Insights on the rise in online fraud and scams

Edvardas Šileris
Head of the European Cybercrime Centre

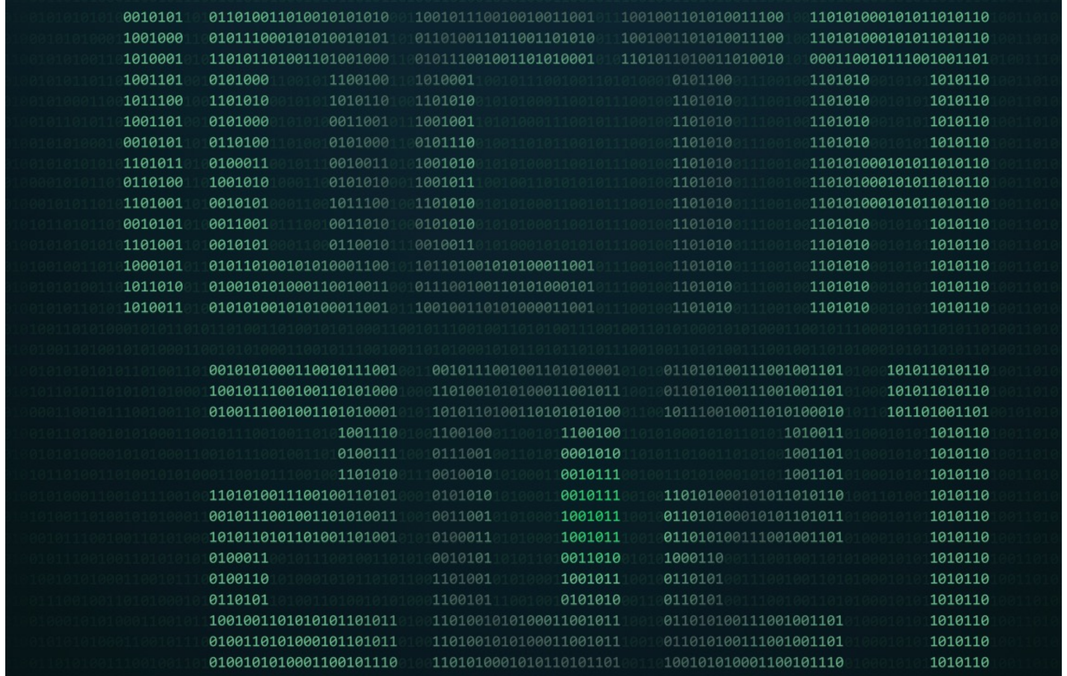
European Cybercrime Centre - EC3

Combating crime in a digital age

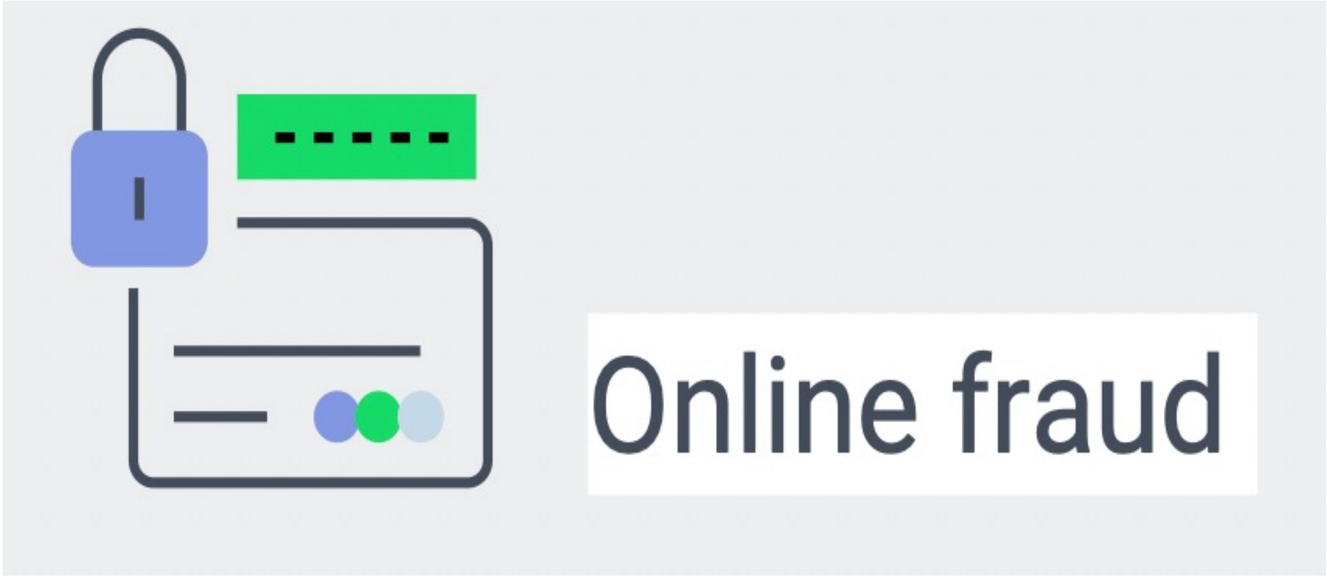
Update date: 19 Nov 2021

Europol set up the European Cybercrime Centre (EC3) in 2013 to strengthen the law enforcement response to cybercrime in the EU and thus to help protect European citizens, businesses and governments from online crime. Since its establishment, EC3 has made a significant contribution to the fight against cybercrime: it has been involved in tens of high-profile operations and hundreds on-the-spot operational-support deployments resulting in hundreds of arrests, and has analysed hundreds of thousands of files , the vast majority of which have proven to be malicious.

EUROPOL



INTERNET ORGANISED CRIME THREAT ASSESSMENT 2021



Online fraud

Key findings

- COVID-19 continues to have a significant impact on the European fraud landscape in the second year of the pandemic.
- Phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication.
- Investment fraud is thriving as citizens incur devastating losses, but business email compromise (BEC) and CEO fraud also remain key threats.
- Card-not-present fraud appears under control as COVID-19 restrictions curb travel-based types of fraud.

The Human Factor

While financial institutions have increasingly improved in securing their assets, the human factor remains the most fragile asset to protect

Financial institutions are increasing their security standards in compliance with security standards developed by public and private parties

There has been an increase on vishing and smishing cases. SIM swapping attacks play an important role as SMS remains the most used system for receiving OTP

Two Factors Authentication for costumers and One Time Passcode (OTP) used by banks and financial operators have significantly reduced fraudulent personification practices

The high amount of personal data available online enables criminals to get direct access to the applications installed on the user's device

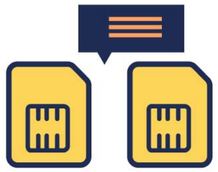
As a result, fraudsters have developed their illicit schemes combining social engineering and technical components. They rely on a widespread of personal information available online

Sim Swapping

How it works

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

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

Am I a Victim?

What do I need to do?

Step 01

Assess if your mobile phone loses reception for no reason

Step 02

Report it immediately to your service provider

Step 03

If your service provider confirms that your SIM has been swapped, **report it to the police**

How to Protect yourself

- Keep your software updated, including your browser, antivirus and operating system.
- Restrict information and show caution with regard to social media.
- Never open suspicious links or attachments received by email or text message.
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- Update your passwords regularly.
- Buy from trusted sources. Check the ratings of individual sellers.
- Download apps only from official providers and always read the apps permissions.
- 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.
- Frequently check your financial statements.

Operation **SECRETO**

Cross-border operation coordinated by Europol and led by the Spanish National Police (Policía Nacional) and the US Secret Service.

The criminal network deceived 50 financial institutions through shell companies.

104
arrests

19
European arrest warrants executed

14
high-end vehicles seized

88
house searches

€406 000
seized in cash

+ €12 million
in damages

87 accounts
> €1.3 million frozen

Hook, line and sinker: cybercrime network phishing bank credentials arrested in Romania

The criminal group sent phishing text messages and emails to get access to victims' bank accounts

Update date: 02 Oct 2020

29 SEP 2020

www.pexels.com


Creativity it is the
way to success
EUROPOL
www.europol.europa.eu