SECURE CODE
WARRIOR

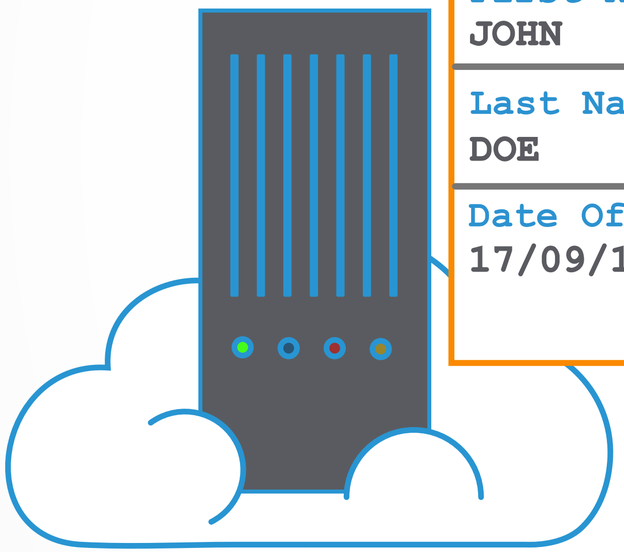
PLAINTEXT STORAGE OF SENSITIVE DATA

We'll go through

some causes and preventions of vulnerabilities in this category

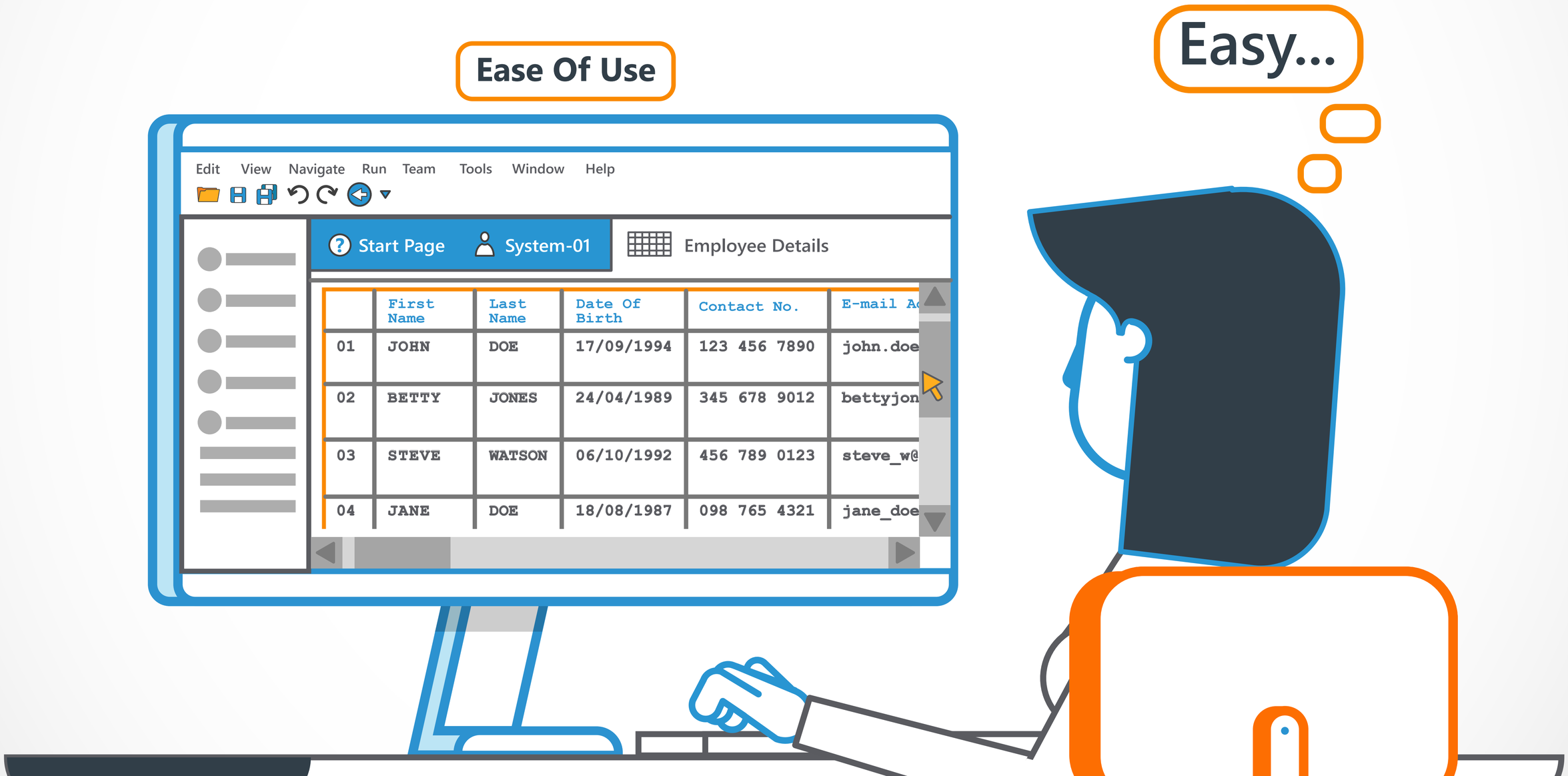
WHAT DO WE MEAN BY PLAINTEXT STORAGE OF SENSITIVE DATA?

Plaintext Storage of Sensitive Data is a vulnerability in which personal information is being stored in a clear text format.



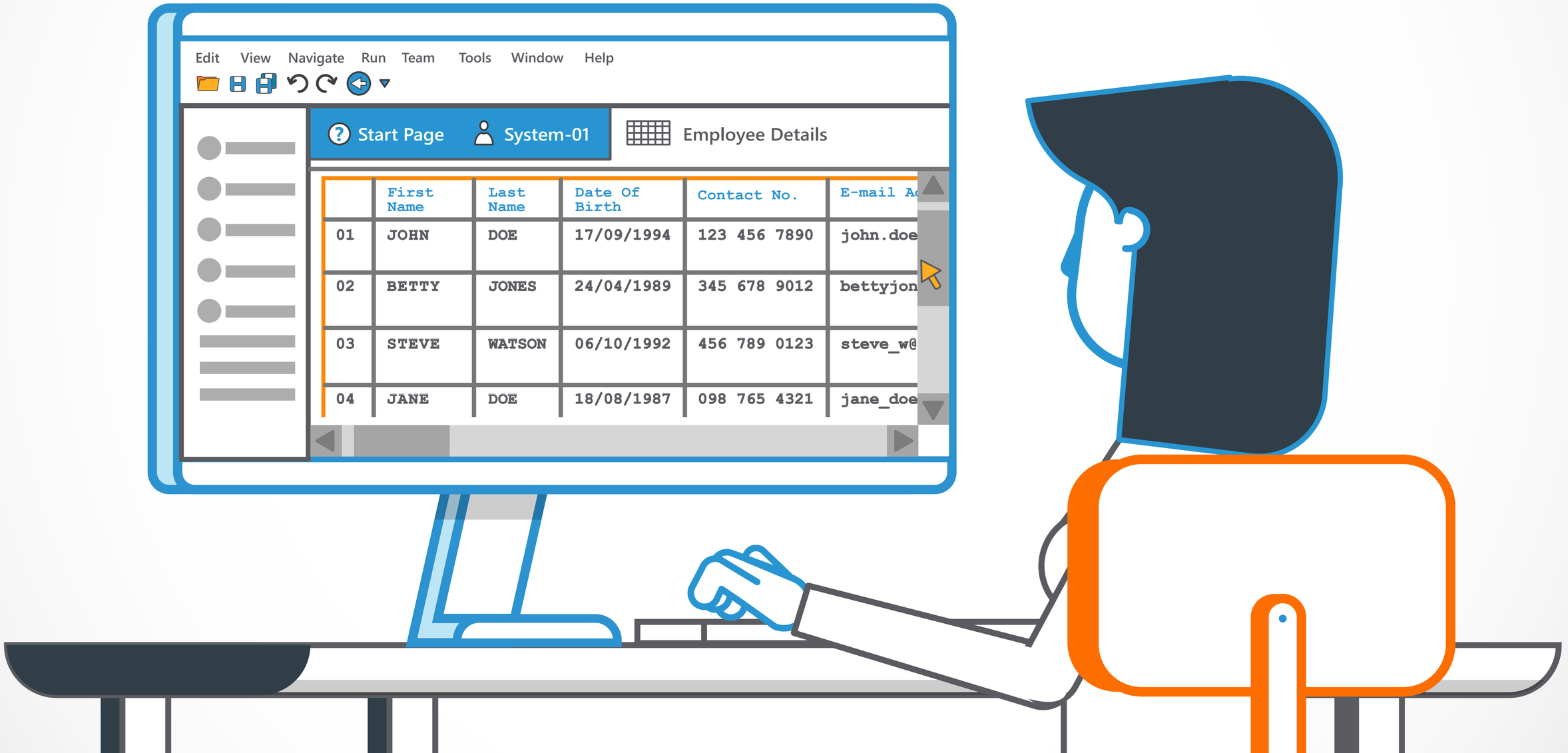
User's Information	Contact Information	Banking and Identification Information
First Name JOHN	Contact No. 123 456 7890	Bank Account NO. 1234 5678 9012 3456 7890
Last Name DOE	E-mail Address john.doe@email.com	Social Security Number 123 45 6789
Date Of Birth 17/09/1994	Address 65D Pitt St, Sydney NSW 2000, Australia	

Sensitive data may have been stored in plaintext for ease of use or simply been overlooked as safe.

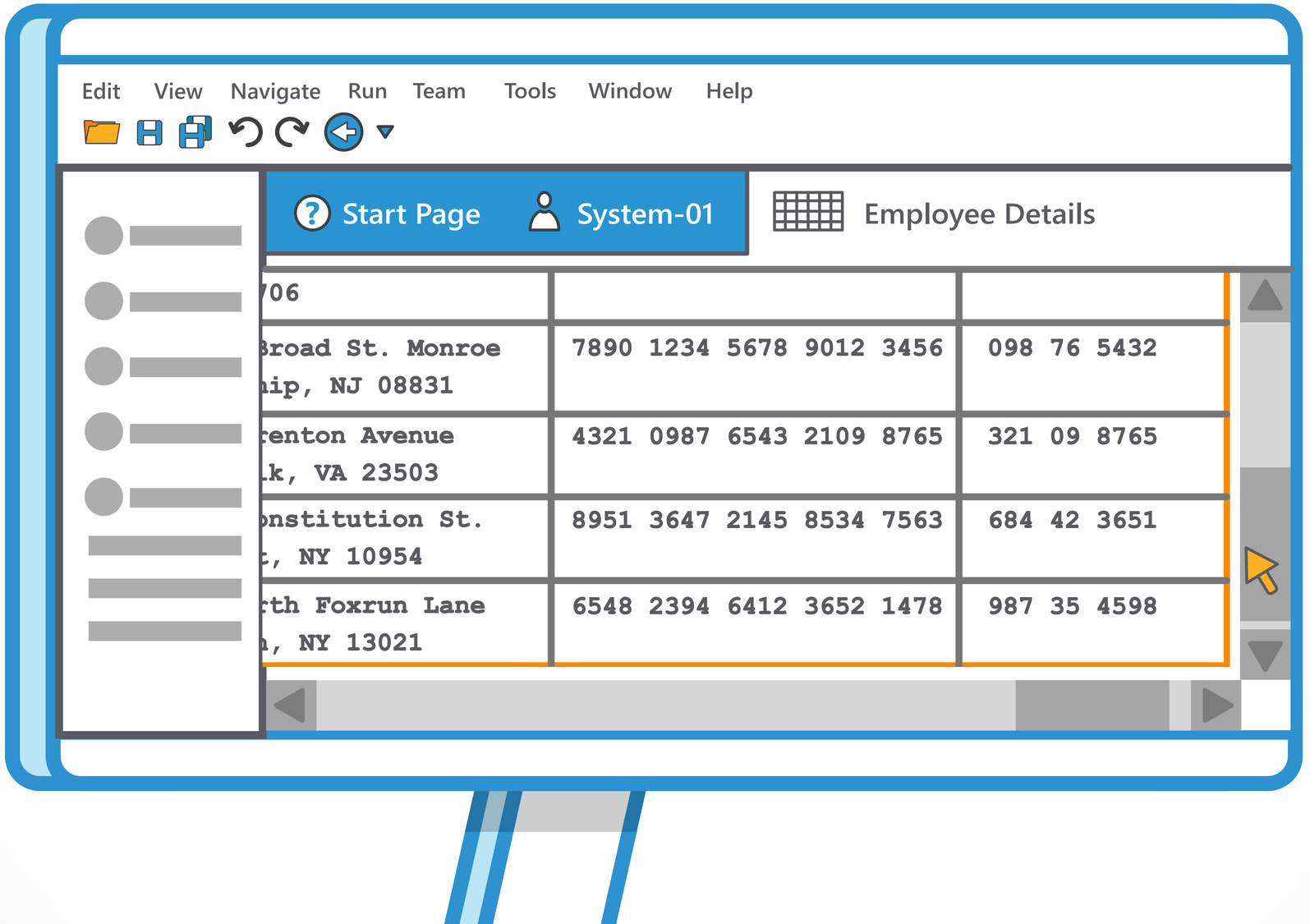


LET’S LOOK AT AN EXAMPLE

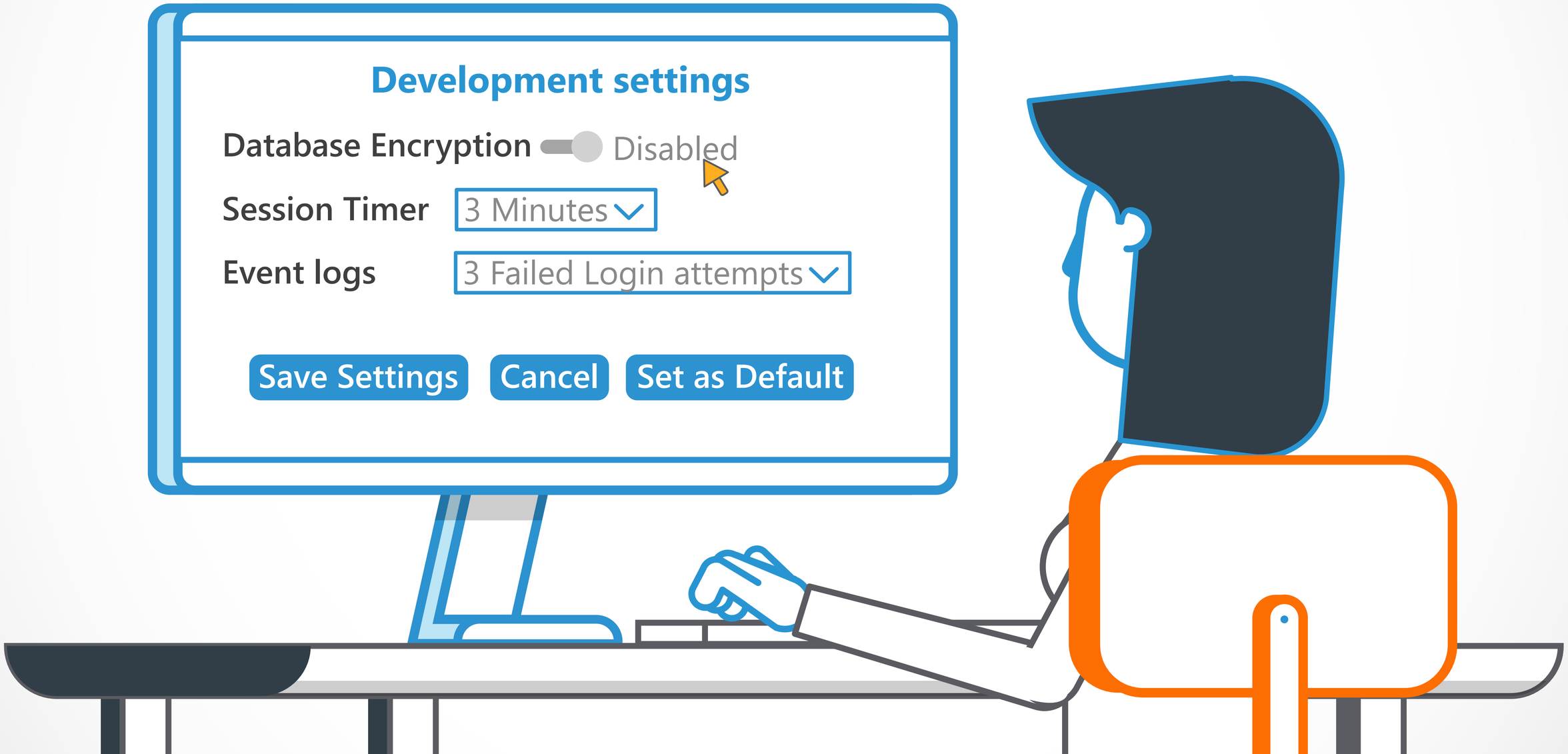
A Human Resources company is using a web app to store all personal data from their clients' employees.



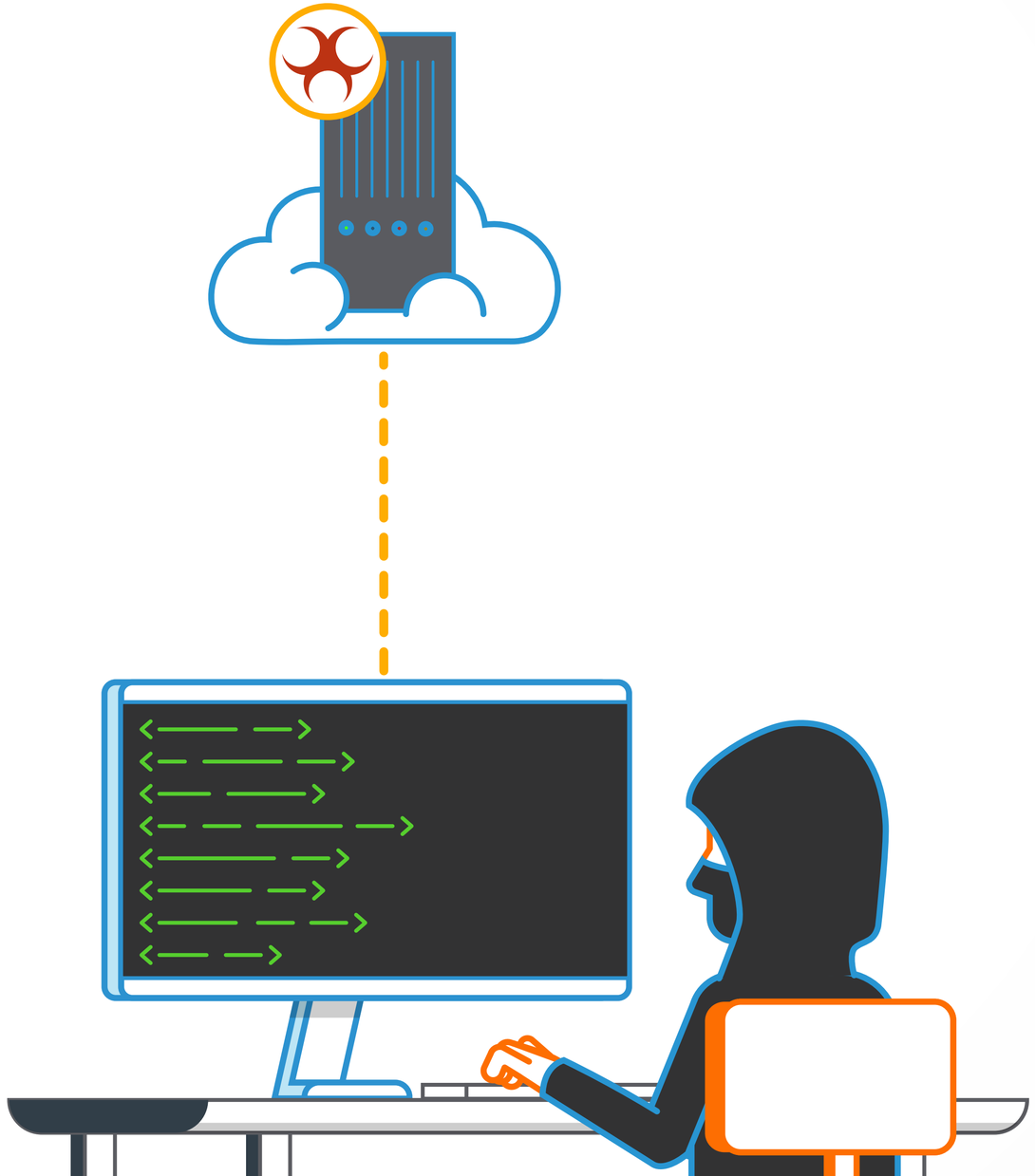
This data includes their paycheck, address, phone number, social Security numbers and so much more.



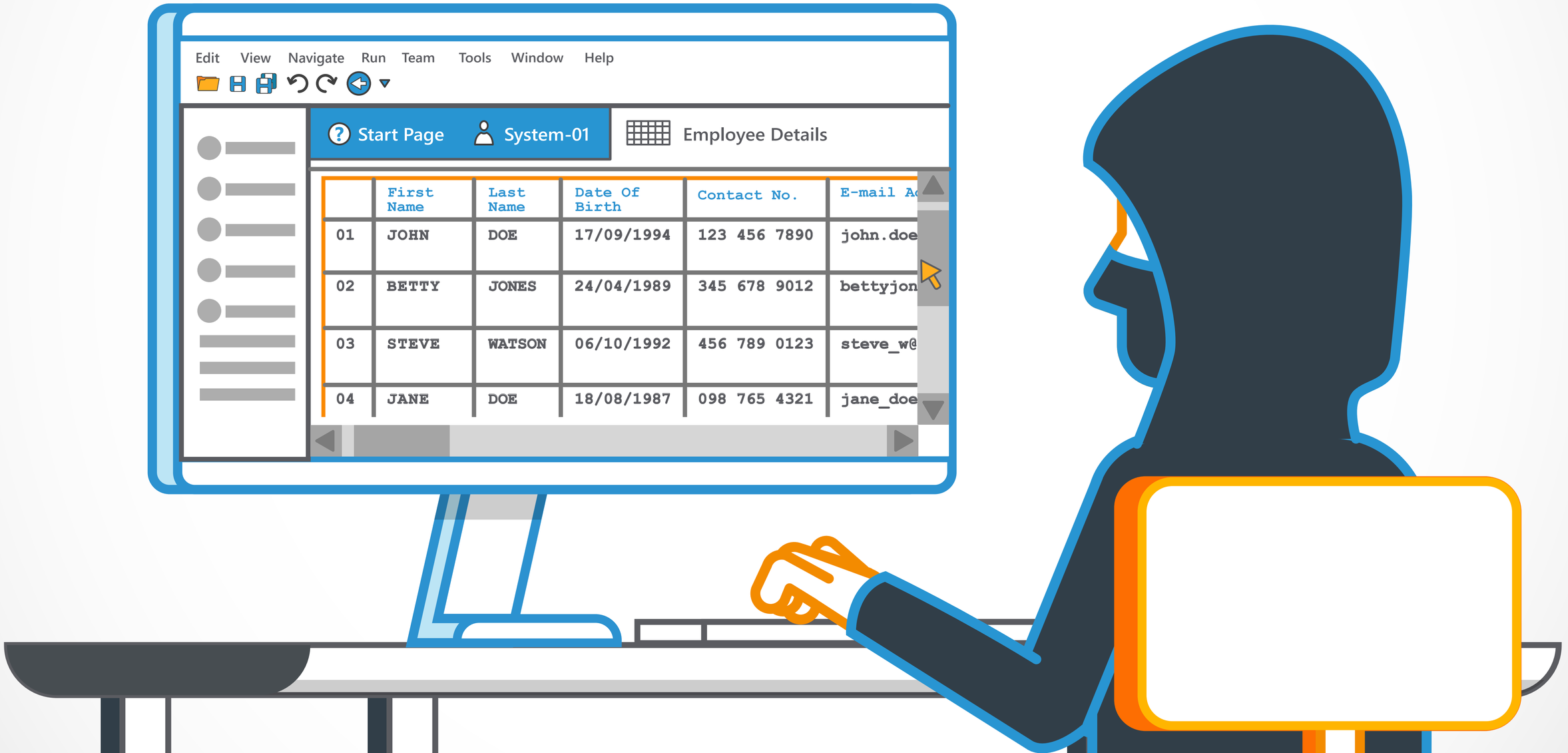
Unfortunately, the database is not encrypted by default.



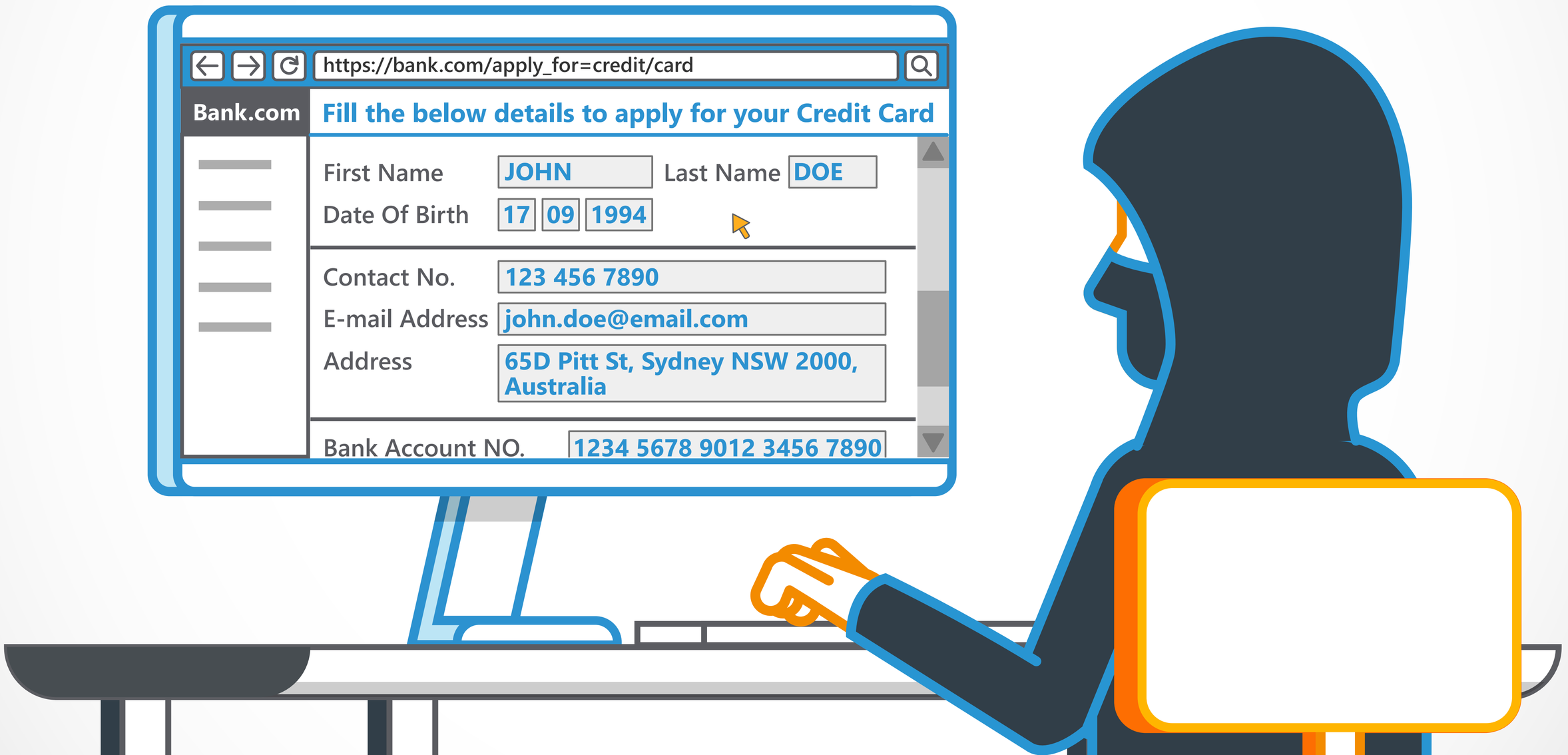
A hacker is able to gain access to the production database.



When analyzing the database the hacker notices unencrypted personal data.



The Hacker can now use the personal data to impersonate the user anywhere.



To avoid attacks relating to the Plaintext Storage of Sensitive Data, developers should

- Ensure sensitive data and personal details are properly encrypted with a strong algorithm prior to storage

Congratulations, you have now completed this module!

SECURE CODE
WARRIOR

www.securecodewarrior.com