



SECURE CODE WARRIOR

INSUFFICIENT SESSION EXPIRATION

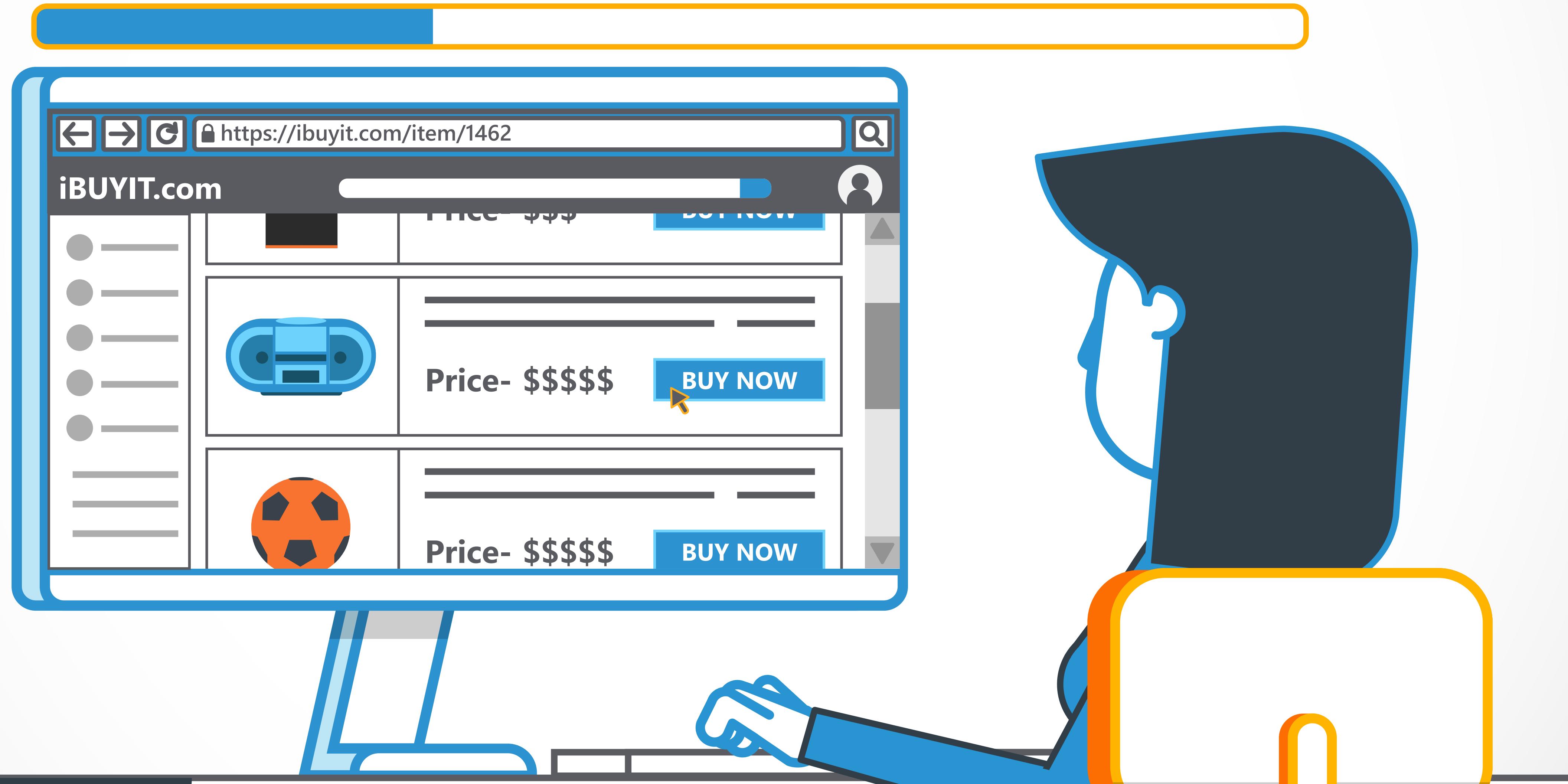
We'll go through

some causes and preventions of
vulnerabilities in this category.

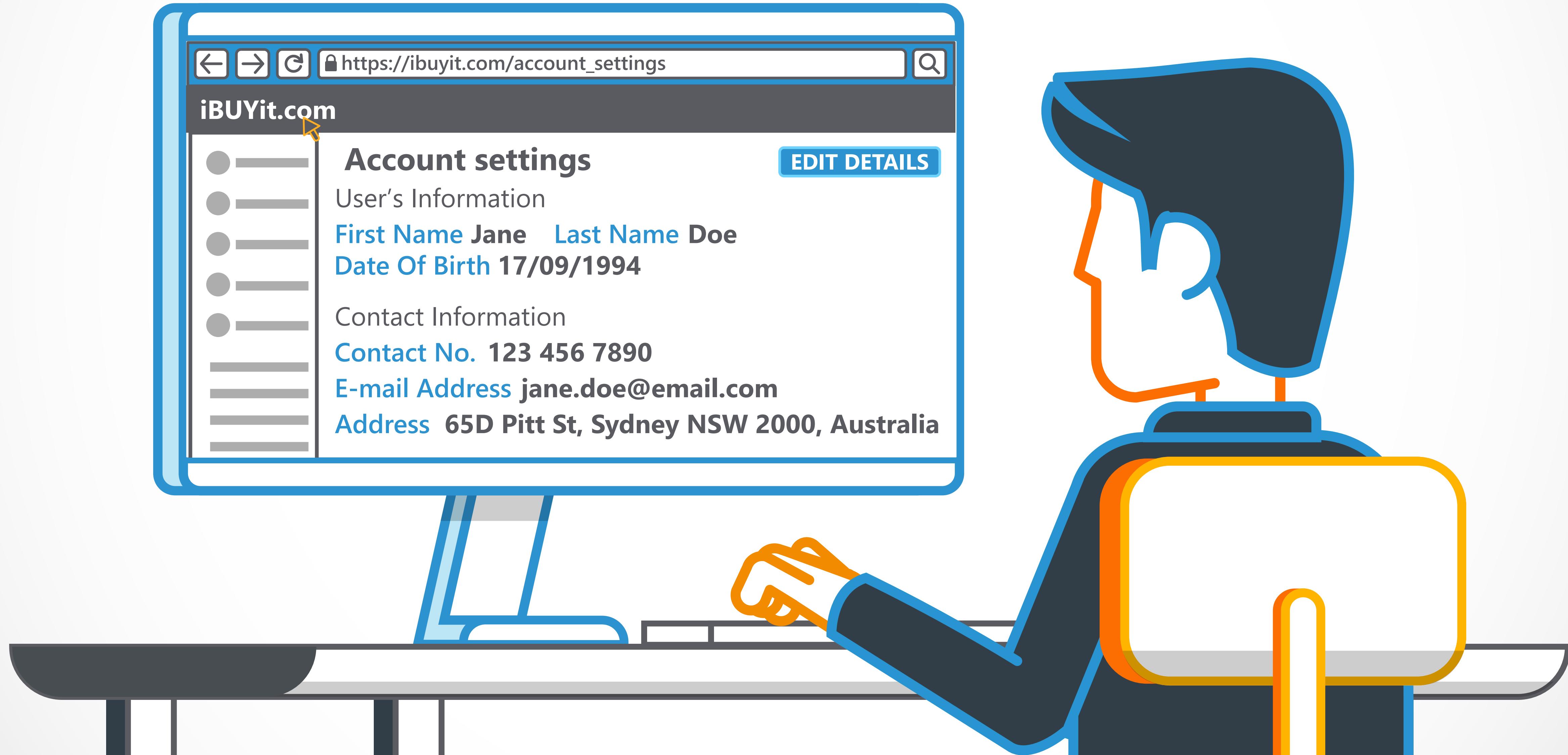
**WHAT DO WE MEAN BY
INSUFFICIENT SESSION EXPIRATION?**

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

Session Token Timer



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.

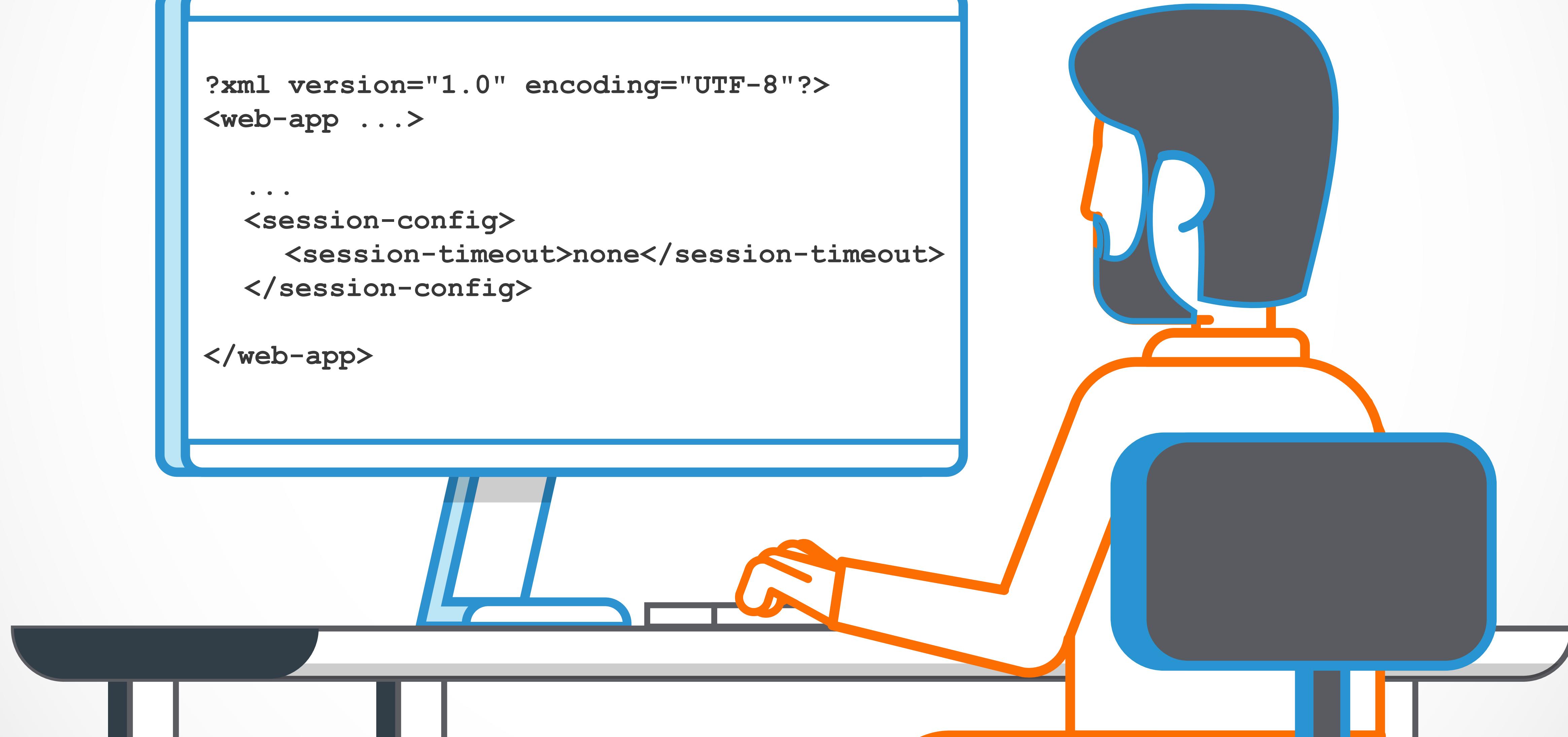


Insufficient Session Expiration vulnerabilities usually occur when an application is not setting a time-out on session identifiers.

```
?xml version="1.0" encoding="UTF-8"?>
<web-app . . .>

. . .
<session-config>
    <session-timeout>none</session-timeout>
</session-config>

</web-app>
```



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

Stored Session Identifiers

3a658d762bc4658fd742445a65345

a354d6957e45456ab36752ef5

326ef56732a456364bc362542456a65423bc6563

3a658d762bc4658fd742445a663255345

632a7563ab6321423ef3652145bc3214a62365ef632145

2206a6327e3641253ef365423623bc365236523622a

ab3625763e362517e362456

3a658d762bc4658fd742445a65345

a354d6957e45456ab36752ef5

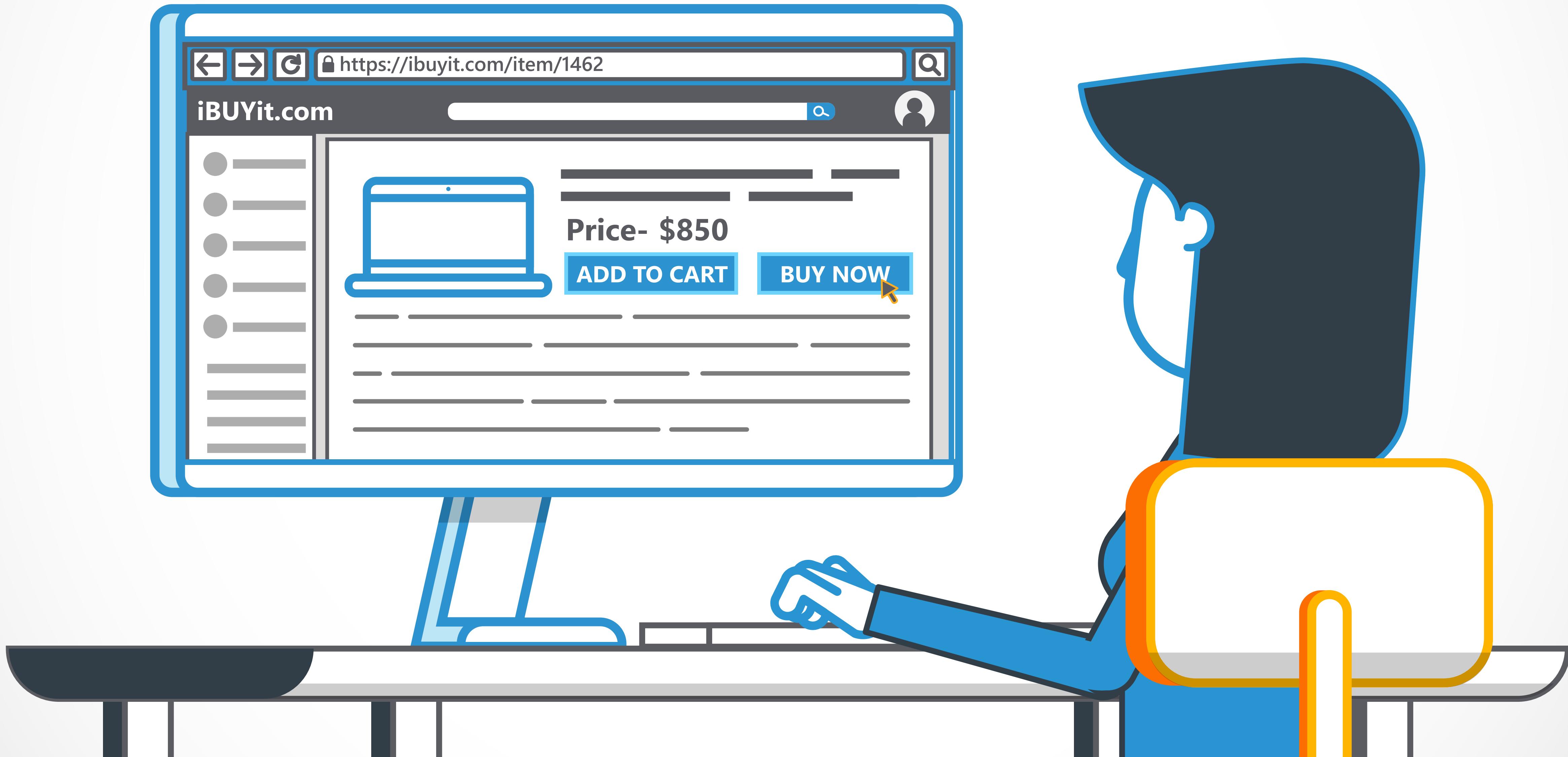


Clear all

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

LET'S LOOK AT AN EXAMPLE

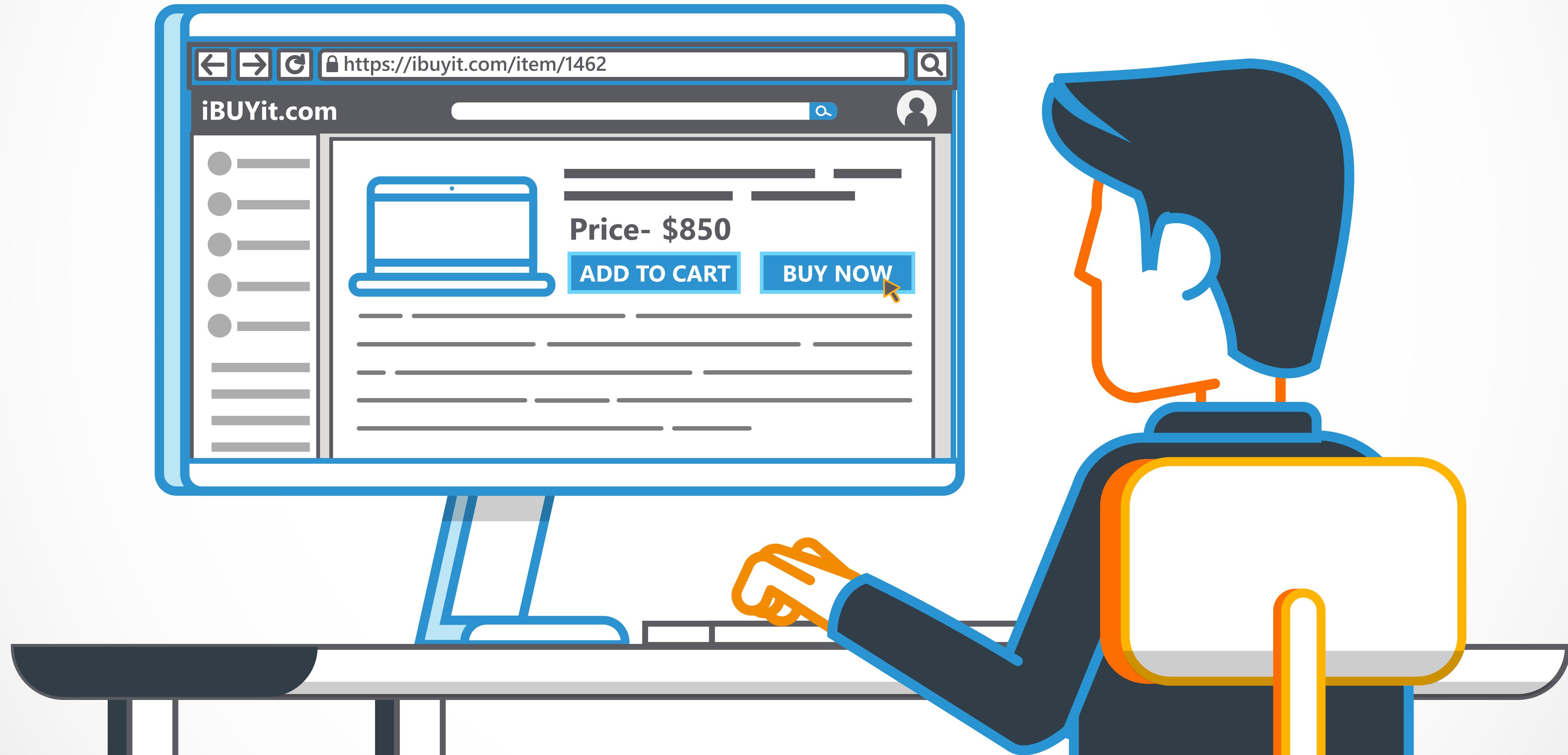
A user is browsing an online marketplace on a public computer.



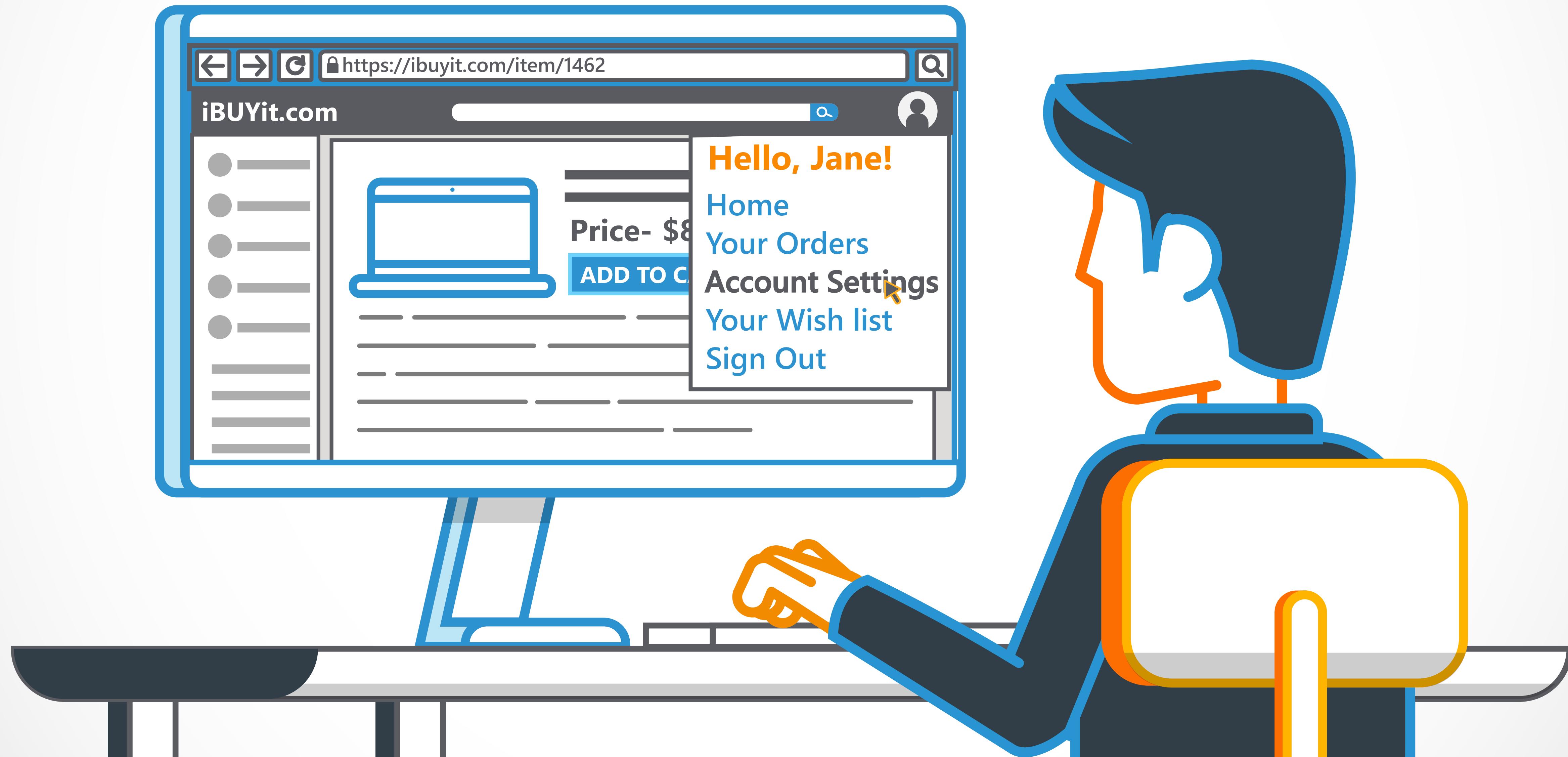
A power cut causes the machine to shut down before they can log out.



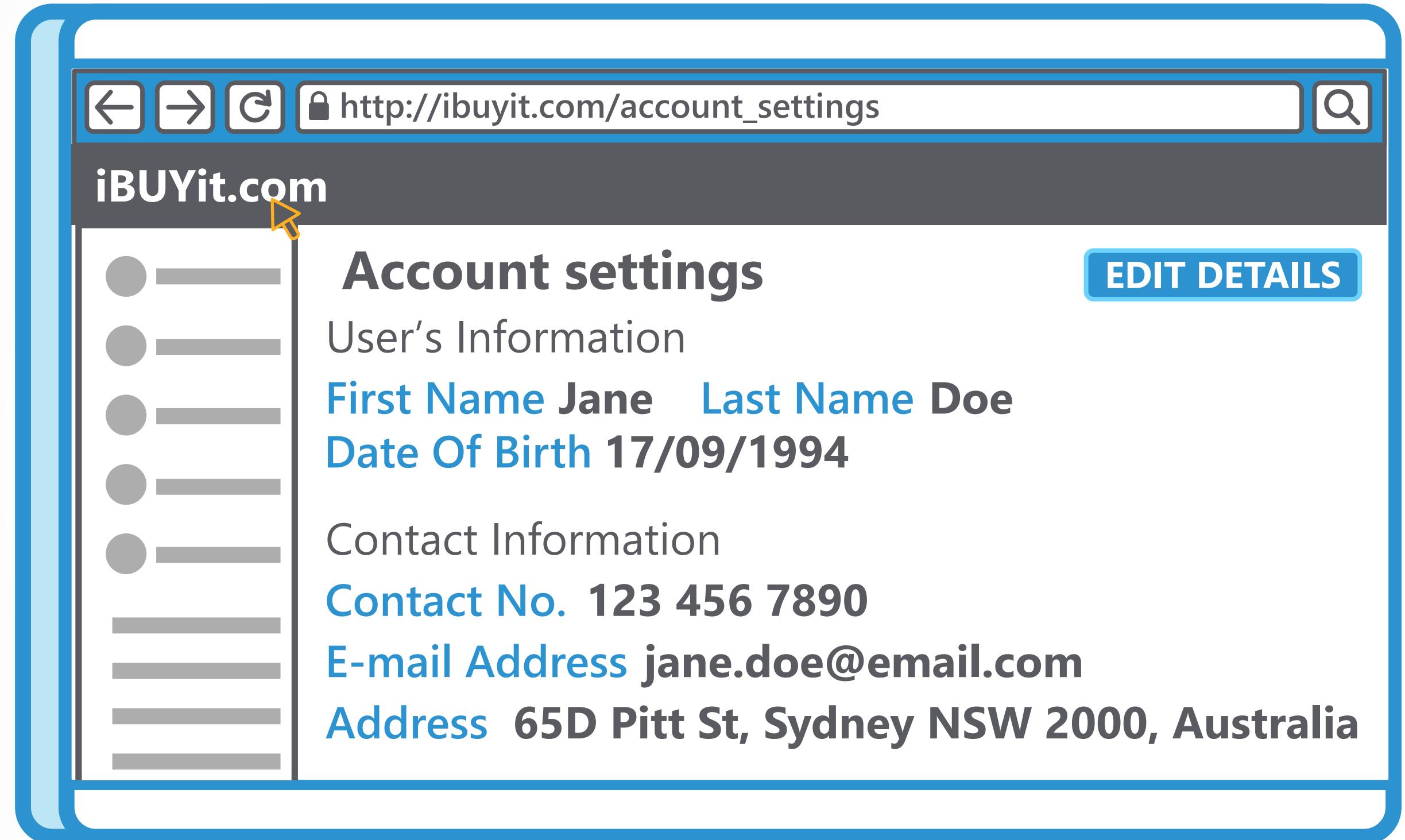
Some time later, another user is using the same computer.



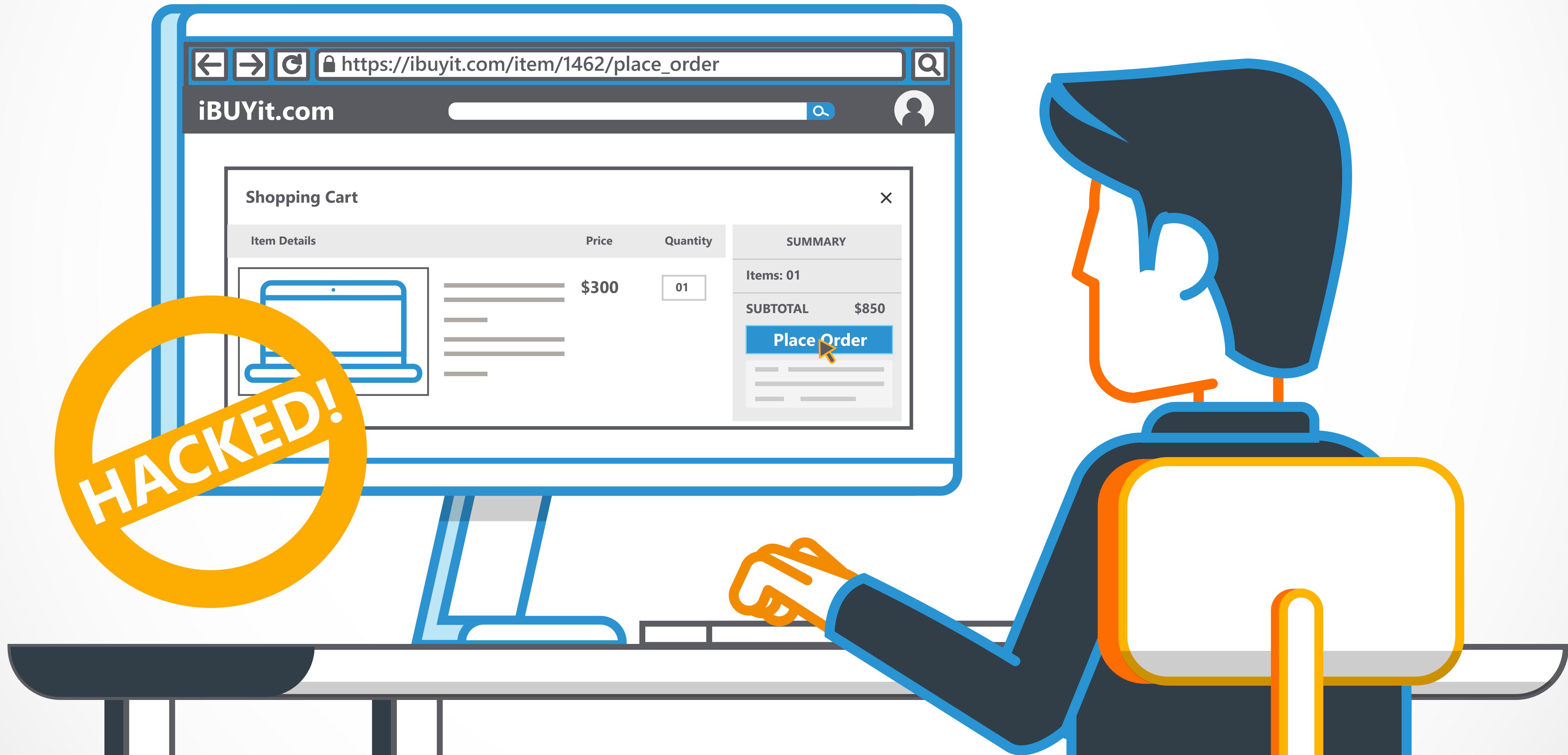
Browsing to the same marketplace, they find that the machine is already logged in to the previous user's account.



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:

- ④ Time-out the session after a long period of inactivity
- ④ Invalidate the session in the event of an identity mismatch
- ④ And finally, require password confirmation for any potentially sensitive account operations

Congratulations, you have now completed this module!



**SECURE CODE
WARRIOR**

www.securecodewarrior.com