GSMA Open Gateway

IPification

Number Verification API

OTP Banka prevents phishing with network-based authentication

Case study for bank payments using the CAMARA standardised Number Verification API - View API Descriptions

Business Problem

In Serbia and surrounding countries, a significant increase in phishing attacks has been reported. Criminals were using impersonation scams to manipulate victims into sharing personal and sensitive information, including one-time passwords they receive from the bank via SMS. OTP Bank responded promptly by implementing an appropriate solution.

Impact

By removing the need to relay one-time passwords by SMS, the new solution effectively prevents fraudsters from pretending to be in possession of the victim's phone, rendering account takeover from such phishing attacks totally ineffective.

Technical Solution

To increase security, the bank is working with IPification. Employing the CAMARA Number Verification API, IPification assigns each user with a unique mobile ID key consisting of device, SIM card and network data. After the user enters their phone number into their banking app, the bank employs the API to verify that the person accessing the bank account is doing so from the correct phone.

Value

The API-based solution is preventing account takeovers and enhancing security. OTP Banka also reports a better user experience.

"We're adding an extra layer of security against phishing and fraud, without making things complicated for our users. This technology helps us ensure that mobile banking stays both secure and effortless, so our customers can bank with confidence. At OTP Banka Serbia, we're always looking for smart solutions that improve both security and convenience."

Bojan Pokrajac
Head of Digital and Online Channels at OTP Banka.