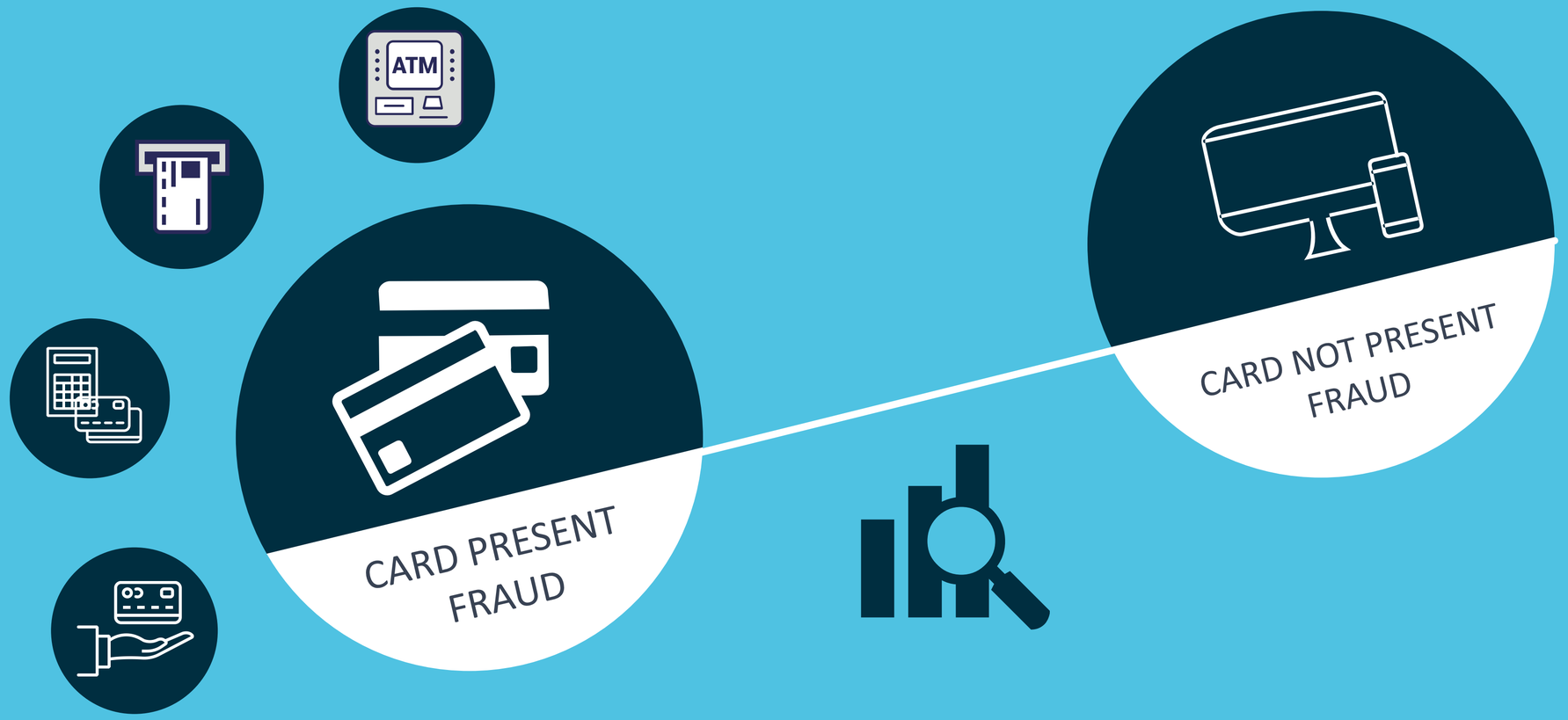
CYBERCRIME AND FRAUD

Crime Prevention Conference
19 February 2020

María Sánchez
European Cybercrime Centre
Europol

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?

Findings

Key element

Data

Stolen credit cards for sale in the darweb
(only in the 1st half of 2019)

23M

Top priority

CNP

Facilitator
No major innovation in the MO
Moving into other sectors

Data breaches

TP breaches

Social engineering

Malware & **network intrusion**

Email & **messages**

Also priority

BEC

C-level

More professional
Millions of profit

Recommendations

01

Cooperation between public and private sector as well as within sectors

02

Speedy access and exchange of information

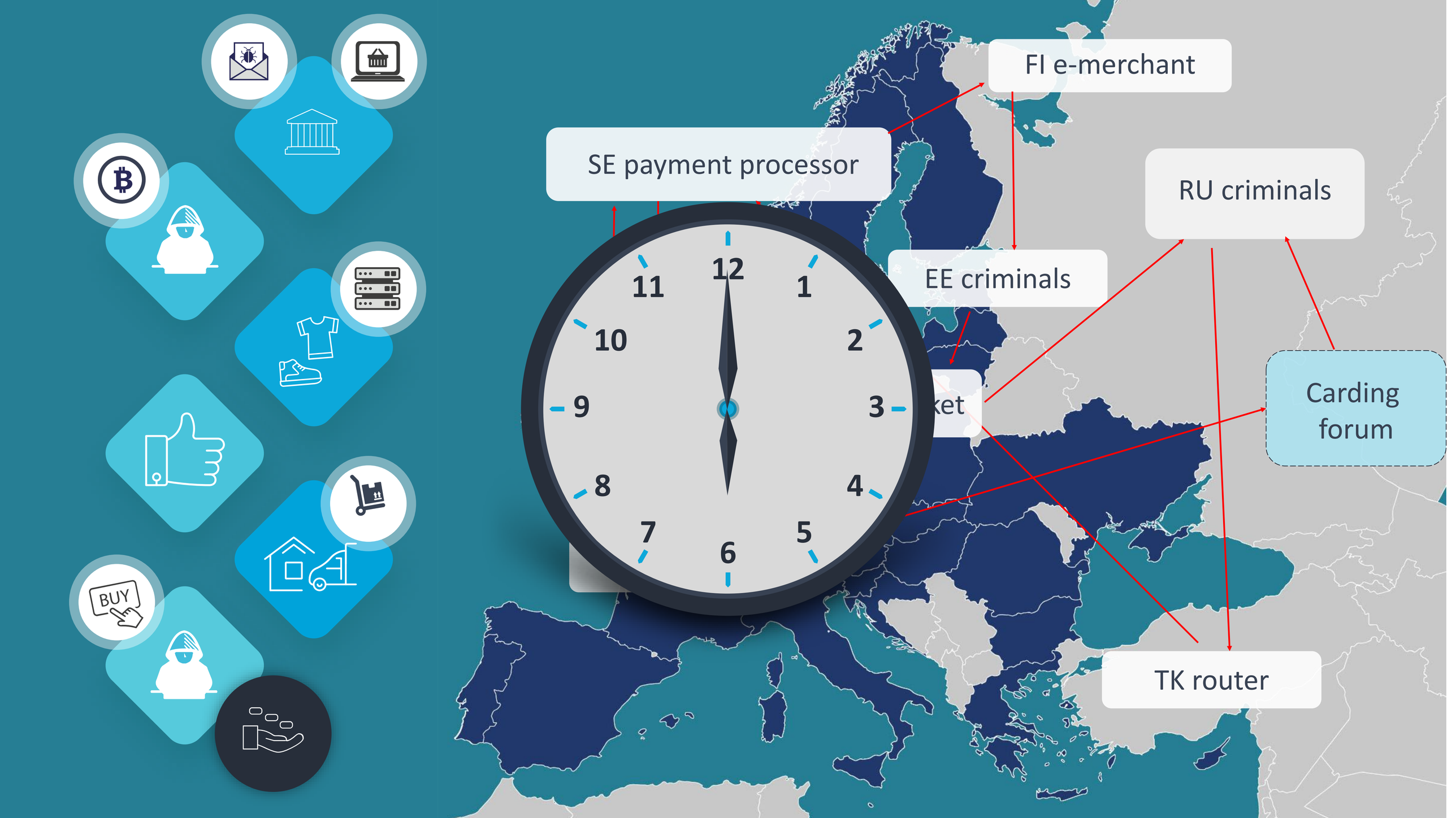
03

Awareness campaigns (customers and employees) on phishing and social engineering

PART II

Case scenario

How does CNP fraud work?


BUY
FI e-merchant
SE payment processor
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

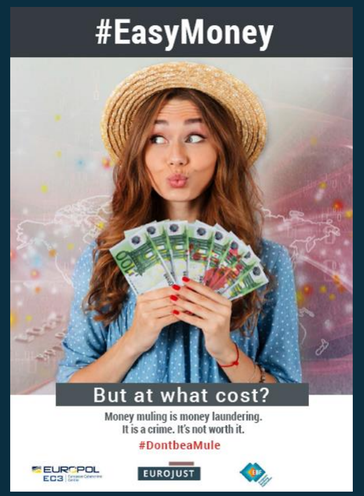
PART III

Awareness

Europol campaigns

Europol Awareness

A crime prevented won't need to be investigated!



#BuySafePaySafe

eCommerce

Black Friday

Cyber Monday

Target

Card-Not-Present fraud

Operation + Awareness

1 month | 1 week

Pan-EU campaign

18 EU Member States | 1 TP

PPP

500+ merchants worldwide

Merchants, logistics firms, financial institutions

Material

Landing page | Videos and flyers | Social media

#2Good2BTrue

eCommerce

Target

Card-Not-Present fraud

Operation + Awareness

GAAD | Special events

English only

1 language

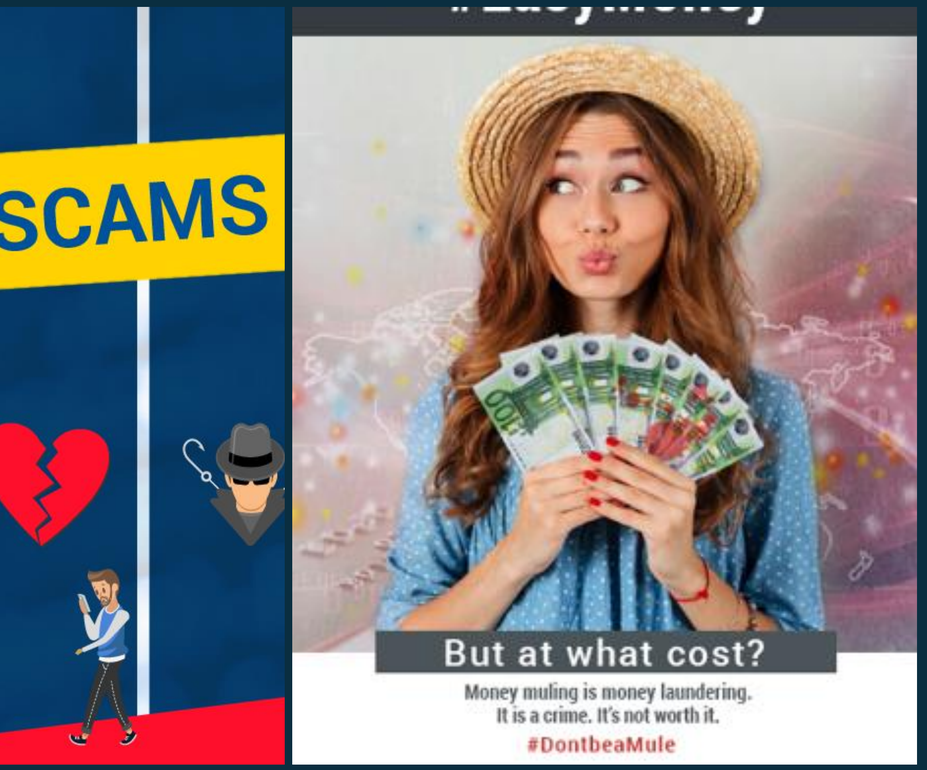
Europol

Partners welcome!

Material

Fake website | Visuals | Social media

www.2good2btrue.eu



#DontbeaMule

Money Muling

Target

Unwilling money mules

Operation + Awareness

3 months | 2-7 days

Pan-EU campaign

25 EU Member States | 6 TPs

PPP

650+ / 21 banks

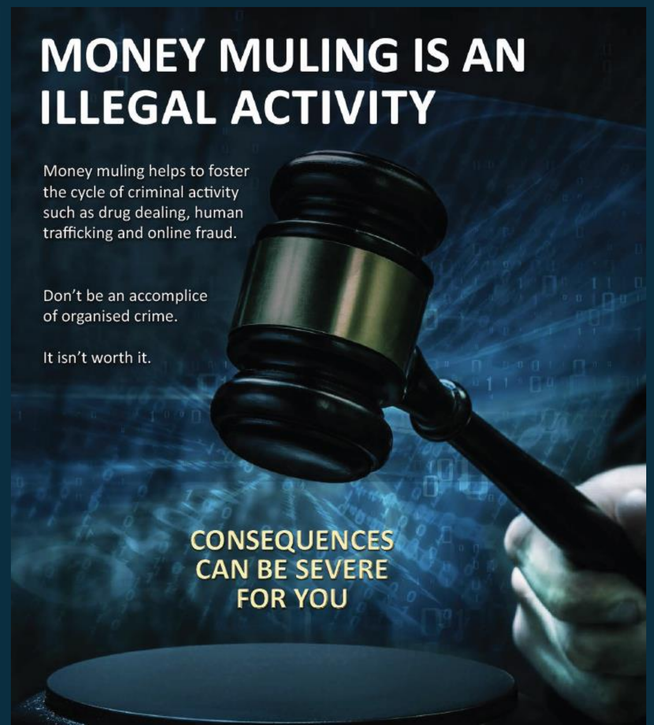
Eurojust

Material

Landing page | Video, posters, flyers | Social media

Participants

Europol
Eurojust
EBF



#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

CEO/BUSINESS EMAIL COMPROMISE (BEC) FRAUD

CEO/BEC fraud occurs when an employee authorised to make payments is tricked into paying a fake invoice or making an unauthorised transfer out of the business account.

HOW DOES IT WORK?

A fraudster calls or emails posing as a high ranking figure within the company (e.g. CEO or CFO).

They have a good knowledge about the organization.

They require an urgent payment.

They use language such as: 'Confidentiality', 'The company trusts you', 'I am currently unavailable'.

They refer to a sensitive situation (e.g tax control, merger, acquisition).

Often, the request is for international payments to banks outside Europe.

The employee transfers funds to an account controlled by the fraudster.

Instructions on how to proceed may be given later, by a third person or via email.

The employee is requested not to follow the regular authorisation procedures.

WHAT ARE THE SIGNS?

INVESTMENT SCAMS

Common investment scams may include lucrative investment opportunities such as shares, bonds, cryptocurrencies, rare metals, overseas land investments or alternative energy.

WHAT ARE THE SIGNS?

- You are promised quick returns and assured that the investment is safe.
- The offer is only available for limited time.
- You receive an unsolicited call, repeatedly.

- The offer is only available to you and you are asked not to share it.

WHAT CAN YOU DO?

- **Always get impartial financial advice** before you hand over any money or make an investment.

INVOICE FRAUD

HOW DOES IT WORK?

- A business is approached by somebody pretending to represent a supplier/service provider/creditor.
- A combination of approaches can be used: telephone, letter, email, etc.
- The fraudster requests that the bank details for a payment (i.e. bank account payee details) of future invoices be changed. The new account suggested is controlled by the fraudster.

WHAT CAN YOU DO?

AS A BUSINESS

Ensure that **employees are informed and aware** of this type of fraud and how to avoid it.

Instruct staff responsible for paying invoices to **always check them for any irregularities**.

Implement a **procedure to verify** the legitimacy of payment requests.

Review information posted on your company website, in particular contracts and suppliers. Ensure your staff limit what they share about the company on their social media.

European Banking Federation @EBFeu · Oct 17

And we have lift-off for the #CyberScams campaign!

Wim Mijs and Steven Wilson press the button at the #EBFCyber18 conference in Brussels. Campaign will run in 33 countries and many different languages worldwide! – at Les Ateliers des Tanneurs

You, Europol, European Banking Federation and Wim Mijs

ROMANCE SCAM

Scammers target victims on online dating websites, but can also use social media or email to make contact.

WHAT ARE THE SIGNS?

Someone you have recently met online professes strong feelings for you, asking to chat privately.

Their messages are often poorly written and vague.

Their online profile is not consistent with what they tell you.

They may ask you to send intimate pictures or videos of yourself.

First they gain your trust. Then they ask you for money, gifts or your bank account/credit card details.

If you don't send the money, they

WHAT CAN YOU DO?

- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used elsewhere.
- **Be alert** to spelling and grammar mistakes, inconsistencies in their stories and excuses such as their camera not working.
- **Don't share** any compromising material that could be used to blackmail you.

3 @EC3Europol · Oct 17

Europol is and will continue to be a key partner in the cooperation with the banking dustry. The #CyberScams campaign is a model to replicate in other sectors". @JKingEU osing remarks at #EBFCyber18.

European Banking Federation, Julian King and Europol

GOAL:

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

SPOOFED BANK WEBSITES

Bank phishing emails usually include links that will take you to a spoofed bank website, where you are requested to divulge your financial and personal information.

WHAT ARE THE SIGNS?

Spoofed bank websites look nearly identical to their legitimate counterparts. Such websites will often feature a pop-up window asking you to enter your bank credentials. Real banks don't use such windows.

These websites usually display:

Urgency: you will not find such messages on legitimate websites.

Pop-up windows: they are commonly used to gather sensitive information from you. Don't click on them and avoid submitting personal data on such windows.

Poor design: be cautious with websites that have flaws in their design or errors in spelling and grammar.

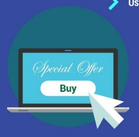
WHAT CAN YOU DO?

ONLINE SHOPPING SCAMS

Online deals are often a good buy, but beware of scams.

WHAT CAN YOU DO?

- **Use domestic retail websites** when possible – it will be more likely that you can sort out any problems.
- **Do your research** – check reviews before buying.
- **Use credit cards** – you have more chances of getting you money back.
- **Pay only by using a secure payment service** – Are they asking for a money transfer service or a wire transfer? Think twice!
- Pay only when connected to a **secure internet connection** – avoid using free or open public wifi.
- Pay only on a **safe device** – Keep your operating system and security software up to date.



- Beware of ads offering outrageous deals or miracle products – **If it sounds too good to be true, it probably is!**
- A pop-up ad stating you have won a prize? **Think twice**, you might just win malware.

28 EU Member States
5 non EU Member States
24 banking associations

BANK SMISHING SMSs

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.

HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- **Don't click on links, attachments or images** that you receive in unsolicited text messages without first verifying the sender.

BANK VISHING CALLS

Vishing (a combination of the words Voice and Phishing) is a phone scam in which fraudsters try to trick the victim into divulging personal, financial or security information or into transferring money to them.

WHAT CAN YOU DO?

- **Beware** of unsolicited telephone calls.
- **Take the caller's number** and advise them that you will call them back.
- In order to validate their identity, **look up the organisation's phone number** and contact them directly.
- **Don't validate the caller using the phone number they have given you** (this could be a fake or spoofed number).
- Fraudsters can find your basic information online (e.g. social media). **Don't assume a caller is genuine** just because they have such details.
- **Don't share** your credit or debit card PIN number or your online banking password. Your bank will never ask for such details.
- **Don't transfer money** to another account on their request. Your bank will never ask you to do so.
- If you think it's a bogus call, **report it to your bank.**

BANK PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

HOW DOES IT WORK?

These emails:

may look identical to the types of correspondence that actual banks send.

replicate the logos, layout and tone of real emails.

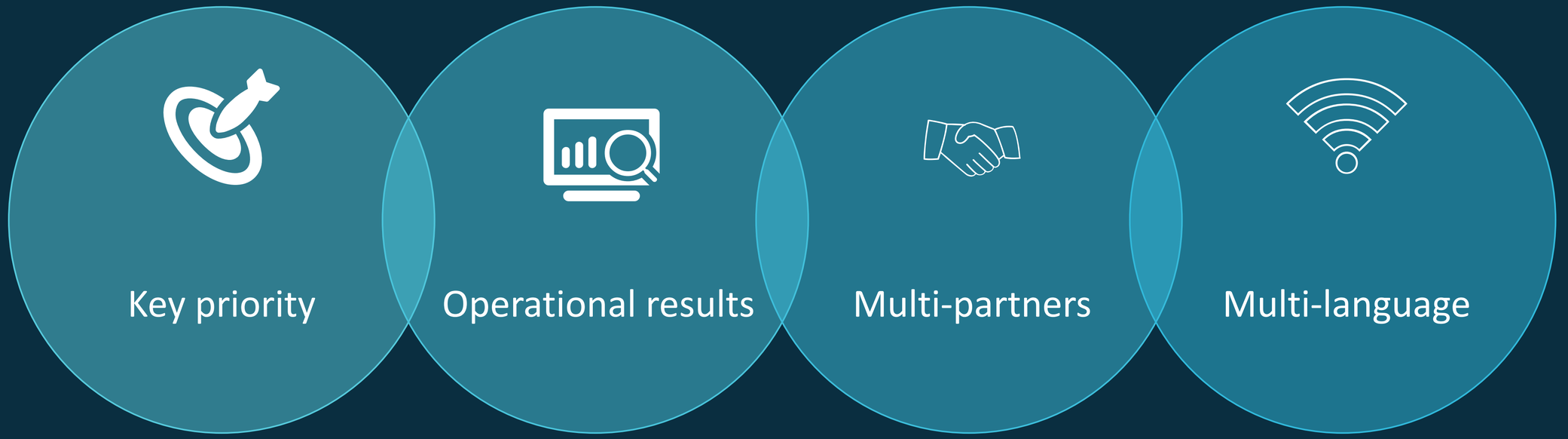
ask you to download an attached document or click on a link.

use language that transmits a sense of urgency.

WHAT CAN YOU DO?

- **Keep your software updated,** including your browser, antivirus and operating system.
- Be especially **vigilant** if a 'bank' email requests sensitive information from you (e.g. your online banking account password).
- **Look at the email closely**: compare the address with previous real messages from your bank. Check for **bad spelling and grammar.**
- **Don't reply to a suspicious email,** instead forward it to your bank by typing in the address yourself.
- **Don't click on the link or download the attachment,** instead type the address in your browser.
- When in doubt, **double check** on your bank's website or give the bank a call.

What do they have in common?



IOCTA
EMPACT
ECSM

Cybercrime isn’t victimless
Education
Tips & Advise
Increase risk perception

Amplifiers
LEA
Private/public sector

National message
Own language
Own logo
Own channel

Thank you for your attention

Any questions?

www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides