# THE SIM HIGHJACKERS: HOW CRIMINALS ARE STEALING MILLIONS BY HIGHJACKING PHONE NUMBERS

13 Mar 2020

Press Release

SIM swappers arrested by Spain, Austria and Romania as police gears up against this growing threat


It is a common story: the signal bars disappears from their mobile phones, they call the phone number – it rings, but it's not their phone ringing. They try to login to their bank account, but the password fails. They have become the newest victim of SIM swap fraud and their phone number is now in the control of a criminal.

SIM swap fraud is committed when a fraudster dupes the victim's mobile phone operator into porting the victim's mobile number to a SIM in the possession of the fraudster and so starts receiving any incoming calls and text messages, including banking one-time-passwords which are sent to the victim's phone number.

The fraudster can then perform transactions, using credentials gathered by other techniques such as malware, and when the bank sends a one-time-password via SMS, the fraudster receives it and completes the authorisation of the transaction.

With SIM swapping making the headlines in recent months, police across Europe has been gearing up against this threat, with two operations targeting SIM highjackers coming recently to fruition.

## OPERATION QUINIENTOS DUSIM

Investigators from the Spanish National Police (Policía Nacional) together with the Civil Guard (Guardia Civil) and Europol targeted back in January suspects across Spain believed to be part of a hacking ring which stole over €3 million in a series of SIM swapping attacks. 12 individuals were arrested in Benidorm (5), Granada (6) and Valladolid (1).

Composed of nationals between the ages of 22-52 years old from Italy, Romania, Colombia and Spain, this criminal gang struck over 100 times, stealing between €6,000 and €137,000 from bank accounts of unsuspecting victims per attack.

The modus operandi was simple, yet effective. The criminals managed the obtain the online banking credentials from the victims of the different banks by means of hacking techniques such as the use of banking Trojans or other types of malware. Once they had these credentials, the suspects would apply for a duplicate of the SIM cards of the victims, providing fake documents to the mobile service providers. With these duplicates in their possession, they would receive directly to their phones the second factor authentication codes the banks would send to confirm transfers.

The criminals then proceeded to make fraudulent transfers from the victims' accounts to money mule accounts used to hide their traces. All this was done in a very short period of time – between one or two hours – which is the time it would take for the victim to realise that his/her phone number was no longer working.

## OPERATION SMART CASH

An eight-month long investigation between the Romanian National Police (Poliția Română) and the Austrian Criminal intelligence Service (Bundeskriminalamt) with the support of Europol has led to the arrest of 14 members of a crime gang who emptied bank accounts in Austria by gaining control over their victims' phone numbers.

The suspects were arrested earlier in February in Romania in simultaneous warrants at their homes in Bucharest (1), Constanta (5), Mures (6), Braila (1) and Sibiu (1).

The thefts, which netted dozens of victims in Austria, were perpetrated by the gang in the spring of 2019 in a series of SIM swapping attacks.

Once having gained control over a victim's phone number, this particular gang would then use stolen banking credentials to log onto a mobile banking application to generate a withdraw transaction which they then validated with a one-time password sent by the bank via SMS allowing them to withdraw money at cardless ATMs.

It is estimated that this gang managed to steal over half a million euros this way from unsuspecting bank account owners.

Both these cases were referred to Europol's European Cybercrime Centre (EC3) due to the demanding investigative measures run across borders. Its dedicated teams of specialists helped the national authorities build an up-to-date intelligence picture of the different criminal groups, facilitating the development of a joint strategy to target the criminals.

"Fraudsters are always coming up with new ways to steal money from the accounts of unsuspecting victims. Although seemingly innocuous, SIM swapping robs victims of more than just their phones: SIM highjackers can empty your bank account in a matter of hours. Law enforcement is gearing up against this threat, with coordinated actions happening across Europe," said Fernando Ruiz, acting Head of Europol's European Cybercrime Centre.

## DON'T BE THE NEXT VICTIM

So how can you prevent SIM swapping? Simplistically put, it all starts with identify theft. Criminals can get hold of your personal data by searching for it on social media, by attacking your device with malware that will grant them access to your sensitive data or through social engineering attacks such as phishing, vishing or smishing. Here are a few tips to help you stay one step ahead:

- Keep your devices' software up to date
- Do not click on links or download attachments that come with unexpected emails
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information
- Limit the amount of personal data you share online
- Try to use two-factor authentication for your online services, rather than having an authentication code sent over SMS
- When possible, do not associate your phone number with sensitive online accounts
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.

If your phone loses reception suddenly in an area where you should have connectivity:

- Report the situation to your service provider
- If there are suspicious transactions in your bank account, contact the bank
- Immediately change all the passwords for your online accounts
- Keep all evidence, in case you will need to contact the police

For more advice on how to protect your financial information from cyber scams, visit our dedicated page.


CRIME AREAS Cybercrime • High-Tech crime • Forgery of money and means of payment
TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other
ENTITIES European Cybercrime Center (EC3)

---

**Source URL:** https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers