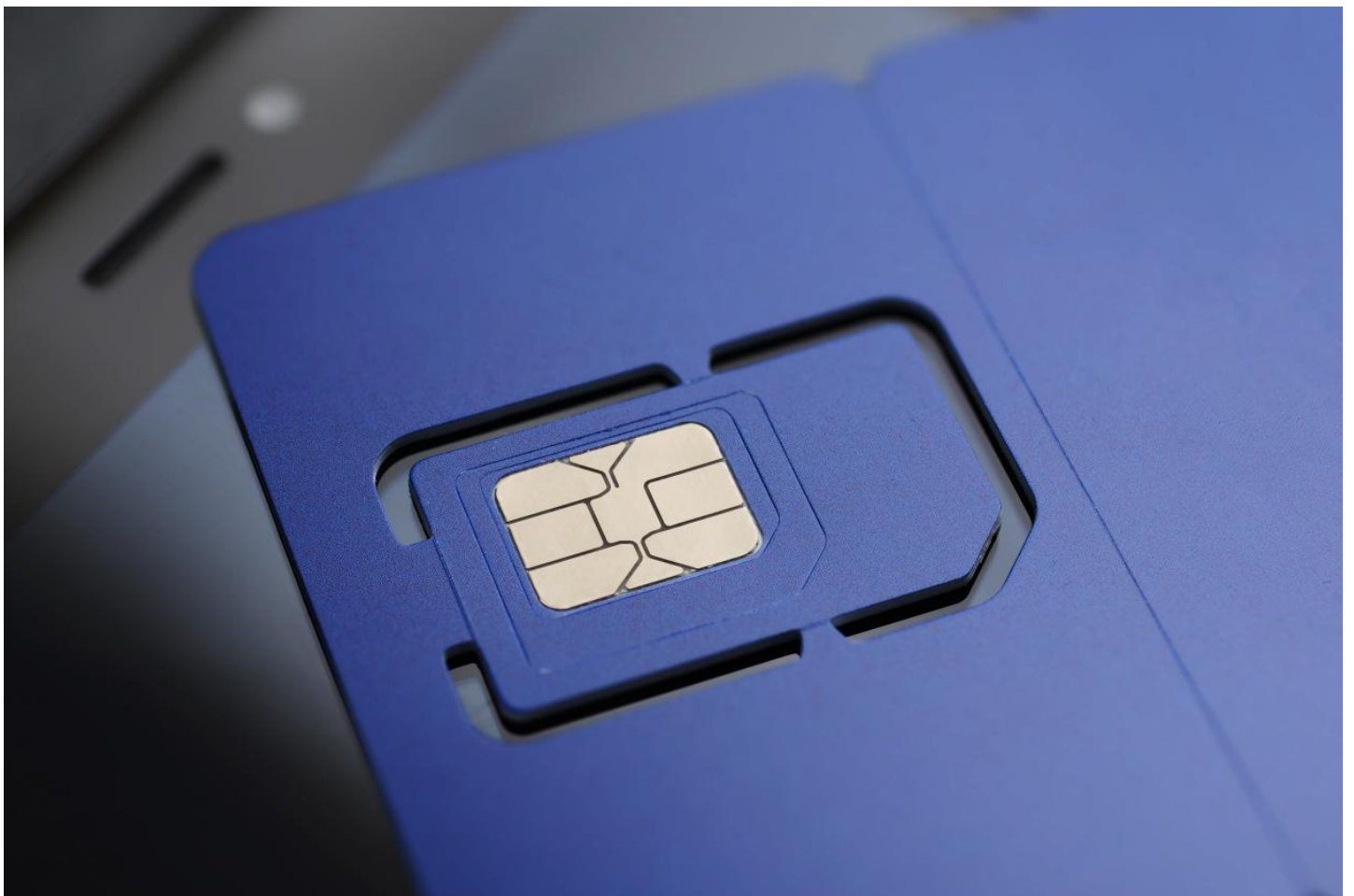


# TEN HACKERS ARRESTED FOR STRING OF SIM-SWAPPING ATTACKS AGAINST CELEBRITIES

10 Feb 2021

[Press Release](#)

Criminals stole over USD 100 million in cryptocurrencies by hijacking phone numbers



A total of 8 criminals have been arrested on 9 February as a result of an international investigation into a series of sim swapping attacks targeting high-profile victims in the United States. These arrests follow earlier ones in Malta (1) and Belgium (1) of other members belonging to the same criminal network.

The attacks orchestrated by this criminal gang targeted thousands of victims throughout 2020, including famous internet influencers, sport stars, musicians and their families. The criminals are believed to have stolen from them over USD 100 million in cryptocurrencies after illegally gaining

access to their phones.

This international sweep follows a year-long investigation jointly conducted by law enforcement authorities from the United Kingdom, United States, Belgium, Malta and Canada, with international activity coordinated by Europol.

## A NETWORK OF SIM HIJACKERS

Initiated in the spring of 2020, the investigation uncovered how a network composed of a dozen criminals worked together to access the victims' phone numbers and take control of their apps or accounts by changing the passwords.

This enabled them to steal money, cryptocurrencies and personal information, including contacts synced with online accounts. They also hijacked social media accounts to post content and send messages masquerading as the victim.

This type of fraud is known as 'sim swapping' and it was identified as a key trend on the rise in the latest [Europol Internet Organised Crime Threat Assessment](#). It involves cybercriminals taking over use of a victim's phone number by essentially deactivating their SIM and porting the allocated number over to a SIM belonging to a member of the criminal network.

This is typically achieved by the criminals exploiting phone service providers to do the swap on their behalf, either via a corrupt insider or using social engineering techniques.

## EUROPOL'S INVOLVEMENT

Europol's European Cybercrime Centre (EC3) supported the case from the onset by providing the following:

- › Organised operational meetings to coordinate the international activity;
- › Facilitated the information exchange between all partners and cross-checked data sent in by the partners against Europol's databases;
- › Supporting the action day by setting up a Virtual Command Post to provide to the investigators in the field real time and secure exchange of information and analytical support.

## DON'T BE THE NEXT VICTIM

It's not just celebrities who are under attack. Anyone and everyone with a mobile phone can fall victim to sim swapping. Here are a few tips to help you stay one step ahead from the criminals after your personal information:

- › Keep your devices' software up to date
- › 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

For more advice on how to protect your financial information from such a scam, [visit our dedicated page](#).

The following law enforcement agencies took part in this operation:

- › **United Kingdom:** National Crime Agency
- › **United States:** US Secret Service, Federal Bureau of Investigation, Homeland Security Investigations, Santa Clara REACT;
- › **Belgium :** Federal Police (Federale Politie, Police Fédérale); Police Zone RIHO (Politiezone RIHO);
- › **Malta:** Malta Police Force (Il-Korp tal-Pulizija ta' Malta);
- › **Canada:** Royal Canadian Mounted Police Force, Hamilton Police Service, Toronto Police Service, Edmonton Police Service.

CRIME AREAS

[Cybercrime](#) • [Forgery of money and means of payment](#) • [Payment Fraud](#)

TARGET GROUPS

[General Public](#) • [Law Enforcement](#) • [Academia](#) • [Professor](#) • [Students](#) • [Researcher](#) • [Press/Journalists](#) • [Other](#)

---

**Source URL:** <https://www.europol.europa.eu/newsroom/news/ten-hackers-arrested-for-string-of-sim-swapping-attacks-against-celebrities>