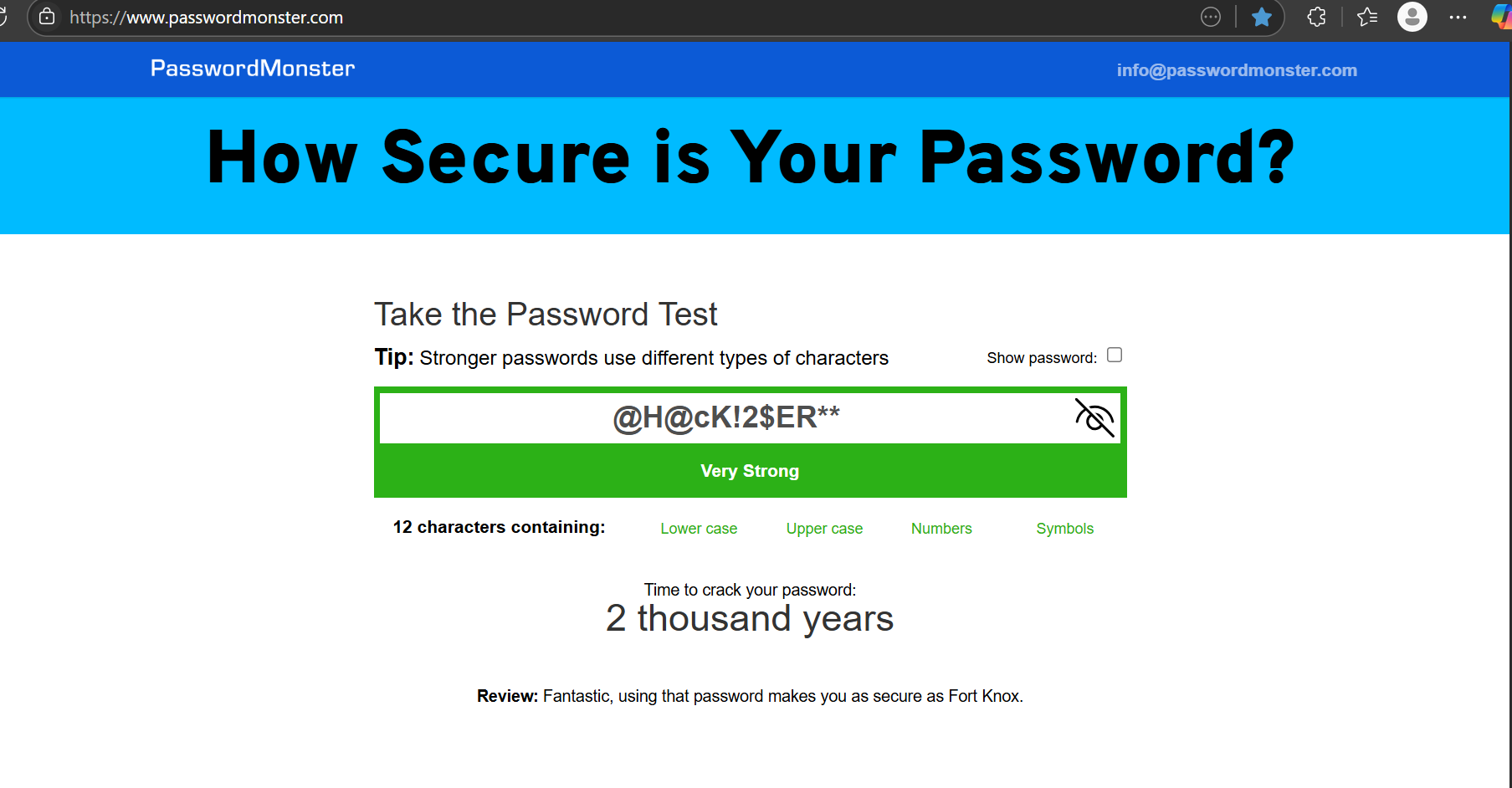
**Case 1**



**Case 2**



**Case 3**



**Best practices For creating Strong Passwords:**

* Password length should be minimum of 8 characters
* It should include combination of Upper case, lower case, numbers and special characters.
* Avoid easily guessable passwords and names of famous ideals
* Always check the strength using password meters available online
* Don’t use same passwords for all accounts
* Don’t have same username and password
* Use password managers to remember passwords

**Common Password Attacks:**

* Dictionary attack using rockyou.txt
* Brute force attack
* Keylogger attack
* Man in the middle
* Rainbow table attack
* Password spraying
* Shoulder surfing
* Social enggineering

**How Password complexity affects Security:**

* Weak passwords are more prone to attacks
* Brute force attacks without protection can crack the password
* Strong passwords may prove tricky to crack
* Having 2 factor authentication for the accounts is best practice
* Strong password and MFA means security is hard to break through
* Reduces unauthorised access
* Reduced data breaches