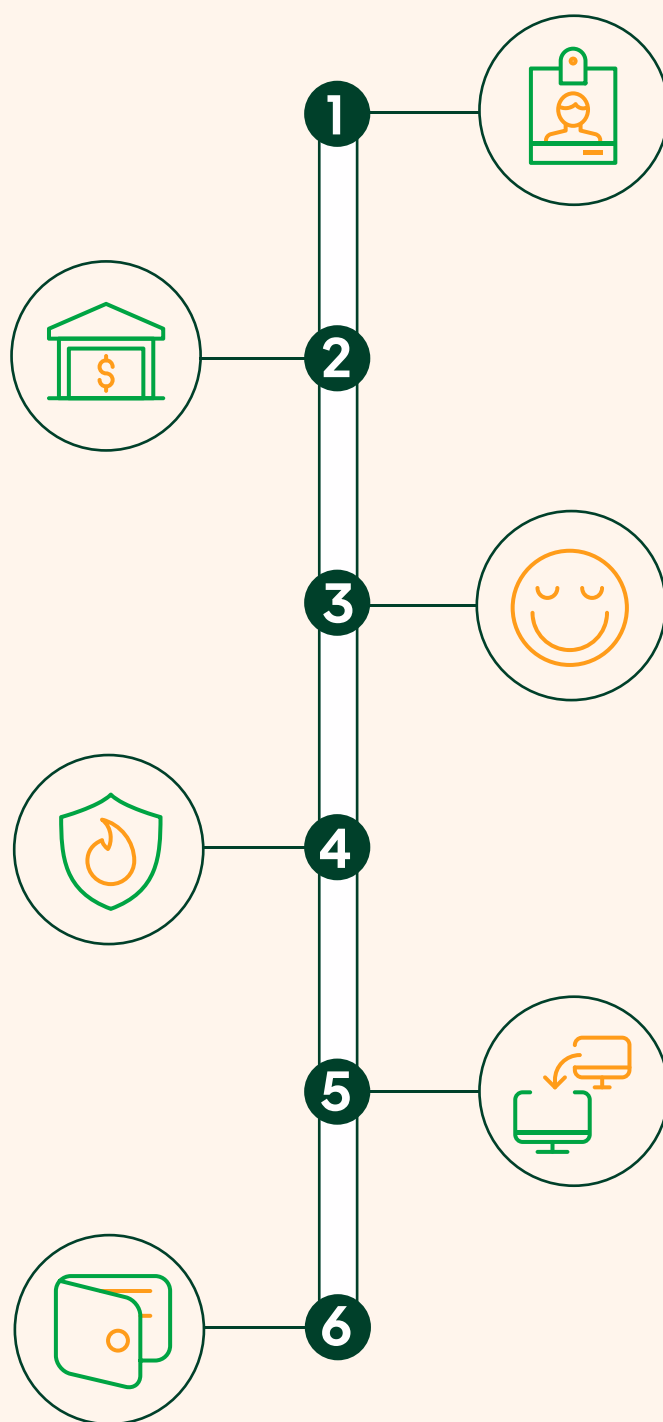


Vishing scam process

The attacker calls the victim and, when the victim answers, **impersonates an employee of an organisation or entity**, such as a bank.

The attacker **asks the victim for sensitive financial information** such as passwords or credit card details.

The offender now has the victim's information with which **to carry out unauthorised transactions**.



The offender makes a **preliminary study of potential victims** in order to obtain information that will help him to carry out the deception.

The offender uses the information he has gathered to **build trust** in the victim.

The user who has been scammed **hands over or completes his confidential information**.

