Best Practices Brief

# What is mobile hijacking, and how to stop it?

Learn how Zumigo prevents the 5 most common ways a hacker can hijack your mobile identity

Zumigo
Mobile in Context

Best Practices Brief

# What is mobile hijacking, and how to stop it?

Mobile hijacking is a term that is used to describe the act of taking over another person's mobile phone number through call forwarding, adding a device, porting, intra-porting, or subscriber identity module (SIM) swapping. After hijacking a phone number, the fraudster is able to intercept one-time passcodes (OTPs) that are sent as part of a multi-factor authentication process. Gaining access to the OTPs allows them to impersonate the consumer and gain unfettered access to bank and other accounts. In this brief, we will explore what these hijacking methods are and how to detect them.

**Method #1: Call Forwarding**

How it works: The fraudster logs into the victim's mobile account and turns on call forwarding so that all calls are automatically forwarded to the fraudster's phone number. The fraudster then requests a voice OTP and intercepts it. Call forwarding scams are also used during security call back procedures. The fraudster is able to answer the phone call that is meant for the victim and successfully impersonate them.

How to stop it: Zumigo has access to call forwarding settings for major mobile carriers to detect whether call forwarding is turned on in real-time. A phone number should be checked for call forwarding before a voice OTP is sent or callback procedure is exercised as forwarded calls may indicate a voice call hijacking.

**Method #2: Adding a Device**

How it works: The fraudster logs into the victim's iCloud account and adds their own device to the network so that all messages go to the fraudster's device as well. The fraudster then requests a short message service (SMS) OPT and intercepts it in the process.

How to stop it: Zumigo silently detects the phone number of a device that is interacting with a website or app without friction. Instead of sending the OTP in the text message itself, a link is sent which must be clicked on to retrieve the code. When the link is clicked, the device will visit a web page where the mobile number can be verified seamlessly in the background. A mismatch between the phone number that the link was sent to and the phone number detected would indicate SMS forwarding and a possible hijacking.

**Method #3: Porting**

How it works: The fraudster obtains the personal identification number (PIN) associated with the victim's phone number and uses it to port the number to another carrier where it can be associated with a SIM card and the device that is in the fraudster's possession. The fraudster then has full use of the victim's phone number to send and receive both texts and phone calls.

How to stop it: Zumigo can obtain real-time information on mobile numbers being ported between carriers from the central authority that manages all US mobile numbers. A number that was recently ported may indicate that it has been hijacked.



Zumigo
Mobile in Context

**Method #4: Intra-Porting**

How it works: This works similar to porting. However, to avoid the detection of porting activity, the fraudster ports the victim's phone number to a mobile virtual network operator (MVNO) of their current carrier, as opposed to an entirely different carrier. An MVNO is a wireless service provider that leases the infrastructure from a mobile network operator at wholesale rates, then sets retail prices for its services independently. The central authority does not recognize this as a port.

How to stop it: Zumigo provides real-time carrier information, which indicates that the number likely belongs to an MVNO. If a number has moved from a major carrier to one of its MVNOs, then the number may have been hijacked.

**Method #5: SIM Swapping**

How it works: The fraudster visits or calls the victim's carrier with a request for a new SIM card due to loss or upgrade. The carrier assigns the number to a new SIM card and device that is in the fraudster's possession. The fraudster then has full use of the victim's phone number to send and receive both texts and phone calls.

How to stop it: Zumigo has access to the international mobile subscriber identity (IMSI) or integrated circuit card identification number (ICCID) – i.e. the SIM card information – and the international mobile equipment identity (IMEI) – i.e. the unique device serial number from the major carriers. Zumigo can baseline this data for all mobile phone numbers and then obtain updated information to detect any changes. A change in the above data associated with the mobile number may indicate that the number was hijacked.

**About Zumigo**

Zumigo is the frontline in digital identity verification, helping the largest enterprises in the world secure transactions, devices and user accounts.

With a multi-layer approach, Zumigo creates a unique digital identity network that spans global carrier providers, third-party data analytics and databases, and payment information to verify the the user across the digital engagement journey, including account opening, multi-factor authentication, and payment validation.

**Learn more at www.zumigo.com.**