

# Transaction Verification

Secure Payments

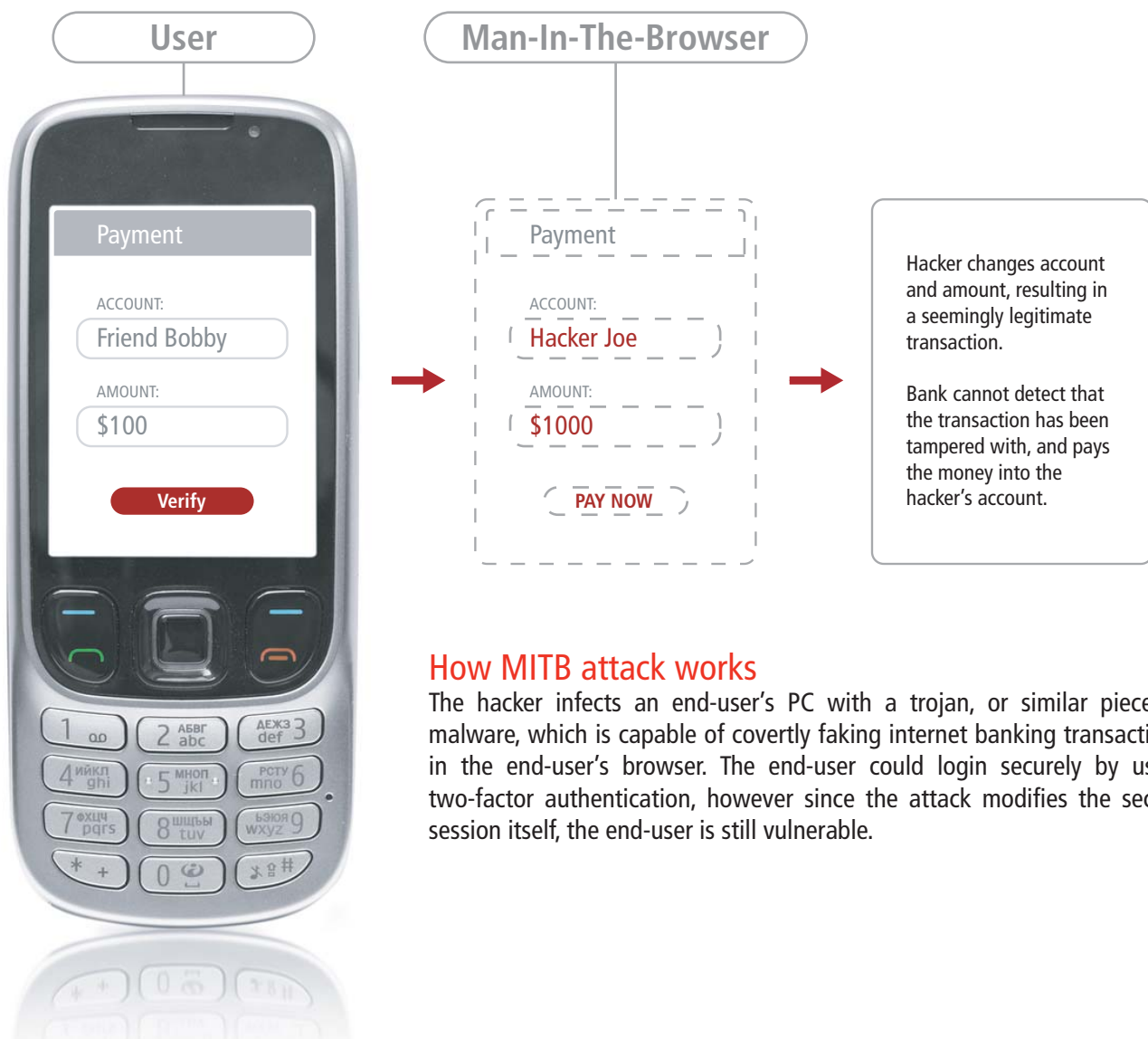


## Introduction

FireID Transaction Verification secures payments and transactions thus preventing man-in-the-browser attacks. Using something the end-user already has, a mobile phone, FireID provides a secure and easy way to ensure that only legitimate payments are made. FireID allows end-users to carry any number of Transaction Verification and OTP tokens on their phone.

## What is a Man-In-The-Browser attack?

A Man-In-The-Browser (MITB) attack is an advanced method of defeating two-factor authentication systems. In this kind of attack a hacker manipulates a legitimately authenticated end-user's browser to create fake banking transactions, allowing the hacker to steal money from an end-user's account.



## How MITB attack works

The hacker infects an end-user's PC with a trojan, or similar piece of malware, which is capable of covertly faking internet banking transactions in the end-user's browser. The end-user could login securely by using two-factor authentication, however since the attack modifies the secure session itself, the end-user is still vulnerable.

## How FireID Transaction Verification Works



## FireID Transaction Verification

- The FireID Transaction Verification application generates a unique code for each transaction. This code is based on the full transaction details (amount and account), and can be verified by the server for authenticity. If an attacker attempts to change any details, the code will become invalid, and the server will detect the tampering.
- This code is generated on the end-user's mobile phone, completely independently of the web browser that could be compromised, thus ensuring protection against man-in-the-browser attacks.
- FireID Transaction Verification provides a simple and secure way to protect transactions without requiring any additional hardware or expensive rollouts.