SECURE CODE WARRIOR

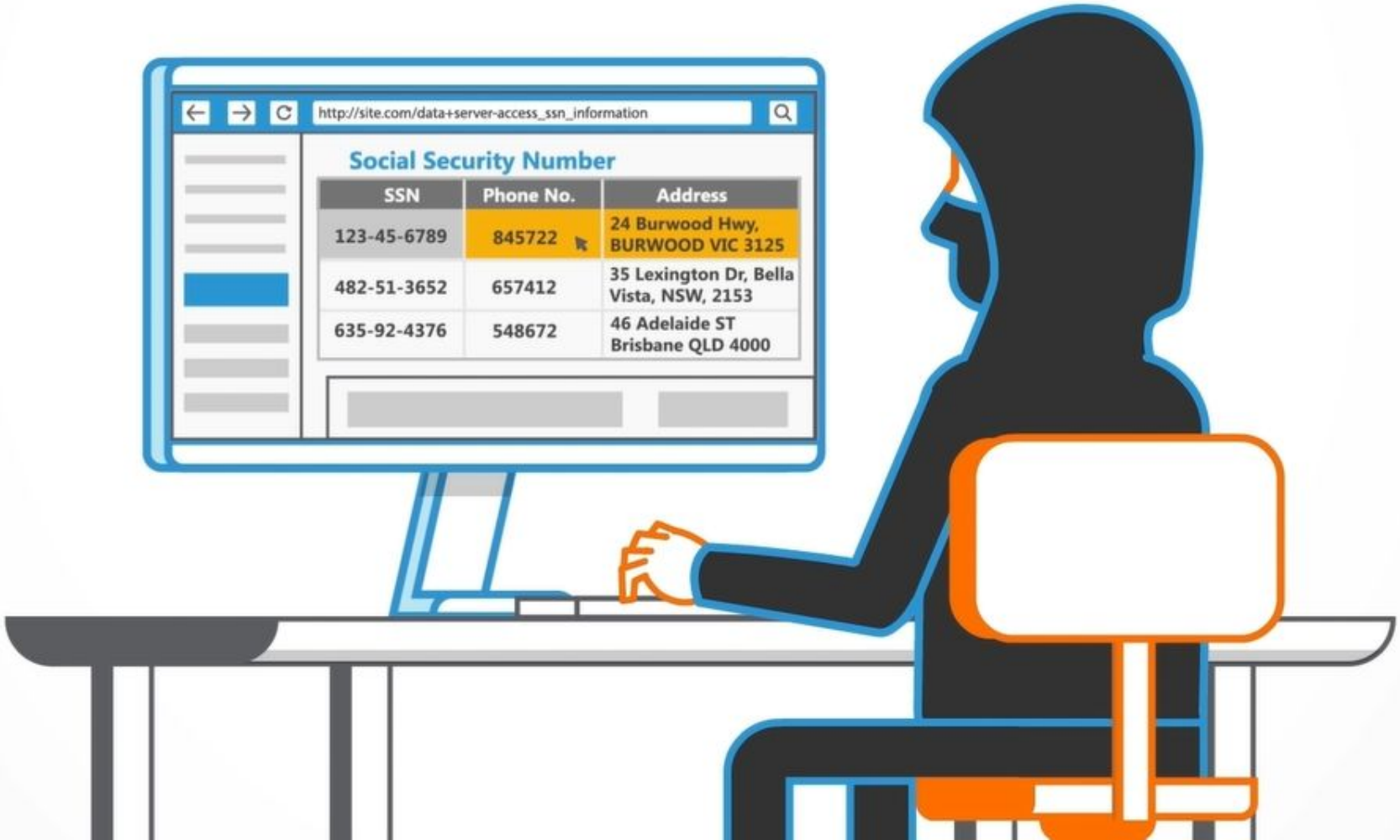
SENSITIVE DATA EXPOSURE

We'll explain

What Sensitive Data Exposure is, its causes, preventions and some potential hazards.

WHAT IS SENSITIVE DATA EXPOSURE?

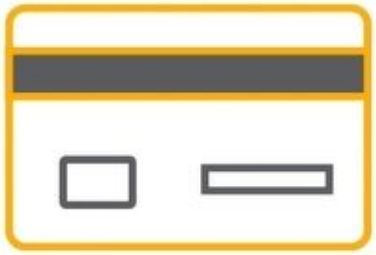
This is where sensitive data is exposed to actors that are not authorized to view that data.



Such data could be user credentials, banking information, credit cards or personal information.

Credentials

Banking Information

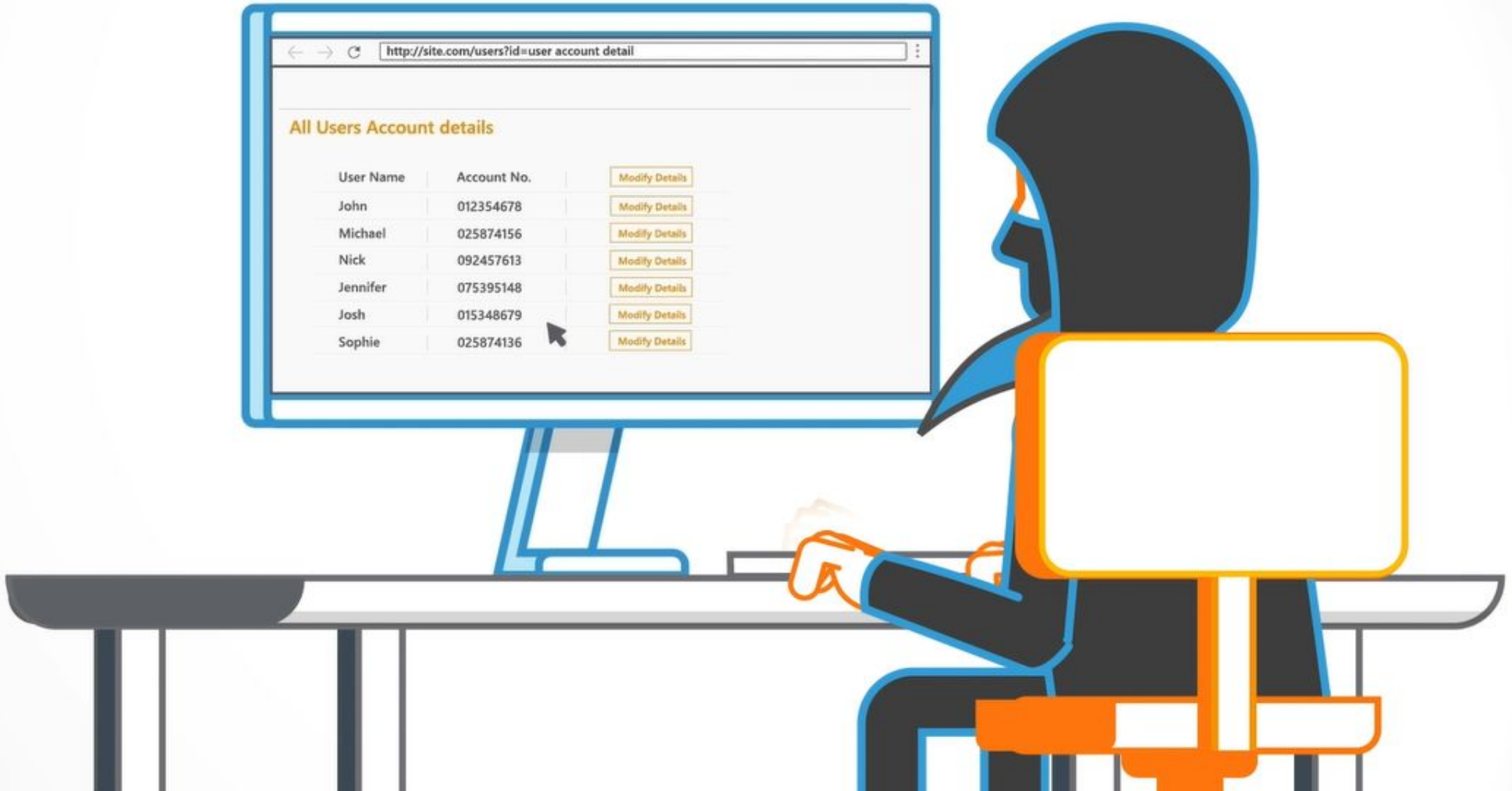


Credit cards

Personal Information

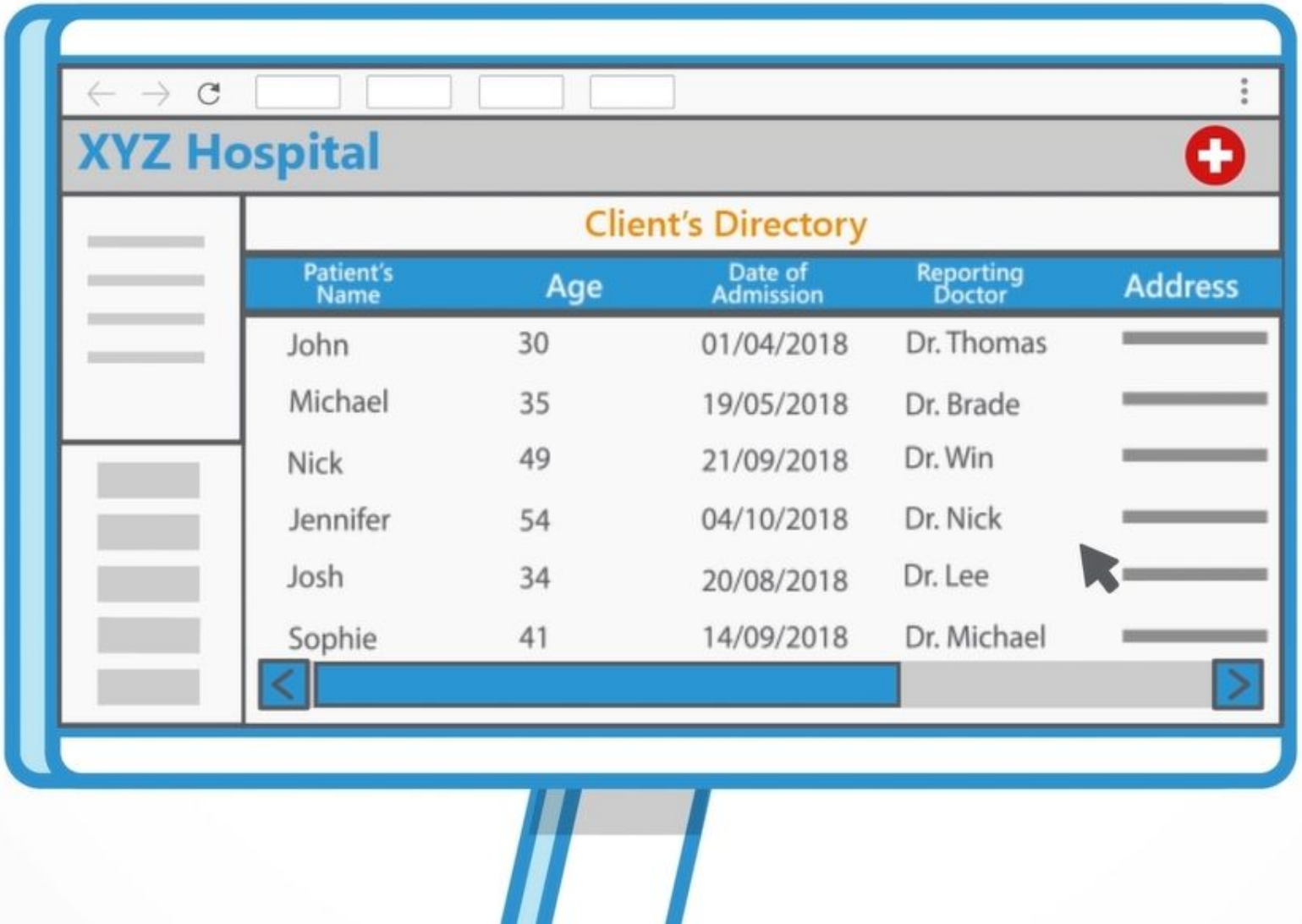
WHAT CAUSES SENSITIVE DATA EXPOSURE?

Sensitive data exposure vulnerabilities can occur when an application does not adequately protect sensitive information from being disclosed to attackers.



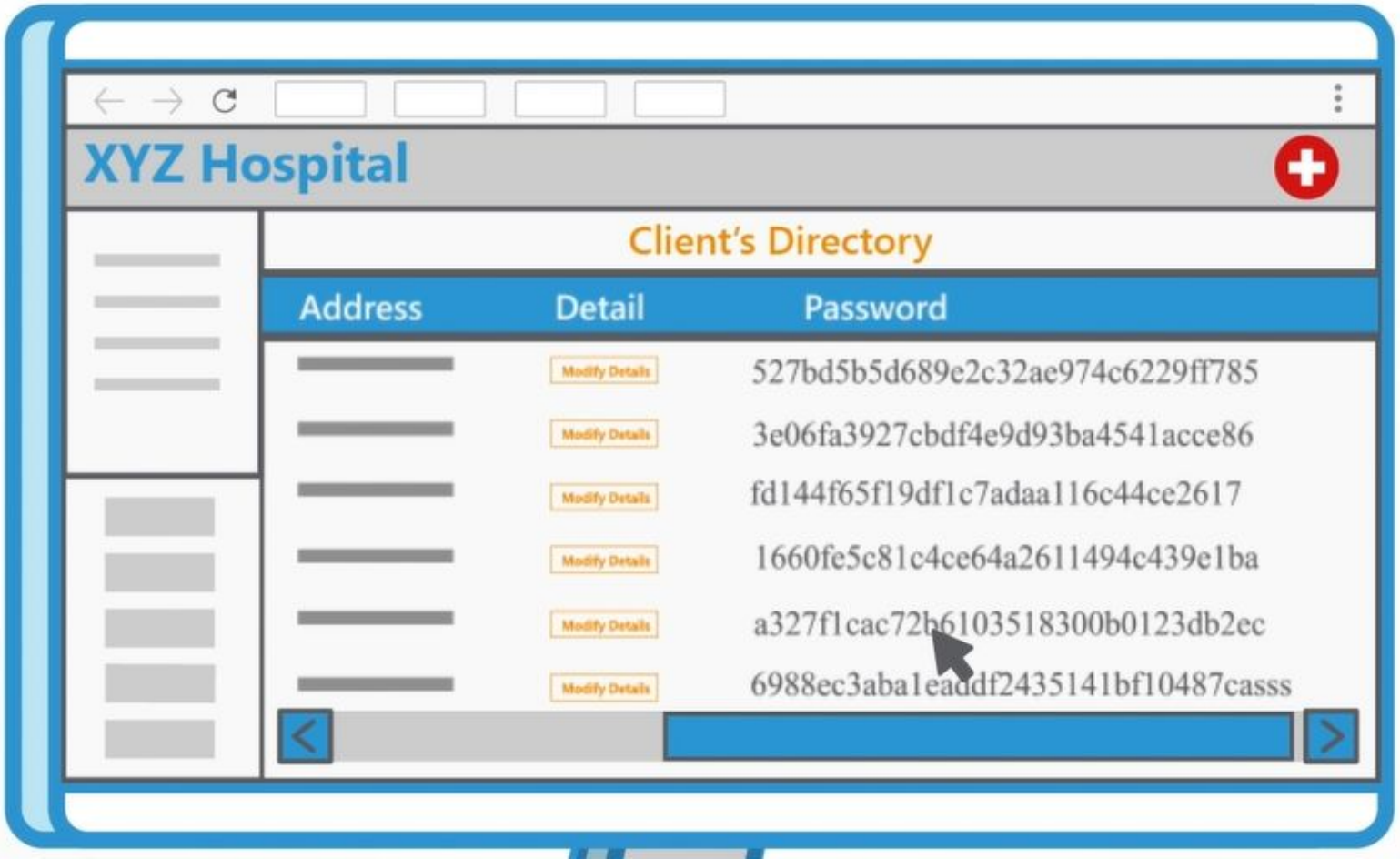
LET'S LOOK AT AN EXAMPLE

Let's say we have a dedicated computer with an application running that stores all medical information about clients from a hospital.



The password database for the application uses unsalted or simple hashes to store everyone's passwords.

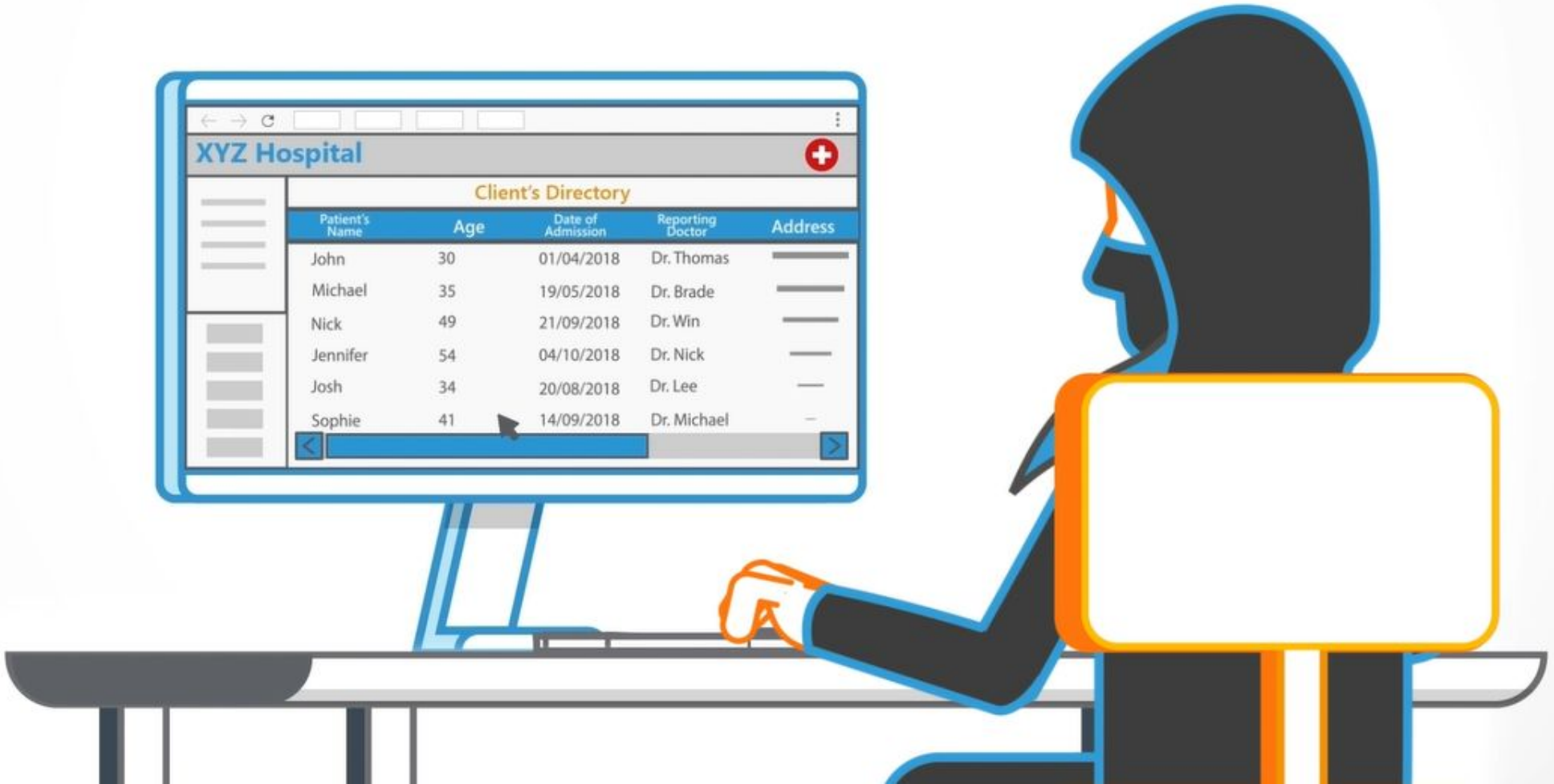
UNSALTED OR SIMPLE HASHES PASSWORD ENCRYPTION



A file upload flaw allows an attacker to retrieve the password database.

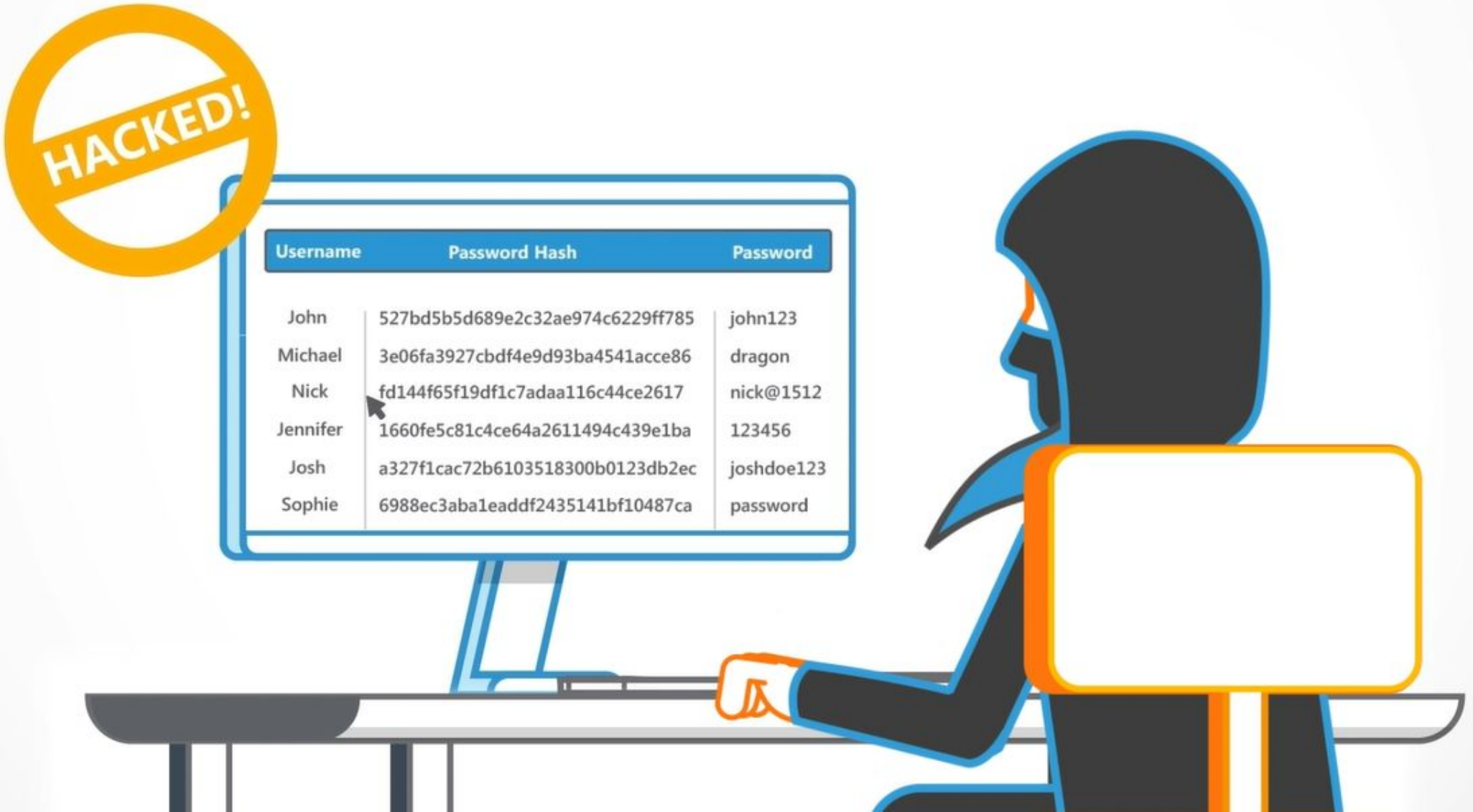
- Remote Access

Now, all the unsalted hashes can be exposed with a rainbow table of pre-calculated hashes.



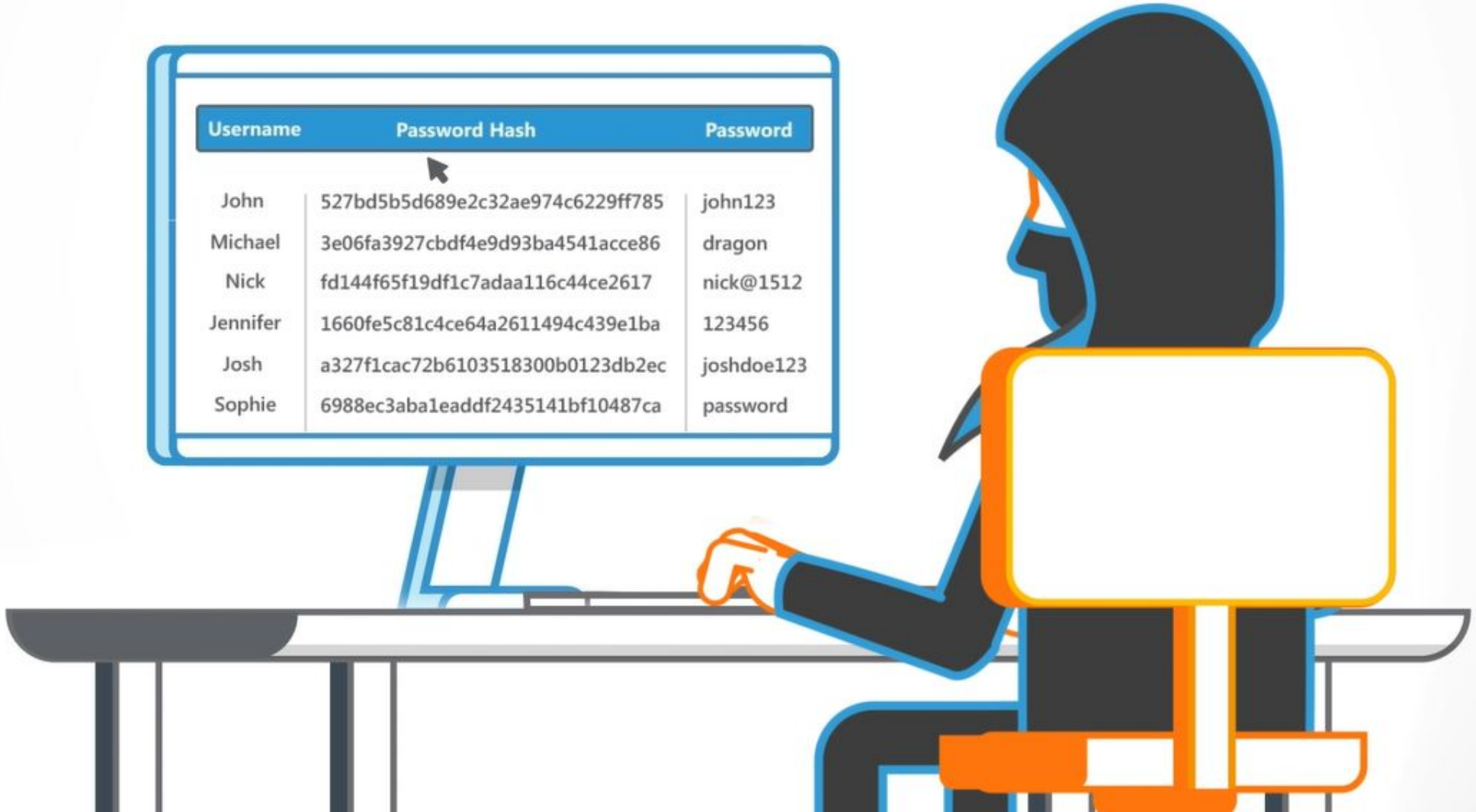
Hashes generated by simple or fast hash functions can also be cracked by GPUs, even if they were salted.

As a result, all user credentials are now exposed.

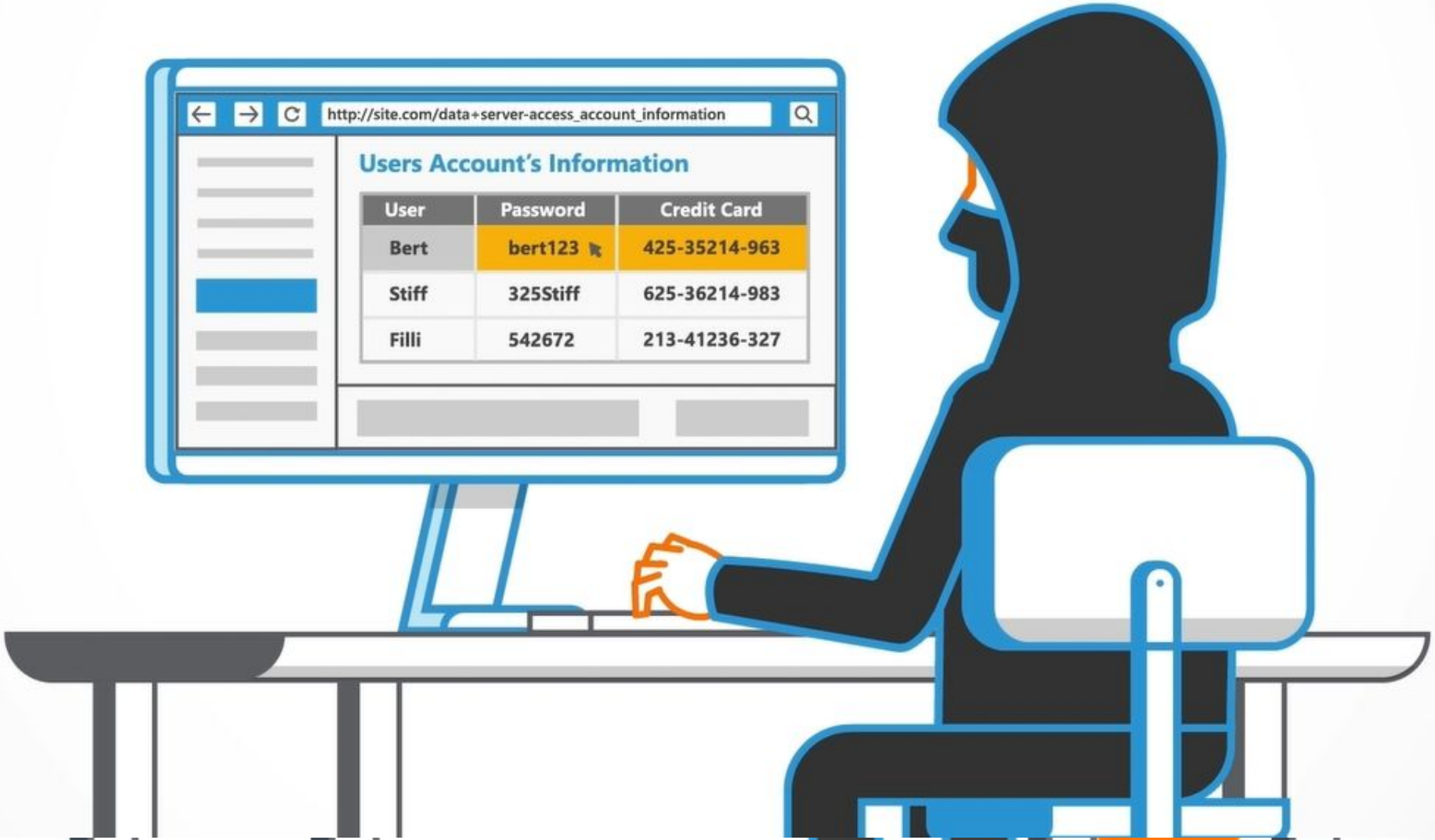


SENSITIVE DATA EXPOSURE COULD HAVE SIGNIFICANT IMPACT

Exposing sensitive data could lead to identity hijacking if credentials or personal information are being leaked.



If banking information or credit card numbers are exposed, this could lead to a financial loss.



To prevent Sensitive Data Exposure vulnerabilities:

- Developers should encrypt data during transport and at rest, using the latest encryption algorithms.
- Encrypt all data in transit with secure protocols such as TLS.
- Don't store sensitive data unnecessarily.
- Use a strong hashing or encryption algorithm where applicable.
- When using a hashing algorithm be sure to use a salt and a pepper.
- For data that doesn’t need to be hashed, use symmetric encryption.
- And finally, disable caching of sensitive data.

Congratulations, you have now completed this module,
Sensitive Data Exposure!

SECURE
CODE
WARRIOR