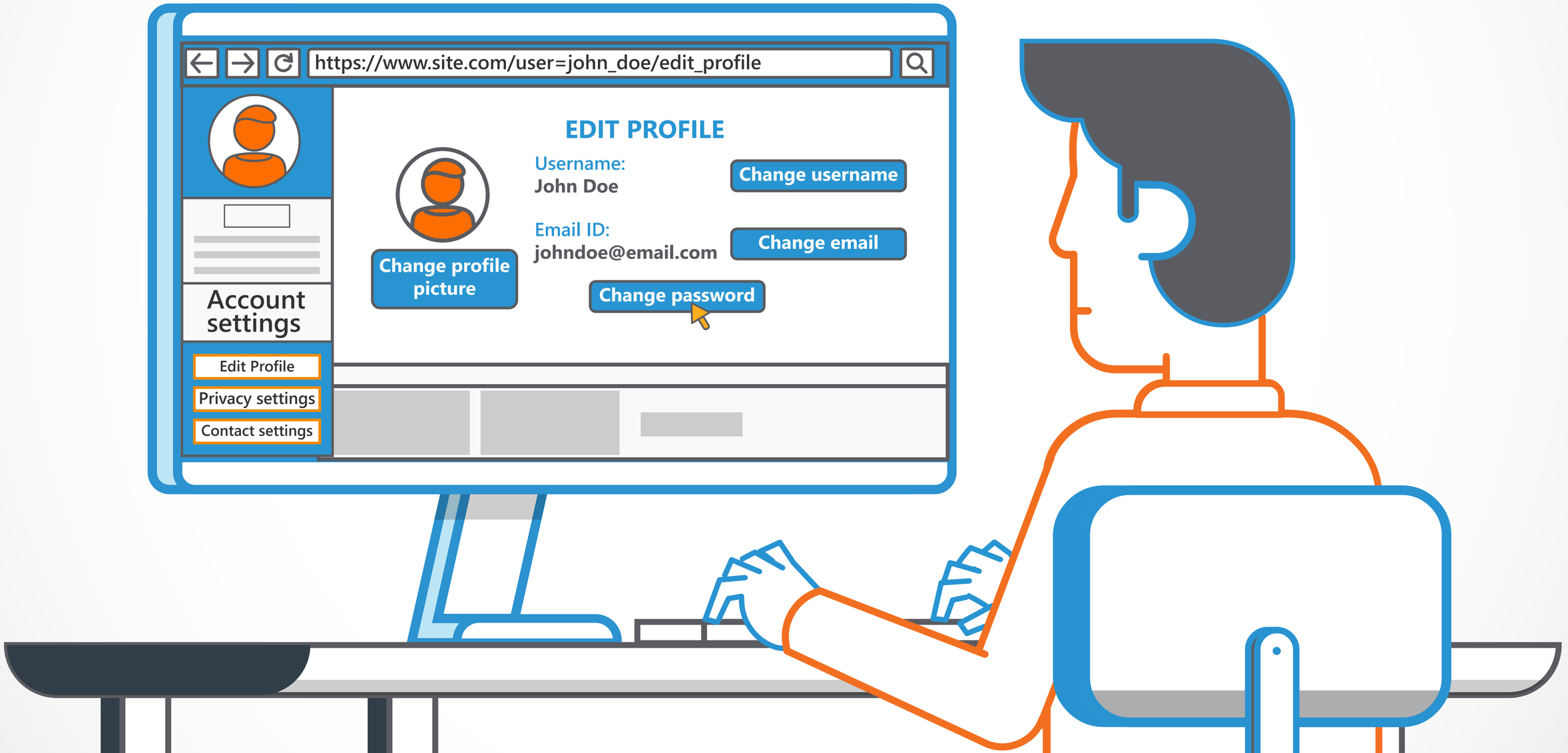
SECURE CODE WARRIOR

INSECURE PASSWORD CHANGE FUNCTIONS

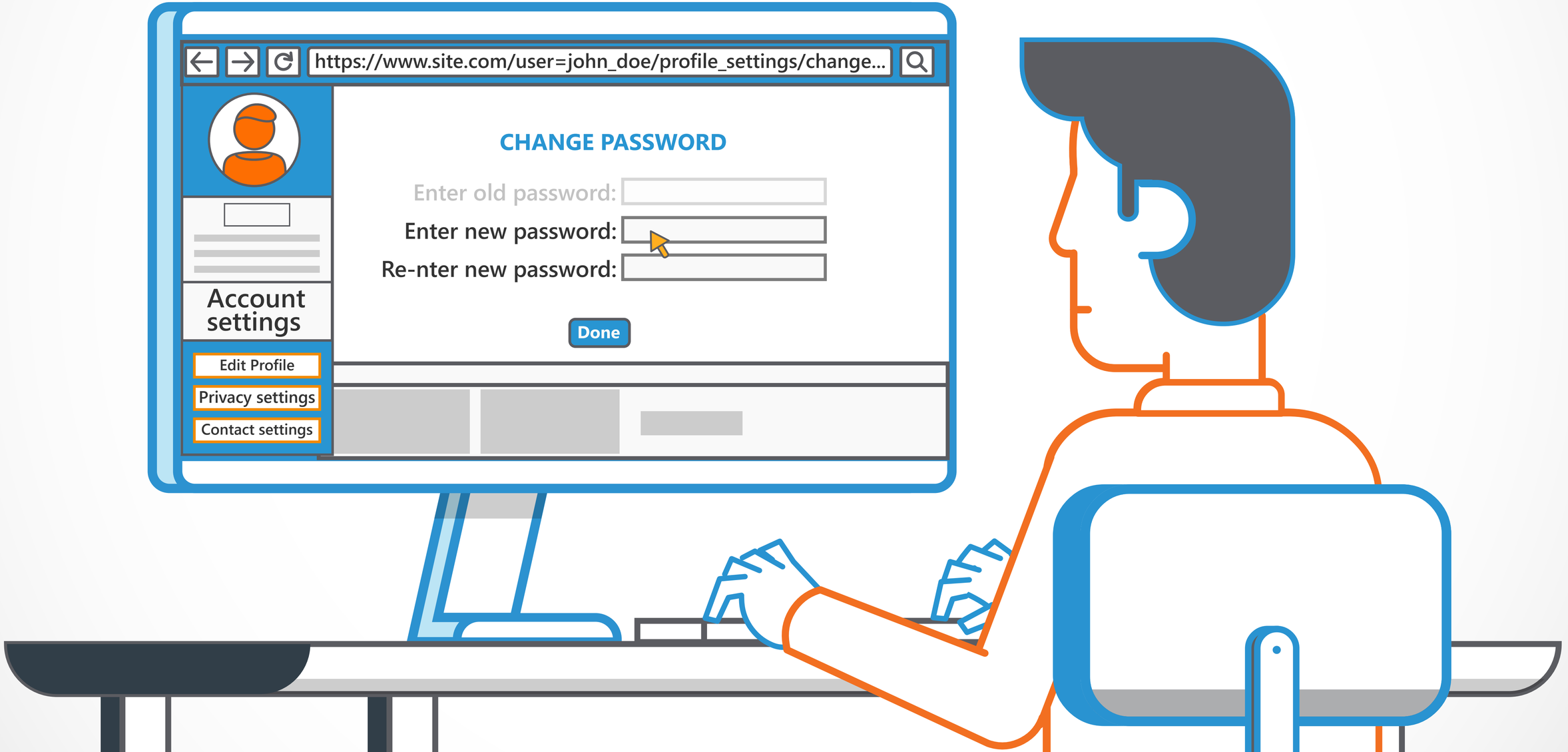
We'll go through

some causes and preventions of vulnerabilities in this category

An Insecure Password Change Function is an authentication vulnerability that affects users

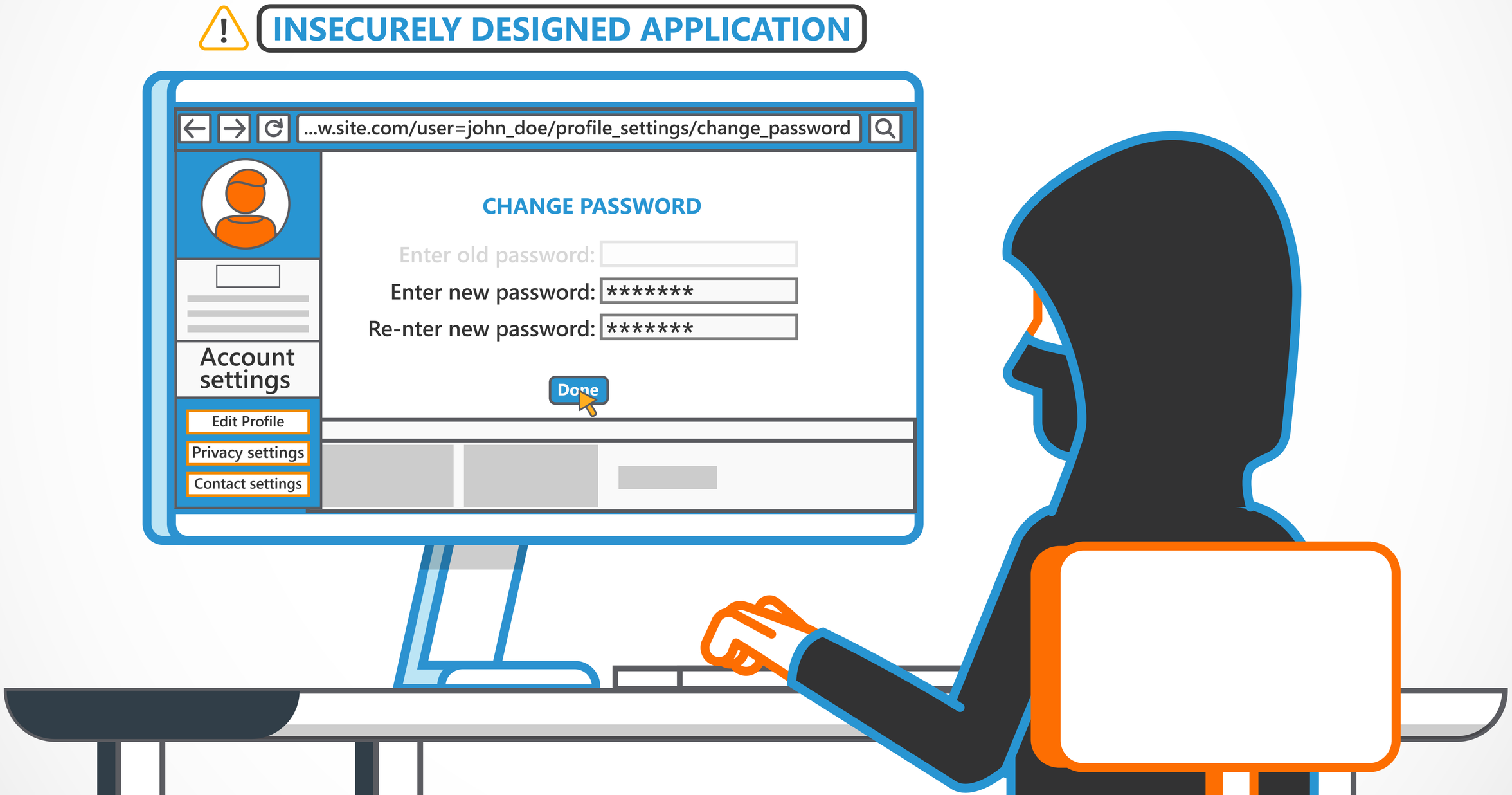


who need to create a new password for any reason, through the self-service ‘Change Password’ function.

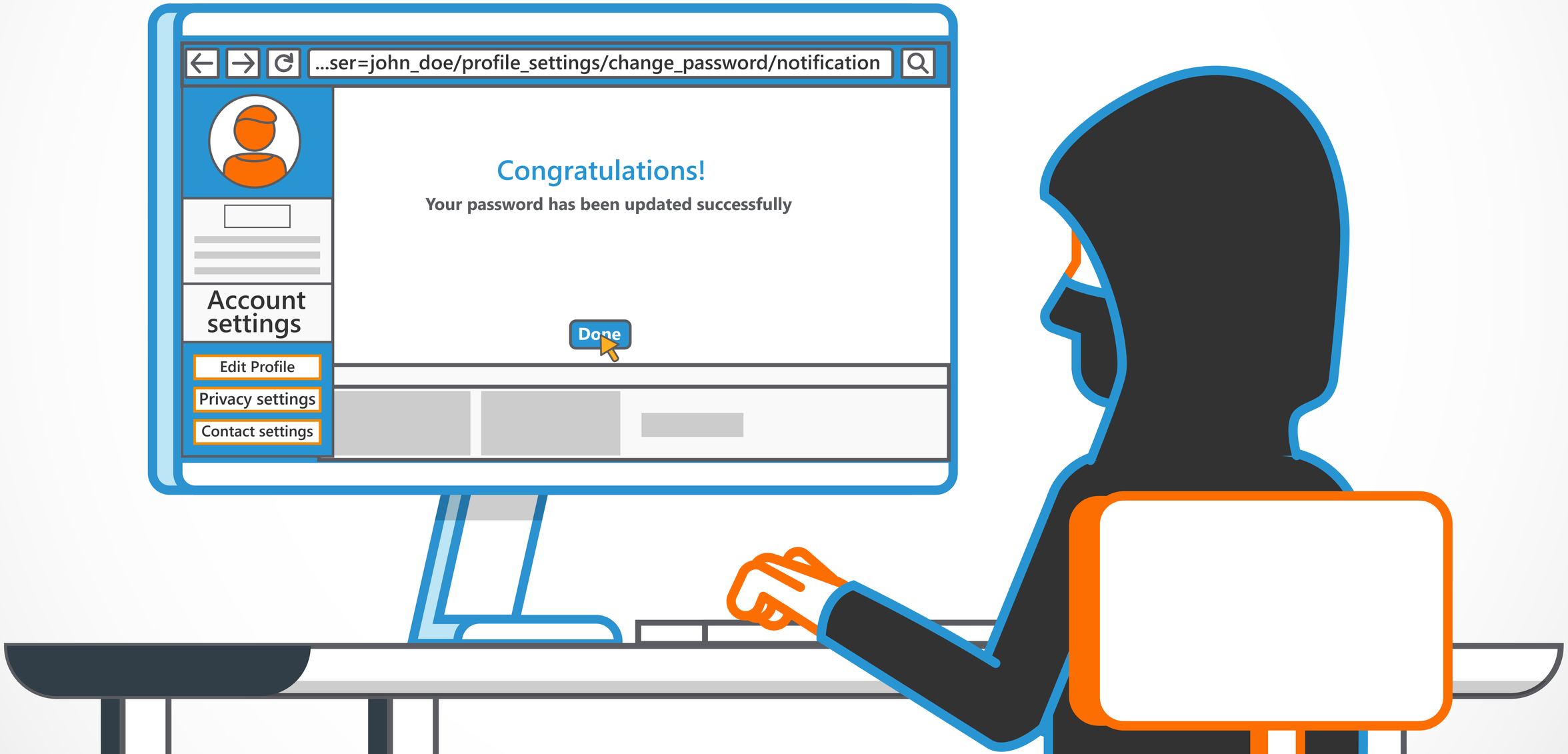


HOW IS THIS VULNERABILITY A RISK?

Insecure Password Change Functions make it possible for unauthorised password changes,

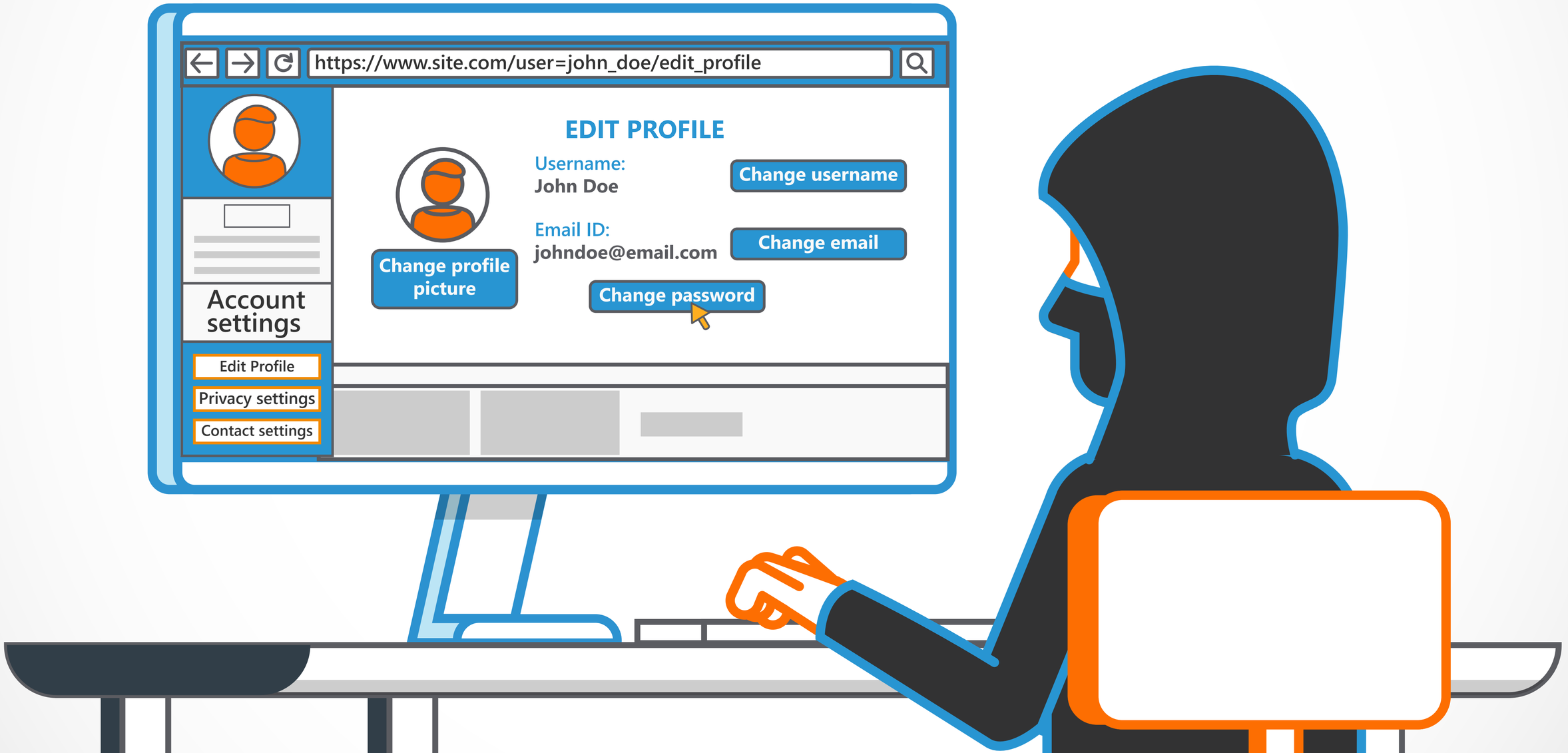


which can result in account compromise.



Unauthorised password changes can happen when the application fails to appropriately verify user identity.

It can also happen when administrative password change functionality is abused

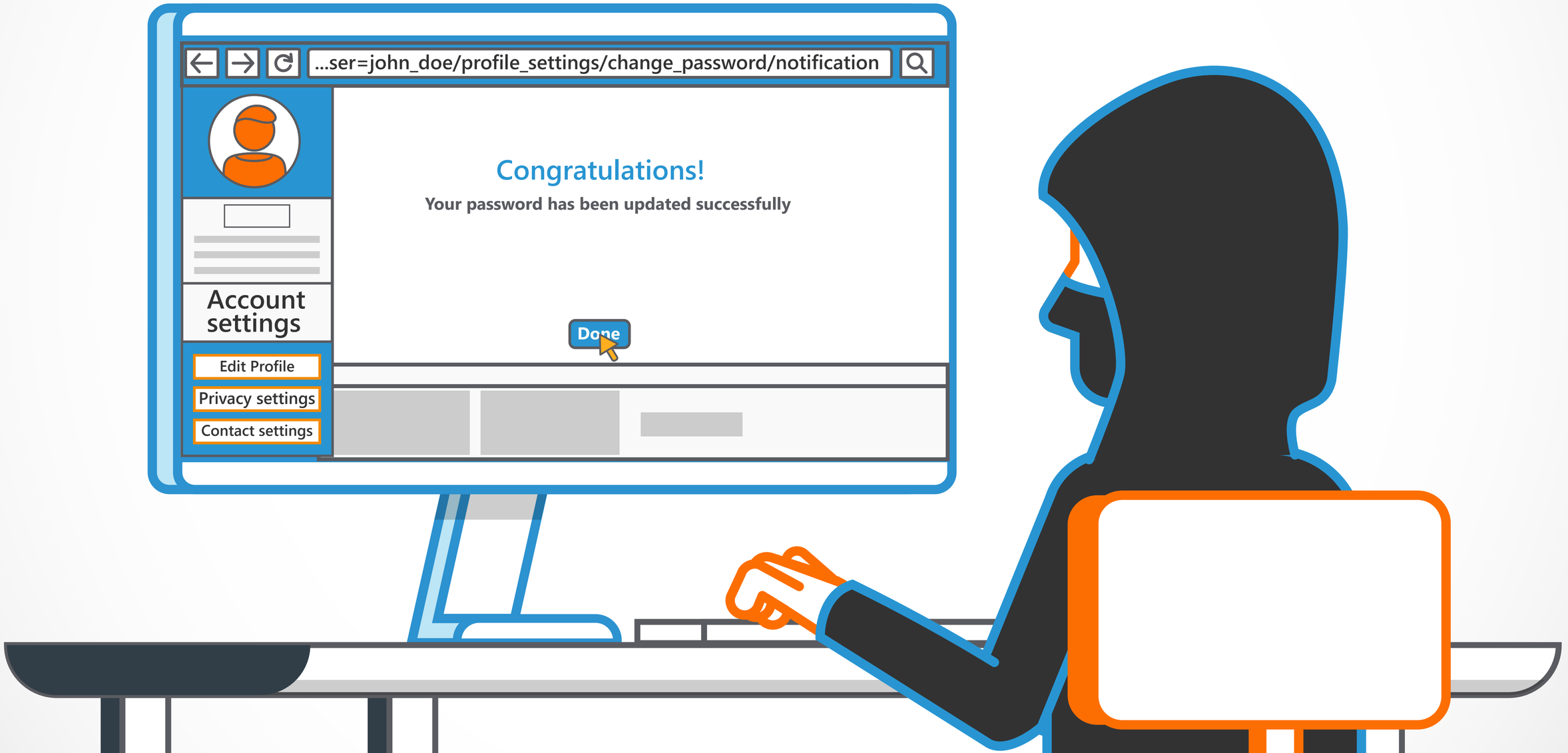


or when other weaknesses exist in the password change process.

So when a user is not required to identify themselves before changing a password

or if the user can manipulate the password change process,

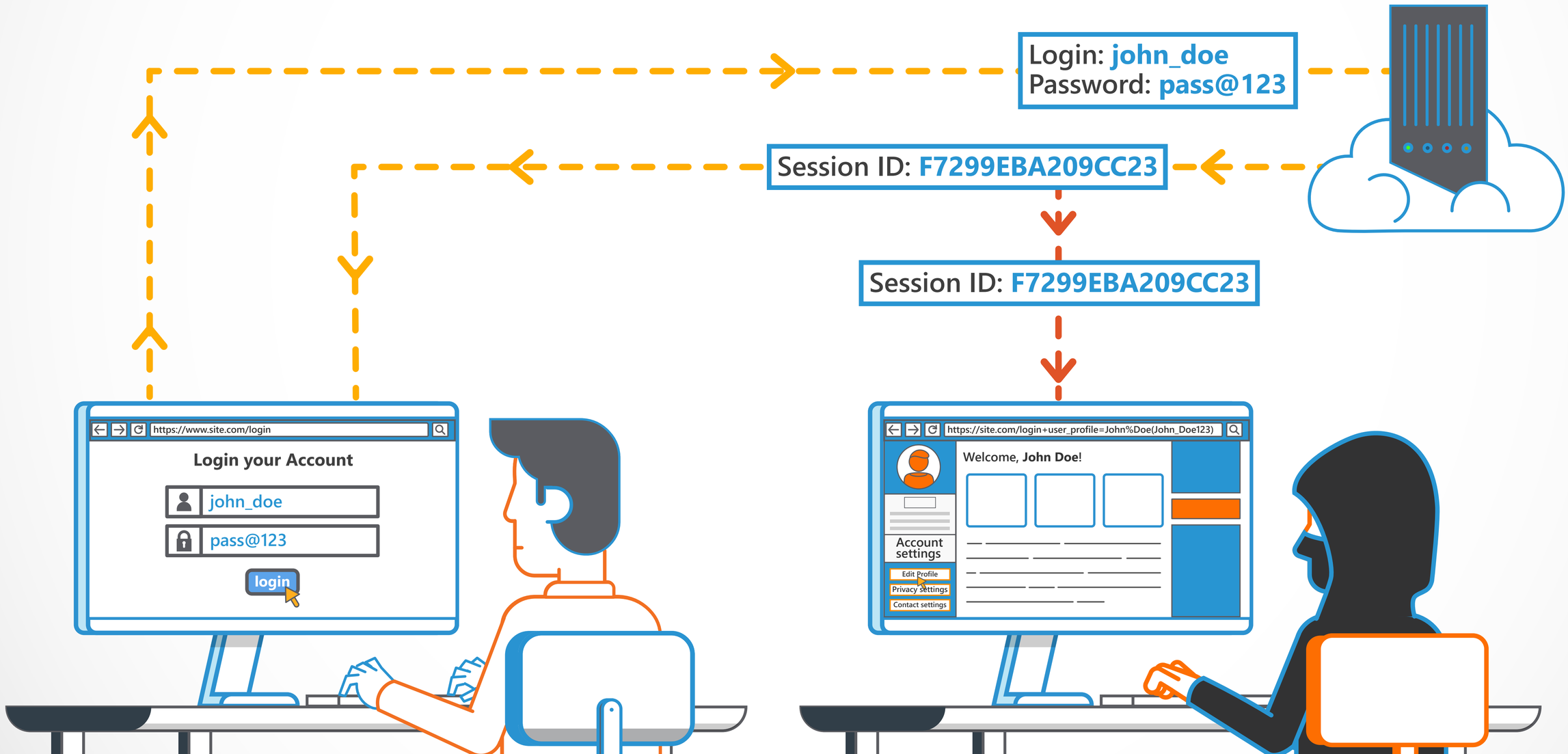
they are able to change the password on another user's account.



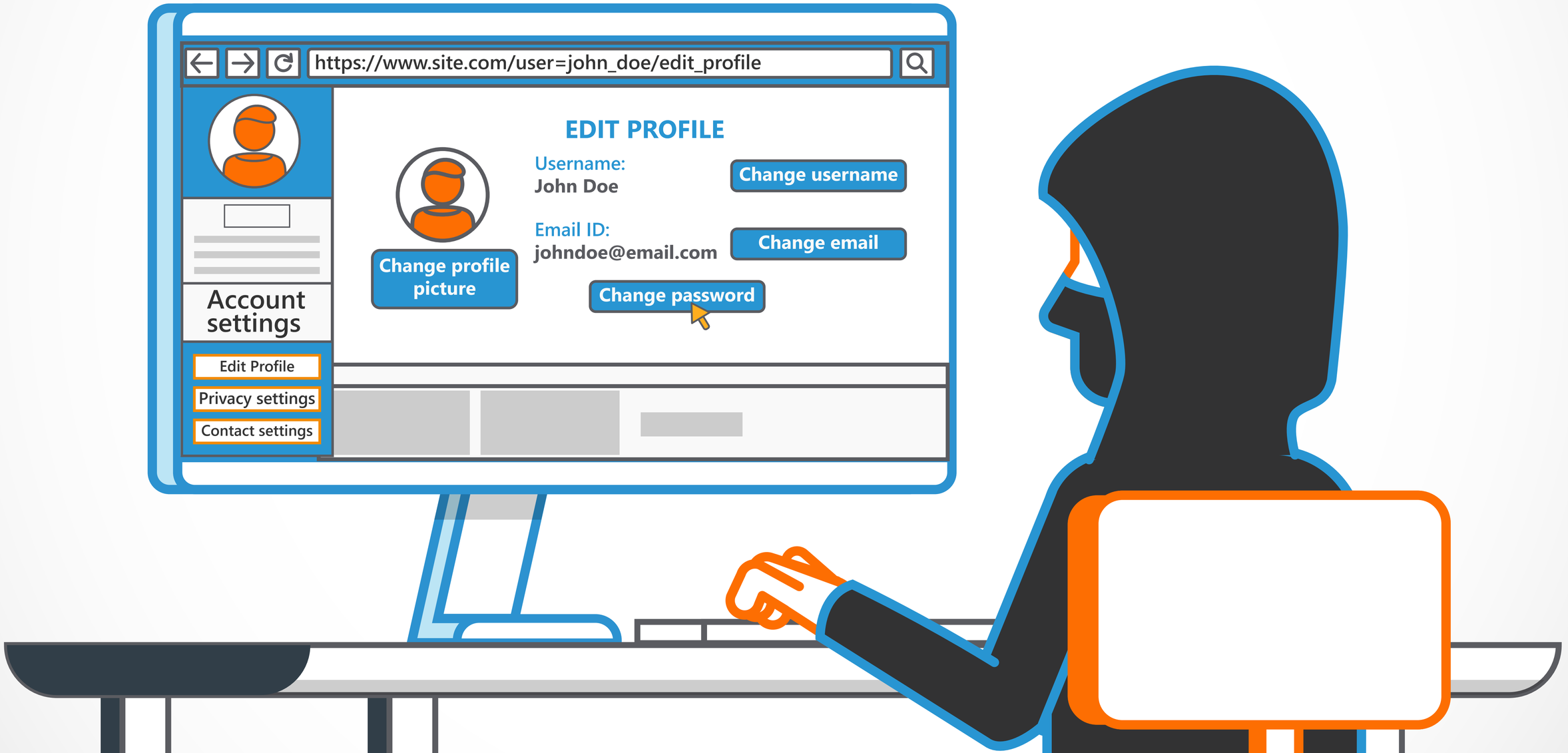
LET’S LOOK AT AN EXAMPLE

Here, an attacker has gained access to a victim's account using Session Hijacking.

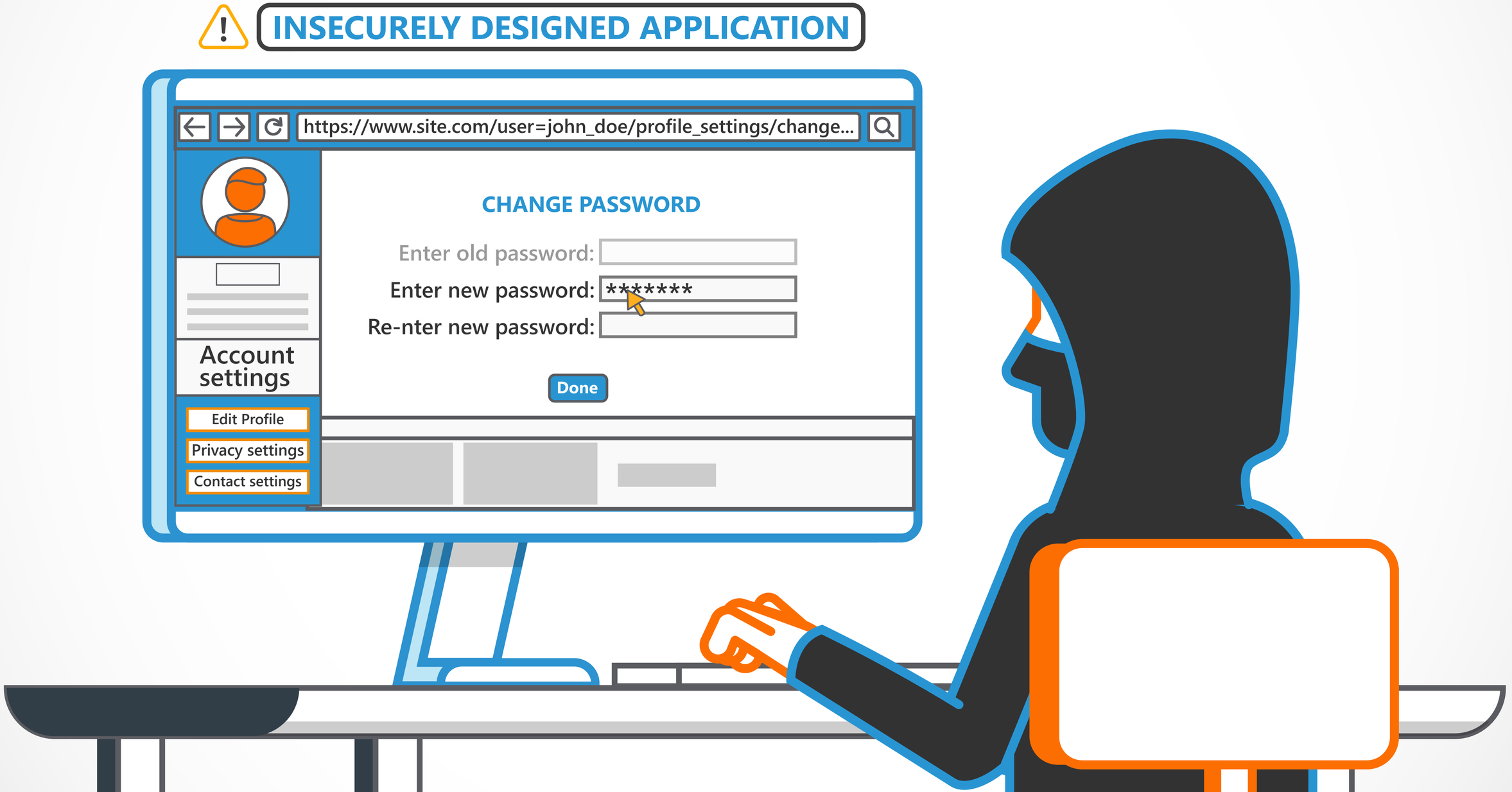
SESSION HIJACKING



To make matters worse, the attacker decides to change the user's password.

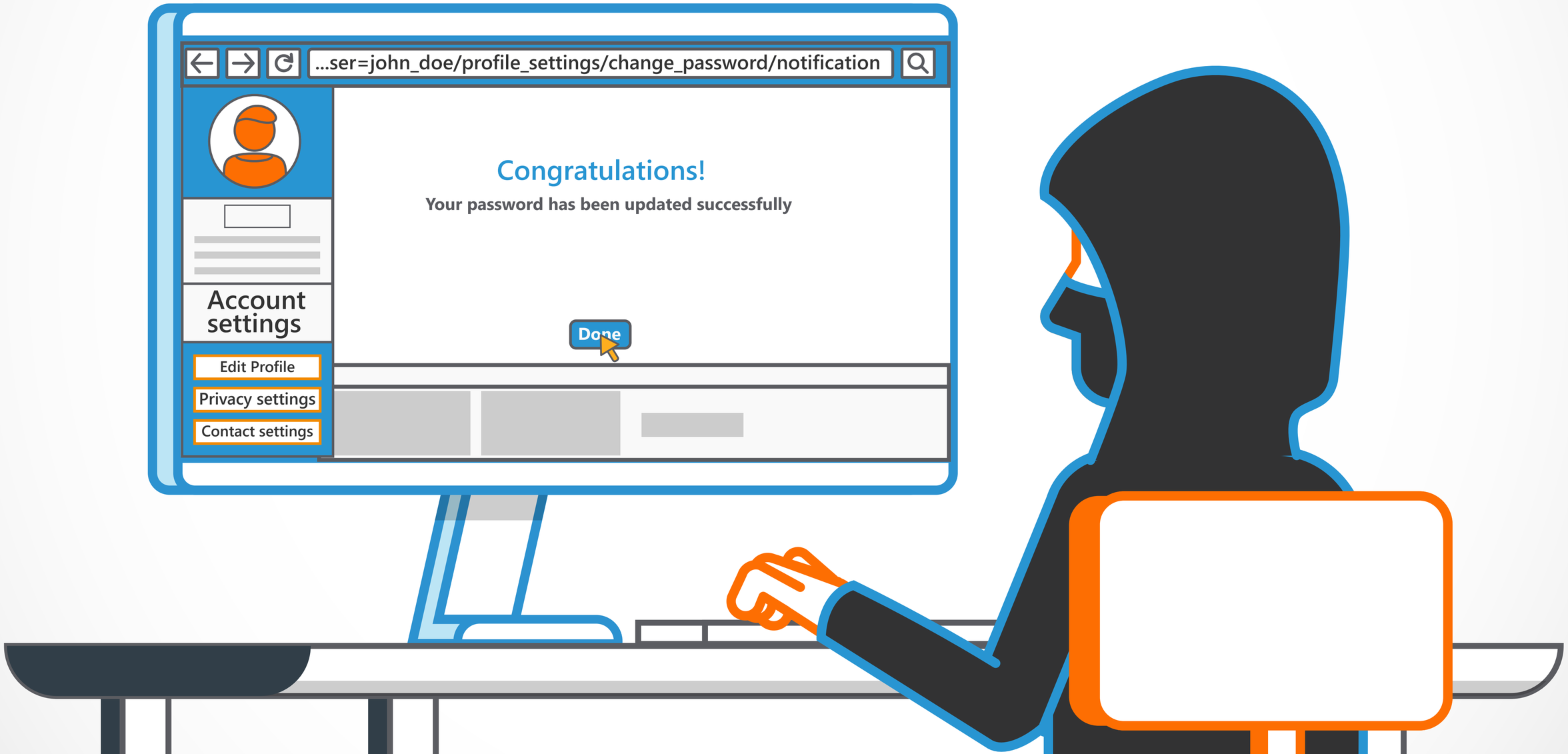


Unfortunately this application is not securely designed,



and does not require the user to enter their current password before changing and confirming a new password.

So the attacker easily changes the password, and now has control over the victim’s account.



To prevent insecure password change function vulnerabilities, developers should:

- Carefully inspect password reset pages
- Ensure password changes require identity verification
- Require users to enter their current password along with the new password

To prevent insecure password change function vulnerabilities, developers should:

- Check that the user ID is not being included in the request and that the application is not using this value to select the user for whom the password change will occur
- Ensure that pages which allow administrators to change user passwords require appropriate privileges to use the functionality

Congratulations, you have now completed this module!

SECURE CODE
WARRIOR

www.securecodewarrior.com