Crime Prevention Conference
19 February 2020
María Sánchez
European Cybercrime Centre
Europol

PUBLIC INFORMATION

CYBERCRIME AND FRAUD
Europol – AP TERMINAL

Supports EU MS in preventing and combating cyber crimes committed by Organised Groups, particularly those generating large criminal profits such as card present and online fraud.
PART I

IOCTA 2019

What does it say about fraud?
Stolen credit cards for sale in the darweb (only in the 1st half of 2019)

Facilitator
No major innovation in the MO
Moving into other sectors

Data breaches
TP breaches
Social engineering
Malware & network intrusion
Email & messages

More professional
Millions of profit

23M

CNP

Top priority

BEC

Also priority

Key element

Findings

Data

Europol Public Information
Recommendations

01. Cooperation between public and private sector as well as within sectors

02. Speedy access and exchange of information

03. Awareness campaigns (customers and employees) on phishing and social engineering
PART II

Case scenario

How does CNP fraud work?
FR bank
Carding forum
RU criminals
TK router
SE payment processor
FI e-merchant
RU criminals
EE criminals
Carding forum
TK router
Online Card Fraud
10 years and it's only getting more complex!

Easy to conduct
Hard to investigate
Low risk of getting caught

Legislation
EU Directives and industry

Secure Payment Systems
Responsibilities for financial sector

LEA collaboration & PPP

Prevention
Awareness campaigns

Europol Public Information
PART III

Awareness
Europol campaigns
Europol Awareness
A crime prevented won’t need to be investigated!
#BuySafePaySafe

**eCommerce**  
**Black Friday**  
**Cyber Monday**

<table>
<thead>
<tr>
<th><strong>Target</strong></th>
<th>Card-Not-Present fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Operation + Awareness</strong></td>
<td>1 month 1 week</td>
</tr>
<tr>
<td><strong>Pan-EU campaign</strong></td>
<td>18 EU Member States 1 TP</td>
</tr>
<tr>
<td><strong>PPP</strong></td>
<td>500+ merchants worldwide</td>
</tr>
<tr>
<td><strong>Material</strong></td>
<td>Landing page Videos and flyers Social media</td>
</tr>
</tbody>
</table>
## Target
Card-Not-Present fraud

## Operation + Awareness
- **GAAD**: Special events

## English only
- **1 language**

## Europol
- **Partners welcome!**

## Material
- **Fake website**
- **Visuals**
- **Social media**
www.2good2btrue.eu
#DontbeaMule

**Money Muling**

<table>
<thead>
<tr>
<th>Target</th>
<th>Unwilling money mules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation + Awareness</td>
<td>3 months</td>
</tr>
<tr>
<td>Pan-EU campaign</td>
<td>25 EU Member States</td>
</tr>
<tr>
<td>PPP</td>
<td>650+ / 21 banks</td>
</tr>
<tr>
<td></td>
<td>Eurojust</td>
</tr>
<tr>
<td>Material</td>
<td>Landing page, Video, posters, flyers, Social media</td>
</tr>
</tbody>
</table>
MONEY MULING IS AN ILEGAL ACTIVITY

Money muling helps to foster the cycle of criminal activity such as drug dealing, human trafficking and online fraud.

Don’t be an accomplice of organised crime. It isn’t worth it.

CONSEQUENCES CAN BE SEVERE FOR YOU

MONEY MULING HELPS PERPETRATE CRIME

Criminals will try to dupe innocent victims into laundering money on their behalf by making the job offer seem as legitimate as possible.

Be wary of adverts that are poorly written with grammatical errors and spelling mistakes.

“IT THOUGHT IT WAS PART OF THE JOB”

MONEY LAUNDERING IS A CRIME

EASY MONEY IS DANGEROUS MONEY

Don’t be a Mule!

If someone asks you to move money through your bank account in exchange for cash, they are asking you to be a money mule.

This is money laundering, it’s illegal, and the consequences can be severe for you.

Easy money without effort?

Too good to be true?

› A stranger approaches you in person and asks you to move money through your bank account in return for a profit.
› The opportunity to make easy money is presented as risk free.
› You are told what to do and how much others have already earned doing the same.
› For different reasons, money launderers will always ask for your bank account and a small balance.

Leaving launder the proceeds of serious organised crime.

Don’t you might be a mule? Get in touch, verify your bank and the offers appropriately.
#CyberScams

Financial sector fraud

Target
Top 7 frauds

Awareness
ECSM 2018

Pan-EU campaign
28 EU MS
5 TPs

PPP
24 national banking associations

Material
Landing page Videos and posters Social media
Europol / EBF joint action

**GOAL:**
Raise awareness at EU level on the most serious scams affecting the banking sector and their customers

---

**WHAT ARE THE SIGNS?**
- **Business Email Compromise (BEC) Fraud:**
  - A fraudster sends an email that looks genuine and is typically sent to an officer in a company.
  - They are impersonated in an attachment or as a sender.
  - They are directed to pay money to an account.
  - They are directed to pay money to a legitimate entity.

**WHAT CAN YOU DO?**
- **Always get important financial advice before you hand over any money or make an investment.
- **Avoid giving personal information.
- **Verify the sender's identity.
- **Check for spelling mistakes.
- **Be suspicious of urgent requests.

---

**ROMANCE SCAM**
- Scammers target singles on online dating websites, but can also use social media or email to make contact.

---

**INVOICE FRAUD**
- A business is approached by a company that looks legitimate.
  - They are asked to pay money for a service or product.
  - They are directed to pay money to a legitimate entity.

**WHAT CAN YOU DO?**
- **Never assume an invoice is genuine.
- **Verify the sender's identity.
- **Check for spelling mistakes.
- **Be suspicious of urgent requests.

---

**ROMANCE SCAM**
- Scammers target singles on online dating websites, but can also use social media or email to make contact.

---

**BANK SMISHING SIMS**
- Smishing is a combination of the words SMS and phishing.
  - A message is sent to a victim's phone.
  - They are directed to a website.
  - They are asked to provide personal information.

**WHAT CAN YOU DO?**
- **Be suspicious of unexpected links.
- **Never download attachments.
- **Verify the sender's identity.
- **Check for spelling mistakes.

---

**PHISHING CALLS**
- Phishing is a combination of the words phone and phishing.
  - A phone call is made to a victim.
  - They are directed to a website.
  - They are asked to provide personal information.

**WHAT CAN YOU DO?**
- **Never give out personal details over the phone.
- **Verify the caller's identity.
- **Check for spelling mistakes.
- **Be suspicious of urgent requests.

---

**28 EU Member States**
- 5 non EU Member States
- 24 banking associations
What do they have in common?

Key priority

Operational results

Multi-partners

Multi-language

Cybercrime isn’t victimless

Education
Tips & Advise
Increase risk perception

Amplifiers
LEA
Private/public sector

National message
Own language
Own logo
Own channel

IOCTA
EMPACT
ECSM
Thank you for your attention

Any questions?