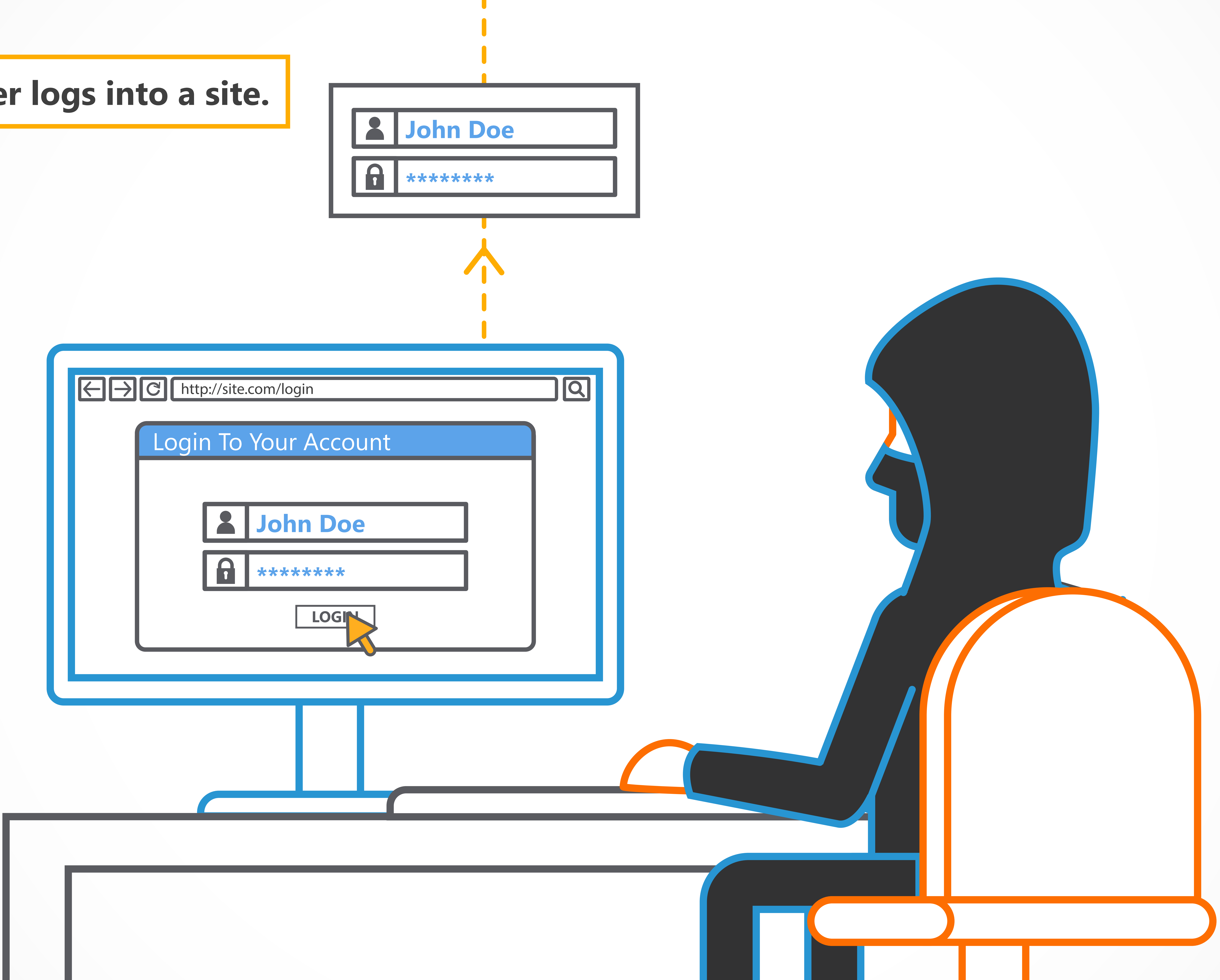
SECURE CODE WARRIOR

WEAK SESSION TOKEN GENERATION

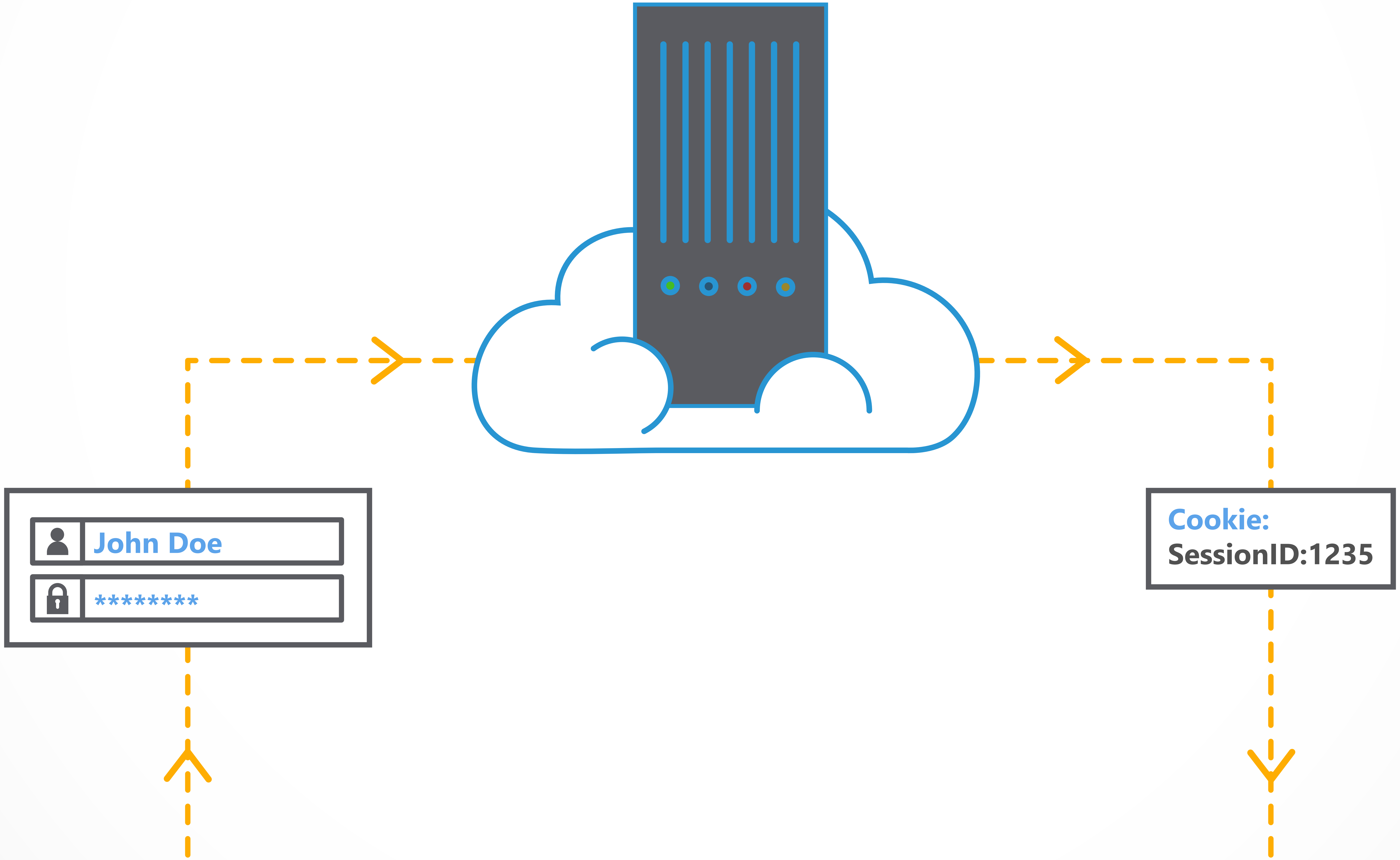
We’ll go through

some preventions steps for vulnerabilities in this category

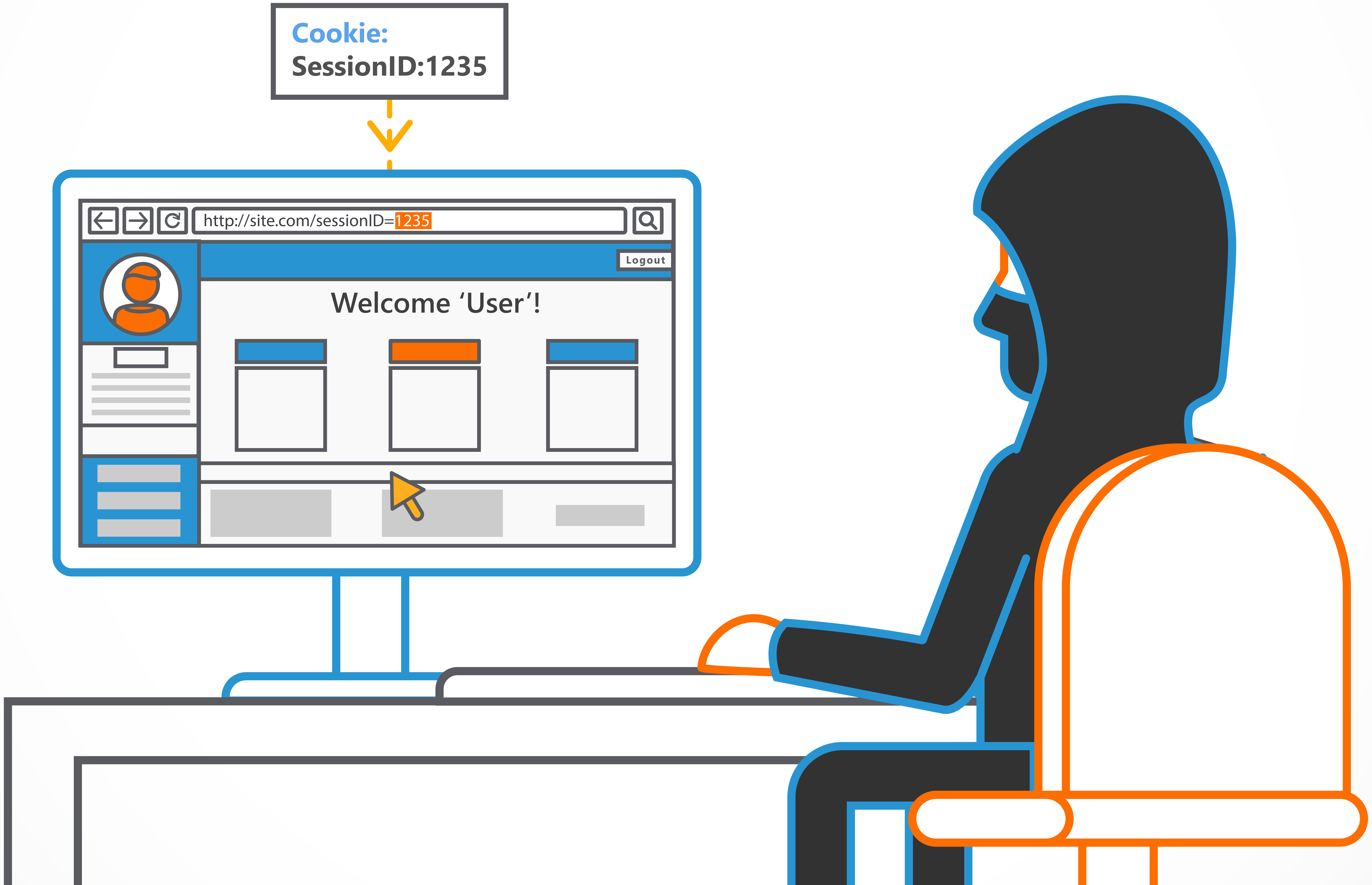
Here, an attacker logs into a site.



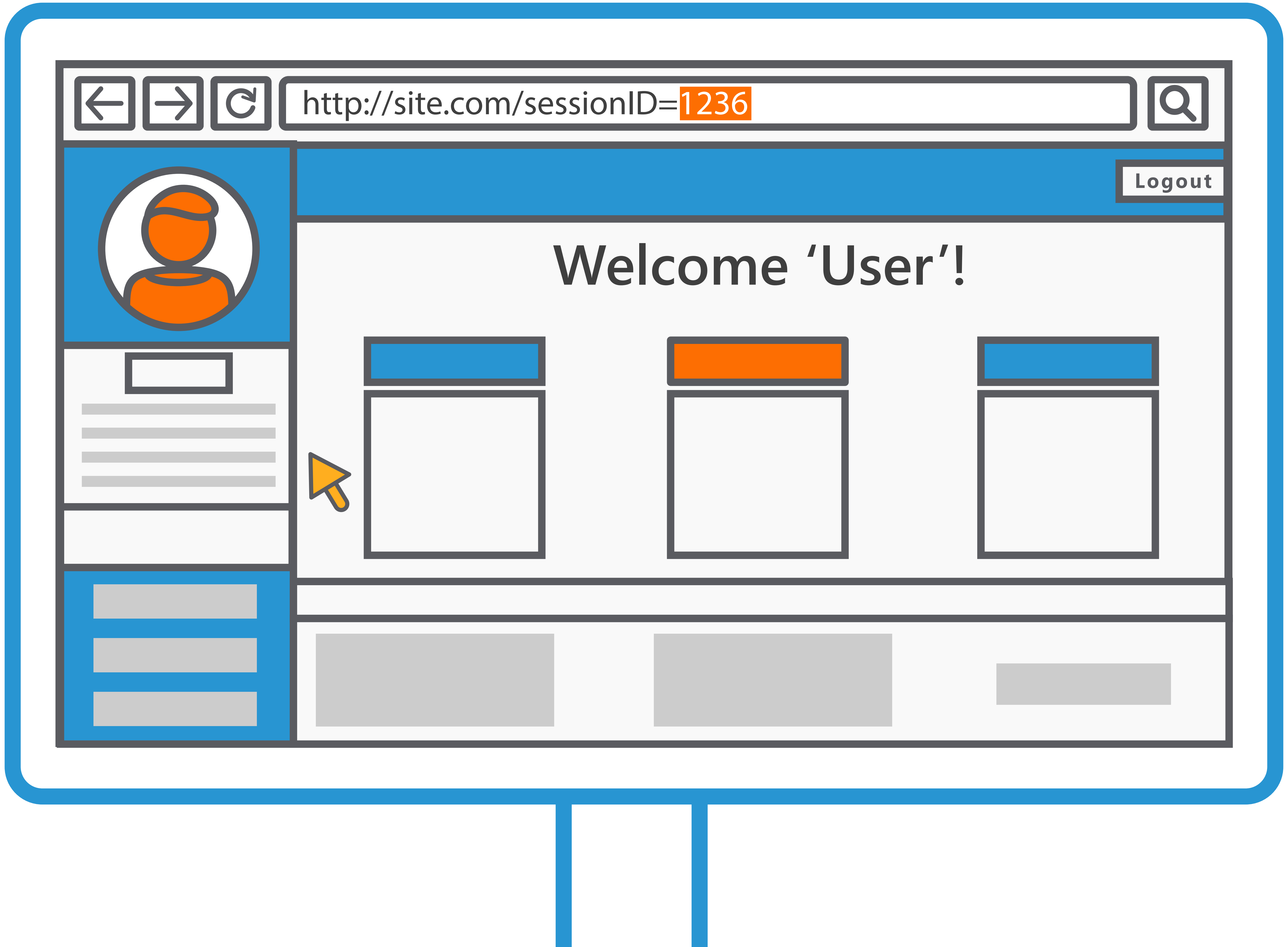
The site uses a simple increment to generate session IDs.



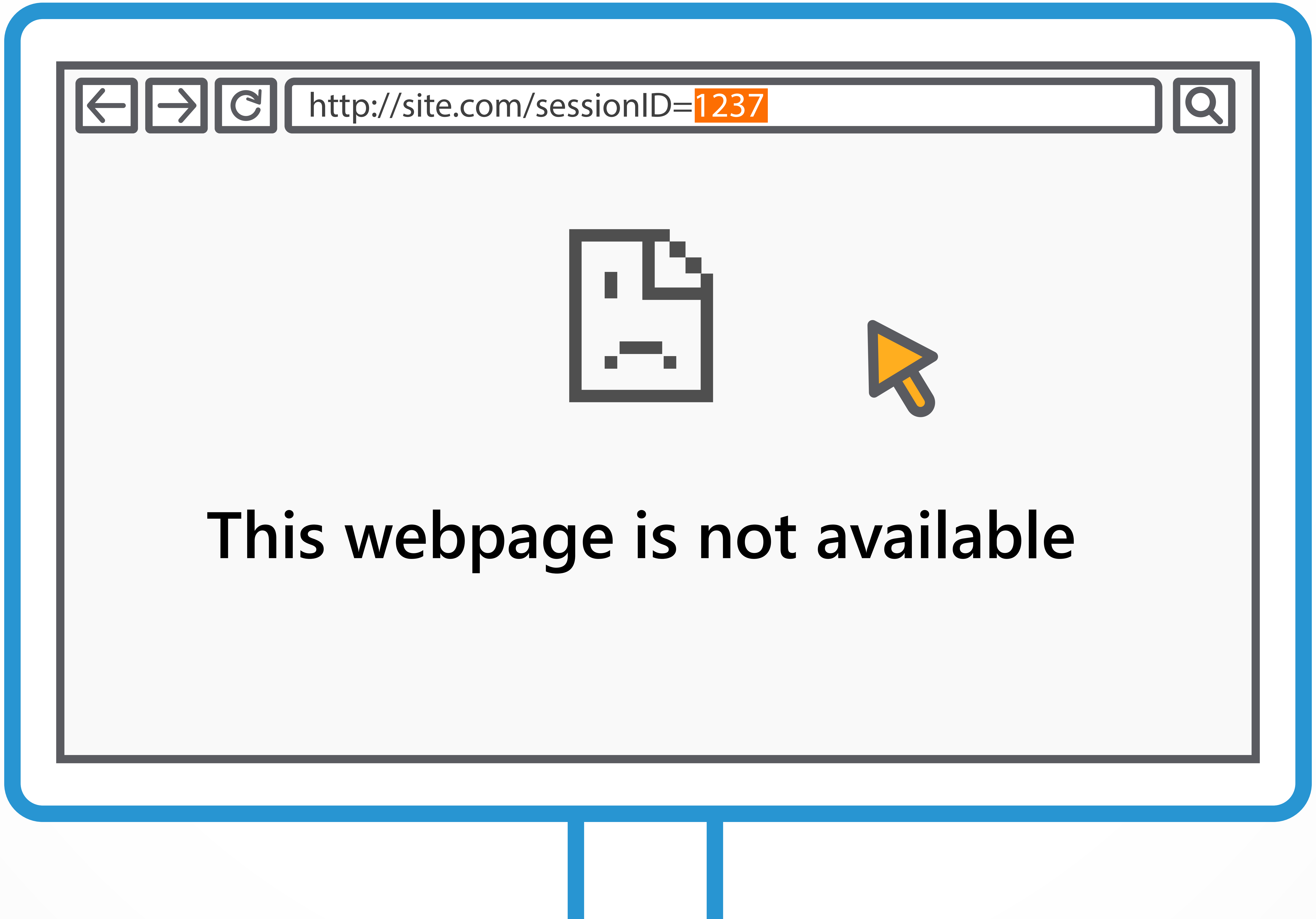
The site uses a simple increment to generate session IDs.



The attacker, noticing the predictability of the ID generation,



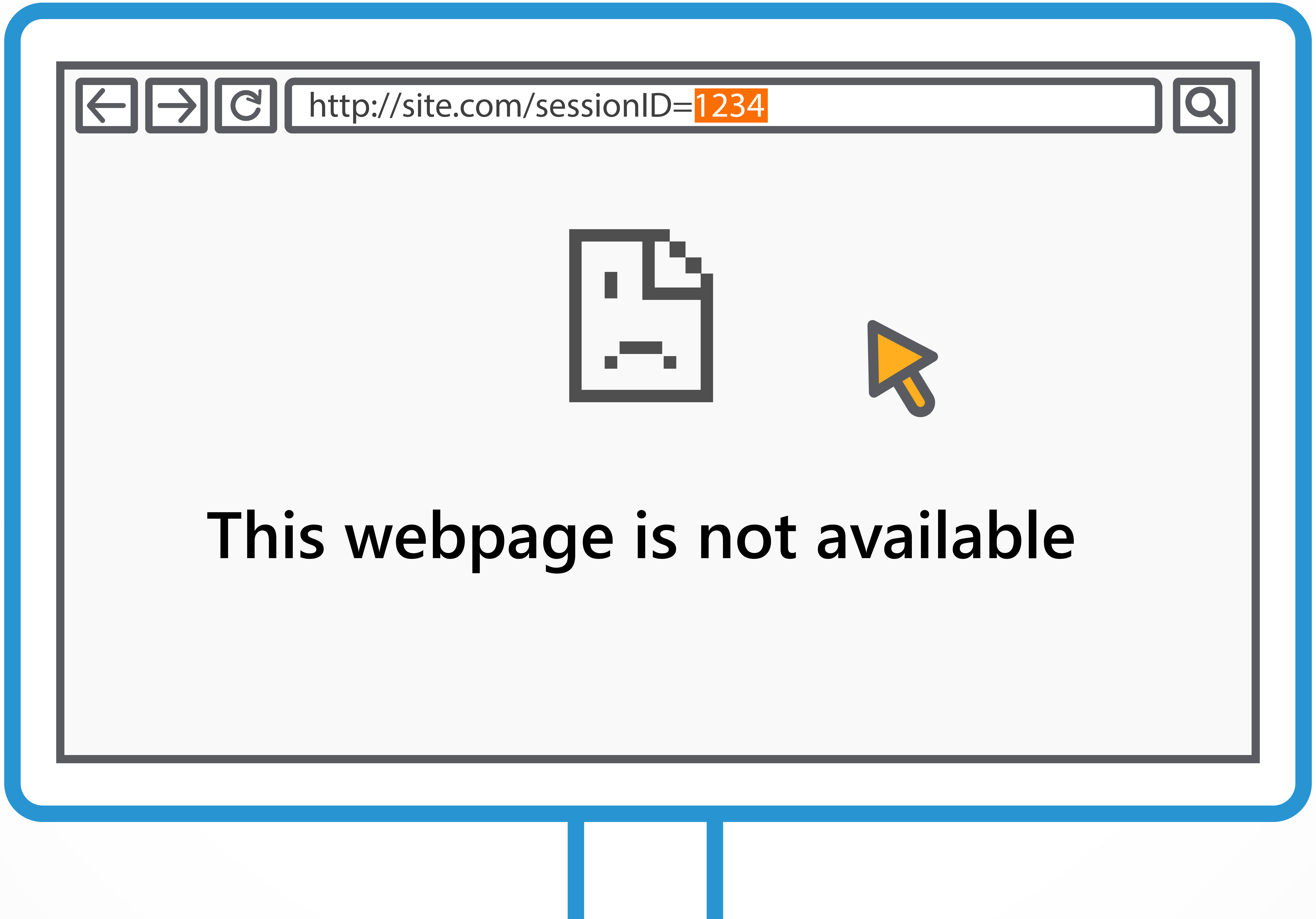
deduces new IDs , which he uses to browse back to the site.



http://site.com/sessionID=1237

This webpage is not available

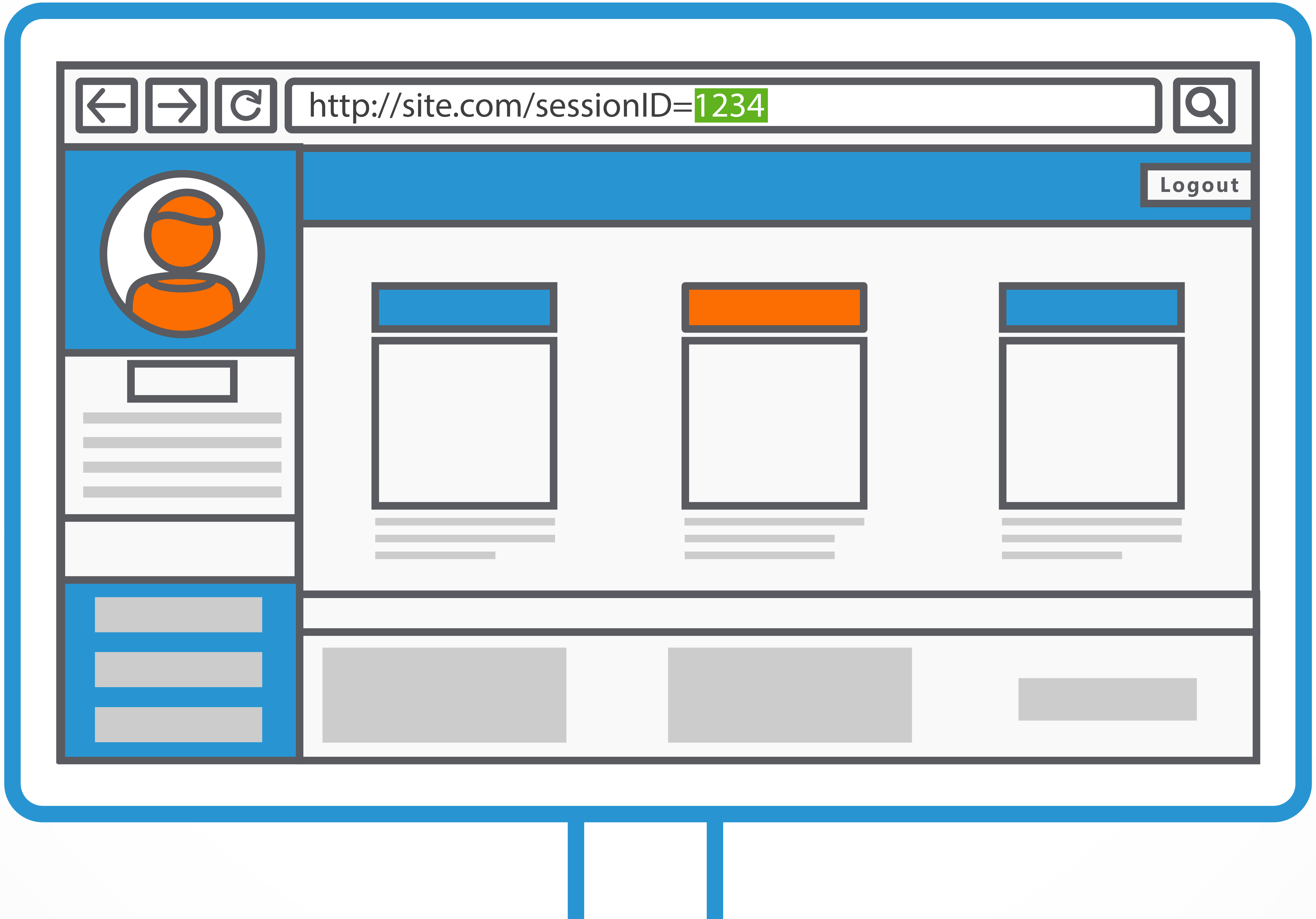
After a few attempts, the attacker finds a session ID that is associated with another authenticated user.



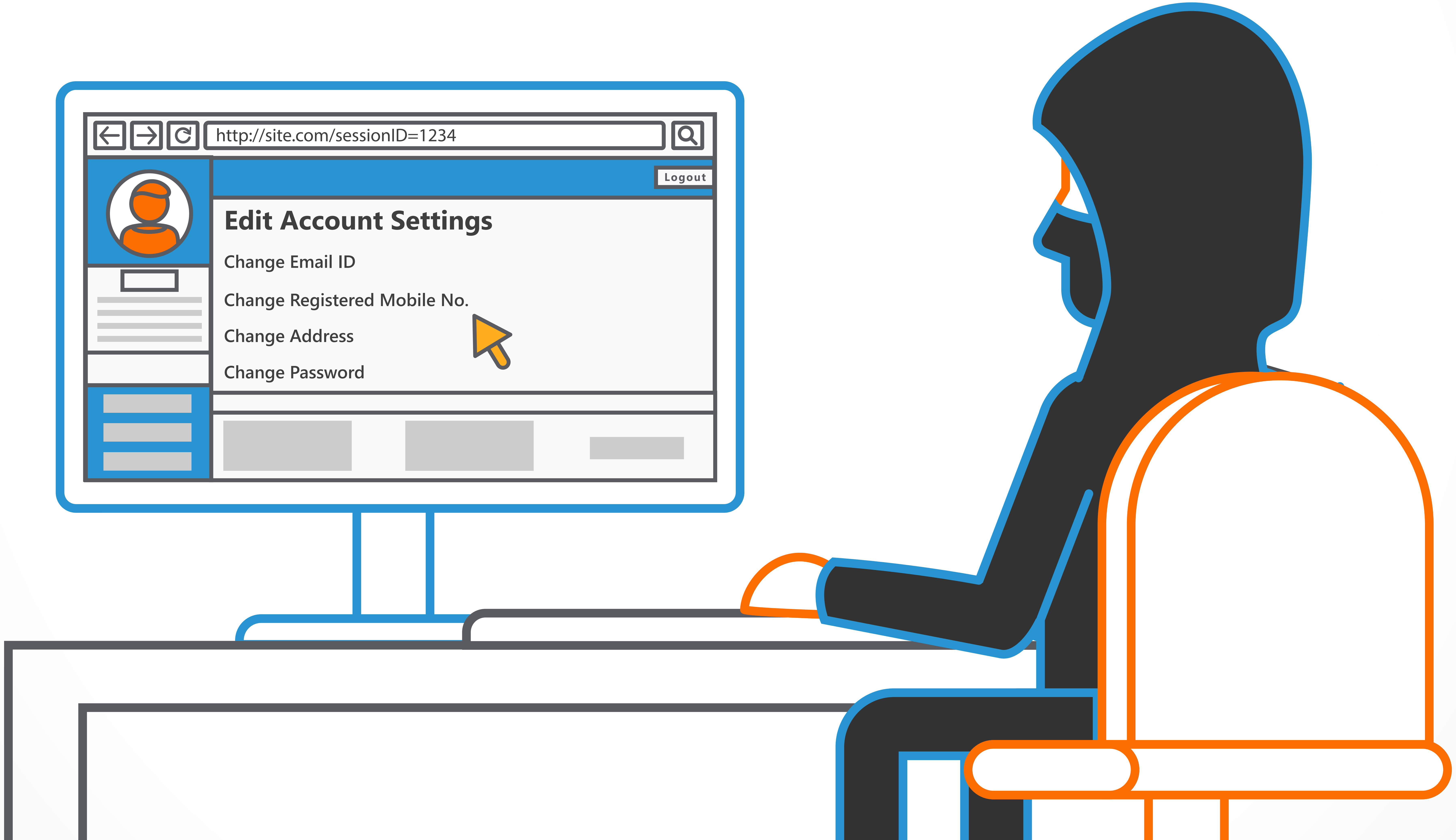
http://site.com/sessionID=1234

This webpage is not available

After a few attempts, the attacker finds a session ID that is associated with another authenticated user.



By being able to predict session IDs he is able to impersonate the authenticated user and is allowed full access to the user's account.



By being able to predict session IDs he is able to impersonate the authenticated user and is allowed full access to the user’s account.

http://site.com/sessionID=1234
Logout
Edit Account Settings
Change Email ID
Change Registered Mobile No.
Change Address
Change Password
HACKED!

POOR SESSION MANAGEMENT CAN BE PREVENTED

using built-in session management functionality provided by your development framework, instead of inventing your own.

To Prevent Poor Session Managemant

- Store the session ID in a cookie and then, protect session cookies.

- This can be done by setting an expiry timestamp, path, “secure” and “HTTPOnly” flag and invalidate on logout.

- Additionally, Session ID properties must be secure.
  Always make them unpredictable, time limited and single session.

- Finally, always use a secure communication channel.
  For more details on this,see the “Insufficient Transport Layer Protection” module.

Congratulations, you have now completed this module!

SECURE CODE WARRIOR

www.securecodewarrior.com