17 October 2018, 10:00 CEST

PRESS RELEASE

Click here and see how your money disappears – criminal #CyberScams of the 21st century

Europol and the European Banking Federation launch awareness campaign on 7 most common online financial scams

BRUSSELS/THE HAGUE - Europol's European Cybercrime Centre (EC3), **the European Banking Federation** and their partners from the public and private sector are kicking off today the **#CyberScams** awareness campaign as part of the European Cyber Security Month.

Over the next week, law enforcement agencies from all **28 EU Member States, 5 non- EU Member States[1], 24 national banking associations** and banks and many other cybercrime fighters will be raising awareness about this criminal phenomenon. This pan-European endeavour will be driven by a communication campaign via social media channels and national law enforcement, bank associations and financial institutions.

Following IOCTA 2018 recommendations, the most effective defence against social engineering is the education of potential victims– who can be anyone of us when we go online. Raising awareness among the general public on how to identify such deceiving techniques will keep both themselves and their finances safe online.

For this campaign, awareness-raising material has been developed **in 27 languages**, available for public download, which includes information on the 7 most common online financial scams, and how to avoid them:

- **CEO fraud**: scammers pretend to be your CEO or senior representative in the organisation and trick you into paying a fake invoice or making an unauthorised transfer out of the business account.
- **Invoice fraud**: they pretend to be one of your clients/suppliers and trick you into paying future invoices into a different bank account.
- **Phishing/Smishing/Vishing**: they call you, send you a text message or an email to trick you into sharing your personal, financial or security information.
- **Spoofed bank website fraud**: they use bank phishing emails with a link to the spoofed website. Once you click on the link, various methods are used to collect your financial and personal information. The site will look like its legitimate counterpart, with small differences.
- **Romance scam**: they pretend to be interested in a romantic relationship. It commonly takes place on online dating websites, but scammers often use social media or email to make contact.

[1] Colombia, Liechtenstein, Norway, Switzerland and Ukraine

- **Personal data theft**: they harvest your personal information via social media channels.
- **Investment and online shopping scams**: they make you think you are on a smart investment… or present you with a great fake online offer.

The internet has become very attractive for cybercriminals. Attackers are using sophisticated tricks and promises to wrench money or valuable financial information out of you. Scams featuring a long-lost deceased relative or Nigerian princes are not the only tricks in the book anymore. The tactics used by cybercriminals are becoming increasingly innovative and harder to detect. From pretending to be the CEO of your organisation to impersonating a romantic interest, the online scammers of today will do what it takes to get what they want – your money and/or banking credentials.

As highlighted in the Internet Organised Crime Threat Assessment (IOCTA) 2018, social engineering continues to grow as the engine of many cybercrimes, with phishing as the most frequent form. Criminals use social engineering to achieve a range of goals: to obtain your personal data, hijack your accounts, steal your identity, initiate illegitimate payments, or convince you to proceed with any other activity against your self-interest, such as transferring money or sharing personal data. One single click can be enough to compromise your whole organisation.

Read more on how to stay protected on the #CyberScams dedicated webpage.

The European Cyber Security Month (ECMS) is an EU awareness campaign that promotes cyber security among citizens and organisations, highlighting simple steps that can be taken to protect their personal, financial and professional data.

Follow the **#CyberScams** campaign:

Europol and EC3 Twitter, Facebook, Instagram, Youtube and LinkedIn
EBF Twitter, Facebook and Linkedin