SECURE CODE WARRIOR®

INSECURE RANDOMNESS

We’ll explain

What Insecure Randomness is, its causes, preventions and some potential hazards.

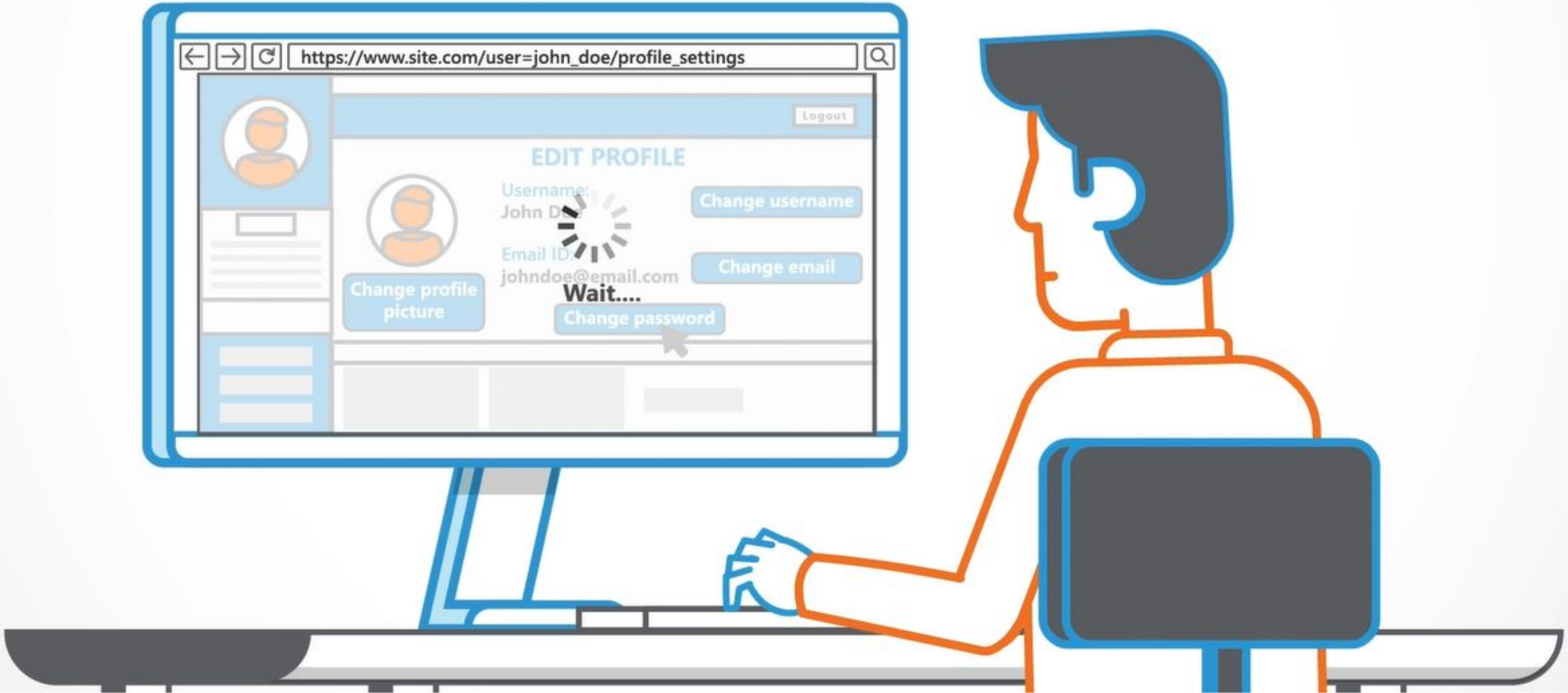
WHAT IS INSECURE RANDOMNESS?

Insecure randomness refers to a situation where predictable values ("Seeds") are generated

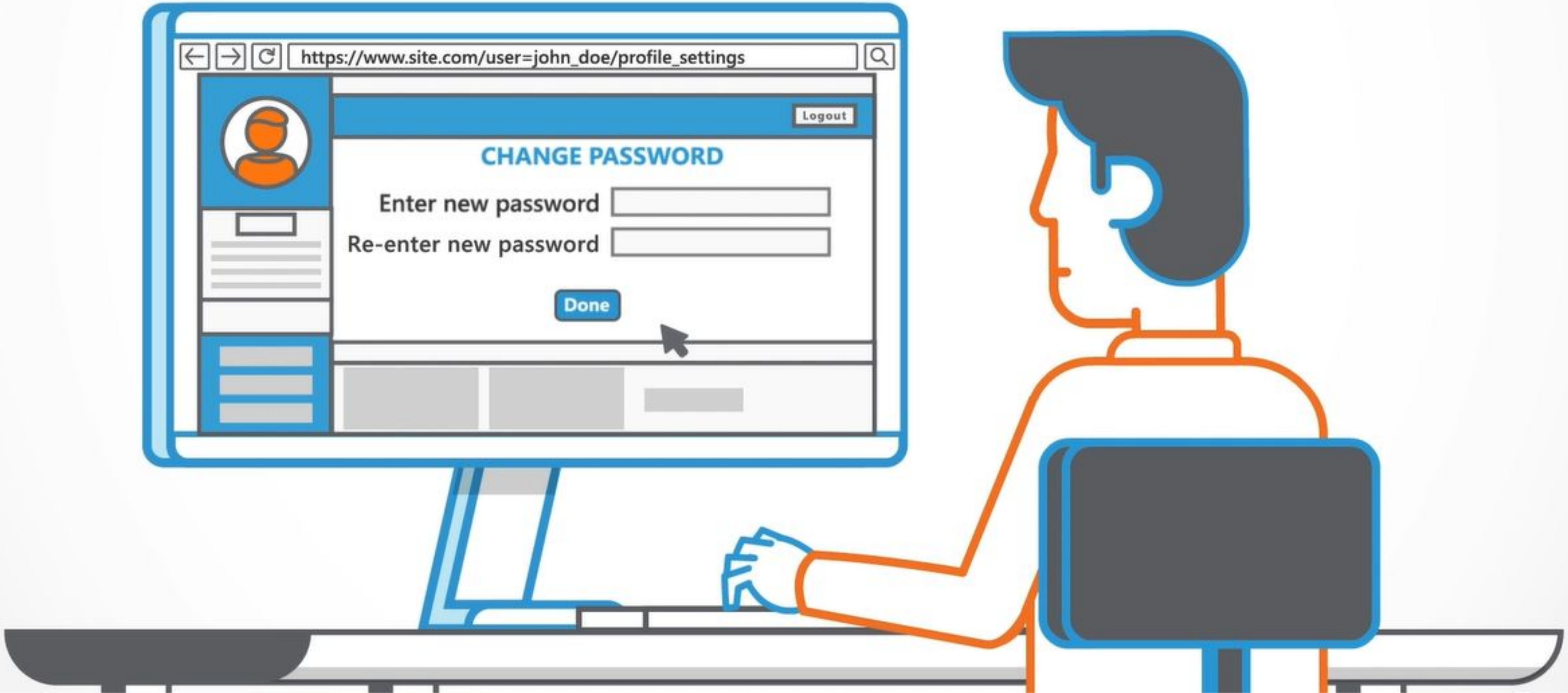
Request: Change password

```
https://www.site.com/password-reset?token=<TOKEN STRING>
```

TOKEN = `base64(date.today + username)`

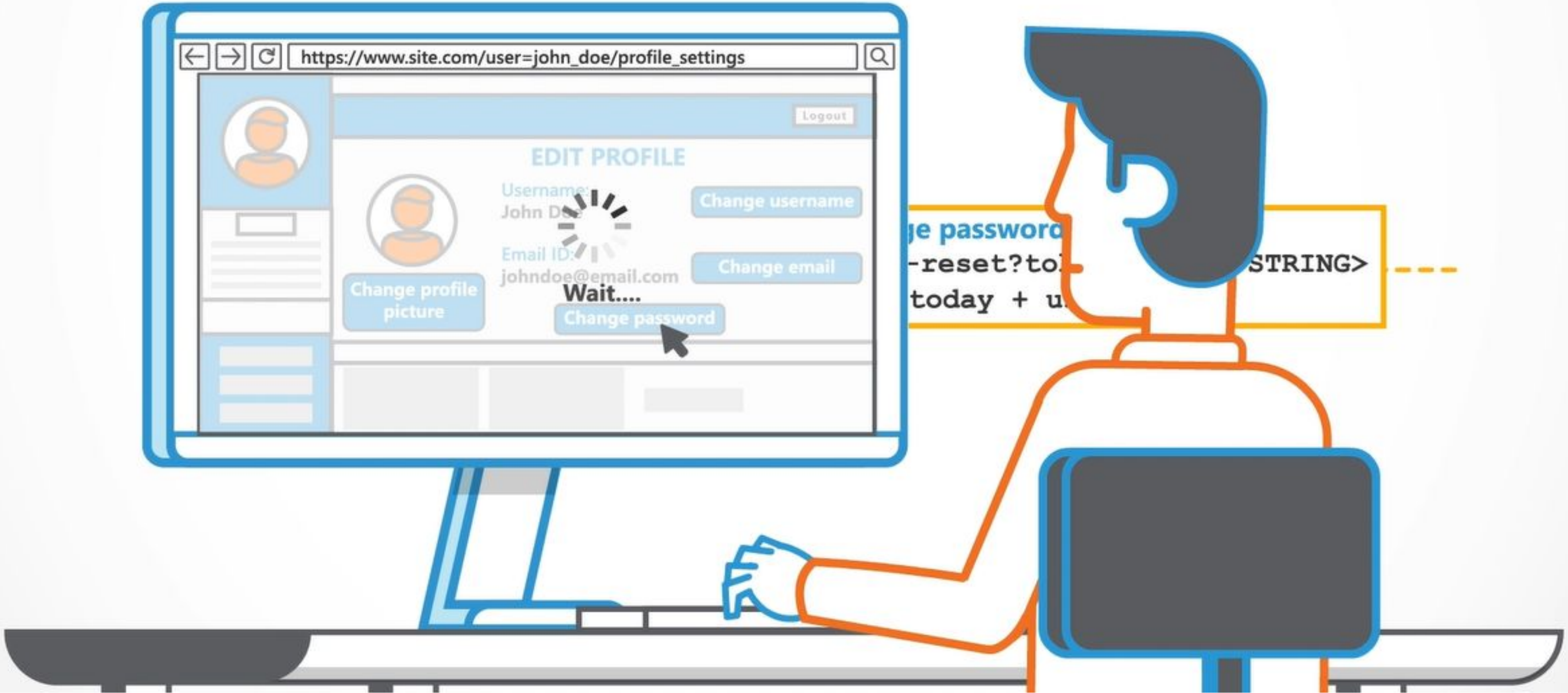


in a context requiring unpredictability.



WHAT CAUSES INSECURE RANDOMNESS?

Insecure randomness errors occur when a function that can produce predictable values is used as a source of randomness in a security-sensitive context.

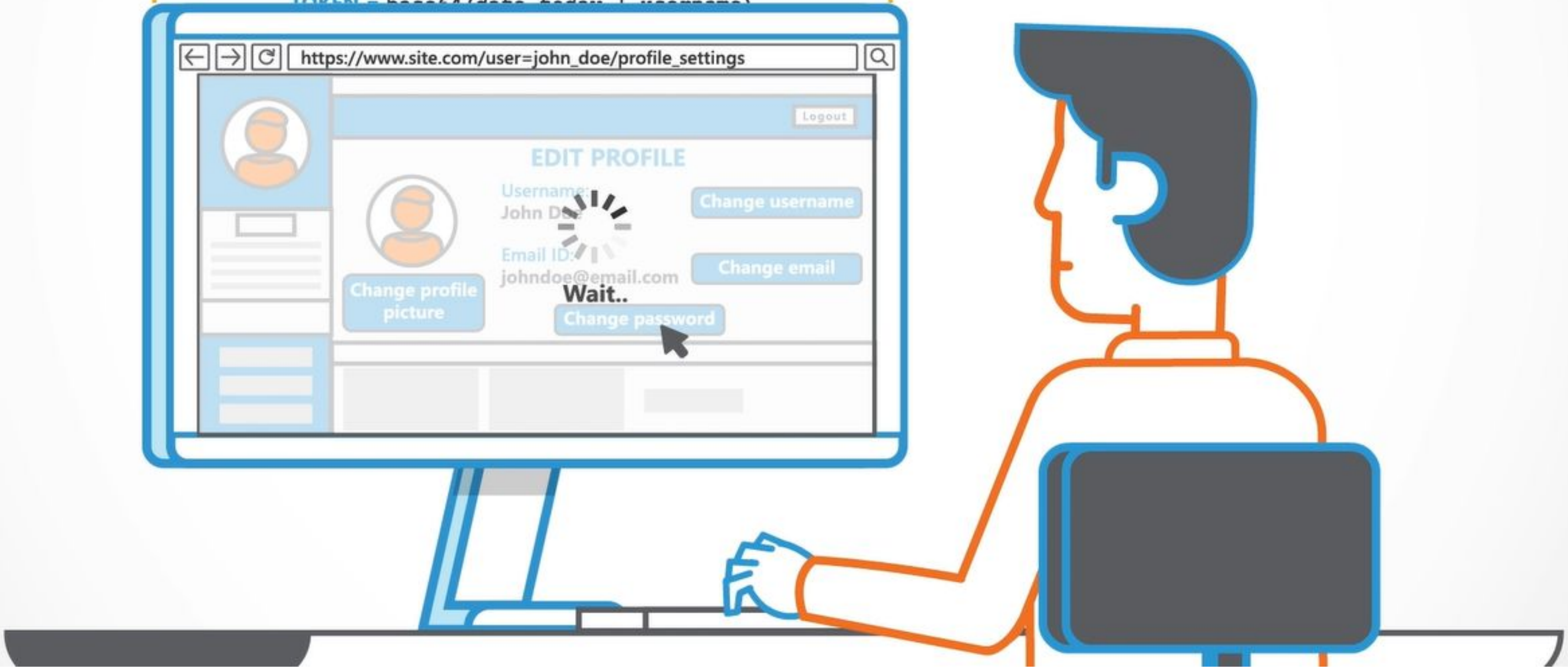


LET'S LOOK AT AN EXAMPLE

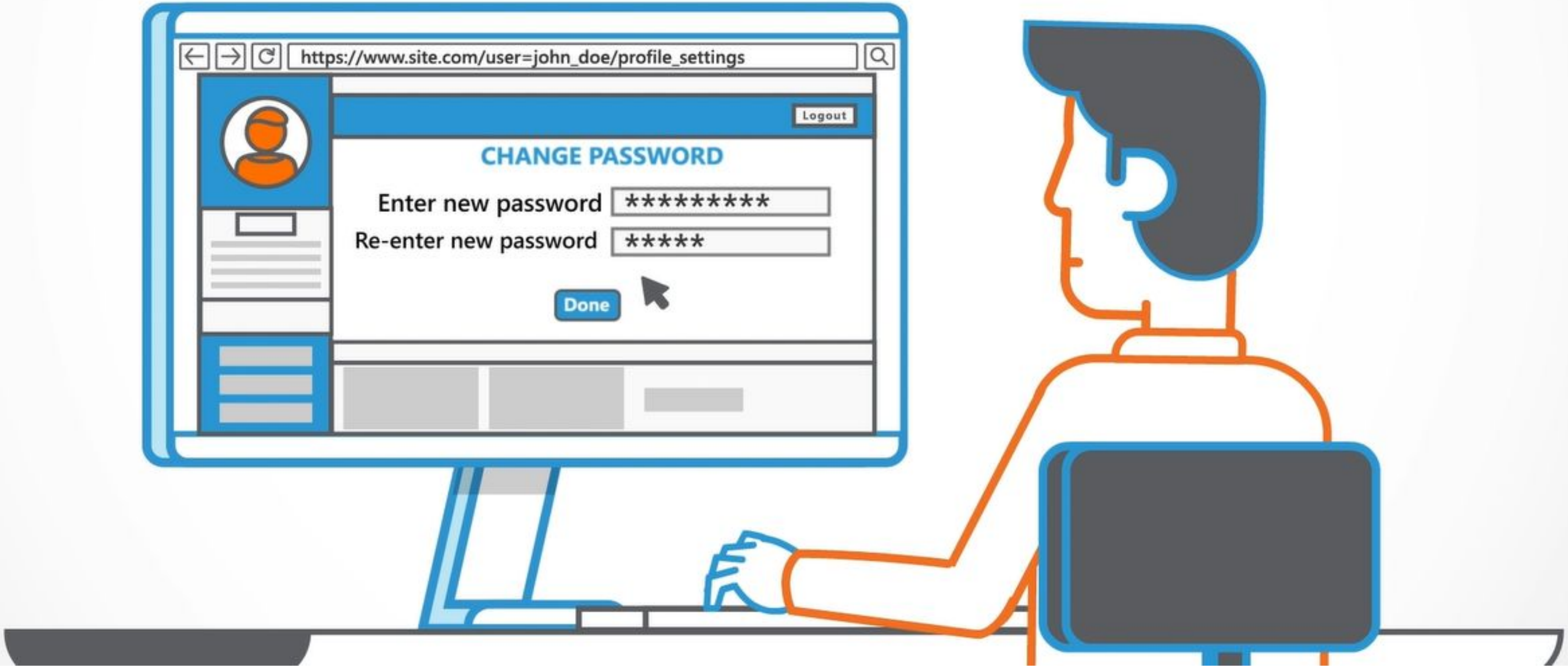
Let’s say a program generated a random string to reset a user’s password.

Response: Change password

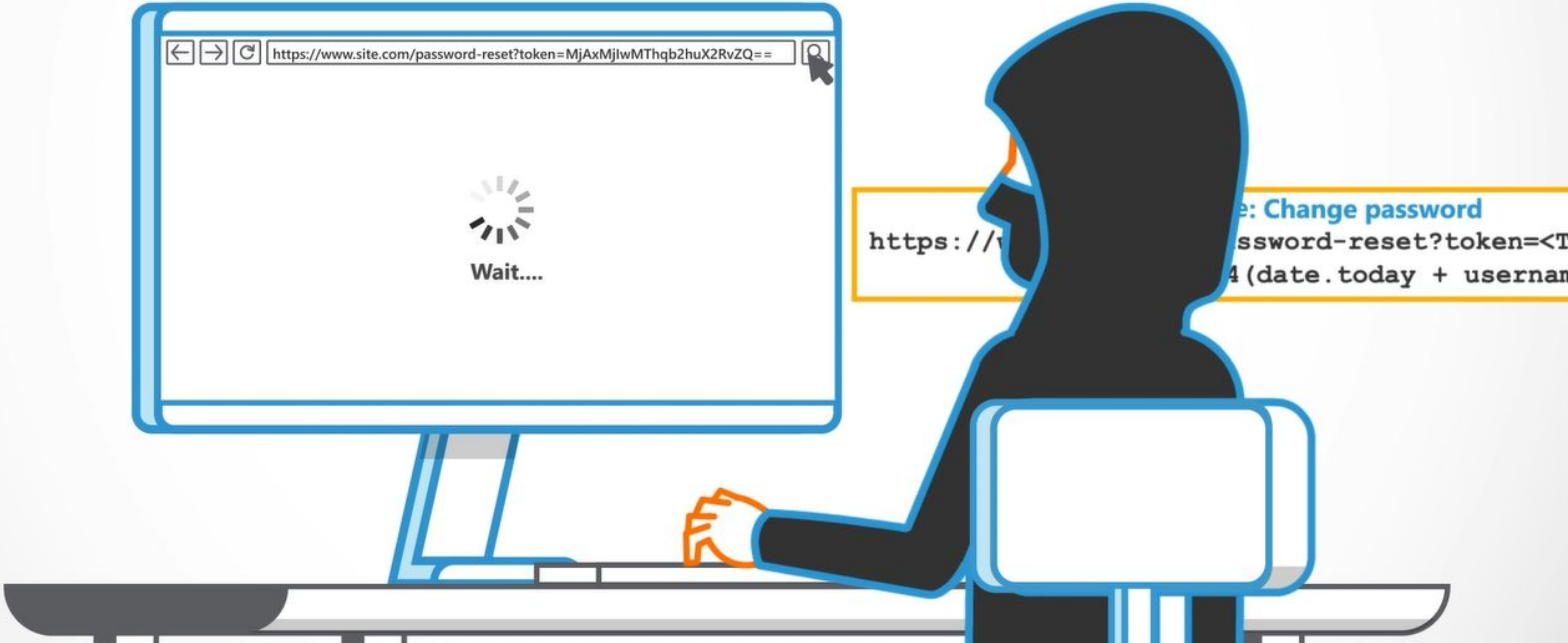
```
https://www.site.com/password-reset?token=<TOKEN STRING>
TOKEN = base64(date_today + username)
```



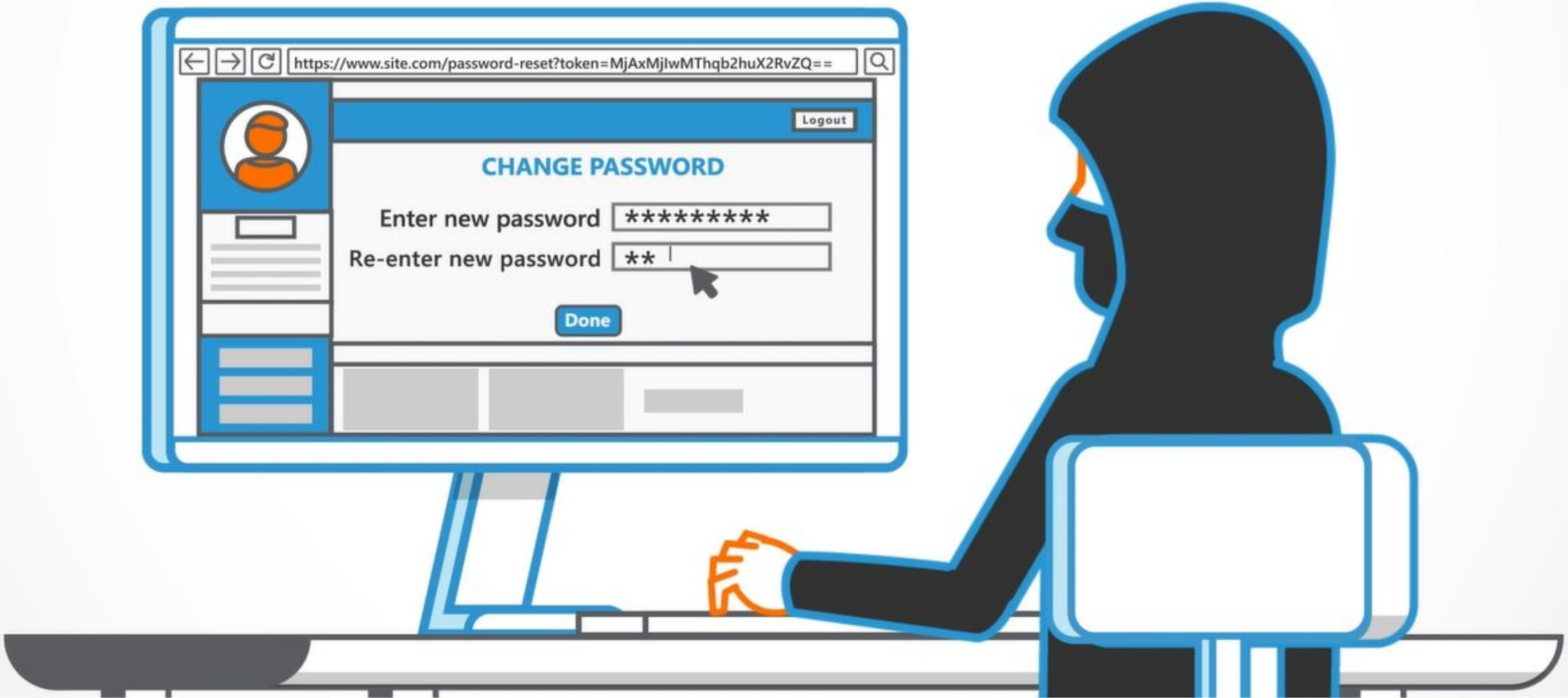
Unfortunately the function that produces the string outputs predictable values.


https://www.site.com/user=john_doe/profile_settings
Logout
CHANGE PASSWORD
Enter new password **********
Re-enter new password *****
Done

So, an attacker is able to guess or calculate the value generated for the user's account.



The attacker can now reset the password



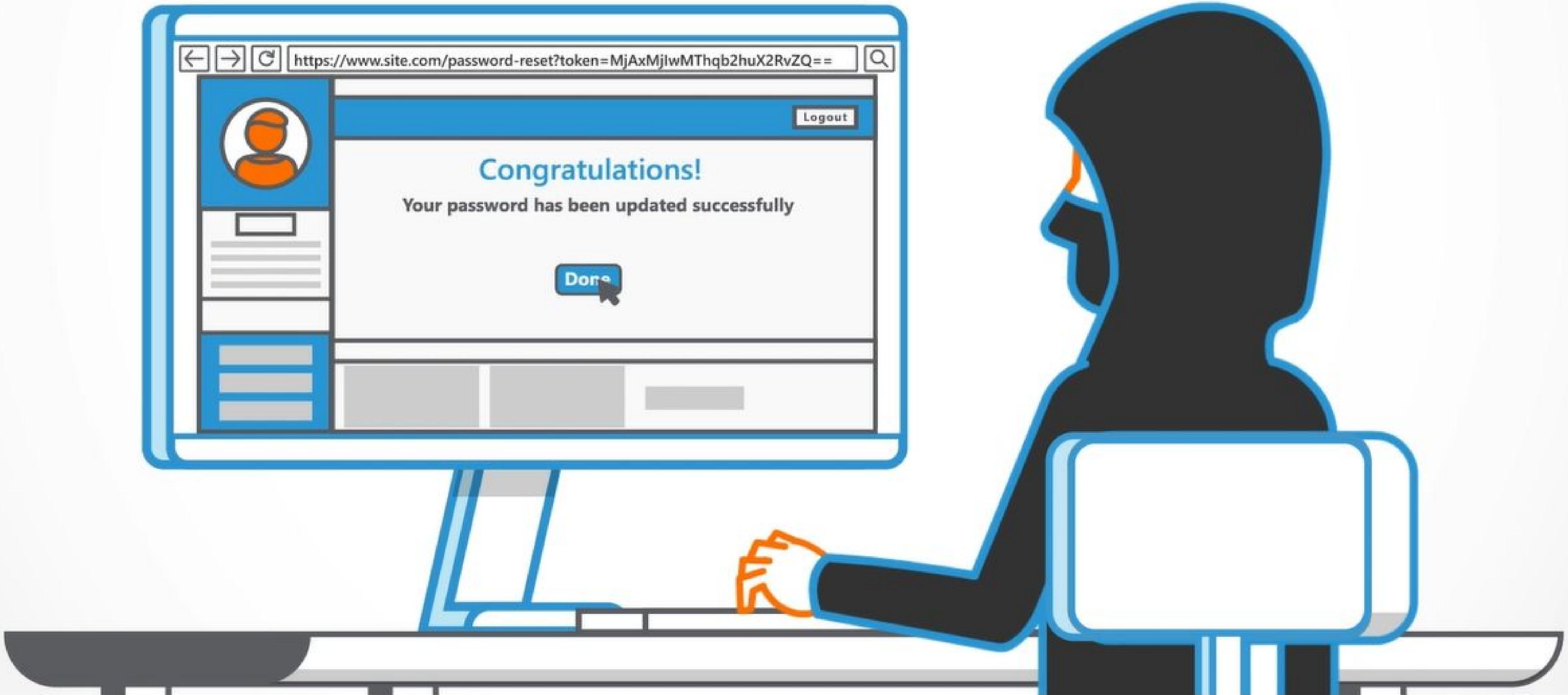
https://www.site.com/password-reset?token=MjAxMjIwMThqb2huX2RvZQ==

CHANGE PASSWORD

Enter new password *********

Re-enter new password **

and access the user's account using the newly set password.

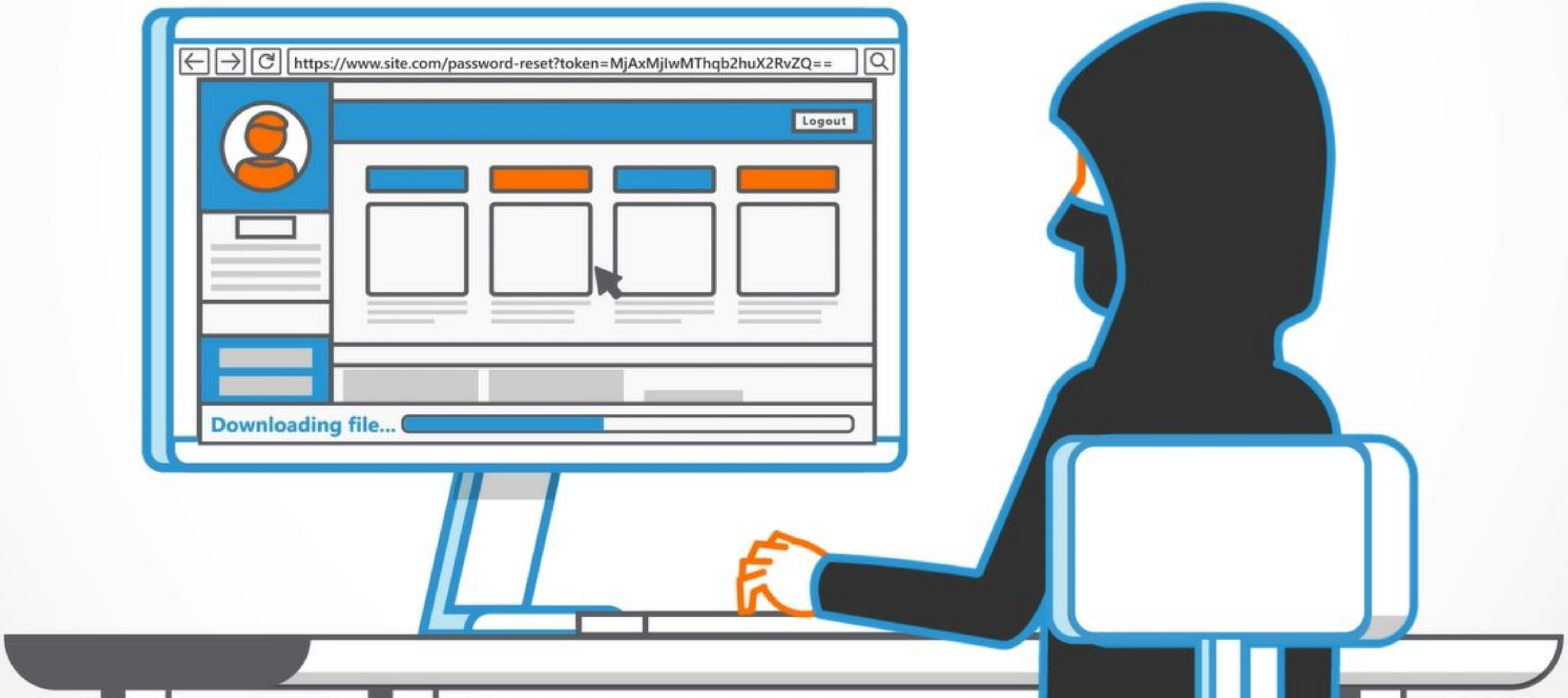


https://www.site.com/password-reset?token=MjAxMjIwMThqb2huX2RvZQ==

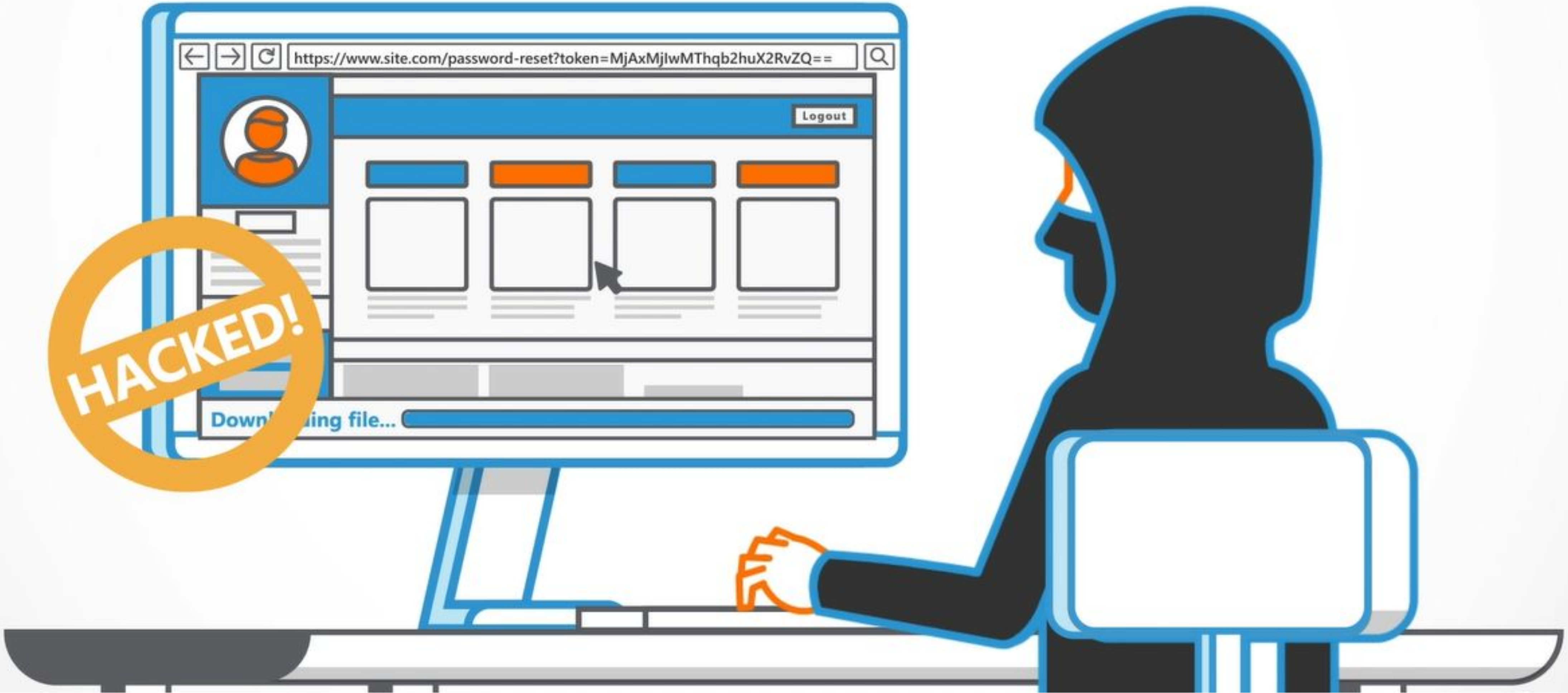
Congratulations!

Your password has been updated successfully

This account can now be used by the attacker to impersonate the user


https://www.site.com/password-reset?token=MjAxMjIwMThqb2huX2RvZQ==
Logout
Downloading file...

Now they can impersonate the user and steal sensitive data from their account.

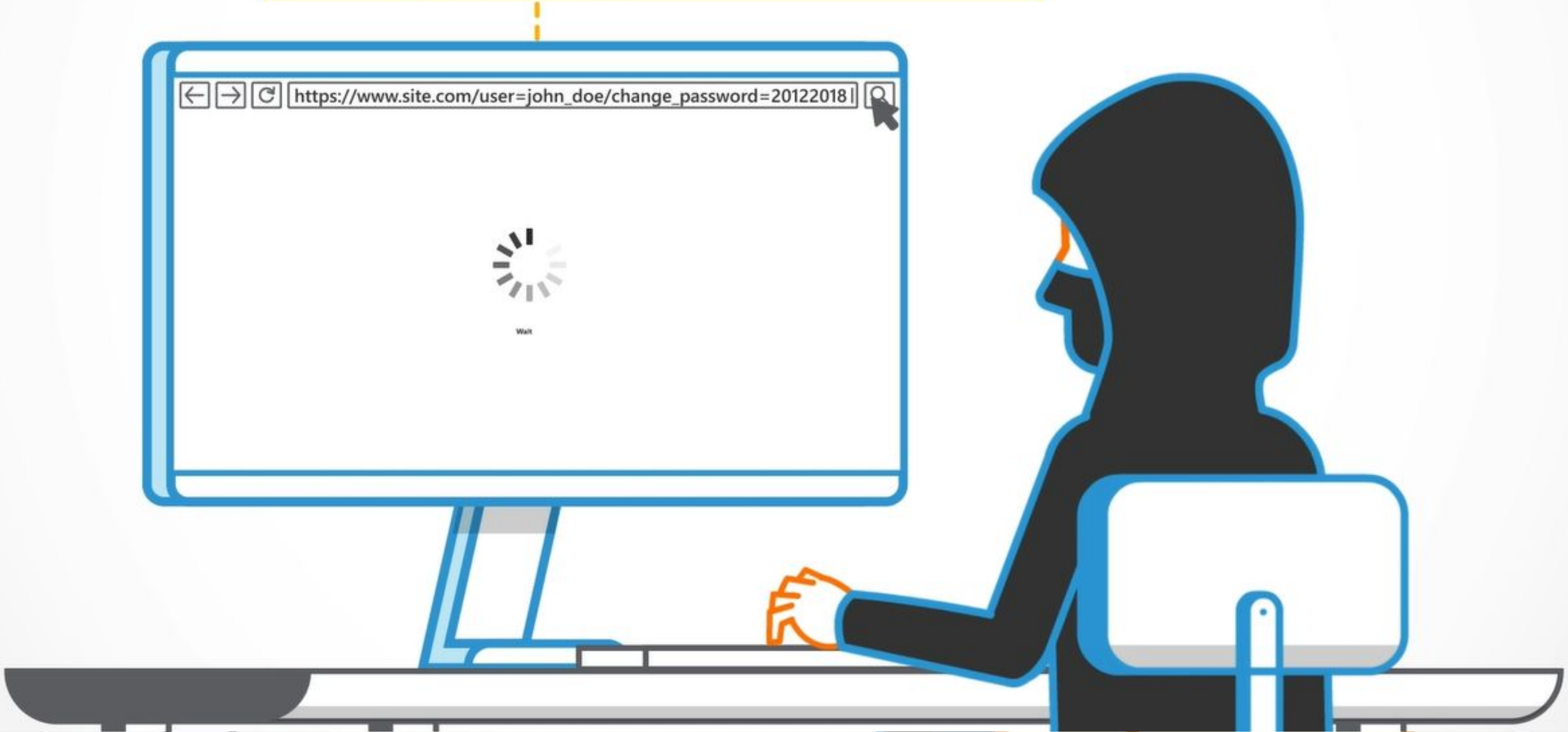

https://www.site.com/password-reset?token=MjAxMjIwMThqb2huX2RvZQ==
Logout
HACKED!
Downloading file...

INSECURE RANDOMNESS COULD HAVE SIGNIFICANT IMPACT

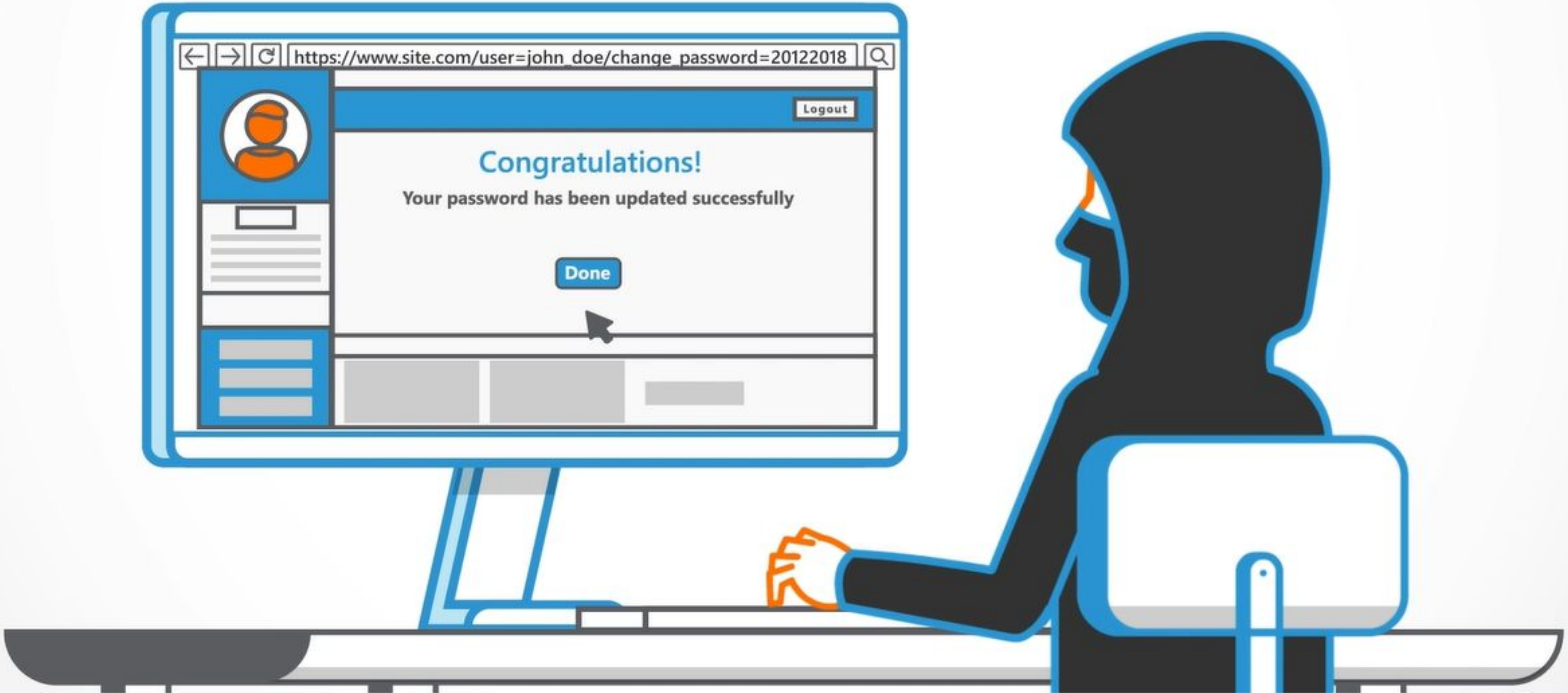
These vulnerabilities could be abused by an attacker to calculate or guess any sequence that should remain secret.

Request: Change password

```
https://www.site.com/password-reset?token=<TOKEN STRING>
TOKEN = base64(date.today + username)
```



For example, accessing unauthorized sensitive information could be an impact of this vulnerability.



https://www.site.com/user=john_doe/change_password=20122018

Congratulations!

Your password has been updated successfully

To prevent Insecure Randomness vulnerabilities, developers should

- Use a Cryptographically Secure Pseudo-Random Number Generator.
- Also, always select well-tested implementations with adequate, random and unpredictable seed lengths.

Congratulations, you have now completed this module, Insecure Randomness!

SECURE
CODE
WARRIOR
®