



SECURE CODE WARRIOR

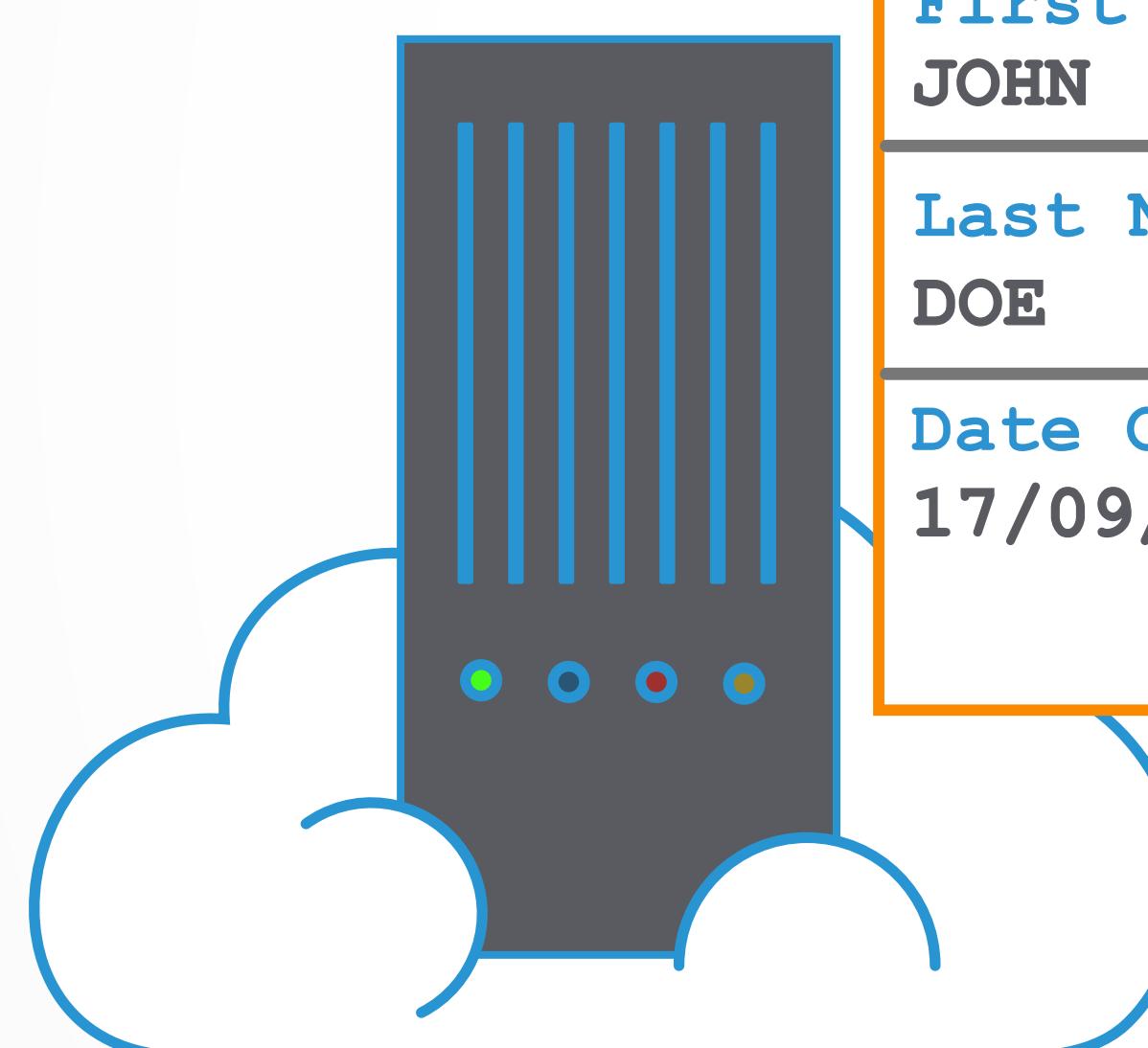
PLAINTEXT STORAGE OF SENSITIVE DATA

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.

Ease Of Use

The screenshot shows a software application window titled "Employee Details". The menu bar includes "Edit", "View", "Navigate", "Run", "Team", "Tools", "Window", and "Help". The toolbar contains icons for file operations like Open, Save, and Print. The main area has tabs for "Start Page" and "System-01". A table lists four employees with columns for Employee ID, First Name, Last Name, Date of Birth, Contact No., and E-mail Ad. The data is as follows:

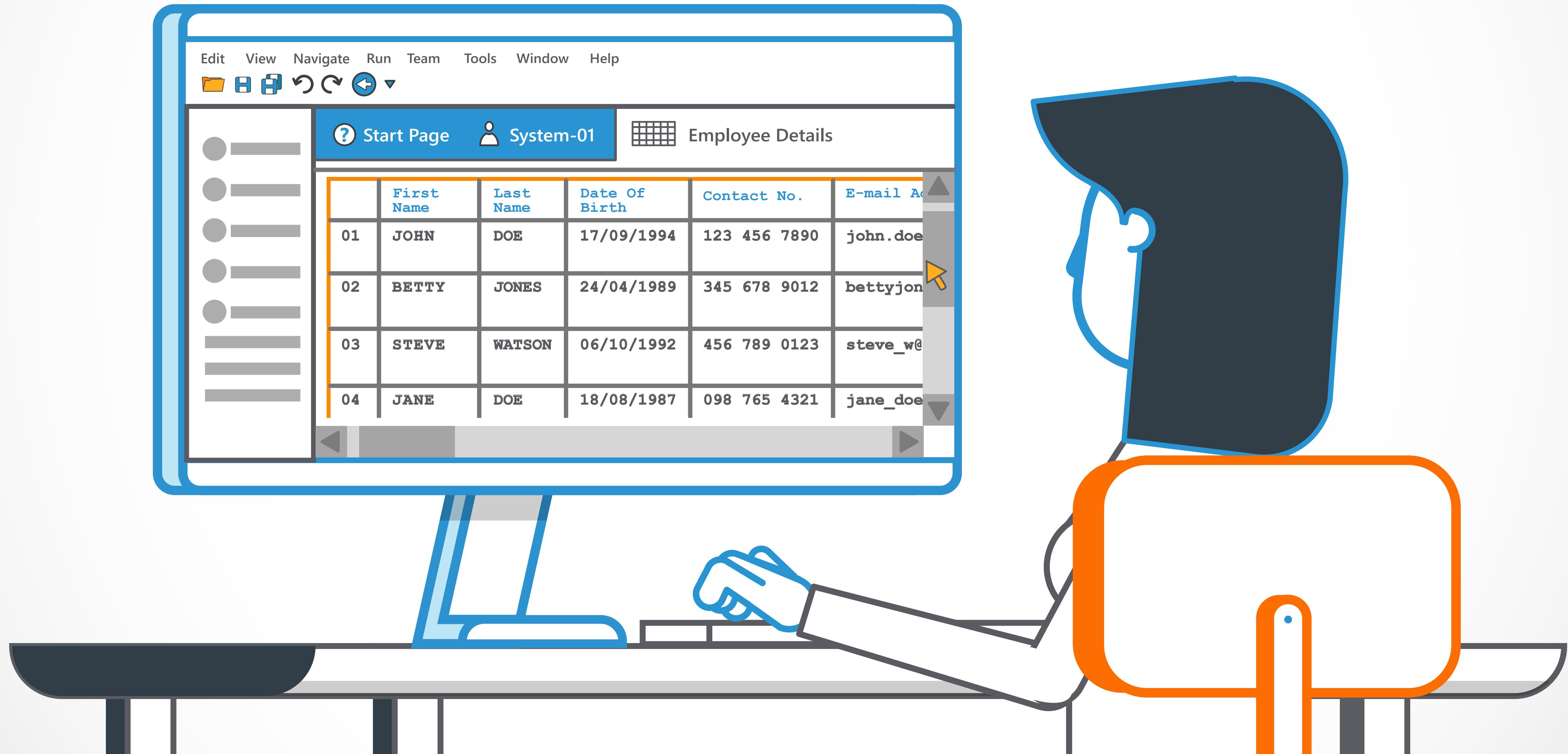
	First Name	Last Name	Date Of Birth	Contact No.	E-mail Ad
01	JOHN	DOE	17/09/1994	123 456 7890	john.doe
02	BETTY	JONES	24/04/1989	345 678 9012	bettyjon
03	STEVE	WATSON	06/10/1992	456 789 0123	steve_w@
04	JANE	DOE	18/08/1987	098 765 4321	jane_doe

Easy...



LET'S LOOK AT AN EXAMPLE

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



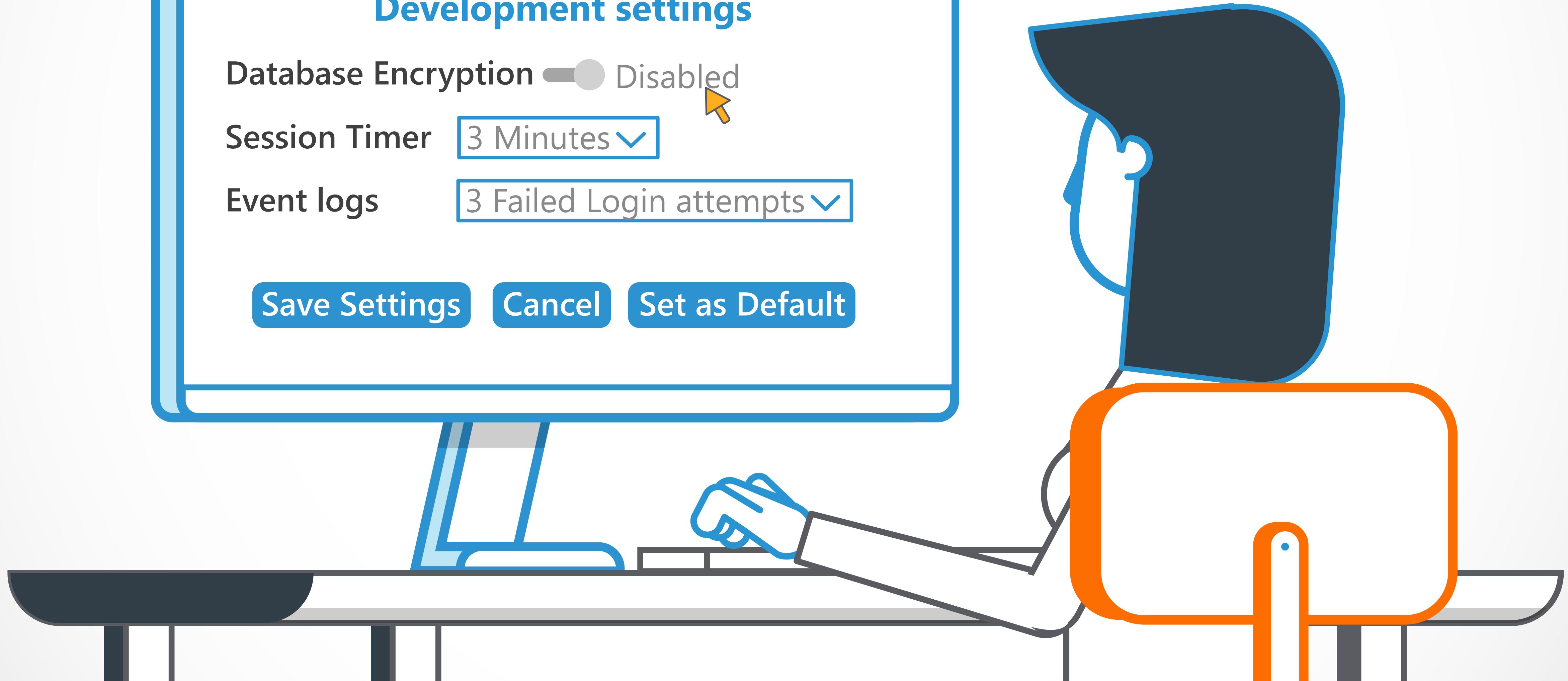
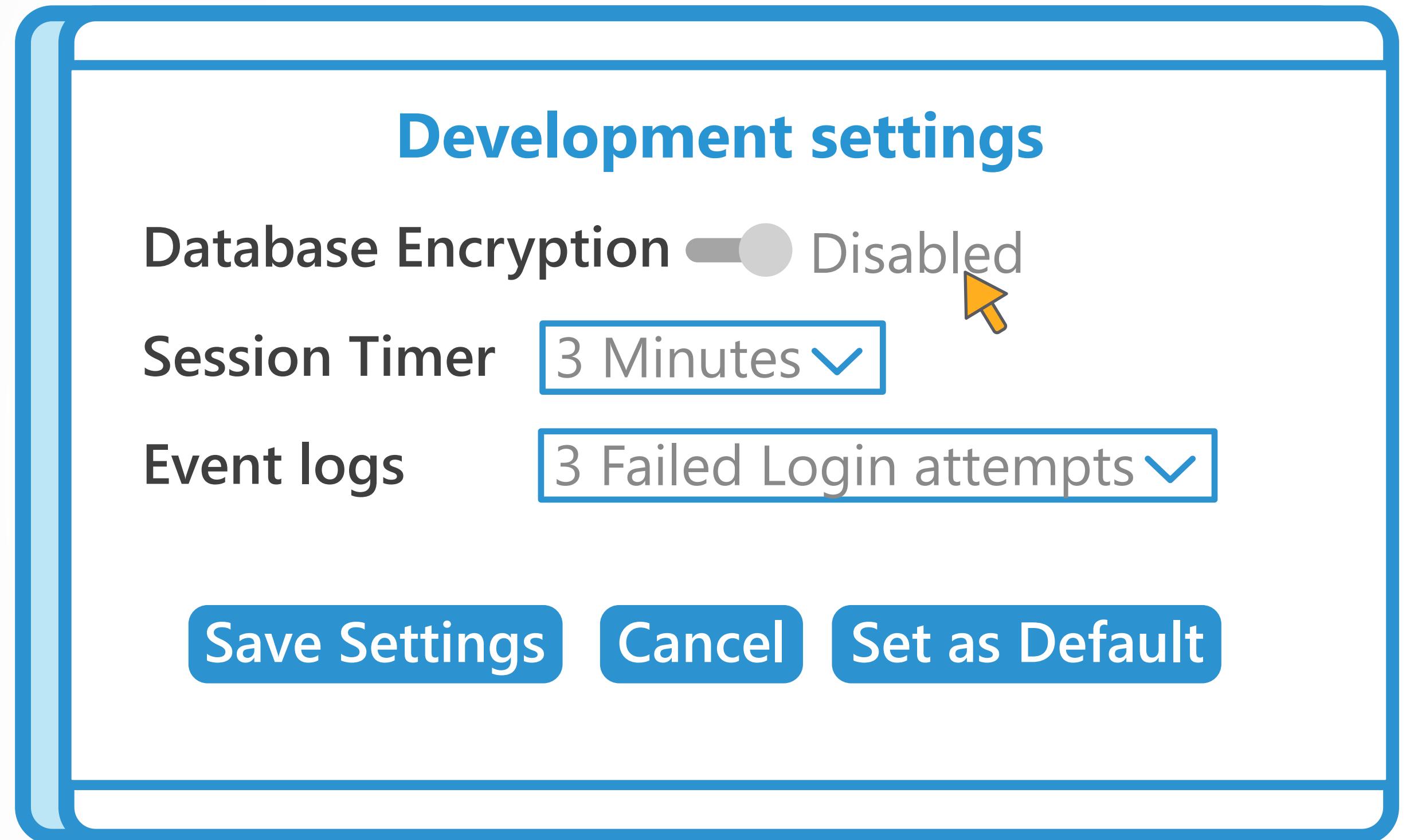
This data includes their paycheck, address, phone number, social Security numbers and so much more.

The screenshot shows a software interface with a blue header bar containing menu items: Edit, View, Navigate, Run, Team, Tools, Window, and Help. Below the menu is a toolbar with icons for folder, home, refresh, and back/forward navigation. The main area has a title bar with 'Start Page' and 'System-01' on the left, and 'Employee Details' on the right. To the left is a vertical sidebar with several grayed-out entries. The central part of the screen displays a table with three columns of data. The first column contains names and addresses:

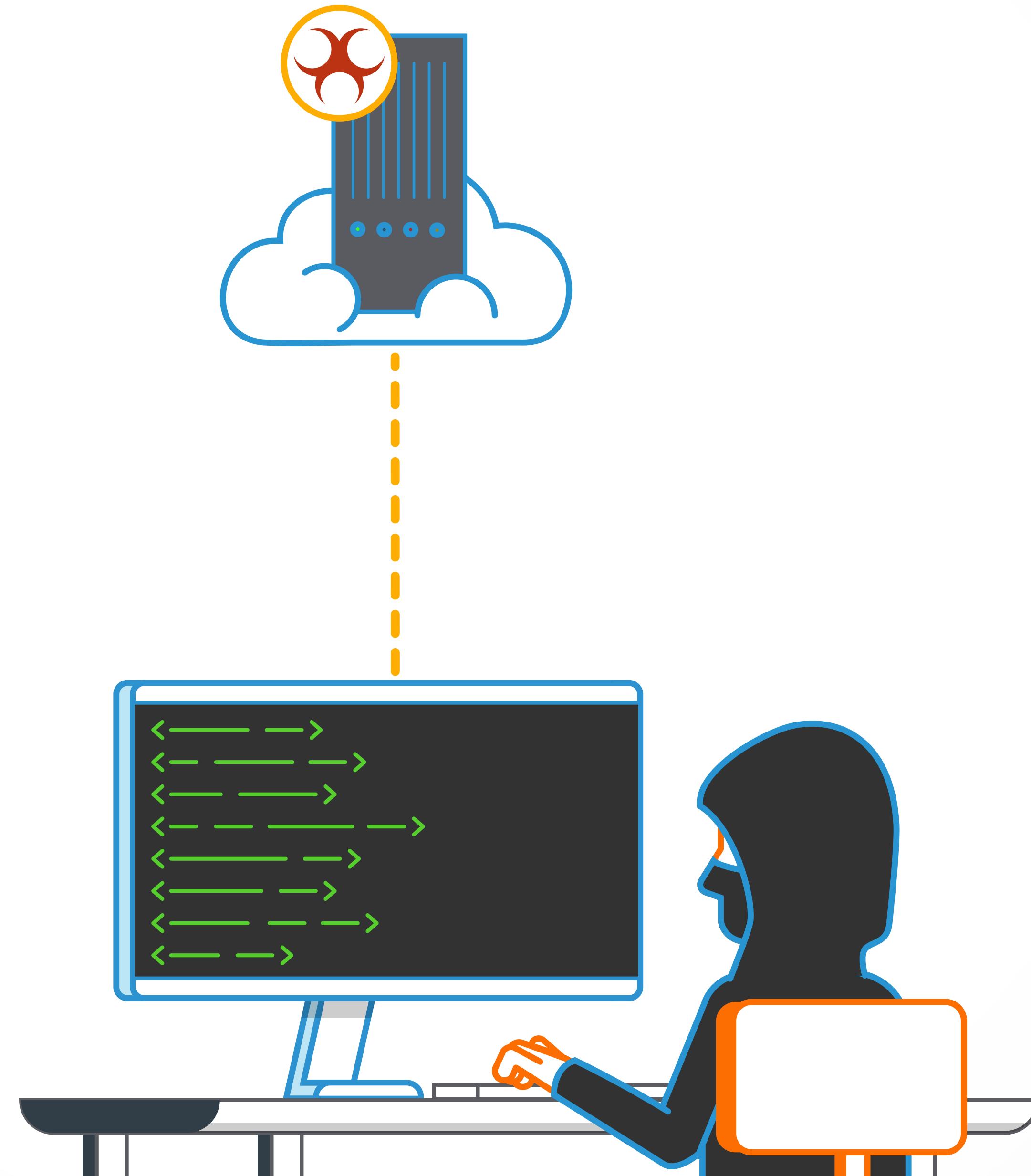
Name	Address	Phone Numbers
John Doe	123 Main St, Anytown, USA	7890 1234 5678 9012 3456
Jane Smith	456 Broad St. Monroe City, NJ 08831	098 76 5432
Mike Johnson	789 Market Avenue, Richmond, VA 23503	321 09 8765
Sarah Williams	101 Constitution St. New York, NY 10954	684 42 3651
David Lee	333 North Foxrun Lane, Albany, NY 13021	987 35 4598

A vertical orange bar highlights the last row of the table. A yellow cursor arrow points to the right edge of the third column in the last row. The bottom of the screen features a footer bar with navigation icons.

Unfortunately, the database is not encrypted by default.



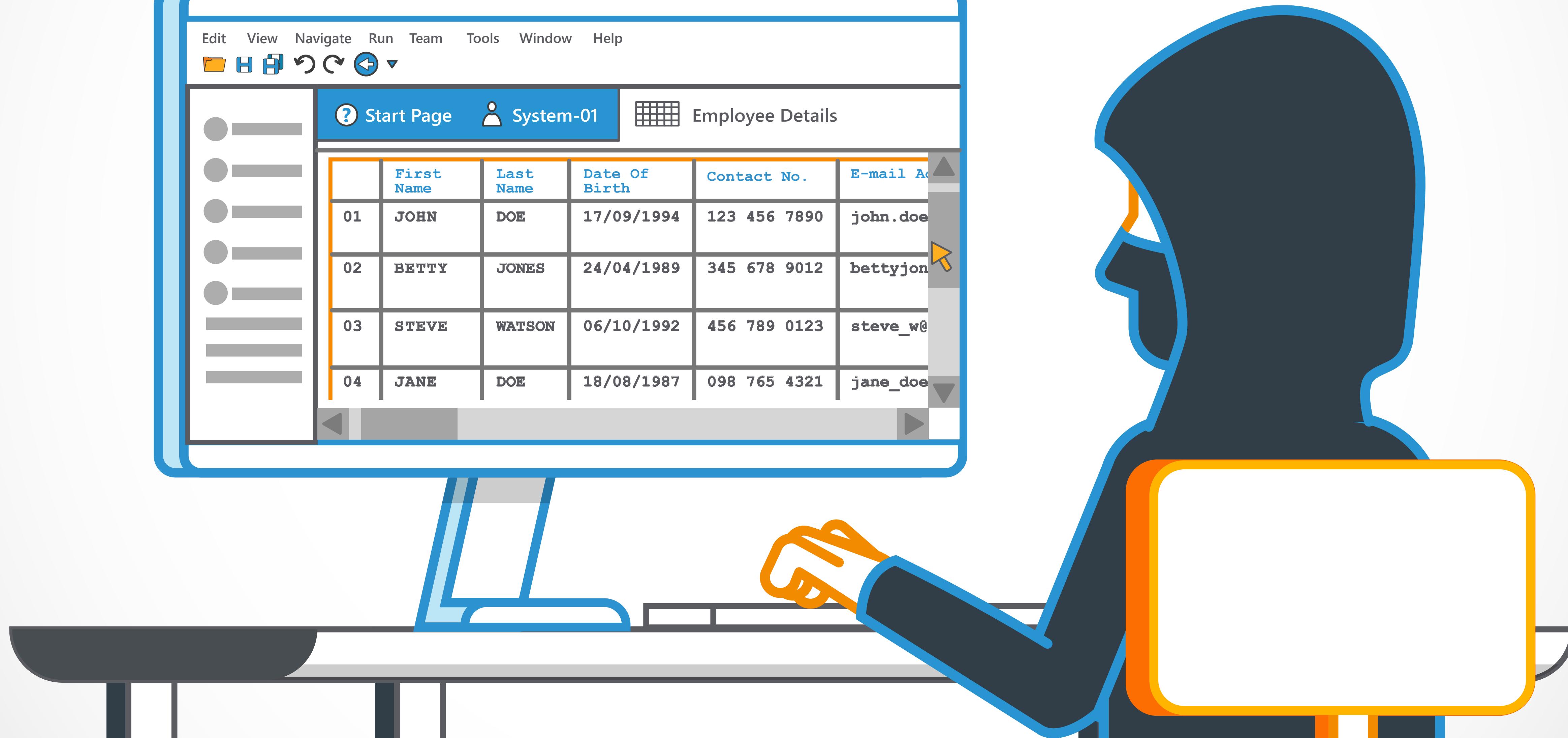
A hacker is able to gain access to the production database.



When analyzing the database the hacker notices unencrypted personal data.

Employee Details

	First Name	Last Name	Date Of Birth	Contact No.	E-mail Address
01	JOHN	DOE	17/09/1994	123 456 7890	john.doe@company.com
02	BETTY	JONES	24/04/1989	345 678 9012	betty.jones@company.com
03	STEVE	WATSON	06/10/1992	456 789 0123	steve.watson@company.com
04	JANE	DOE	18/08/1987	098 765 4321	jane.doe@company.com



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

- ④ 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