SECURE CODE

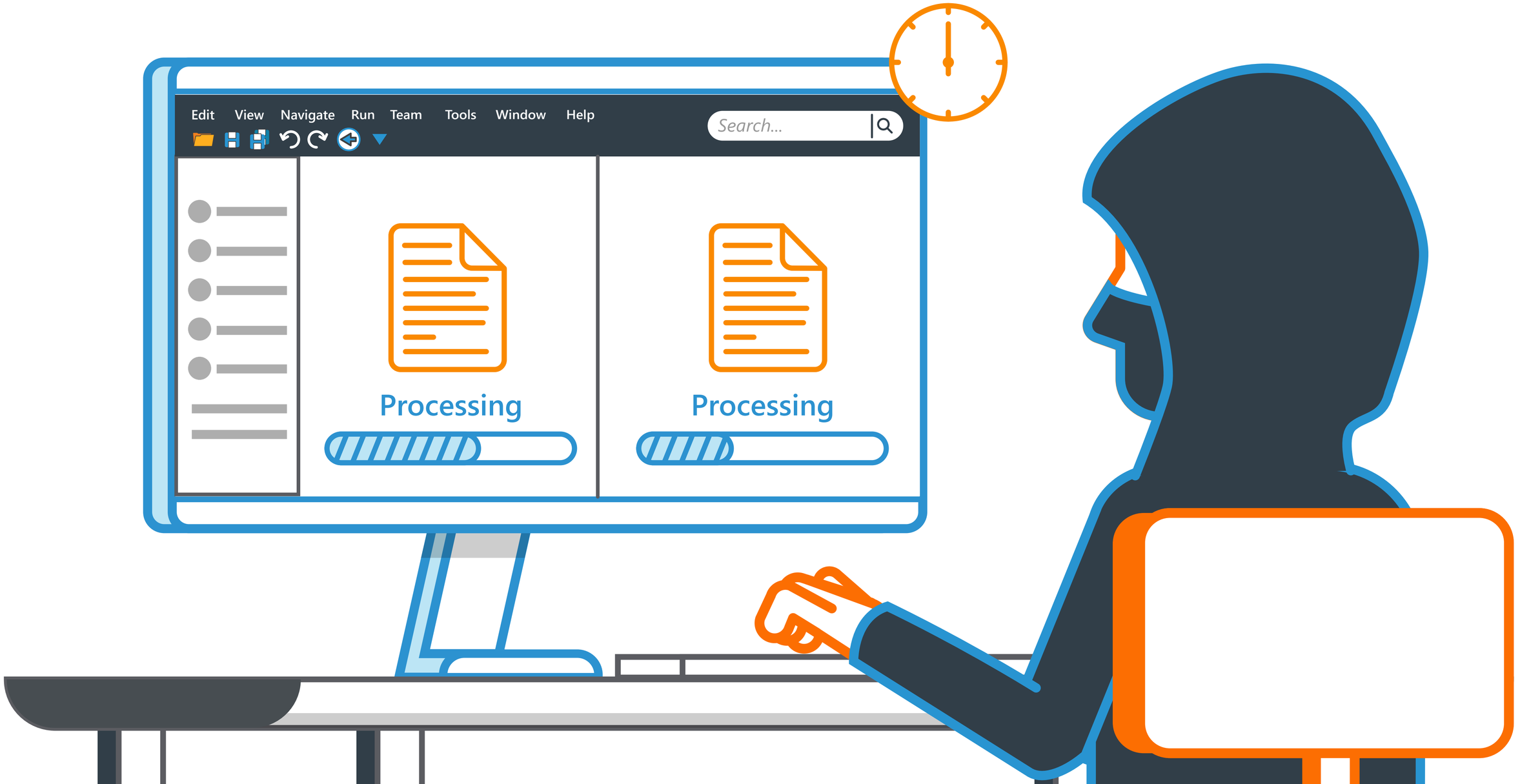
WARRIOR®

TIMING ATTACKS

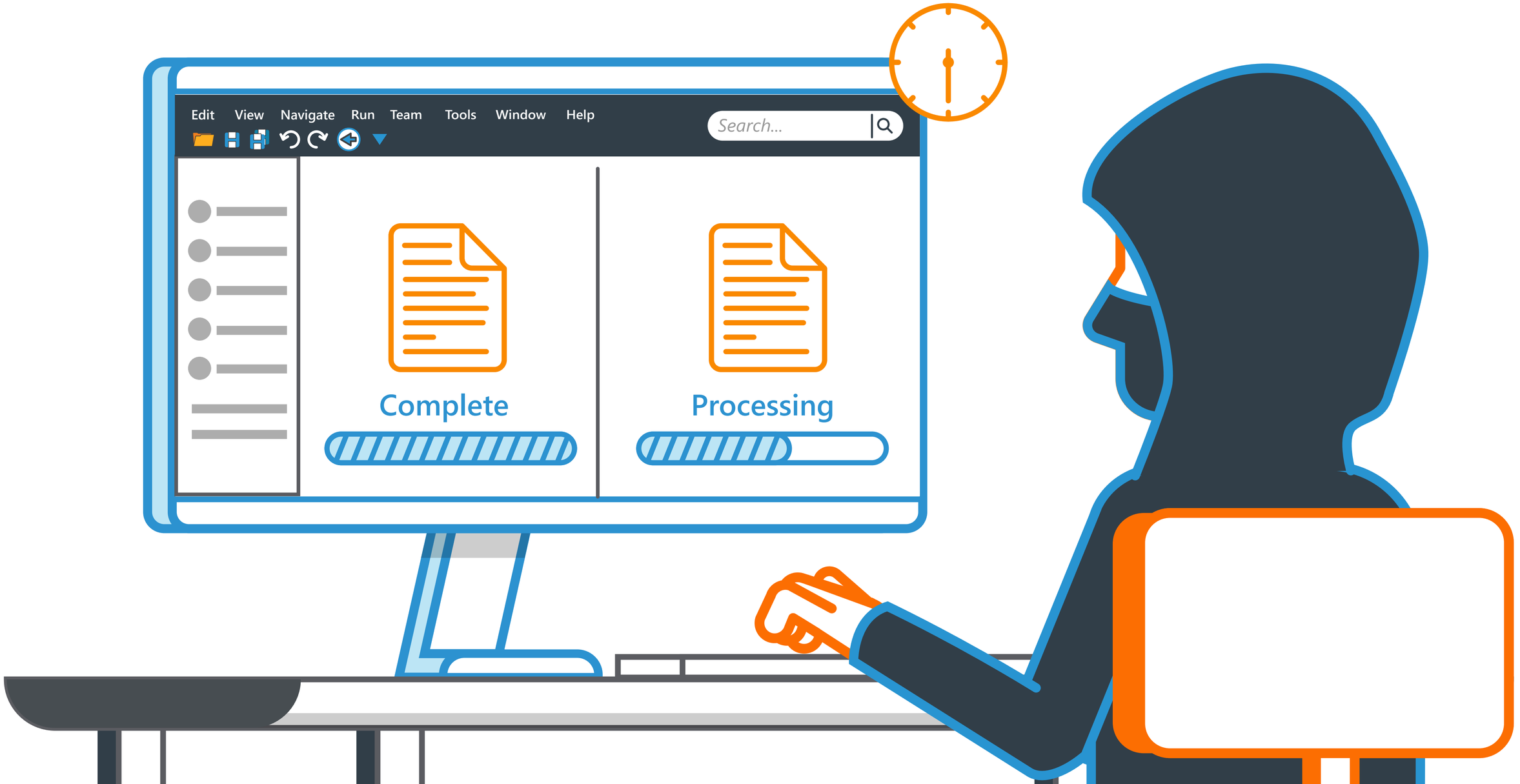
We'll go through

some causes and preventions of vulnerabilities in this category

A Timing Attack is a side channel attack that happens when an attacker is able to discover how long it takes the system to respond to various outputs.

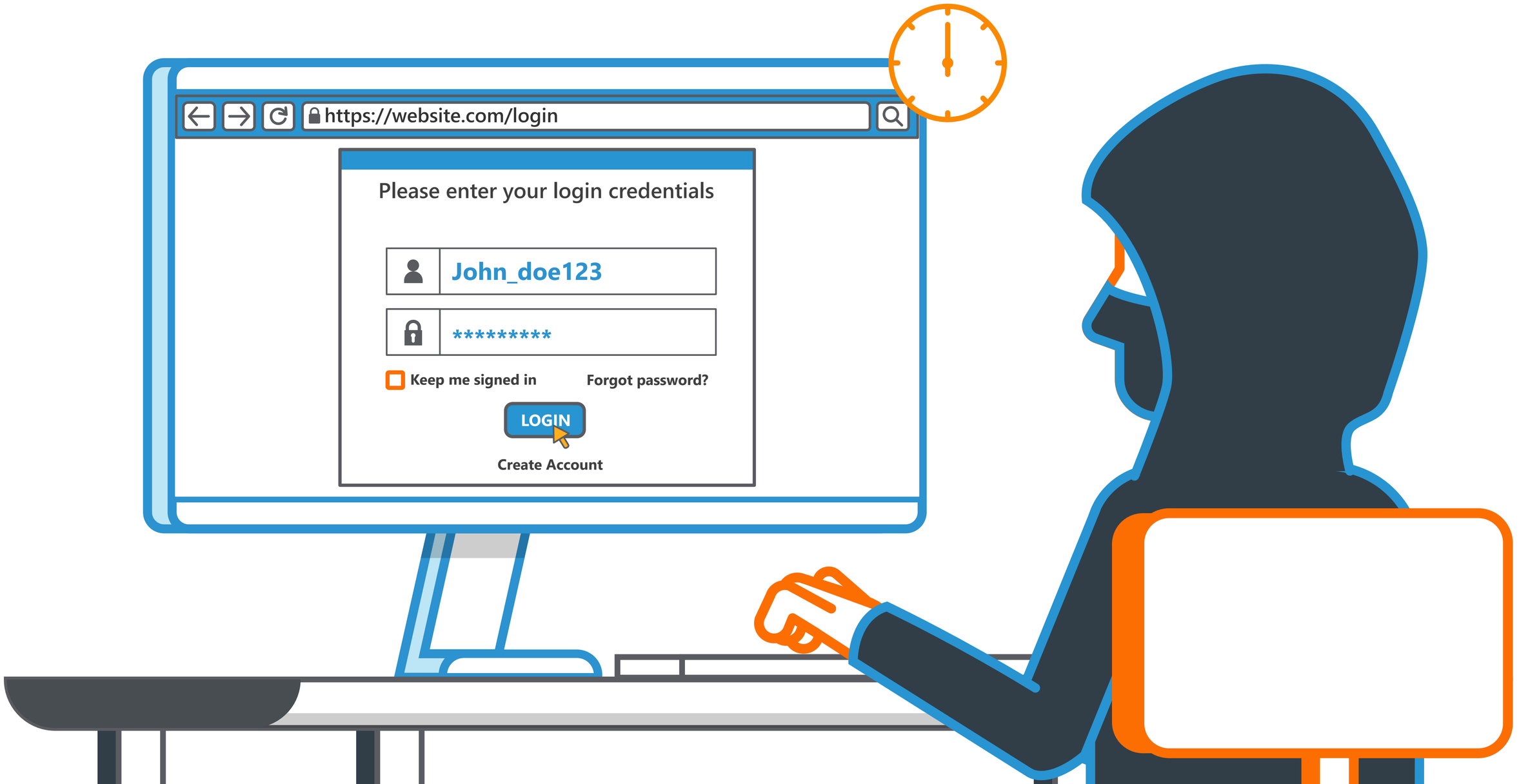


Even subtle differences in response times can allow attackers to see vulnerabilities in the application, expose sensitive information, or even change the flow of a process in the application.

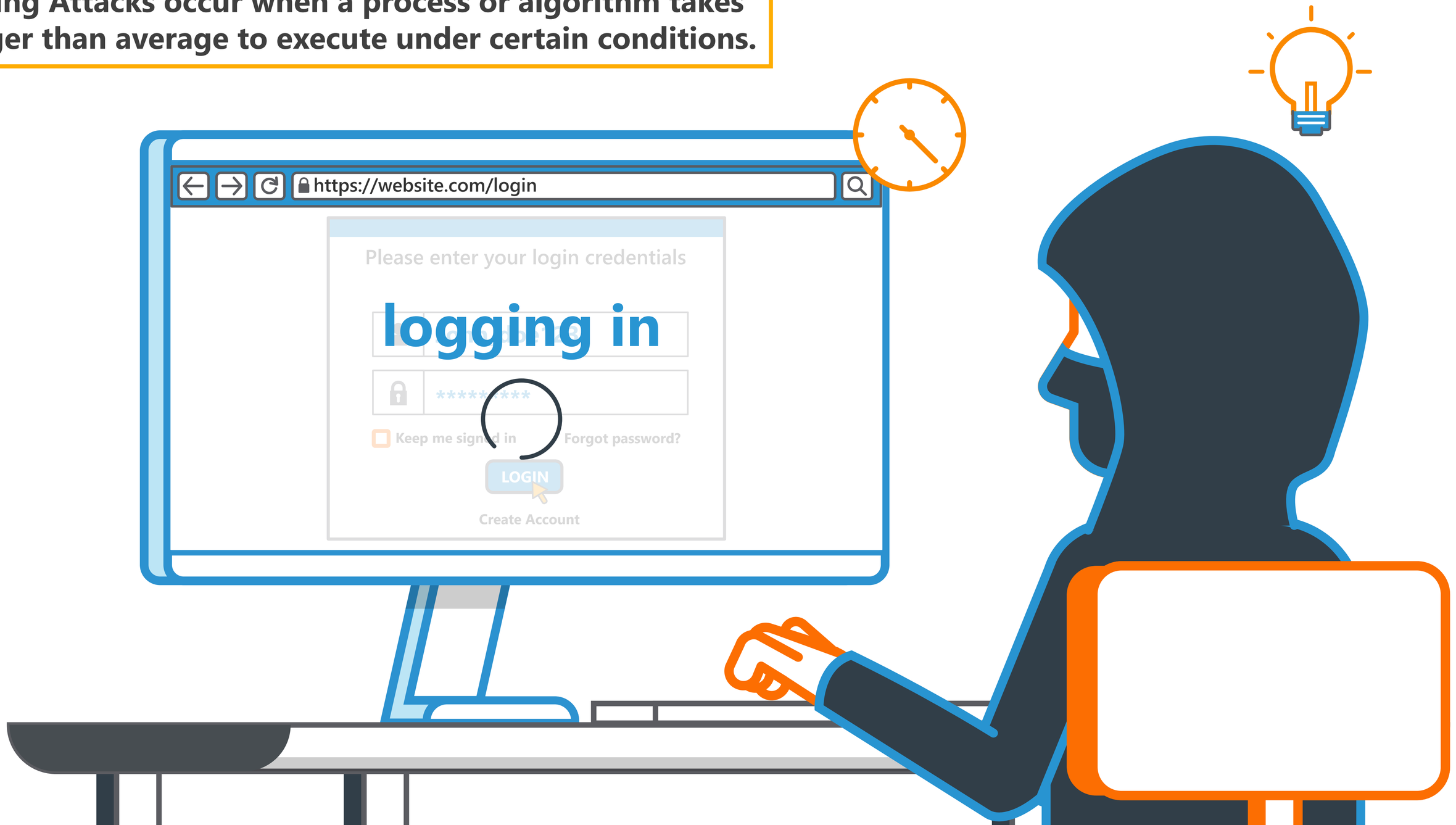


WHERE DOES THIS VULNERABILITY OCCUR?

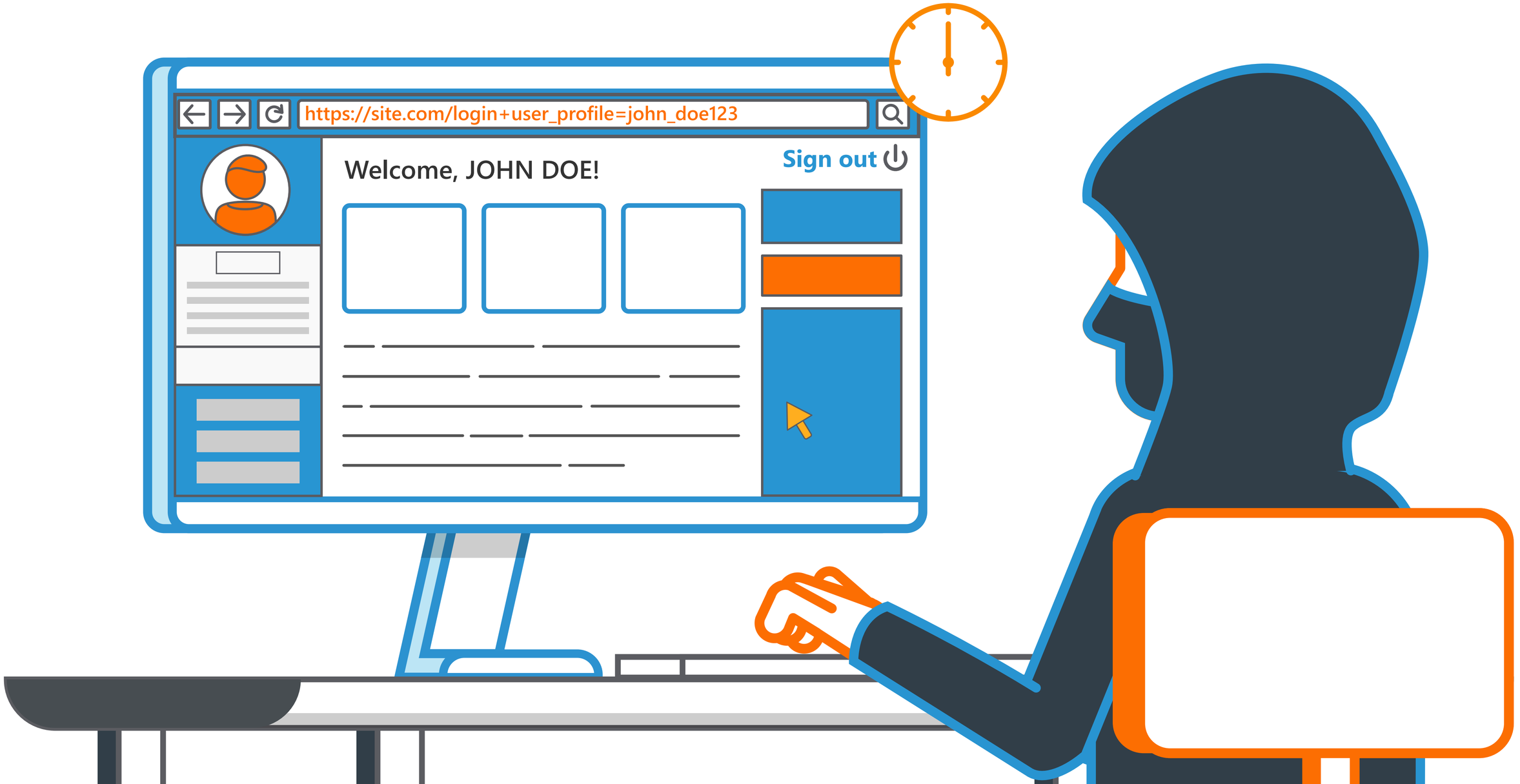
Every execution of code takes time.



Timing Attacks occur when a process or algorithm takes longer than average to execute under certain conditions.

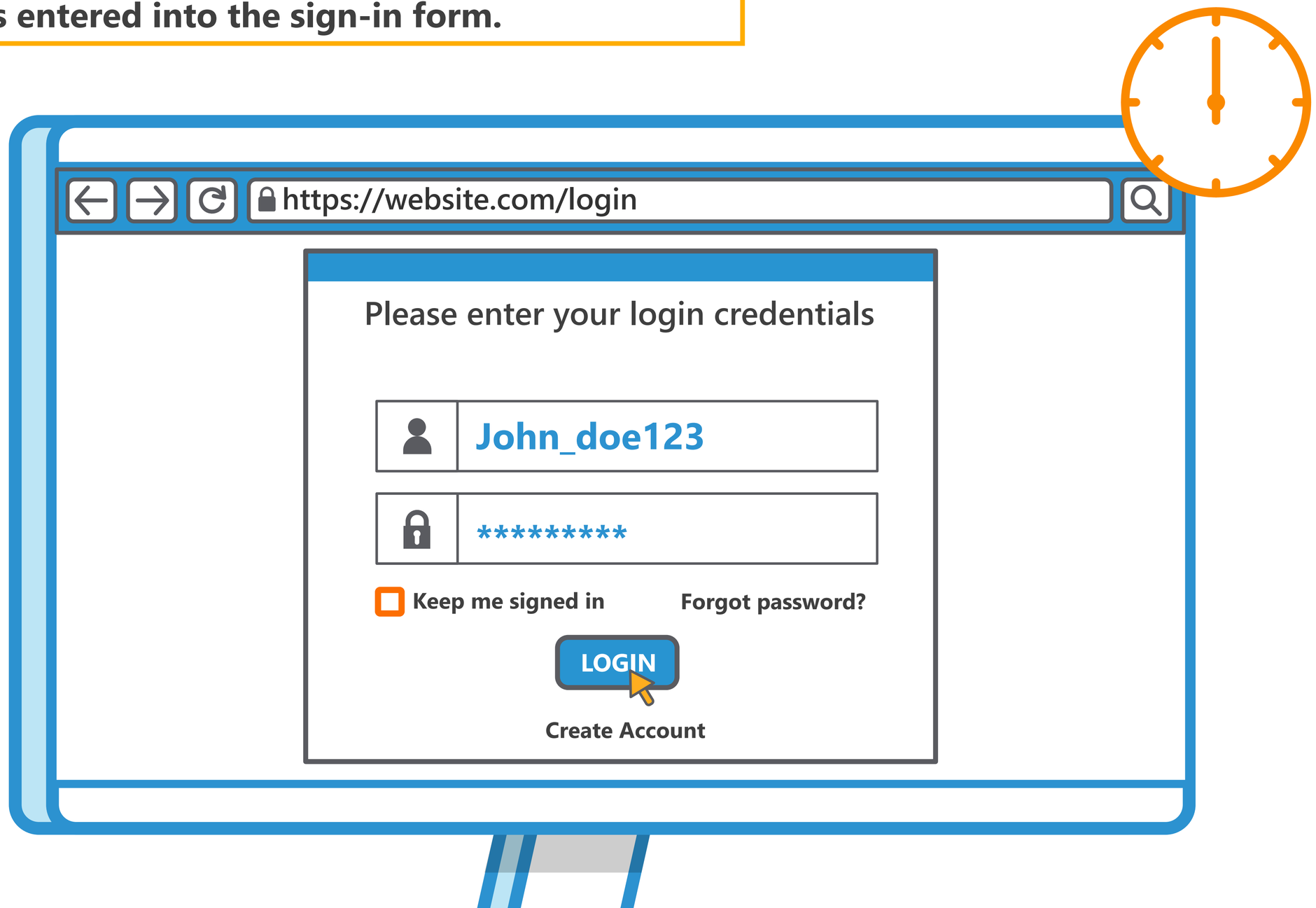


Consider what an attacker could learn by knowing that such a process is taking place.

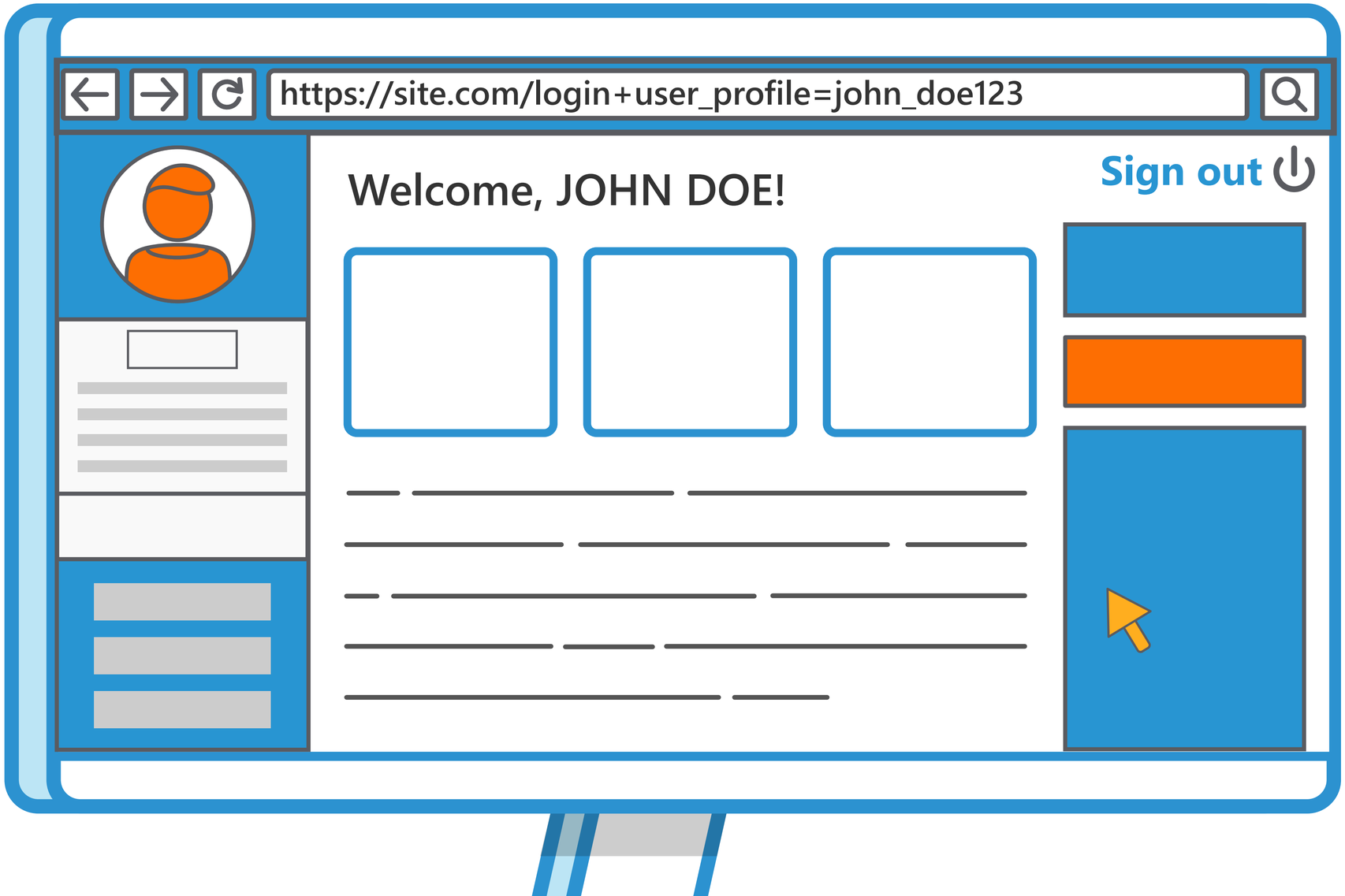


LET’S LOOK AT AN EXAMPLE

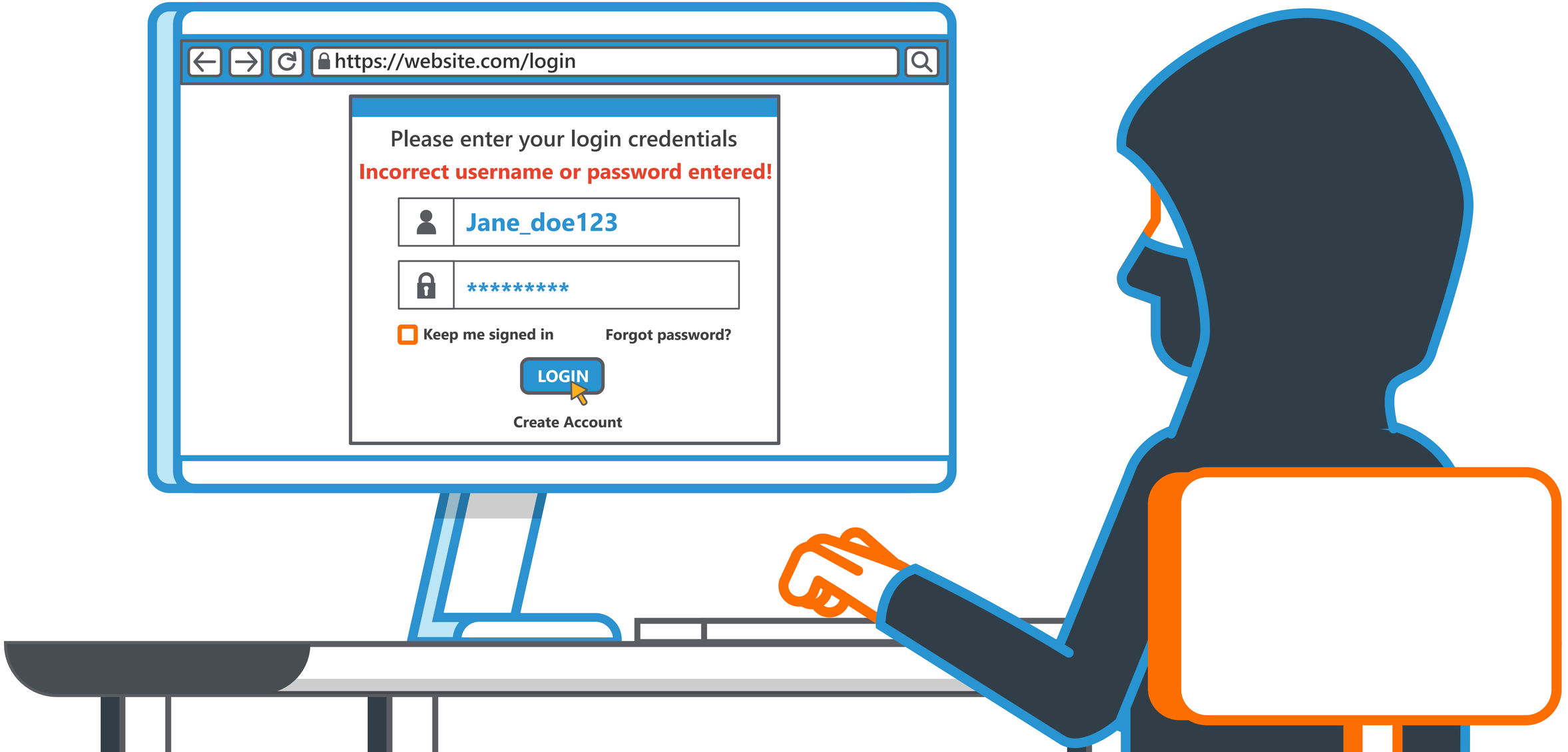
In this application a password hashing process is run whenever a valid username is entered into the sign-in form.



However, if the username is not valid, this process is skipped.

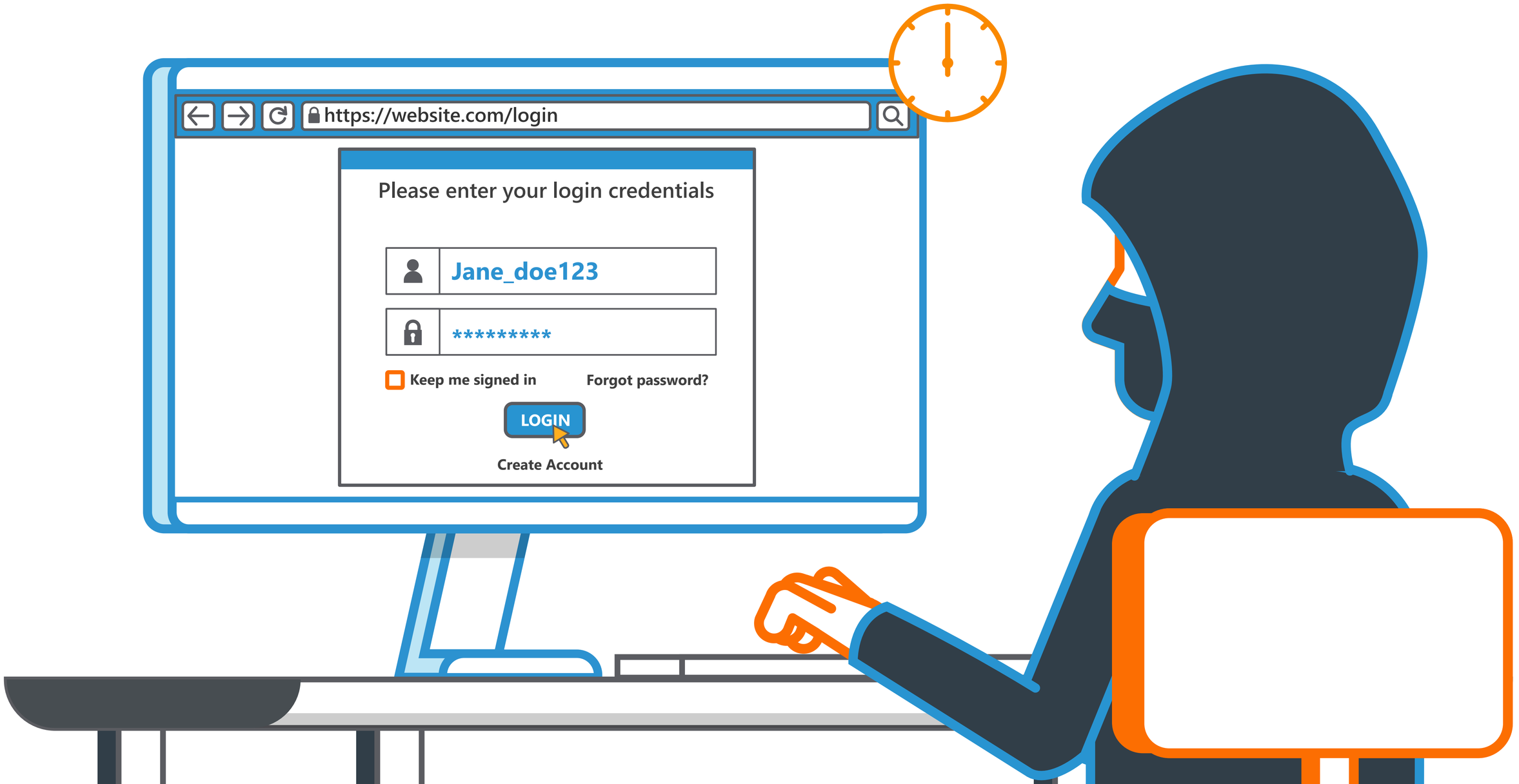


Knowing this helps an attacker who is using a dictionary attack to maliciously login to a user account.

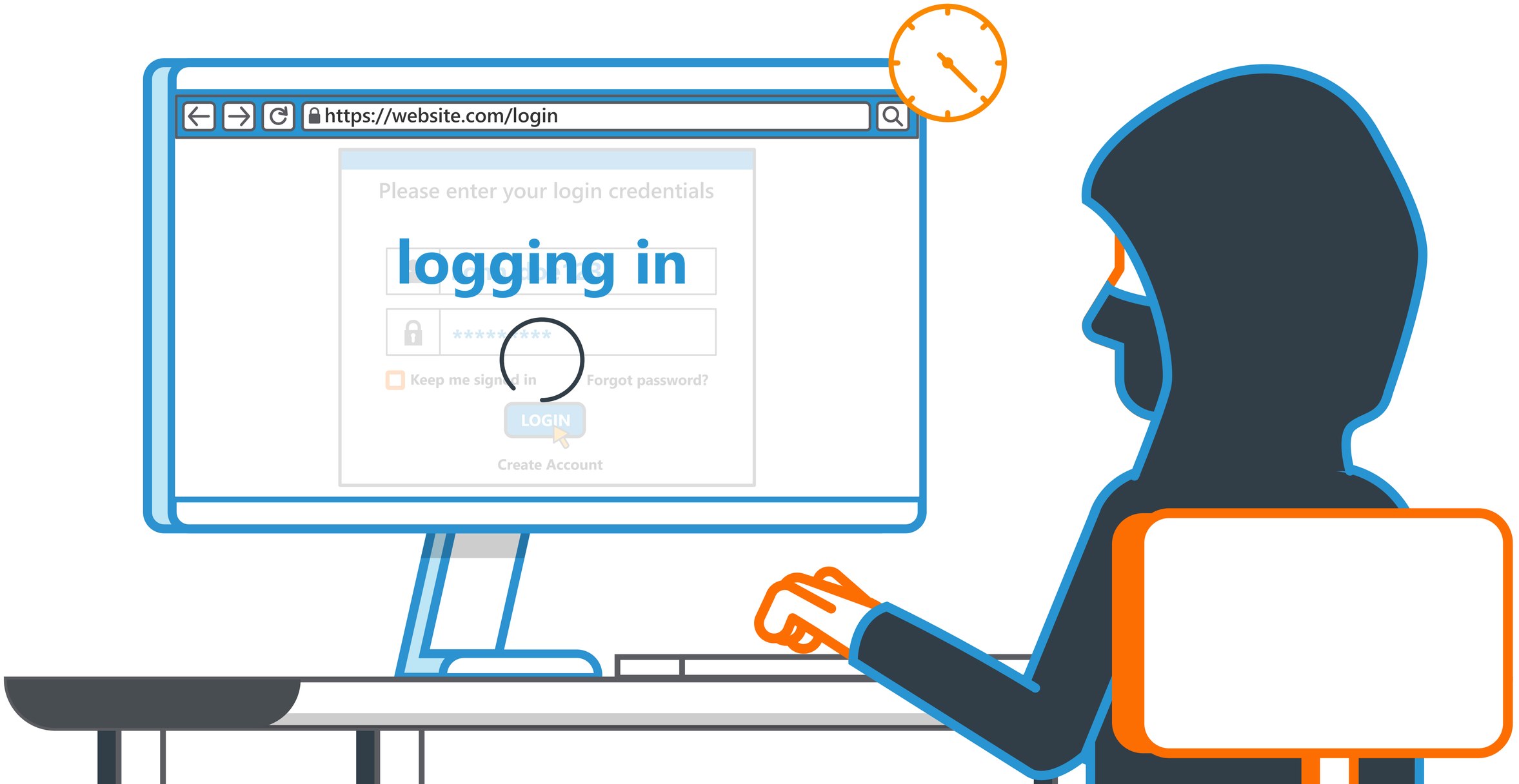


The attacker first needs to work out a valid username. He tries many combinations,

until finally one attempt causes the system to start working in the background.



Because the time required to generate a response for a valid username is noticeably longer,



it tells the attacker that the username does, in fact, exist.

To prevent Timing Attacks, developers should:

- Be sure to run timing-based testing on the application
- When a sensitive action that may take some time is executed, ensure the application makes the same processing actions regardless of the other flow it take
- Where required, create dummy values in the code that make up for significant time differences

Congratulations, you have now completed this module!

SECURE CODE

WARRIOR®

www.securecodewarrior.com