SECURE CODE

WARRIOR

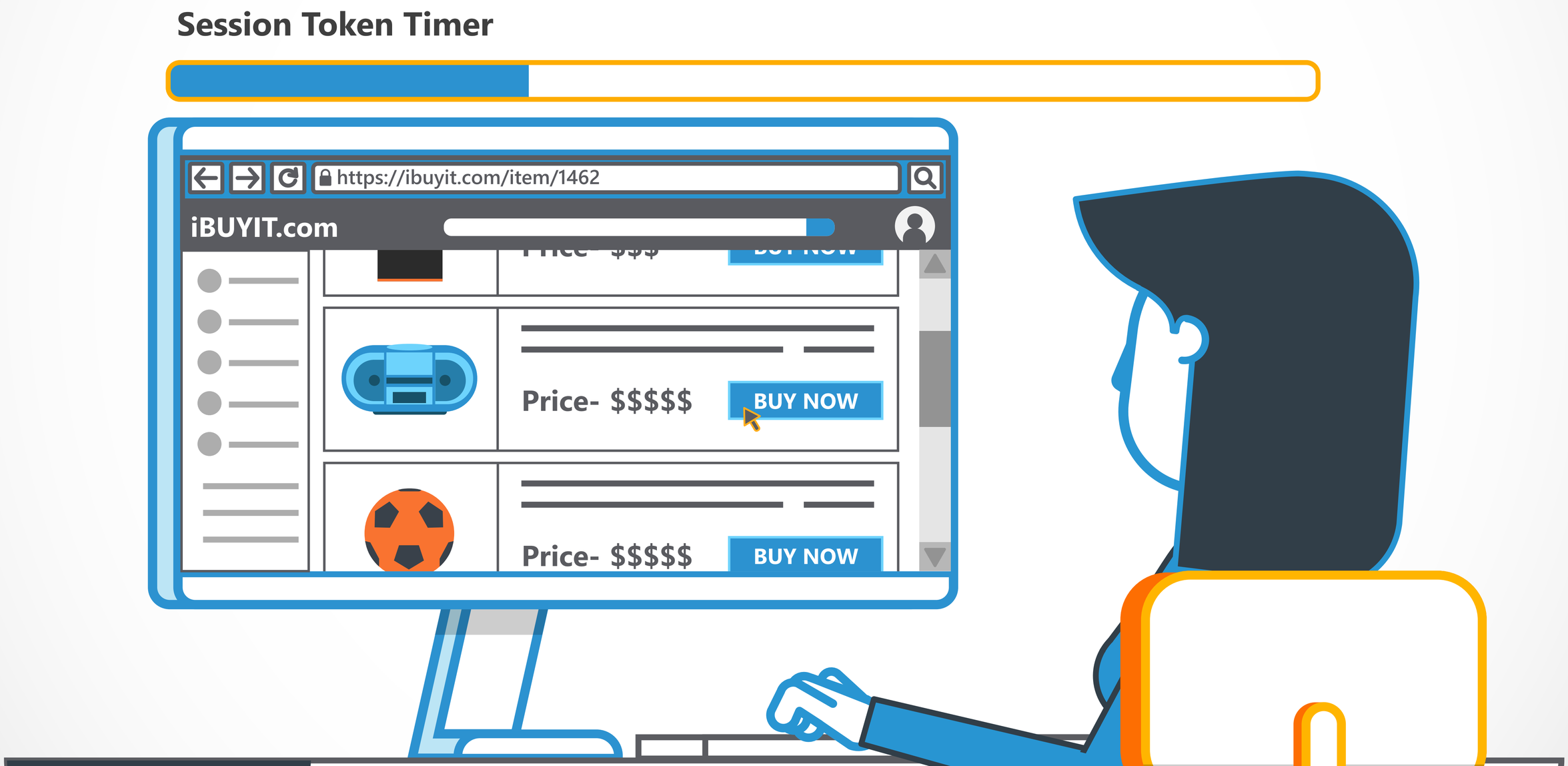
INSUFFICIENT SESSION EXPIRATION

We'll go through

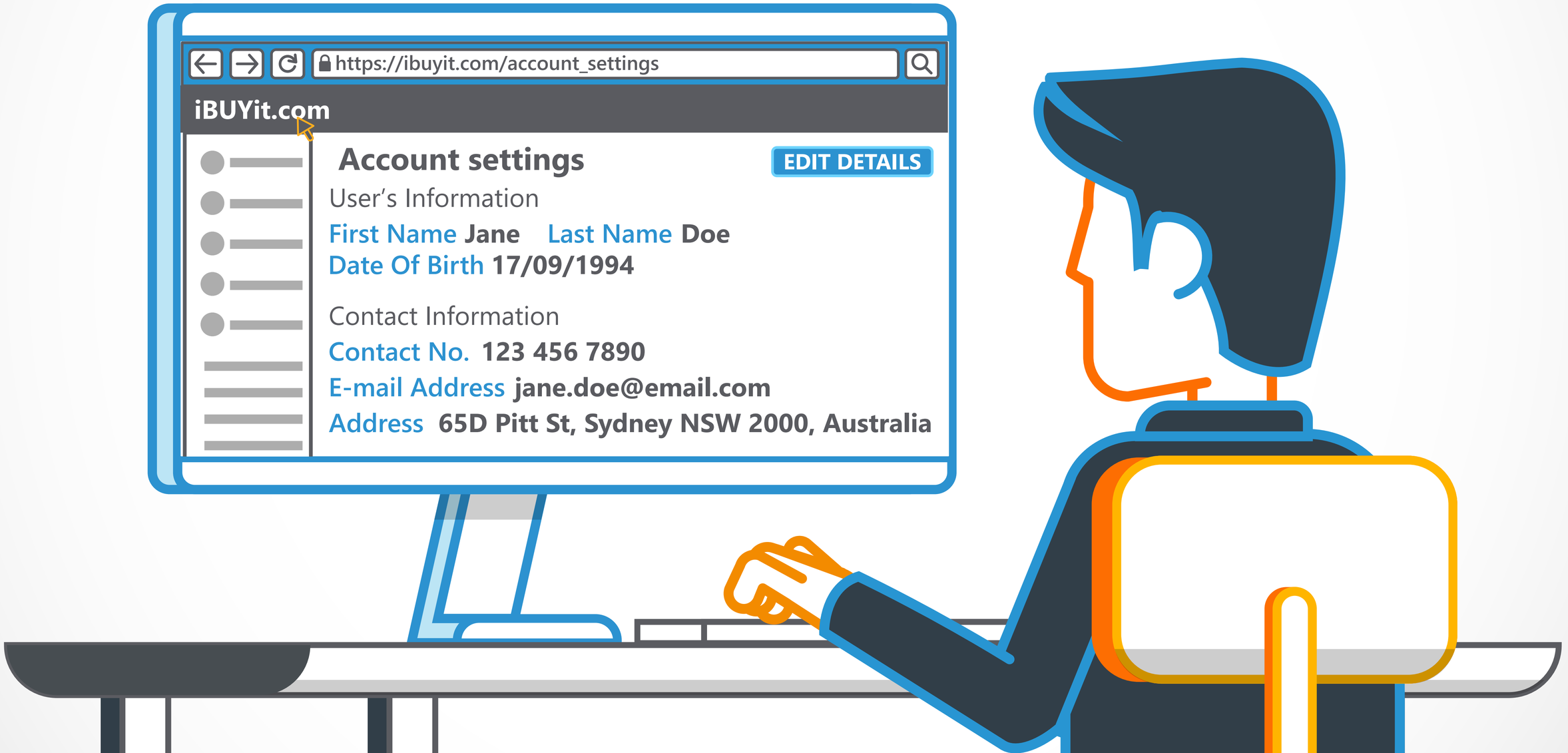
some causes and preventions of vulnerabilities in this category.

WHAT DO WE MEAN BY INSUFFICIENT SESSION EXPIRATION?

Insufficient Session Expiration is a vulnerability in which the lifespan for the user session's token persists for longer than it should.

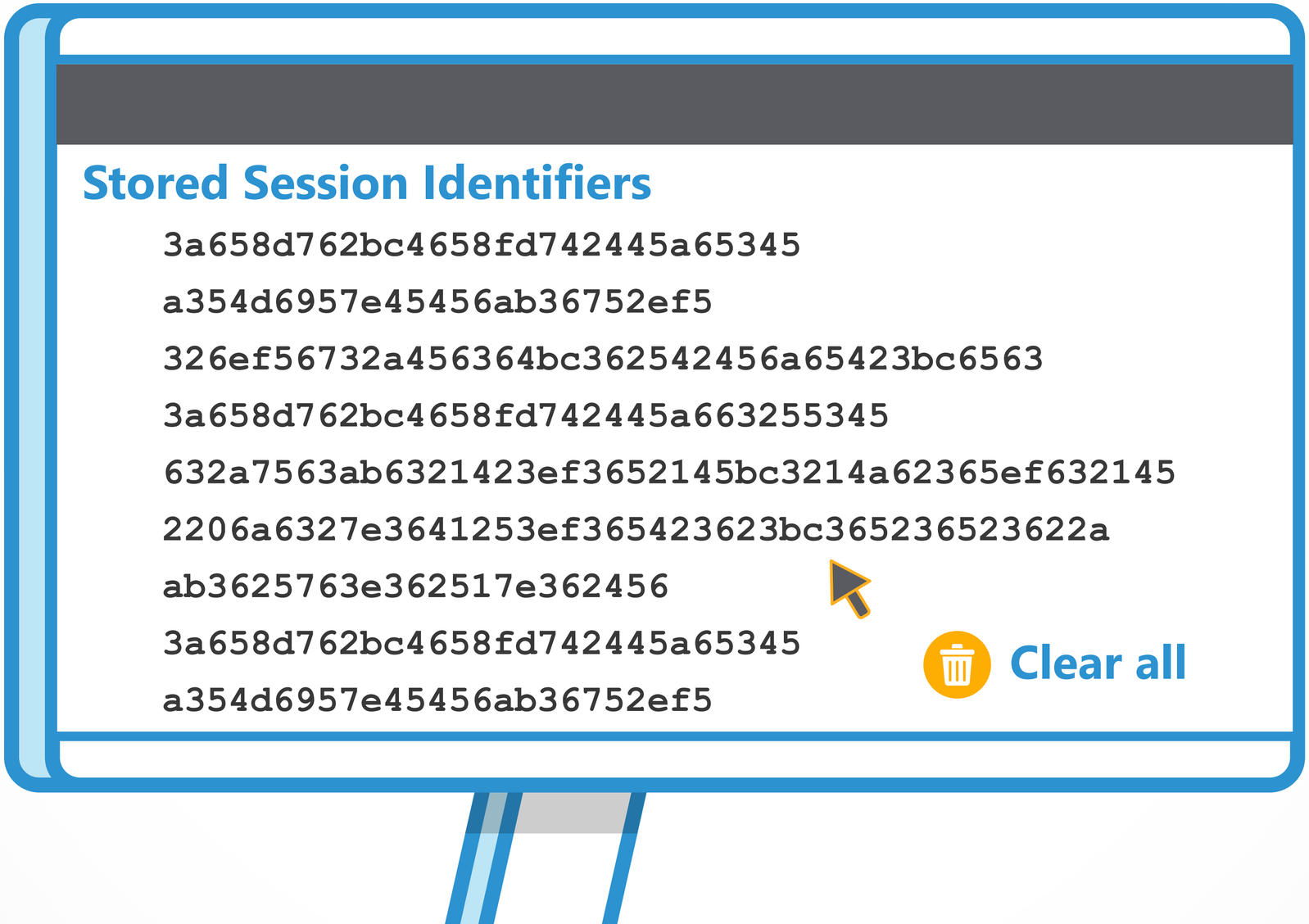


If a session token remains valid for longer than it is needed, it increases the risk of the session being leaked or taken over by a malicious person or script.



Insufficient Session Expiration vulnerabilities usually occur when an application is not setting a time-out on session identifiers.

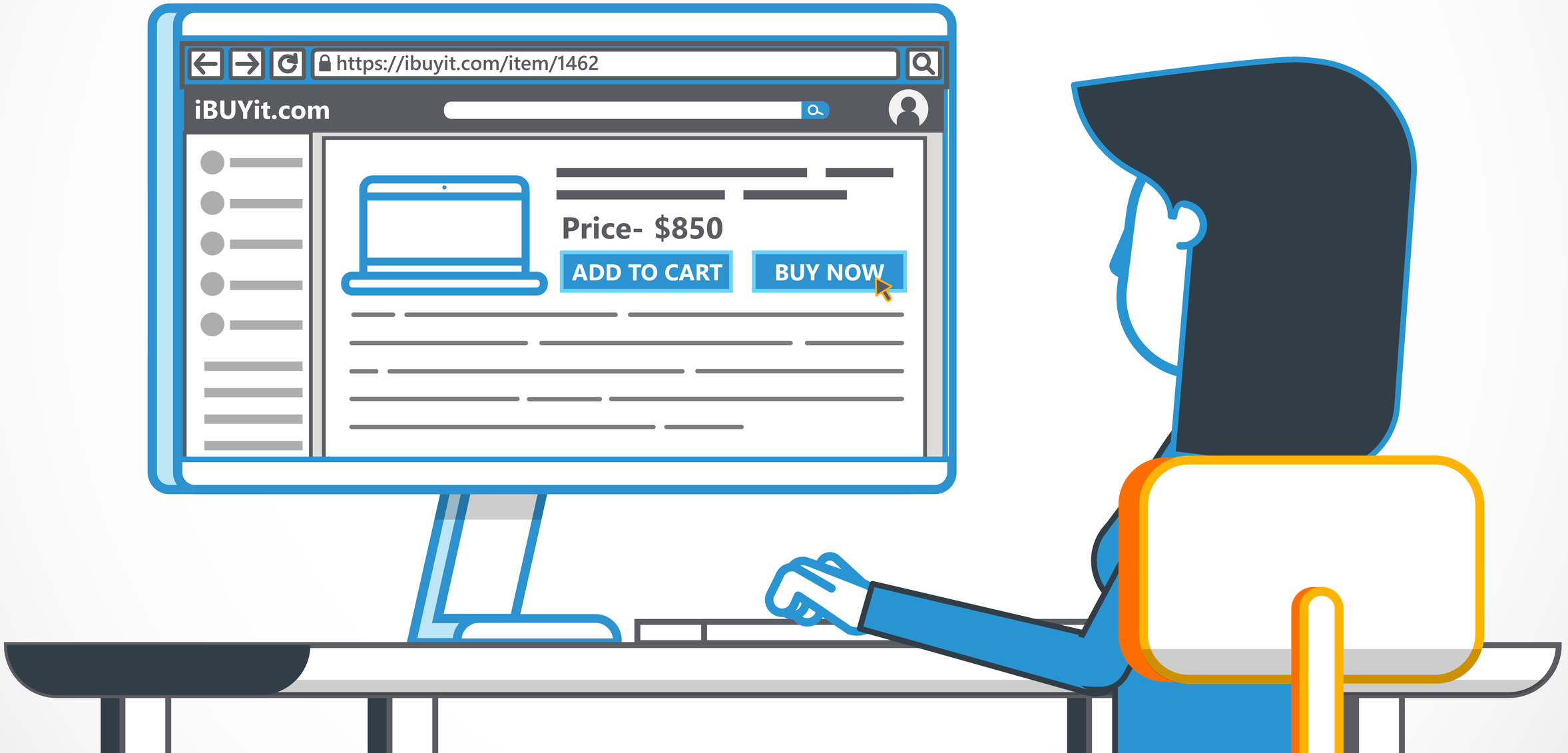
Or alternatively, the application might not be clearing old session identifiers.



IN BOTH CASES, THE SESSION IDENTIFIERS ARE LEFT USABLE LONG AFTER THE USER HAS DISCONNECTED.

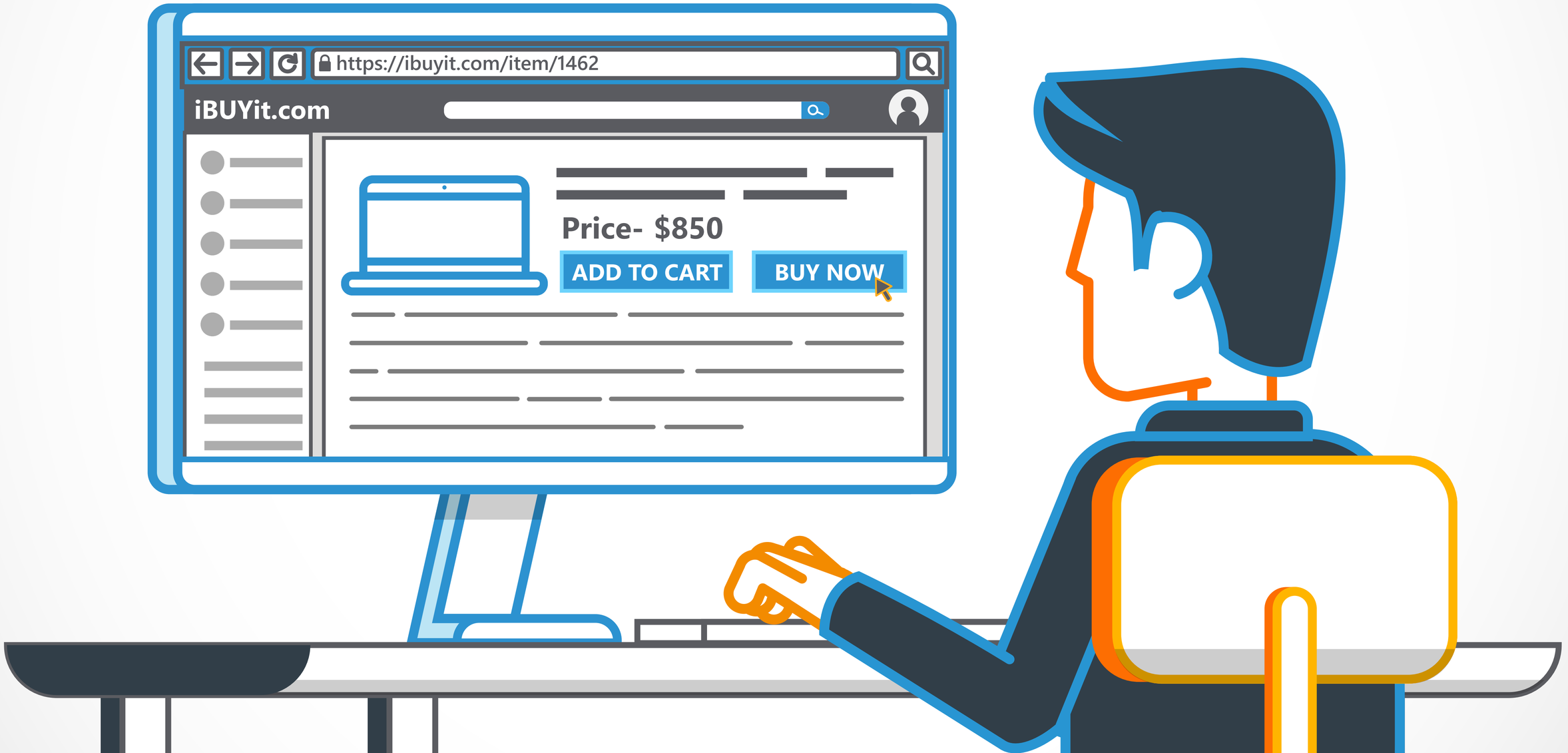
LET’S LOOK AT AN EXAMPLE

A user is browsing an online marketplace on a public computer.



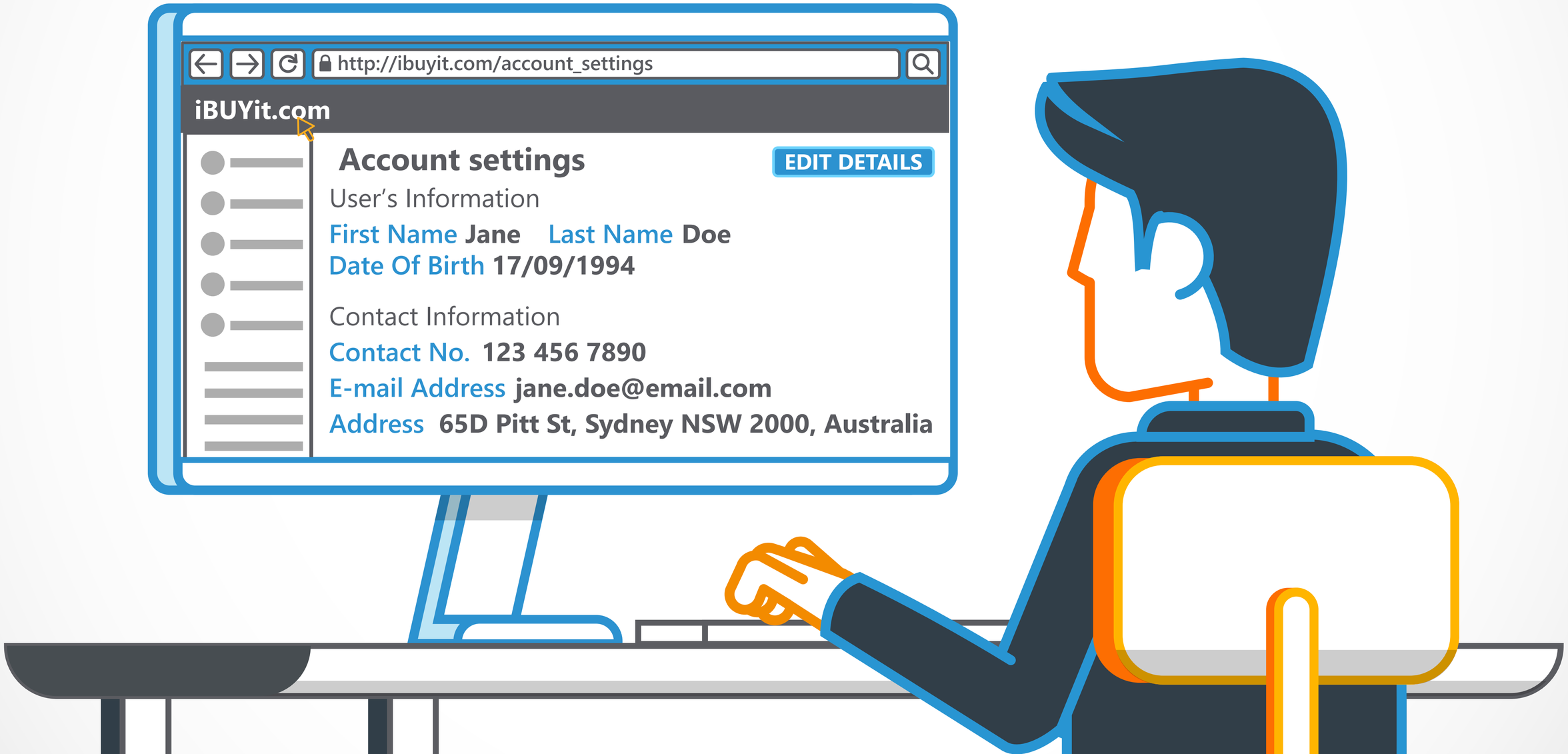
A power cut causes the machine to shut down before they can log out.

Some time later, another user is using the same computer.



Browsing to the same marketplace, they find that the machine is already logged in to the previous user's account.

Now, the new user has access to the previous user's private information, including their name, shipping address, email address and past orders



If an “instant payment” solution is set up, they can also create orders as that user.

To avoid attacks relating to Insufficient Session Expiration, developers should:

- Time-out the session after a long period of inactivity
- Invalidate the session in the event of an identity mismatch
- And finally, require password confirmation for any potentially sensitive account operations

Congratulations, you have now completed this module!

SECURE CODE
WARRIOR

www.securecodewarrior.com