

A photograph of the Europol building, a modern, multi-story structure with a grey brick facade and large windows. The word "EUROPOL" is visible on the building's facade. In the top left corner, there is a white circular graphic with the Europol logo and some decorative lines.

 **EUROPOL**

# **GSMA** **FINANCIAL** **SERVICES** **COMMUNITY**

**22 / 10 / 20**

---

Jorge Rosal  
EC3/ AP Terminal

**PUBLIC INFORMATION**





- ***CYBER-DEPENDENT CRIME***
- ***CHILD SEXUAL EXPLOITATION ONLINE***
- ***PAYMENT FRAUD***
- ***THE CRIMINAL ABUSE OF THE DARK WEB***

<https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020>

# ***Key threats in Payment Fraud***

***SIM  
Swapping  
&  
Smishing***


***Business  
Email  
Compromise  
BEC***



***Investment  
Fraud***

***Digital  
Skimming***



- *Two main varieties* 
  - CEO fraud*
  - INVOICE Fraud*
- *Different Modus operandi (phishing, spear phishing, ...)*
- *Global problem (businesses, organizations, ...)*
- *High degree of sophistication*



# INVESTMENT FRAUD

- *Attractive investment opportunities*
- *Social media*
- *Thousands of victims, millions of losses*
- *High level of complexity*



# DIGITAL SKIMMING

- *Evolution from physical skimming to e-skimming*
- *Hundreds of affected e-merchants*
- *Difficult detection*
- *Crime as a Service*



Thank you for your  
attention

Any  
questions?

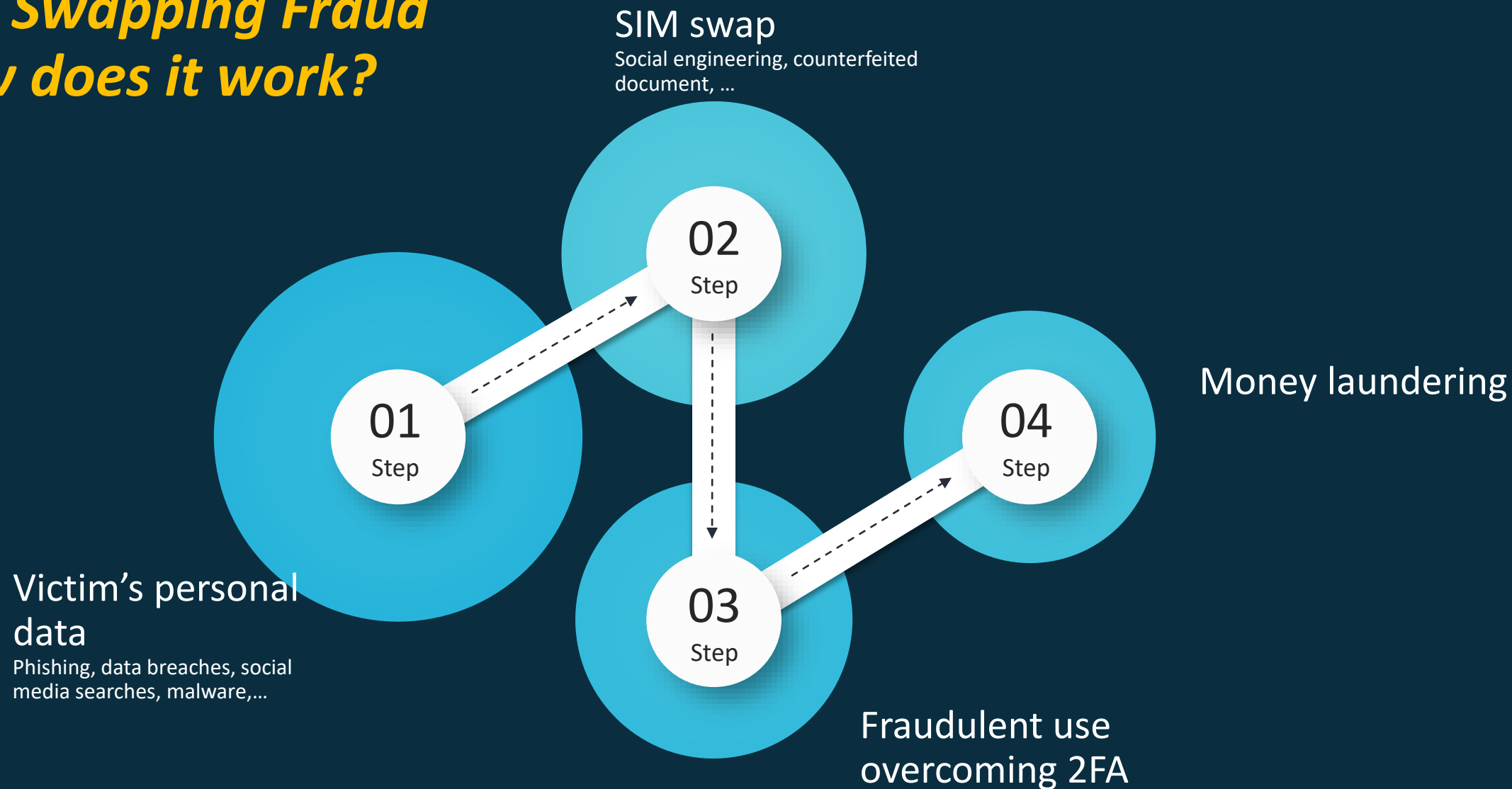
EUROPOL

[www.europol.europa.eu](http://www.europol.europa.eu)



# ***SIM Swapping Fraud***

## ***How does it work?***





# *OPERATION QUINIENTOS*

- A joint investigation against an international OCG dedicated to online and financial fraud using the SIM swapping method
- The investigation initiated in 2019 by the Spanish authorities was supported by Europol and the Italian authorities.
- The OCG operated in different Spanish locations and conducted more than 100 attacks, which generated more than 3 million Euros
- Victims were defrauded with amounts from 6.000 to 137.000 Euros

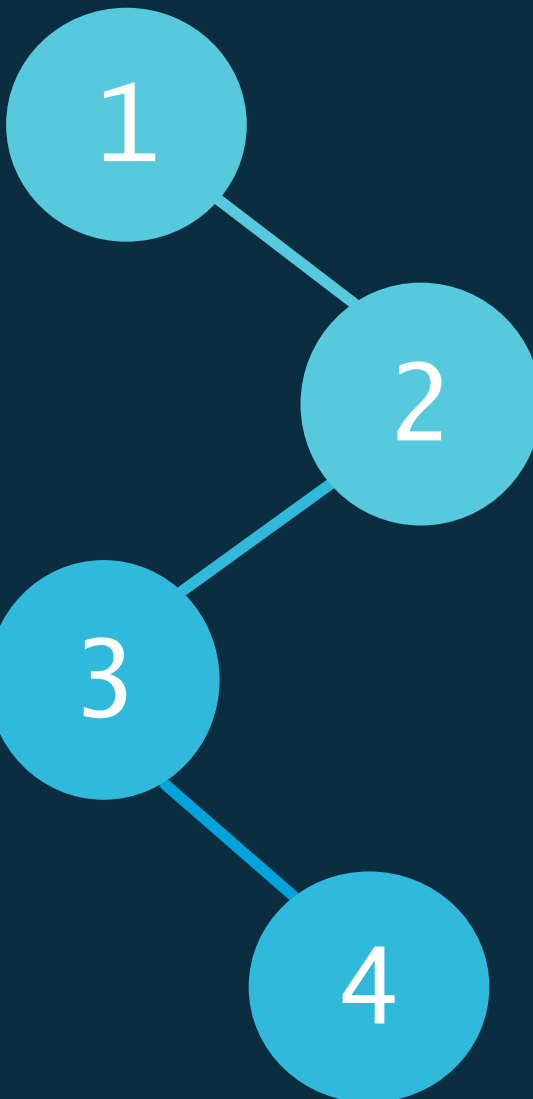
## *Targeting victims*

Criminals got access to banking information (accounts, passwords) via phishing, malware

## *Illegal proceeds*

Wire transfers

Loans and financial products



## *Op. Quinientos*

## *Modus operandi*

### *SIM duplicate*

Impersonation of the victims  
using counterfeited documents

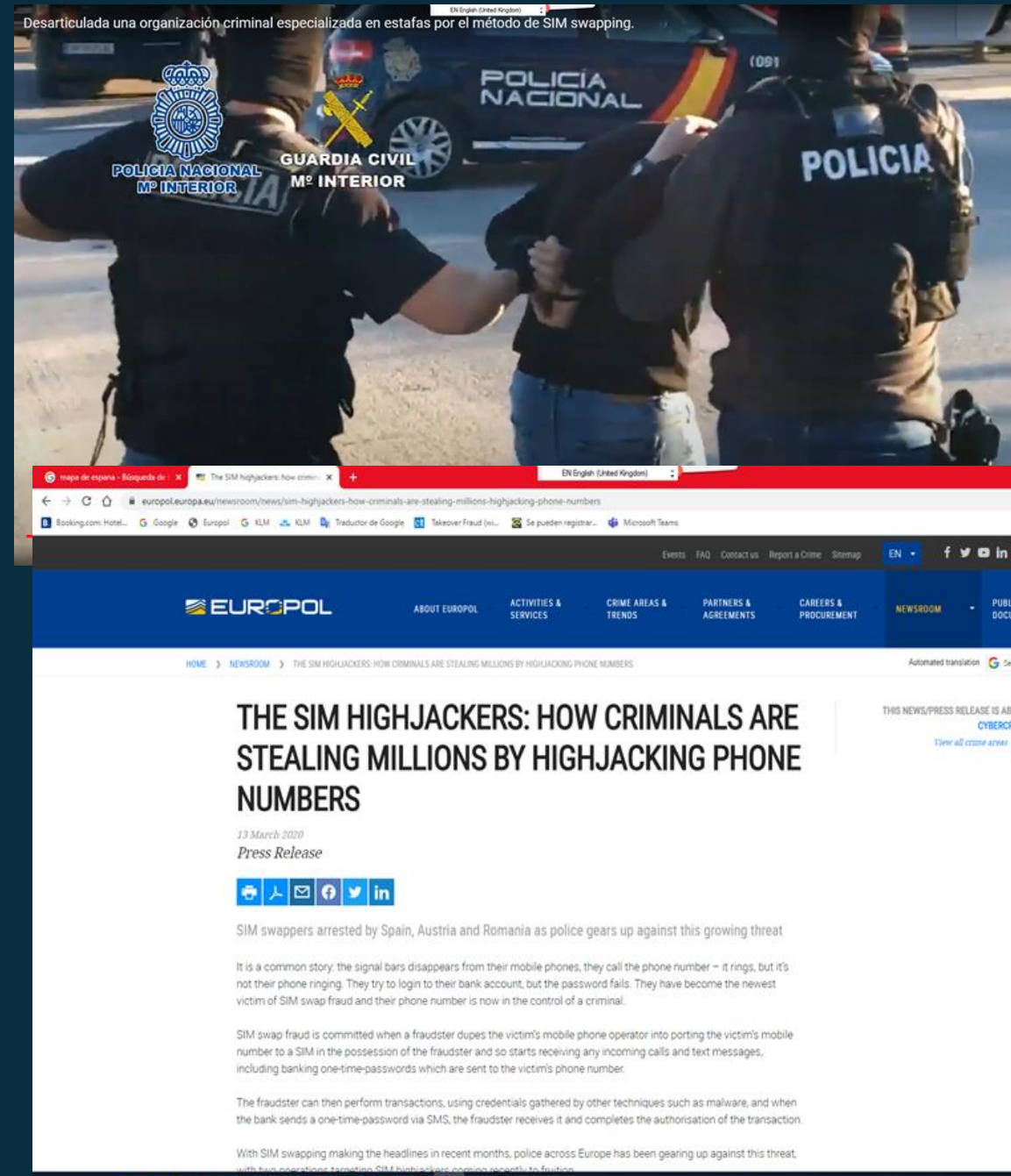
### *Obfuscation / Money laundering*

Shell companies

Money mules network

# RESULTS

- Twelve arrests in different Spanish locations
- Two house searches
- Cash, jewellery, high-end cars, more than 100 cc, numerous duplicated SIMs and equipment to produce fake documents
- The arrests, from 4 different nationalities, were charged with financial fraud, forgery, money laundering



# PREVENTION & AWARENESS

## SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.

### HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.

With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession

The fraudster can now receive incoming calls and text messages, including access to the victim's online banking

The victim will notice the mobile phone lost service, and eventually will discover they cannot login to their bank account

### WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Buy from trusted sources. Check the ratings of individual sellers.
- Restrict information and show caution with regard to social media.
- Download apps only from official providers and always read the apps permissions.
- Never open suspicious links or attachments received by email or text message.
- When possible, do not associate your phone number with sensitive online accounts.
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.
- Update your passwords regularly.
- Frequently check your financial statements.

### ARE YOU A VICTIM?

- If your mobile phone loses reception for no reason, report it immediately to your service provider.
- If your service provider confirms that your SIM has been swapped, report it to the police.



#TelecomFraud

EUROPOL  
EC3 | European Cybercrime Centre



**Thank you for your attention**  
Any questions?

The Europol logo, featuring a stylized blue and yellow graphic to the left of the word "EUROPOL" in blue capital letters.

**EUROPOL**

[www.europol.europa.eu](http://www.europol.europa.eu)

