Preventing Individual Fraud

Toolbox

Series No 13

EUCPN
EUROPEAN CRIME PREVENTION NETWORK

eu2018bg.bg
Българско председателство на
Съвета на Европейския съюз

> Individual fraud is a type of fraud in which individual citizens are being targeted by criminals and are persuaded into a cooperative mindset. The essential tactic to nudge the victim into this compliant relationship is called social engineering. This allows the offender to obtain the confidence from the victim that is crucial to the success of the scam.

ACKNOWLEDGEMENTS

This toolbox has been developed in close collaboration between the EUCPN Secretariat and the Bulgarian Presidency. We would like to thank them for their efforts during their Presidency and organising a seminar on phone scams.

Furthermore, we would like to thank all EUCPN National Representatives, Substitutes and Academic Contact Points for their continuous support of our work, for sharing their expertise and for providing information for this toolbox.

We particularly would like to thank the experts who were willing to participate in the workshop we organized in relation to this toolbox:

- Mark Button, University of Portsmouth, United Kingdom
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Fraud Section in National Police General Directorate, Bulgaria
- Charlotta Mauritzson, National Fraud Centre, Sweden
- Andries Bomans, Centre for Cybersecurity, Belgium
- Constantin Lica, Fight against Fraud Department, Romania
- Aurelian Bocan, General Directorate of Bucharest Police, Romania
- Romana Mazalová, 'Nedáme se' project, Czech Republic

Citation
EUCPN (2018). EUCPN Toolbox Series No.13 Preventing individual fraud. Brussels

Legal notice
The contents of this publication do not necessarily reflect the official opinion of any EU Member State or any agency or institution of the European Union or European Communities.

Authors/editors
Jorne Vanhee, Research Officer, EUCPN Secretariat, Brussels, Belgium
Febe Liagre, Strategy and Policy Officer, EUCPN Secretariat, Brussels, Belgium

In the framework of the project 'The further implementation of the MAS of the EUCPN and the Informal Network on the Administrative Approach' - EUCPN Secretariat, November 2018, Brussels

With the financial support of the Prevention of and Fight against Crime Programme of the European Union
European Commission – Directorate-General Home Affairs

CONTENTS

03

PREFACE

The 13th toolbox in the series published by the EUCPN Secretariat focusses on the main theme of the Bulgarian Presidency: fraud with a special focus on phone scams. As fraud covers a whole range of topics, we decided to narrow down our focus to individual fraud. This entails frauds committed against individuals by individuals or criminal organisations. Increasingly, this type of fraud has become a profitable and cross-border enterprise, some scholars even call these offenders 'scampreneurs'. Consequently, this type of crime deserves an EU-wide approach. This is also made apparent in the policy paper which is written in tandem with this toolbox.

This toolbox consists of three parts. The first tries to lay out the current intelligence picture on individual fraud. We discuss interesting good practices in the second part and also posit some recommendations on how to prevent phone scams. These good practices are listed in the third part. An executive summary is also provided to the reader.

EXECUTIVE SUMMARY

The 13th toolbox in the series published by the EUCPN Secretariat focusses on the prevention of *individual fraud.* The Bulgarian Presidency (first half of 2018) decided to focus on:

> “[...] *fraud-related issues, in particular telephone scams. This type of crime has become a profitable criminal activity in recent years, which is developing at both national and cross-border levels. Criminal groups specializing in this activity are developing dynamically and are striking a wider range of victims. Given the active participation of victims and their involvement in criminal scenarios and the traumatizing effect on victims' mind, serious preventive efforts need to be made, taking into account the specificities at local, national and cross-border level”*

Individual fraud is a type of fraud in which individual citizens are being targeted by criminals. Victims are persuaded into a cooperative mindset and defrauded afterwards. Our current understanding of this type of fraud is mainly linked to its contemporary forms, with phishing as the most likely example. However, it is important to recognize that individual fraud has been around for ages. The technological evolutions of the last decades have only allowed these scams to be industrialised on a larger scale than ever deemed possible. Who has not received a phishing e-mail in his life?

As is made clear in the *rationale* from the Bulgarian Presidency, victims actively participate in their victimisation. The offender has set his eyes on the victim's money, but he can only get access to it by persuading the victim to do so. The essential tactic to nudge the victim into this compliant relationship is called **social engineering**. This allows the offender to obtain the confidence from the victim that is crucial to the success of the scam. Social psychology offers us a better understanding of this phenomenon. By appealing to everyday social principles and exploiting these 'human weaknesses', offenders are capable of activating what is called the second route of persuasion. The first route requires a great deal of thought and cognitive effort. The second however needs no real elaboration and reacts almost unconsciously. For example, by pretending to be a person in authority such as a police officer, offenders can easily obtain a level of obedience from their victims. These social and cognitive rules of thumb have their daily uses, but allow offenders to exploit them to their own benefits.

These deceptive tactics are put to use in a wide **variety of scams**. *419 scams, granny scams, romance scams, CEO fraud, …* the possibilities are as endless as the creativity of the scammers. This gamut of deceptive schemes allows fraudsters to target a very large public at once or to adopt a more tailored approach. Increasingly, the latter seems to be the case. Scammers have come to realize that by cleverly targeting their victims, their 'return on investment' is higher. Phishing emails are becoming more and more sophisticated and addressed to a singled-out target (group). The surprising last step in this evolution involves the combination of new and older technology: the telephone. Vishing or voice phishing gives the opportunity of combining the advantages of both the internet and the telephone. Making an online phone call has almost no costs, is harder to trace and can be made automated. Using the telephone has additional benefits: people trust it more and due to the more intimate setting, victims are persuaded more efficiently. Illustrative of the growing level of sophistication: offenders even hire native speakers to make the phone calls feel as genuine as possible.

Our current understanding of individual fraud is limited however. Surrounding this crime is a huge **dark number** as so much of it goes unreported. Victims do not know they were victimised, they do not perceive it as severe enough, they do not think reporting will lead to anything, or they simply do not know where to report in the first place. In addition, because of the active role the victim plays in his own victimisation, feelings of self-blame and embarrassment withhold victims to tell their story. Some scams even have 'build-in' anti-reporting mechanisms, as the victims have to undertake illegal actions in the scheme, incriminating himself in the process. Reporting the scam, would feel as turning yourself in.

This dark number has also given rise to the **myth** that elderly people are the main victims of this crime as they are easy prey. Some studies have disproven this myth, although we should remain cautious due to the limited research that is available. Nonetheless, the younger population and middle-aged group are reported to be more susceptible to scams. Another myth that exists is that victims are typically portrayed as uneducated or financially illiterate, but the opposite seems to be true. One possible explanation is called the 'knowing-doing gap', where people are successful in recognize the signals of a scam, but fail to apply this knowledge to their own situation.

Unfortunately, the existence of so-called ‘**sucker lists**’ is not a myth. Phone scammers can contact their victims randomly or by looking at public registries, but they also share lists amongst themselves with targets that already have been defrauded. The use of such lists is indicative of the high level of repeat victimisation. For example, some scammers will try and ‘help’ you recover your lost assets…

As policing this crime is extremely difficult, the need for prevention is high. However, little academic and evaluative research has been conducted on individual fraud. Nonetheless, we can posit some general findings. The most common prevention tactic is educating the public. This can be done in a general awareness raising campaign, but especially when delivered in some kind of training format, there are some positive effects to be noted. In essence, these trainings try to close down the ‘knowing-doing’ gap to which we referred earlier. Another key tactic is to work with victims. Because of their active role and the existing risk of falling victim multiple times, victims should be supported and be made aware of their specific position.

During the Bulgarian Presidency, the Secretariat gathered a number of **good practices** on this topic. These can be categorised according to their target group. A first category focusses on the entire population. These are awareness raising campaigns, such as the examples from Bulgaria, Sweden, Belgium or Europol. These involve radio spots, posters, flyers, gadgets,… that provide useful information to the public and show how to protect yourself from being harmed. A second set of activities is targeted at the elderly. Here, more interactive methods are being deployed, as is the case in the Czech Republic. The elderly take part in an interactive educational stage play where they learn about the most common deceptive schemes and how to react to them. This ‘lived experience’ should enable them to react adequately in real-life scenarios. The evaluation of this project proved this assumption to be true as the group refused fake deals two and a half times more than a control group that did not watch the play. The last category of prevention activities centred on victims. Examples from Australia, the United Kingdom and Canada showed the need for this type of prevention. There are however – even globally – few support services to victims of individual frauds.

Finally, the EUCPN Secretariat organised a workshop with different experts to draw up some **recommendations** on how to prevent phone scams. These are structured according to the five strategies of situational crime prevention. The first possible strategy is to increase the effort an offender has to take in order for the scam to succeed. Restricting the publication and access to phone numbers can already achieve this. Another technique could be to limit the amount of phone numbers one person is allowed to have or at least link this with a bank account or ID number.

A second strategy is to increase the risks. It is of key importance here to share information. This sharing should not stop at the borders of the public or private sector, or at the national level. All partners have an important piece to fill in the information puzzle. Knowing what you are dealing with increases the chances of preventing it from happening in the first place. Needless to say, reporting should be made more easy and approachable. Information needs to be gathered before it can be shared. Other recommendations were made to reduce the anonymity of the caller, by making it nearly impossible to spoof your location. Voice recognition software could also be of interest here.

Reducing the rewards that can be attained by committing this crime is a third strategy to prevent phone scams. Seizing the illegally obtained assets is the main recommendation here. To do this, monitoring the flow of money is crucial to detect suspicious transactions. An EU-wide initiative with the banking sector to facilitate was recommended by our experts.

Another strategy is to reduce provocations. In this regard, it is import not to share too much information on how the scam was actually executed as this will prevent copycats. It could also help to prevent some forms of repeat victimisation.

The final strategy was to remove the excuses. This is mainly focussed on raising awareness on phone scams and how to protect yourself. The good practices from earlier are shown as key examples here. Awareness campaigns should spread the same message. Therefore, public-private partnerships and international cooperation need to be established to be as consistent as possible: *just say no.*

INTRODUCTION

There is no shortage of examples of fraudulent activities from criminals trying to obtain hard-earned money and/or personal information and no shortage of people falling for them either (Crosman, 2017). Who has not received that ‘once in a lifetime offer’ in his e-mail inbox or has not heard of the Microsoft support scam where you get called in order to be able to repair your computer that was working just fine some minutes ago?

Contrary to popular belief, these types of scams are anything but new. Scams and frauds have been around for centuries (Murphy & Murphy, 2007). Current understanding of personal fraud is intrinsically linked to new technologies, such as the internet, but fraud has occurred since people have been able to speak and own assets (Button & Cross, 2017). Indeed, the internet has provided a new space for criminals to scam a much larger pool of victims than ever deemed possible (Whitty, 2013). New and older technologies such as the telephone are being combined to tailor attacks and maximize profit. The scope and effectiveness have increased, the costs have lowered, but the core techniques remained the same (Crosman, 2017; Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). These new developments, combined with the detrimental impact – financially, emotionally, relational,... – these types of crime have (Button, Lewis, & Tapley, 2009; 2014), have urged the need for prevention and Bulgaria chose this as their focus during their Presidency of the EUCPN in the first half of 2018:

> ‘In the context of prevention, the Bulgarian Presidency will focus on fraud-related issues, in particular telephone scams. This type of crime has become a profitable criminal activity in recent years, which is developing at both national and cross-border levels. Criminal groups specializing in this activity are developing dynamically and are striking a wider range of victims. Given the active participation of victims and their involvement in criminal scenarios and the traumatizing effect on victims’ mind, serious preventive efforts need to be made, taking into account the specificities at local, national and cross-border level.’

This toolbox provides useful insights into these types of fraud and scams and the prevention thereof. The first part of this effort will draw upon existing literature to shed light on this subject that has increasingly come under scrutiny by scholars. Until recently, (criminological) studies have relatively neglected fraud to the benefit of other volume crimes but this has taken a turn (Button & Cross, 2017; Button, Lewis, & Tapley, 2009; Button, Lewis, & Tapley, 2014; Titus & Gover, 2001; Levi, 2008; Button, Tapley, & Lewis, 2012).

In the second part, we will show some good practices related to this crime and posit some recommendations and tips for preventive measures directed at phone scams in particular. These recommendations are based on a workshop that was held with a variety of experts from across the European Union. Finally, a third part will list up some good practices that were gathered during the production of this toolbox.

01

PART I:
INTELLIGENCE PICTURE

1. Introduction

This first part of the toolbox will explore current literature on the topic of scams and frauds. More specifically, in this toolbox we will be focusing on fraud on the individual level, committed mainly (but not exclusively) through the use of ICT (Button, Tapley, & Lewis, 2012). Fraud is a very diverse offence and encompasses a wide range of behaviours (Button, Lewis, & Tapley, 2014). Levi and Burrows (2008) define it as such:

> *'Fraud is the obtaining of financial advantage or causing of loss by implicit or explicit deception; it is the mechanism through which the fraudster gains an unlawful advantage or causes unlawful loss'* (Levi & Burrows, 2008, p. 7)

In general, we can state that all types of fraud involve some kind of deceit or trickery with the intention that it will result to some sort of gain (Button, Lewis, & Tapley, 2009; Murphy & Murphy, 2007; Button & Cross, 2017). Categorizing frauds according to the type of victim, Levi (2008) came up with the following typology:

Victim sector	Victim sub-sector	Examples of fraud
Private	Financial services	- Cheque fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Data-compromise fraud - Embezzlement - Insider dealing/market abuse - Insurance fraud - Lending fraud - Payment card fraud - Procurement fraud
	Non-financial services	- Cheque fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Data-compromise fraud - Embezzlement - Gaming fraud - Lending fraud - Payment card fraud - Procurement fraud
	Individuals	- Charity fraud - Consumer fraud - Counterfeit intellectual property and products sold as genuine - Counterfeit money - Investment fraud - Pension-type fraud
Public	National bodies	- Benefit fraud - Embezzlement - Procurement fraud - Tax fraud
	Local bodies	- Embezzlement - Frauds on Council taxes - Procurement fraud
	International (but affecting public)	- Procurement fraud (by national against other – mainly but not always foreign – companies to obtain foreign contracts) - EU funds fraud

When we focus on the private victim sector and more specifically on the sub-sector of individuals as victims, there are still many different ways to be defrauded, as illustrated by the same figure. Within this toolbox however, we will focus on consumer fraud, which Levi and Burrows (2008) define as:

> *'a broad category including lottery/prize scams; rogue dialling and other communications-based frauds; 'dishonest' mis-descriptions of products and services (such as some 'alternative health care products ' or sex aids); gaming frauds (e.g. ' fixed ' races and matches upon which bets (including spread betting) have been made); purchases of goods and services that are not sent by the supplier'* (Levi & Burrows, 2008, p. 7).

Other terms that circulate within literature are 'individual fraud' (Button, Tapley, & Lewis, 2012) and mass-marketing fraud (Button, Lewis, & Tapley, 2009; Whitty, 2018; 2015; Wood, Liu, Hanoch, Xi, & Klapatch, 2018), although the latter has a more strict focus on mass communication techniques which are being exploited (Button & Cross, 2017). For the purpose of consistency within this toolbox, we will hereafter use the term 'individual fraud', as this reflects our focus the most. Current ideas of this type of fraud are indeed strongly linked to these new technologies, nevertheless it is important to recognise that individual fraud has existed for as long as we have been able to speak and have private property. The evolution of technology has simply altered the means to conduct this type of crime and allowed it to industrialise itself on a larger scale (Button & Cross, 2017; Leukfeldt & Stol, 2011; Crosman, 2017). As such, we can classify these newer forms as 'cyber-enabled crimes', i.e. traditional crimes, which can be increased in scale and reach with the use of ICT. Phishing is probably the best known example of this evolution and takes on massive proportions (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018).

Without categorizing all types of individual fraud as cyber fraud, the focus of this toolbox will be on these contemporary forms of fraud and their current mixed online/offline characteristics. In the following chapters, we will first take a deeper interest into the used persuasive tactics and more specifically into social engineering, which underlies most of these types of fraud (Button, McNaughton, Kerr, & Owen, 2014; Europol, 2017). As the Bulgarian Presidency decided to focus on scams in which the victim actually has an active participation, it is imperative to study how perpetrators nudge people into this cooperative mindset (Button & Cross, 2017). Next, an overview of different types of individual frauds will be given. Finally, we will also look at the profiles of the victims and perpetrators.

Could you please give your employee ID and password to reconcile your salary data?

https://cyberessentialsdotblog.wordpress.com/2017/02/25/phishing-evolved/

2. The art of persuasion

Regardless of the type of scam, building a relationship with the victim is imperative. The offender must attain the confidence of his or her victims through trust, sympathy and persuasion in order for the scam to work (Crosman, 2017). The means that are utilized nowadays might differ; the technique is still basically the same (Maggi, 2010). **Social engineering** is the essential tactic to obtain this confidence and involves deceiving a person in order to convince him or her to either unwittingly divulge sensitive information or carry out some act which they would not normally do (Europol, 2017; Atkins & Huang, 2013; Europol, 2016). Specifically, we will focus on deception based on human interaction: social engineering that takes advantage of the victim's natural inclination to be liked. Additionally, there is however a second category of social engineering that involves computer-based deception, for example with the use of malware that is installed in the email, key loggers, or fake pop-ups (Atkins & Huang, 2013; Singh & Imphal, 2018).

The dubious relationship between the victim and the offender is of key importance within individual fraud. The offender is essentially dependent on the ability to develop a trusting relationship with his or her victim in order to succeed in his malicious intent (Atkins & Huang, 2013). Indeed, the offender must nudge victims to perform actions that they were not intending to do and can even be detrimental to themselves (Yeboah-Boateng & Amanor, 2014; Ollmann, 2007). Most literature surrounding this topic is to be situated in studies within the wider framework of social psychology (Rusch, 1999). According to this body of work:

> *'Social engineers often attempt to persuade potential victims with appeals to strong emotions such as excitement or fear, whereas others utilize ways to establish interpersonal relationships or create a feeling of trust and commitment'* (Workman, 2008, p. 1).

Moreover, Atkins and Huang (2013) add that 'social engineers rely on cognitive biases or social errors in the mental process to initiate and execute their attacks and produce automatic emotional responses in their victims' (Atkins & Huang, 2013, p. 24). These automatic emotional responses hint at what is known as the peripheral route within the Elaboration Likelihood Model. This model seems to have a rather hegemonic position in the literature on scams and why people fall for them. At its core, it assumes that there are two routes of persuasion. One is the central route, which requires a great deal of thought and as a consequence needs high elaboration. The second route, the peripheral route, needs no real elaboration as individuals instead focus on emotional triggers, such as attractiveness or perceived credibility (Petty & Cacioppo, 2012; Petty & Cacioppo, 1986; Rusch, 1999; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Whitty, 2013). Scammers push their victims into this second route and traditionally invoke negative emotions such as greed, loneliness or fear, and recently have started to incorporate mundane and legitimate business enquiries as well (e.g. CEO fraud) (Workman, 2008; Jakobsson, 2016). In order to direct the victim towards this second route, literature defines some principles that are being (mis-)used by perpetrators (Jakobsson, 2016). It is however very important to note that these principles – these cognitive 'rules-of-thumb' – all have their daily uses and utilities. The key here is that perpetrators of scams create a setting where they can apply these 'weapons of persuasion', most of the time a combination of them, to their own benefit. We will now discuss the three most influential authors identified by literature in this regard (Ferreira, Coventry, & Lenzini, 2015).

Among those three, Cialdini and his 'six principles of influence' are cited most often (Rusch, 1999; Workman, 2008; Ferreira, Coventry, & Lenzini, 2015; Bullée, Montoya, Pieters, Junger, & Hartel, 2018; Cialdini, 2001).

1. Authority:

This principle describes people's inclination to comply with the request of authoritative figures. In the right situation, people are highly likely to be responsive to assertions of authority. This also works for symbols of authority, e.g. uniforms, badges and titles or in telephone conversations where authority can easily be claimed.

Example: This principle is very apparent in scams involving fake police officers. We *naturally believe and comply with officers based on their uniform, titles, … Imagine being called by a man claiming to be a police officer and he needs your PIN code as fast as possible in order to shut down your account that has been hijacked by perpetrators. The only thing going down however, will be the amount of money on your account.*

2. Scarcity:

People assign more value to items that are perceived as scarce. This particular item or offer is seen as in short supply or only available for a limited period. As a consequence, it is being perceived as more attractive and desirable.

Example: A lot of phishing emails indicate in their title that the offer is 'limited', 'only 50 remain', 'one of a kind',…

3. Liking and similarity:

People tend to like others who are similar in terms of interests, attitudes, and beliefs. It is a truly human tendency to like people who are like us. Our identification of a person as having characteristics identical or similar to our own also provides a strong incentive for us to adopt a mental shortcut in dealing with that person.

Example: This principle is very apparent with social media influencers. Part of their success stems from the fact that they appear as the 'boy or girl next door'. Of course you would also want to have the same outfit. Similarly, you would also want to buy the same shirt as the one your favourite football player wears. Scammers easily exploit this by referring to known people in their schemes.

4. Reciprocation:

This is a well-known social rule which obliges us to return others what we have received from them. Commonly, this is referred to as 'you scratch my back, I scratch yours'. Even if the favour that someone offers was not requested by the other person, the person who received the favour may feel a strong obligation to respect the rule of reciprocation by agreeing to the favour that the original offeror asks in return. Even if that favour is significantly more costly than the original offer.

Example: If something of value is offered, for instance a free sample, people feel obligated to return this favour by purchasing the full product or service. Even if this free sample is not received yet or exists at all.

5. Commitment and consistency:

Another social rule is consistency in behaviour and the commitment to do so. If we promise something, we will most likely keep our promise because otherwise we seem untrustworthy or undesirable. Consistency is activated by looking and asking for smaller, initial commitments that can be made more easy.

Example: The classic scam involving the Nigerian prince (cf. infra), also known as the 419 scam, typically asks for a smaller favour first to which the victim can say yes easier. Next, a bigger request will be made, which will be difficult to neglect or refuse as the victim will not be consistent with his or her previous behaviour..

6. Social proof/ conformity:

This last principle is also apparent in many social situations. In order to decide what action is most appropriate, we synchronize with other people (peer groups, role models,…). This can even lead to actions that are against our own interest, but allow us to be accepted within the group.

Example: On Facebook, we can see if a page or product is seen as popular by the amount of likes it has. Scammers can create a new page as easily as anyone and with the use of fake likes, this social proof principle can be incited to persuade the victim of its realness and popularity.

Cialdini's principles were originally drawn upon marketing findings, but have proven their importance in social engineering literature as well as scammers mis-using these principles to their benefits. However, some authors have come up with different, yet similar principles with a more applied focus to scams (40). One of these is Gragg and his 'seven psychological triggers' (40,49):

1. Strong affect

This trigger uses a heightened emotional state to allow the perpetrator to get away with more than what would be rationally possible in a normal situation. For example, making the victim feel surprised or angry, will impede him/her from thinking rationally.

Example: Promising the potential victim a prize worth millions, will most likely evoke strong emotions and work as a powerful barrier to evaluate the offer logically and rationally.

2. Overloading

If the victim has too much information to process at once, this will affect the evaluation of the information in a negative way, leading to decisions that would normally not have been made.

Overloading can also be triggered by arguing from an unexpected perspective. A new perspective takes time to process, however if this is not available, it could lead to a reduced capacity of processing the information and consequently, bad decision-making.

Example: In order to comply with GDPR (General Data Protection Regulation), companies throughout the world sent out a massive amount of emails to ask their customers if they agreed with their renewed privacy policy. It did not take long however for fraudsters to exploit this overload and started sending similar messages, but with other intentions than the protection of the population's privacy.

3. Reciprocation

Similar to Cialdini's principle, one should return the favour when given or promised something.

Example: In the 419 scam, victims are promised large rewards. They feel naturally inclined to return the favour by transferring the money.

4. Deceptive relationships

Here, the scammer builds a relationship on false premises, with the purpose of exploiting the other person.

Example: The granny scam makes clever use of the elderly's relation to their grandchildren. Under false premises, they con their way into this intimate and trusting relationship and exploit it to their benefits.

5. Diffusing of responsibility and moral duty

Following this trigger, the target is made to feel only partially responsible for the acts she/he will commit. The actions that follow, will be less difficult to commit and this is especially the case when the target feels as if it is his 'moral duty'.

Example: In CEO fraud, the target can be made to believe that he will be responsible for failing to sign a big contract if he does not make an advanced payment.

6. Authority

Again, similar to Cialdini, people are conditioned in modern-day society to respond to authority and this can easily be exploited by perpetrators.

Example: Using the same example as above, who are you to say 'no' if the order seems to come from the CEO herself?

7. Integrity and consistency

This last trigger is also similar to ‘commitment and consistency’ from Cialdini. People have a tendency to follow through with previous commitments, even if these are potentially harmful to themselves.

Example: This can be used to keep a scam going, but can also initiate the scam by appealing to actions a person would normally do or by mimicking a scenario where the victim already seems to have committed himself to something.

Stajano (2011) is another influential author who came up with ‘seven principles of scams’ that perpetrators use:

1. Distraction principle

While the victim is distracted by what keeps his/her interest, the scammer can commit the real ‘act’ and the victim will most likely not notice it.

Example: In street scams, where the target needs to follow the ball that is hidden under a cup and mixed with other cups, the perpetrators will often talk about the prize the victim can win and show them an example of the prize. All while mixing up the cups and the attention of the victim is gone.

2. Social compliance principle

Similar to Cialdini’s and Gragg’s ‘authority’, Stajano argues that scammers exploit this ‘suspension of suspiciousness’ to make you comply with their wishes.

Example: Perpetrators can also act as if they are legitimate workmen and enter the victim’s house on this premise. Once inside, they can easily rob the house.

3. Herd principle

Consistent with ‘social proof’ from Cialdini, this social principle allows even suspicious victims to let their guard down if they perceive that this is also the case for their peers.

Example: Some phishing emails claim that they have the cure to baldness. Often they will use a quote from a happy ‘customer’ to show that it works. The victim can feel less suspicious as clearly others have also purchased the product.

4. Dishonesty principle

To a certain extent mimicking the ‘diffusing of responsibility and moral duty’ from Gragg, this principle makes sure that you will find it harder to find help. Once you have realised you have been scammed, you are actually involved in a criminal scheme yourself which will make it less likely for you to go to the police. This can also be achieved by shaming the victim.

Example: In a lot of scams, the victim will feel ashamed of having fallen for the trap. This will withhold him for reporting the crime. Fraudsters will specifically fabricate such scams in order to shame the victim (see also infra).

5. Deception principle

Scammers know how to manipulate and will make the victim believe that things and people are real, even if they are not.

Example: In fact, nearly all scams exploit this principle. Things and people are never what they seem in scams. If it seems too good to be true, it probably is.

6. Need and greed principle

Also related to ‘scarcity’ from Cialdini, this principle means that the perpetrators will manipulate your needs and desires in order to get what they want.

Example: When you are in a country with a different currency, you will need to exchange money. This need can easily be exploited by scammers to lower the exchange rates.

7. Time principle

Giving the victim a sense of urgency and time pressure, he or she will most likely speed up the decision making process. This allows for less reasoning, which is to the advantage of the perpetrator as this allows for a more susceptible target.

Example: In many email scams, the victim will be led to believe that he needs to be quick if he does not want to miss out on this 'once in a lifetime chance'.

Ferreira, Coventry and Lenzini (2015, p.3) came up with the following figure to compare these three important groups of principles used and misused by scammers:

	C	G	S
1	Authority	Authority	Social Compliance
2	Social Proof	Diffusion Responsibility	Herd
3	Linking & Similarity	Deceptive Relationship	Deception
4	Commitment & Consistency	Integrity & Consistency	Dishonesty
5	Scarcity	Overloading	Time
6	Reciprocation	Reciprocation	Need & Greed
7	-	Strong Affect	Distraction

Now that we understand some of the key techniques and principles perpetrators of scams use and mis-use, we will take a look at the diversity of scams that exist.

3. Pick your scam

As we already mentioned elsewhere, the tactics that are used by the scammers might still be the same, the means through which they are pursued, differ nowadays. In this section, we give a non-exhaustive overview of the variety of scams that exist today. First, some examples of scams are given based on their content. A classification based on the mode of delivery is provided afterwards.

Although criminological research only recently took an interest in this type of crime, the *419 scam*, more widely known as the *Nigerian Prince scam*, has received considerably more attention by scholars (Whitty, 2015; Whitty, 2018; Mba, Onaolapo, Stringhini, & Cavallaro, 2017). Hinted at by its name – and even though Nigeria has no prince – the origins of this scam are typically to be found in Nigeria. This makes it difficult for law enforcement to apprehend its perpetrators (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). In the classic scenario, the victim is offered a percentage of a large sum of money, but only if the victim helps to get the money out of the country. The victim is persuaded to pay the extra fees in order to transfer the money. Needless to say, the money and the prince never existed (Murphy & Murphy, 2007).

This type of individual fraud is what is called ‘advance fee fraud’. A smaller amount has to be paid in order to benefit from an even bigger amount (Mba, Onaolapo, Stringhini, & Cavallaro, 2017). *Romance scams* can fall under this category as well (Whitty, 2018), but encompass more than only monetary losses. Indeed, emotionally, this type of scam has devastating effects as well due to the intimate relationship that needs to be built in order for this scam to work.

> *“Criminals pretend to initiate a relationship with the intention to defraud their victims of large sums of money. Scammers create fake profiles on dating sites and social networking sites with stolen photographs (e.g., attractive models, army officers) and a made-up identity. They develop an online relationship with the victim off the site, ‘‘grooming’’ the victim (developing a hyperpersonal relationship with the victim) until they feel that the victim is ready to part with their money. This scam has been found to cause a ‘‘double hit’’–a financial loss and the loss of a relationship”* (Whitty, 2018, p. 105)

https://blog.eset.ie/2017/09/18/email-phishing-is-old-but-not-dead/

Equally building on a false relationship, albeit in a different manner, is the *granny scam*. As explained in previous EUCPN research (EUCPN, 2017), elderly people are led to believe they are actually talking to a relative. A long lost grandchild is supposedly in the hospital and would need immediate money transfer in order to be able to pay for his surgery (Jakobsson, 2016). They have not heard from him in a long time and probably will never again…

Another ‘famous’ scam with the same characteristics is the *technical support scam* (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). More often than not, this technical support comes from Microsoft and informs the victim via phone or email of a latent computer problem. *‘You might not have noticed this yet, but there is a virus on your computer’.* With only a small money transfer, the staff member will be able to fix your problem remotely (Harley, Grooten, Burn, & Johnston, 2012; Bullée J.-W. , Montoya, Junger, & Hartel, 2016). As many people are aware of this scam, the perpetrators have recently come up with more sophisticated fake support webpages that nudge the victim to call the support centre himself, which is most likely a premium rate number (Rauti & Leppänen, 2017).

Out of the 13 Member States that answered our questionnaire, the following phone scams were said to be most common: granny scam, police impersonation, lottery scam, legal business scam, (relative) accident scam

Other examples are *lottery scams, gambling scams, business opportunity scams, chain letter scams, telemarketing scams, etc.* (Button, Lewis, & Tapley, 2014; Button & Cross, 2017; Button, Lewis, & Tapley, 2009; Jakobsson, 2016; Stajano & Wilson, 2011). Button (2017) provides us with a classification based on eight categories of the most common frauds.

1. Consumer investment fraud

Here stocks or shares are being sold to victims which are portrayed as highly profitable. In reality, these are worthless or non-existent.

2. Consumer products and services fraud

This fraud involves the sale of non-existent products and services or the sale of products and services that are significantly different upon delivery.

3. Employment fraud

The victim is offered a fake or inadequate service to secure employment or training which is portrayed to lead to employment.

4. Prizes and grants fraud

Either the victim is led to believe that he or she is entering a real lottery and pay their participation fee or the victim is informed that he or she already won and needs to pay a fee first to be able to collect this prize.

5. Phantom debt collection fraud

Often by impersonation of trustworthy actors or organisations, the victim is tricked or pressured into paying debts he does not owe.

6. Charity fraud

Here, the fraudster acts as a legitimate charity in order to obtain donations from individuals.

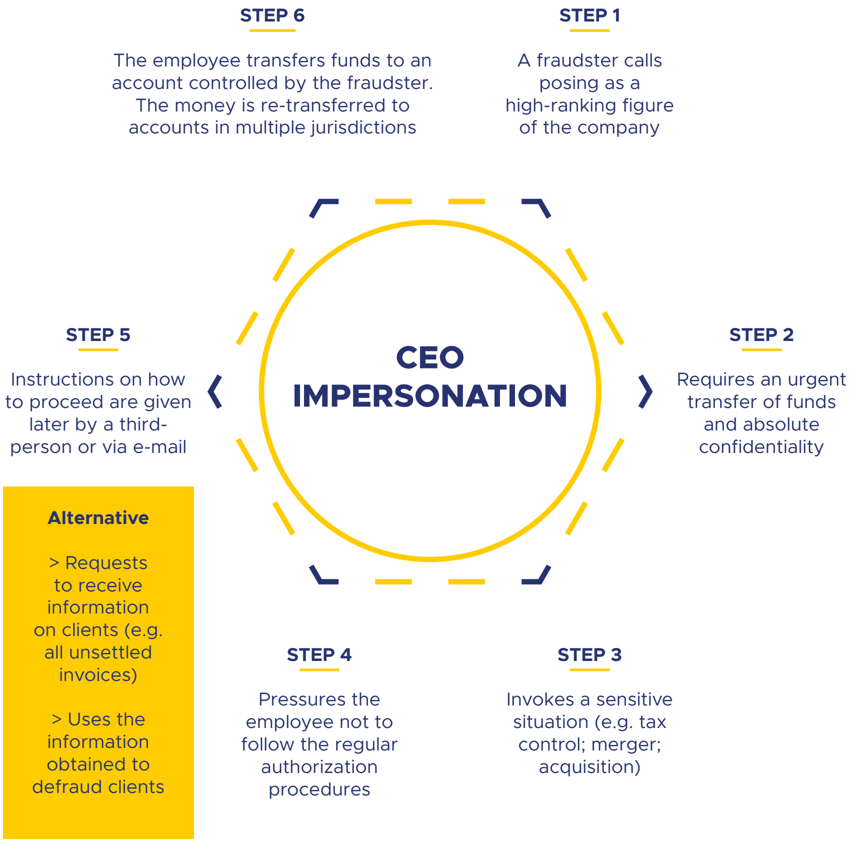
7. Relationship and trust fraud

Romance fraud, granny scam, accident scam,… are classic examples of frauds that abuse the intimacy of a personal relationship.

8. Identity fraud

This involves use of personal information from a victim to perpetrate other frauds or criminal activities. We do not include this type of fraud in this toolbox, as this type does not need an active participation of the victim in the transaction.

The list is as impressive as the creativity of the scammers and they can reach all segments of the population. However, scammers can also use a more targeted approach. This is the case in *business email compromise (BEC) scams* (Jakobsson, 2016). Here, the victim is selected as he works for a specific company or has a specific role in that company. Most likely after some reconnaissance, the perpetrator acts as the victim's boss (CEO fraud) or another trusted third party (mandate fraud) and asks for a seemingly normal payment (Europol, 2017). For example, your boss emails you to make a transfer to company X. This is an urgent matter, which is the reason for using her ‘personal’ email address, and she can only ask you to do it. Neither the company, nor the email address is right, but you follow the orders (Jakobsson, 2016). According to the latest *Internet Organised Crime Threat Assessment* (Europol, 2018), 65% of all Member States reported cases of CEO fraud and over half of them indicate rising figures.



CEO IMPERSONATION

STEP 1

A fraudster calls posing as a high-ranking figure of the company

STEP 2

Requires an urgent transfer of funds and absolute confidentiality

STEP 3

Invokes a sensitive situation (e.g. tax control; merger; acquisition)

STEP 4

Pressures the employee not to follow the regular authorization procedures

STEP 5

Instructions on how to proceed are given later by a third-person or via e-mail

Alternative

> Requests to receive information on clients (e.g. all unsettled invoices)

> Uses the information obtained to defraud clients

STEP 6

The employee transfers funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions

https://www.europol.europa.eu/socta/2017/fraud.html

Another way to classify these scams is to divide them according to the way by which they are delivered to the victim. Logically speaking, this can be either face-to-face, real life interaction or the victim can be contacted remotely, with the use of communication methods such as email or telephone. It is however imperative not to be blinded by focussing on one single mode of delivery for a scam to work. Perpetrators can easily switch between email, telephone, website,… This allows them to tailor their attack to the utmost (Button & Cross, 2017).

Classical examples of the **in-person scam** are acting as fake police officers in order to con the victim into paying a supposed fine or giving delicate information. Similar to this are perpetrators who act as handymen, who would like to do some chores in the house. To make it more comfortable for the unknowing victim, they offer to fulfil their duties while the victim is at work or on a holiday... Other common examples are fake money rolls or typical traps such as 'follow the ball' or the selling of fake gadgets (Stajano & Wilson, 2011).

Fake money roll: for example, exchanging foreign currency with fake money

'Follow the ball': the classic game where a ball is hidden under a cup which is then mixed around with two other cups, the victim needs to guess where the ball is, which is impossible because the ball is under none of them

In most social engineering cases however, the perpetrators refrain from coming into physical contact as this offers them more protection. In addition, relying on email or the telephone is the ideal setting to steer victims into the peripheral route (Workman, 2008). As Anderson (2016) describes this evolution from an American point of view:

> *'As recently as the 1980s, the problem of frauds and scams was largely a local problem or one that involved the mails. Perpetrators located their victims by going door to door, mechanics misrepresented the need for repairs at the local auto repair shop, and hucksters sold their bogus goods at the county fair or sent their bogus promises through the*

> *mail. Today, fraudsters peddle mass-market frauds in a nationwide or even international market where they contact potential victims via telemarketing, infomercials on late night television, or the Internet. Fraudsters located in India tell consumers who have sought out technical support on the web that their computers have 133 problems, which they can fix remotely if you will just pay their fees. Rather than being limited to going door-to-door or using the U.S. mail, purveyors of a host of bogus products can run infomercials on late night television, advertise their wares on the Internet, or place computer-generated telemarketing calls to millions of consumers in a couple of minutes.* (Anderson, 2016, p. 4)

The revolution in communications technology has allowed perpetrators to industrialise old fraud at low costs and come up with new types of scams (Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). As such, this is what is known as a *cyber-enabled crime*, i.e. a traditional crime that enhanced itself with the use of ICT (Whitty, 2018; Button & Cross, 2017). The digital environment has generated an atmosphere of anonymity which the perpetrators of scams happily embraced (Agustina, 2015). Apart from this (perceived) anonymity and low costs, the amount of reachable targets has multiplied to the extent that the whole world is at bay (Leukfeldt & Stol, 2011). Even worse, this globalisation of fraud impedes law enforcement agencies to attribute and/or apprehend the perpetrators. Some have even become 'scampreneurs' by realising the full potential of the technological changes (Button & Cross, 2017).

The most common among these 'industrial scams' is phishing (Europol, 2017; Europol, 2016). The same goals are pursued as in real-life scams, but most likely the scammer acts as a trusted or legitimate entity as the victim is deceived in order to disclose personal and/or financial information (Singh & Imphal, 2018; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). It is the easiest method to reach a massive amount of potential victims. It is reported that perpetrators contact their victims 95% of the time through email. 40% of the Member States highlighted investigations into phishing and it is a phenomenon that keeps increasing year after year. From 2015 to 2016, there was a notable increase of 65 percent in the number of phishing attacks (Europol, 2017). We have to be cautious with these numbers because of reporting problems (cf. infra), but nonetheless, these numbers are alarming.

What we refer to here is deceptive phishing, implying the use of social engineering tactics. To be complete, there is also a form of phishing that is based on malware or computer based deception, using key loggers, hacking, trojans,… to achieve the perpetrators goals, as was already referred to above and in earlier publications (EUCPN, 2017).

Until quite recently, email scams were rather easily detectable. They were characterised by poor grammar and spelling mistakes and had rather outlandish stories. But scammers have come to realize that by cleverly targeting their victims, they can have a bigger 'return on investment'. Targeting the attack increases the chance of the email being read twenty times (Jakobsson, 2016). This evolution paved the way for a new and wider variety of phishing forms and more professional and believable modi operandi (Europol, 2017; Jakobsson, 2016; Ollmann, 2007). Phishing has become more and more targeted. Whereas before the perpetrators sent out as much emails as possible, nowadays scammers do their research and exploit this knowledge to appear more natural and plausible; CEO fraud is the perfect example of this (Jakobsson, 2016). Spear phishing is another term to indicate the targeting of a specific group. Whale phishing on the other hand targets *high level* people (Singh & Imphal, 2018). Other variants also exist such as pharming, where a fake website is hosted in order to deceive the victim (Europol, 2014) or smishing, which is a form of phishing that uses SMS or online text messages (Europol, 2018).

Phishing is a very common phenomenon. More than 30% of the adult population has received at least one phishing email. Within student populations, this number even rises to more than 50%. Moreover, 1 out of 14 targets actually opens a link or attachment leading to possible victimisation (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018).

With low risk levels for the perpetrator, the losses for the victim can be substantial: financial losses, reputational harm, identity theft,… (Ollmann, 2007).

As phishing becomes increasingly more sophisticated, the surprising last step involves the renewed interest to an older technology: the telephone (Maggi, 2010). These phone scams are increasingly known as vishing, as they have embraced

https://www.pinterest.co.uk/pin/760897299514084725/

the potential of the internet as well (Europol, 2017). Literally voice phishing, vishing uses the phone channel to deceive its victims (Maggi, 2010). However, the phone channel has also gone through some changes. Voice Over Internet Protocol (VOIP) has made it possible to make a phone call using the internet (Singh & Imphal, 2018). This brings along some benefits. Using this protocol lowers the costs of calling significantly, perpetrators are harder to trace and they are capable of spoofing their caller information (Ollmann, 2007). Spoofing is the falsification of the information that is being transmitted by the caller. Not only this, but scammers can also 'robodial' their victims. This involves a computerized autodialer that delivers a pre-recorded message (Marzuoli, Kingravi, Dewey, & Pindrop, 2016). Nowadays, people are used to give information to strangers or even machines as call centres are very apparent in modern day society (Maggi, 2010). Scammers make easy use of this evolution.

Phone scams have a much higher effect rate and the yield is equally bigger than in normal phishing (Yeboah-Boateng & Amanor, 2014). This success is derived from the fact that vishing combines the best of both worlds, in-person and by communication technology. The power of the telephone over the internet is that it gives the perpetrator the ability to create a believable persona much faster. On top of that, the person behind the line can still be who he or she wants to be and enjoy anonymity. This way, it also combines this intimate setting with the impossibility to spot the scam in real life by visual clues. Indeed, one can tailor his attack to the limits by having a real-time conversation and control the timing of the delivery of the message (Ollmann, 2007). Organised crime groups even started hiring native speakers to be as believable and professional as possible (Europol, 2016).

Combined with these benefits, traditionally, people also place a higher amount of trust on the phone channel than on the internet. According to the most recent Eurobarometer on communication technology in the EU (European Commission, 2018) 60 % of the respondents think the phone is more reliable and offers them more protection than the internet. Moreover, telephone access is almost universal, with 97% having access at home compared to 70% having access to internet at home. Furthermore, calling someone is also still the most used method of communication, with 92% of the respondents frequently receiving or making phone calls compared to 72% sending emails (European Commission, 2018). This profound trust is of course easily exploited by scammers and in addition, while email spam has led to a multi-billion anti-spam industry, phone scams and frauds are not under that much protection (Gadhave & Sirsat, 2015).

4. Crunching the numbers

Generally speaking, there is a huge dark number surrounding this topic (Button, McNaughton, Kerr, & Owen, 2014). The biggest difficulty in getting an accurate idea of these types of crime is that much of it goes unreported (van de Weijer, Leukfeldt, & Bernasco, 2018; Crosman, 2017). Even the data that we do have, gives us a skewed image as they are probably an underestimation of the problem due to this lack of reporting (Bidgoli & Grossklags, 2017). The reasons for this problem are however well known. One of these is that victims often do not even know that they were contacted by a fraudster (Bidgoli & Grossklags, 2017; Button & Cross, 2017). In a survey with 745 victims, done by Button, Tapley and Lewis (2012), 40% of the respondents did not know they were a victim until they were notified by a third party. Another reason for not reporting is the perceived gravity of the crime by the victim. As mass-phishing attack for example will lead to a large total amount, the individual cases have rather small losses. Victims often believe that filing a complaint is not worth the trouble and on top of this, it is unlikely the offenders will ever be apprehended (Bidgoli & Grossklags, 2017; Button & Cross, 2017). In addition, reporting to the police is not self-evident. There are multiple actors to whom to report the fraud and the police do not necessarily see this as a priority either (Button & Cross, 2017). According to the Eurobarometer Cybersecurity (European Commission, 2017), only half of the respondents would go to the police if they encountered a fraudulent email or phone call. 18 percent of them would not report it at all, four percent does not even know where to go. This has also been confirmed by other research (Button & Cross, 2017; Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014).

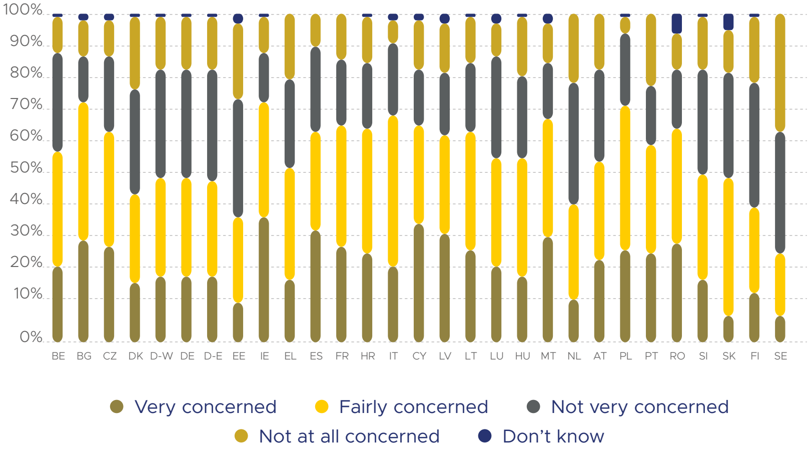
Perhaps the biggest positive side effects for the offender of socially engineering his victim into compliance, are the feelings of self-blame and embarrassment the victim has afterwards. Conversely, this is another reason why reporting rates are this low (Cross, Richards, & Smith, 2016; Titus & Gover, 2001). For example with CEO fraud, victims are afraid of reputational damage within the company or even losing their job (Europol, 2016). Victims often blame themselves as they had an active involvement in the fulfilment of the crime and are embarrassed that they fell for it (Bidgoli & Grossklags, 2017; Button, McNaughton, Kerr, & Owen, 2014). Seeing themselves as indispensable to the crime and ashamed by their actions, they fear not to be believed by the police or to be taken seriously (Button, Tapley, & Lewis, 2012). So not only does this active involvement of the victim in the crime obscures our view of the problem, this can even lead to secondary victimisation (Button & Cross, 2017). Some scams, such as the 419 scam, have this build-in anti-reporting mechanism as the victim is also undertaking illegal actions by transferring illegal money in some cases (Button, Lewis, & Tapley, 2009) (cf. supra) and fraudsters specifically create embarrassing schemes to avoid reporting (Button, McNaughton, Kerr, & Owen, 2014).

If the scams are reported to the official institutions, they are most likely to be found under the broader umbrella of 'fraud', which makes it very hard to isolate individual fraud (Button & Cross, 2017). In a questionnaire that was sent to the Member States in preparation of this toolbox, we found similar observations. In eleven of the 13 Member States that answered, phone scams are reported under 'fraud'.

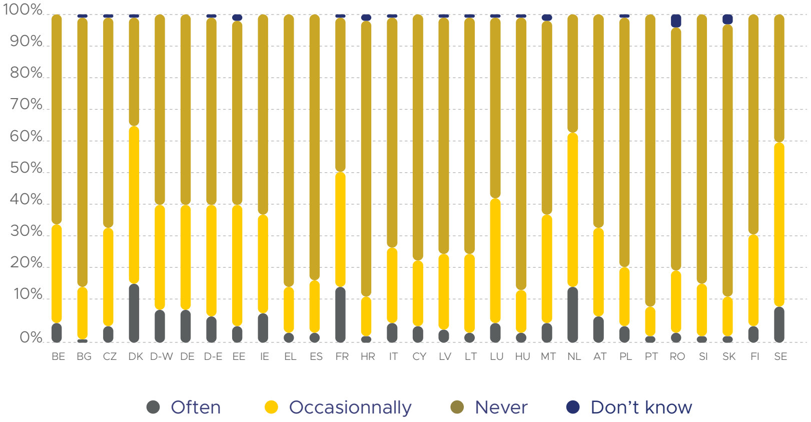
A solution to this dark number problem with official statistics is the use of victimisation surveys. However, the same problems are raised again by scholars. Many of these studies do not distinguish between frauds that are committed online or by 'old school' methods, or cover individual fraud issues at all. And again, there is still reluctance to report here, there are still victims who do not know that they are victim or who think their particular case is not worth reporting (Button & Cross, 2017; Button, McNaughton, Kerr, & Owen, 2014). Notwithstanding these critical issues, the Special Eurobarometer on Cybersecurity (European Commission, 2017) did specifically ask almost 30 000 EU citizens at home some questions regarding scam emails or phone calls. Levi (2017) describes this survey as the 'only cross-national comparative data collection on fraud victimization in the EU' (Levi, 2017, p. 4).

In all but five Member States, at least half of the respondents of the Eurobarometer expressed some degree of concern about being the victim of fraudulent emails or phone calls, with Ireland and Bulgaria showing the highest numbers (73%). Denmark (45%), the Netherlands (42%), Finland (41%), Estonia (38%) and Sweden (27%) are the exceptions to these general findings. Interesting though, three of these countries have amongst the highest self-reported victimisation numbers. In Denmark (66%), the Netherlands (64%), Sweden (61%) more than half of the respondents have received fraudulent emails or phone calls. Slovakia (14%), Croatia (14%) and Portugal (11%) report the lowest percentage

How concerned are you personally about experiencing or being a victim of the following situations: receiving fraudulent emails or phone calls asking for your personal details (including acccess to your computer, logins, banking or payment information)



How often have you experienced or been a victim of the following situations: receiving fraudulent emails or phone calls asking for your personal details (including access to your computer, logins, banking or payment information)



Aside from the huge dark number, there also is a paucity of research on the victimology of this crime (Whitty, 2018; Button, Lewis, & Tapley, 2014). Most studies on victim profiles also focus on online frauds, so the following statements are mainly based on these findings. As was shown however in the section on the different types of scams, there is a wide variety of frauds, which provides the basis for almost everyone in society to become a potential victim. This makes it difficult to make general statements on a typology of victims. Nonetheless, studies have shown that certain groups are particularly vulnerable to specific scams. Consumer investment scams are for example more prevalent amongst the elderly and the working population, as they have the actual means to invest (Button & Cross, 2017).

Perhaps the most important addition of victimology studies surrounding this topic, is busting the myth that exists on the level of prevalence amongst difference age groups. There is a common perception, especially in media, that mainly elderly people are victims of this crime (Button, Lewis, & Tapley, 2009). Contrary to this popular belief however, surveys have shown that younger adults are the most prevalent victim group (Button, Lewis, & Tapley, 2009; Ross, Grossmann, & Schryer, 2014). This popular idea is derived from the stereotype of elderly people as lacking financial skills, being more trusting, having slower cognitive functions, … These findings are of course true to a certain extent, but it is important to understand *why* the elderly are being targeted in the first place. When we focus on the attractiveness of the target, elderly people have easy access to life savings, are more likely to have private property, more additional lines of credit (Barnes, 2017). This is according to Button and Cross (2017) the main reason why they are targeted at a high rate. The younger population and middle-aged group however, are reported to be more susceptible for these scams (Button & Cross, 2017; De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Whitty, 2018). Most of the studies indeed conclude that older consumers have a lower risk of becoming a victim of individual fraud. On the other hand, within the elderly population, fraud is the most likely crime they will encounter (Button & Cross, 2017). However, this remains an ambivalent topic that needs further examination as specific types of fraud, such as investment fraud or lottery scams, show a higher prevalence among elderly people (Anderson, 2016).

Elaborating on this, especially young people (15-25y) are identified to be vulnerable (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018; Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). This could refer to lower levels of education, having spent fewer years online, less exposure to training materials and less of an aversion to risk (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). This last point is also put forward by Button, Lewis and Tapley (2009) as people with a more positive attitude towards financial risk taking and persons with low self-control are seen as more susceptible. Research by De Kimpe, Walrave, Hardyns, Pauwels and Ponnet (2018) claim that a high level of trust or 'compliance' leads to a higher susceptibility which is a positive predictor of responding to phishing mails. A high sense of duty is also said to be positively related to victimisation. There is however a point of discussion within academic studies on whether or not more internet experience and technological knowledge leads to less susceptibility towards phishing or exactly the opposite, because being technically skilled also means a higher exposure level to threats (De Kimpe, Walrave, Hardyns, Pauwels, & Ponnet, 2018). In addition, Button (2017) states that studies have pointed out that although fraud victims are typically portrayed as uneducated and financially illiterate, the opposite seems to be true. They offer three possible explanations for this phenomenon. The first is the 'knowing-doing gap', by which they mean that often people recognize the signals of a scam, but fail to apply this knowledge to their situation. A second explanation is called the 'expert snare', referring to the pitfall financially literate people fall into as they are overly confident and ignore the dangers. A final explanation could be that victims might have sufficient financial knowledge, they lack this level of literacy on persuasion and social engineering tactics (Button & Cross, 2017).

When looking into how individual victims are actually contacted, literature has also identified some selection techniques that are used by fraudsters. For example, within certain phone scams, some fraudsters just randomly dial numbers out of telephone books or registers of public companies. Others however use what is known as 'sucker lists'. These lists are registers that are shared and sold amongst fraudster with targets that already have been defrauded (Wood, Liu, Hanoch, Xi, & Klapatch, 2018). Levi (2008) describes this as follows:

> *'Once someone has subscribed to one lottery or other product by internet, post or telephone, they soon experience allied scam 'offers' from other fraudsters'* (Levi, 2008, p. 404)

The use of such lists also indicates towards a high level of repeated victimisation (Button, Lewis, & Tapley, 2009). Equally, a relatively small number of perpetrators seems to be responsible for the majority of telephone scams. In a study done by Marzuoli, Kingravi, Dewey and Pindrop (2016), a honey pot system was used to analyse the fraud ecosystem. Out of 8 000 000 received phone calls, the researchers analysed 40 000 of them. Only 1.8% of the calling sources were responsible for 66% of the complaints. These findings point in the direction of what has been called 'scampreneurs', referring to the entrepreneurial spirit of some fraudsters as they diversify their scam supply and try to maximise their effectiveness (Button, Lewis, & Tapley, 2009; Button, McNaughton, Kerr, & Owen, 2014).

Nevertheless, not all fraudsters are equally professional and organised. In the phone scamming business, some fraudsters operate on an ad hoc basis and change operations the moment law enforcement agencies seem to notice them. Other networks are bigger and take on more 'formal' proportions, having some sort of hierarchy, division of labour and graduated pay. These types of fraudsters might also be involved in traditional organised crime (the drug scene for example) or have a sole focus on scams (Levi, 2008; Barnes, 2017; Button, Lewis, & Tapley, 2009).

When it comes to the origins of the scammers, Nigerians are almost by definition involved in the Nigerian Prince scam, but in general, offenders from West-African countries are active in all types of scams (Button, Lewis, & Tapley, 2009; Levi, 2008; Button & Cross, 2017). Within internet based fraud, eastern European criminal groups (Russia, Romania, Lithuania,..) have developed a particular skill and reputation (Button, Lewis, & Tapley, 2009; Levi, 2008). Cross-border frauds are especially prevalent, making it very hard for law enforcement and national policy to tackle these issues (Button & Cross, 2017). All the more reasons for preventing this crime from happening in the first place.

5. Conclusions

In the first part of this toolbox, we have given a summary of the current **intelligent picture** on individual fraud. As fraud is a very diverse offence, encompassing a wide range of activities, we have narrowed down our focus to individual fraud, while emphasizing the current mixed online and offline characteristics of this type of crime.

Underlying most individual frauds is a technique called social engineering. This technique is the essential tactic to obtain the trust from victims and to convince them to follow the scam. As such, the victim has a very active part in the fulfilment of the crime, leading to feelings of shame and guilt. We situated **social engineering** within studies in social psychology and showed some of the basic principles that are involved in the art of persuasion.

There are however many different **forms and types** of scams. We categorized these types based on either their content or on their mode of delivery (in-person or with the use of ICT). In addition to this huge variety, they seem to be growing in levels of sophistication and complexity. Furthermore, we are most likely only scratching the surface, as there is a huge **dark number** surrounding this crime. Victims do not report this crime due to a variety of reasons: feelings of shame, perceived gravity of their losses, not knowing they were victimised, not knowing where to report,…

Victimisation surveys, such as the Eurobarometer, do however offer a solution to this lack of reporting to the official bodies. Nonetheless, more research on the gravity of this crime and the profile of victims remains crucial. This way prevention activities can be made more focussed and efficient. We will now proceed to take a look at current good practices in this field.

02

PART II:
GOOD PRACTICES

1. Introduction

In the second part of this toolbox, we will dig deeper in how to prevent individual frauds from happening. As was explained in the previous part, tackling this issue is extremely difficult for the police. Button (2017) claims that the police do not have the necessary means to investigate the majority of these kinds of fraud, which makes prevention all the more important (Europol, 2016). In addition to this peril, fraud prevention has typically received little academic attention. This makes it harder to make statements about effectiveness, even though numerous activities exist in this area (Button & Cross, 2017). In this part of the toolbox, we will take stock of some of the academic insights on preventing individual fraud but also show some good practices. Finally, we will make some recommendations, with a specific focus on preventing telephone scams.

The most common tactic to prevent individual fraud is educating the public. Technical measures, such as spam filters, spell checking software, monitoring spoofed website domains,… all have their own merits. However, they remain reactive as they are ultimately conceived as a response to certain methods (Jakobsson, 2016; Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). Perpetrators can adapt to these measures, which is illustrated by their continuously growing level of sophistication. Moreover, these technical and procedural measures are not a 100% safe as there will always be flaws in these systems and people. Nonetheless, every security measure brings us to a safer base line and is important to tackle this complex crime.

Closing this ‘security leak’ is the most likely reason why a lot of preventive efforts are being done to educate the public and to raise awareness (Workman, 2008). As already mentioned, a big part of these efforts remain unevaluated (Mears, Reisig, Scaggs, & Holtfreter, 2016), however there are some general findings to be found. Online trainings, contextual learning[1], embedded training[2] and interactive games[3] have all been shown to be effective in improving user’s security (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010). People are trained for example on recognizing certain linguistic characteristics (Tabron, 2016) or on visceral discrimination tactics (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). These trainings are key to close the ‘knowing-doing gap’ to which we referred earlier. Awareness raising leads to a better understanding of the phenomenon, but not necessarily to an increased application of this knowledge to one’s particular situation (Moreno-Fernández, Blanco, Garaizar, & Matute, 2017). A combination of both awareness raising and training seems to have the most benefits (Cross, Richards, & Smith, 2016; Europol, 2016; Bullée J.-W. , Montoya, Junger, & Hartel, 2016). A study done by Sheng, Holbrook, Kumaragur, Cranor and Downs (2010) mixed these trainings and showed a 40% improvement after the introduction of training material compared to a control group (online, contextual and embedded training and interactive games combined).

Characteristic for this type of crime is the active participation of the victim and the high level of repeat victimisation (Button, Lewis, & Tapley, 2009; Cross, Richards, & Smith, 2016). Because of this active role, the victim is often blamed and shamed. Awareness campaigns should also focus on this aspect, allowing victims and their environment to recognise that this is not their fault but the result of a malicious action from the offender (Burgard & Schlembach, 2013). A lot of emotional damage can be prevented in this regard. In addition, victims should also be made aware of the risk of falling victim a second time, for example due to the existence of ‘sucker lists’ (Cross, Richards, & Smith, 2016).

There is one academic publication of particular interest to this topic. Recently, Mark Button and Cassandra Cross published a book called *Cyber frauds, scams and their victims* (2017). Apart from offering numerous insights on this type of crime, there is an entire chapter dedicated to preventing cyber frauds and scams. The authors built their chapter around the framework of situational crime prevention.

“Situational crime prevention can be characterized as comprising measures (1) directed at highly specific forms of crime (2) that involve the management, design, or manipulation of the immediate environment in as systematic and permanent a way as possible (3) so as to reduce the opportunities for crime and increase the risks as perceived by a range of offenders” (Lab, 2010, p. 192). In essence, the idea is to prevent crime by reducing characteristics of situations that facilitate offending. Specific situational characteristics are manipulated in order to block crime opportunities (Jacques & Bonomo, 2017).

Following the work of Clarke, they have adapted the 25 techniques of situational crime prevention (Cornish & Clarke, 2003) to the context of cyber frauds and scams.

These 25 techniques can be categorised under five broad strategies (what works in crime prevention):

1. Increasing the effort associated with committing an offence
2. Increase the risk associated with committing an offence
3. Reduce the benefits of the criminal action
4. Reduce provocations that might otherwise precipitate crime
5. Remove excuses that offenders might otherwise use to justify criminal action

Button and Cross (2017, p203) summarised their work into the figure below. We refer all interested readers to this book, as it gives a very thorough overview of cyber scams and frauds and combines many research insights.

	Increasing the effort	Increasing the risks
Individual	> Protecting accounts with complex passwords, anti-virus protection > Protective registrations > Pursue measures to make personal contact information more difficult to find for third persons	> Regular cleansing of computers of viruses, spyware > Check websites, emailers and callers
Organisation	> Suitable controls to protect the personal information of clients > Background checks: verifying that clients are who they say they are	> Information sharing: datamatching and datamining > Verifying voice and location of clients
Policing Bodies	> Disrupting the activities of fraudsters > Scambaiting > Pursue orders and restrictions on fraudster by using the civil, regulatory or criminal law	> Information sharing: datamatching and datamining > Central reporting > Publishing information on suspected scams, suspect websites > Fake scams to alert potential victims

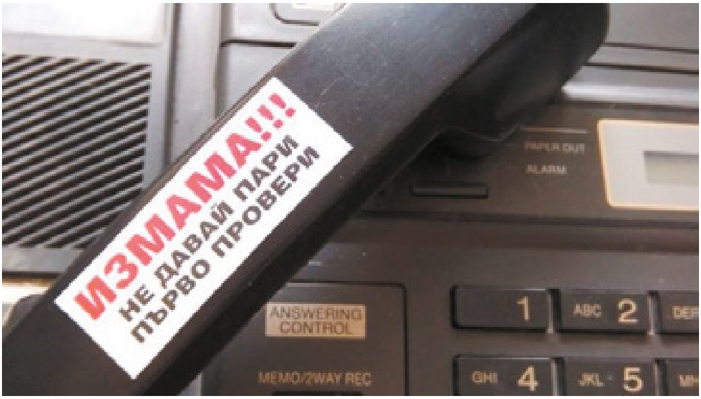
Reducing the rewards	Reducing provocations	Removing excuses
If fraudster known and has assets, pursue civil action to secure damages or seek reparation through criminal process		
If fraudster known and has assets, pursue civil action to secure damages or seek reparation through criminal process		Communicate with clients to educate them of the risks and good practice to reduce the risk
> If fraudster known and has assets, pursue civil action to secure damages or seek reparation through criminal process > Monitoring financial transfers to high-risk third countries to identify possible victims to warn them of potential victimisation	> Restrict information on how certain scams have been conducted > Regulation of advertising and promotion activities	> Communicate with general public and at risk groups to highlight the risks and good practice > Advertising campaigns: television, radio, newspapers, specialist publications, online > News releases to secure media interest > Specialists websites > Mailshots > Social media emails, texts, tweets > Community and interest group activities > Storylines in dramas

2. If it sounds too good to be true, it probably is

In this section, we will give an overview of some of the good practices we have encountered during the Bulgarian Presidency. The projects and campaigns are being discussed under different categories, each representing the target group: universal, selected or indicated prevention, respectively the entire population, a specific risk group or people who were already victimised. All these campaigns and projects can also be found in the third part of this toolbox.

Universal prevention

It was the Bulgarian Presidency that decided to focus on frauds and scams and this sense of urgency is reflected in the policy of the national police. An entire 'fraud section' within the National Police General Directorate is dedicated to this issue, in particular to phone scams. They work reactively, but prevention is also a fundamental task to tackle this crime. As part of their work, increasing the population's knowledge and awareness of this crime is done by information campaigns. For example, information leaflets are spread, but also advice is given on a national radio show. Another example from Bulgaria are stickers that are handed out. These stickers have preventive messages and people are asked to stick them to their phone. The idea is that when they are called, they are being remembered to the preventive message because they see the sticker as they pick up the phone.



In Sweden, a similar body operates on the prevention of fraud: the Swedish National Fraud Center. Their preventive work focusses on raising awareness through traditional media and social media channels, but also on building external partnerships with authorities and enterprises. Some campaigns serve a dual purpose. Aside from raising awareness on the dangers of scams through media campaigns, they also used the media to pressure a certain app that had severe security issues which was being exploited by fraudsters. This media exposure prompted the app designers to upgrade their security.

On a European level, the European Cyber Security Month (ECSM)[4] is held every year in October. This EU wide campaign aims to promote cyber security among citizens and organisations and highlights simple steps that can be taken to achieve this. The European Union Agency for Network and Information Security (ENISA), the European Commission, Europol and in specific the European Cybercrime Centre (EC3) and a wide range of public and private partners from the Member States work together to achieve this goal and organise numerous events and campaigns during the month. During the third week of the 2018 campaign, the focus was on cyber scams. The goal was to educate the general public on how to identify deceiving content in order to keep both themselves and their finances safe online. EC3, the European Banking Federation (EBF) and other partners joined forces to make an awareness raising campaign on this topic. Some examples of the material can be found below.

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 may try to blackmail you. If you do send it, they will ask for more.

ARE YOU A VICTIM?

Don't feel embarrassed!

Stop all contact immediately.

If possible, keep all communication, such as the chat messages.

File a complaint with the police.

Report it to the site where the scammer first approached you.

If you have provided your account details, contact your bank.

WHAT CAN YOU DO?

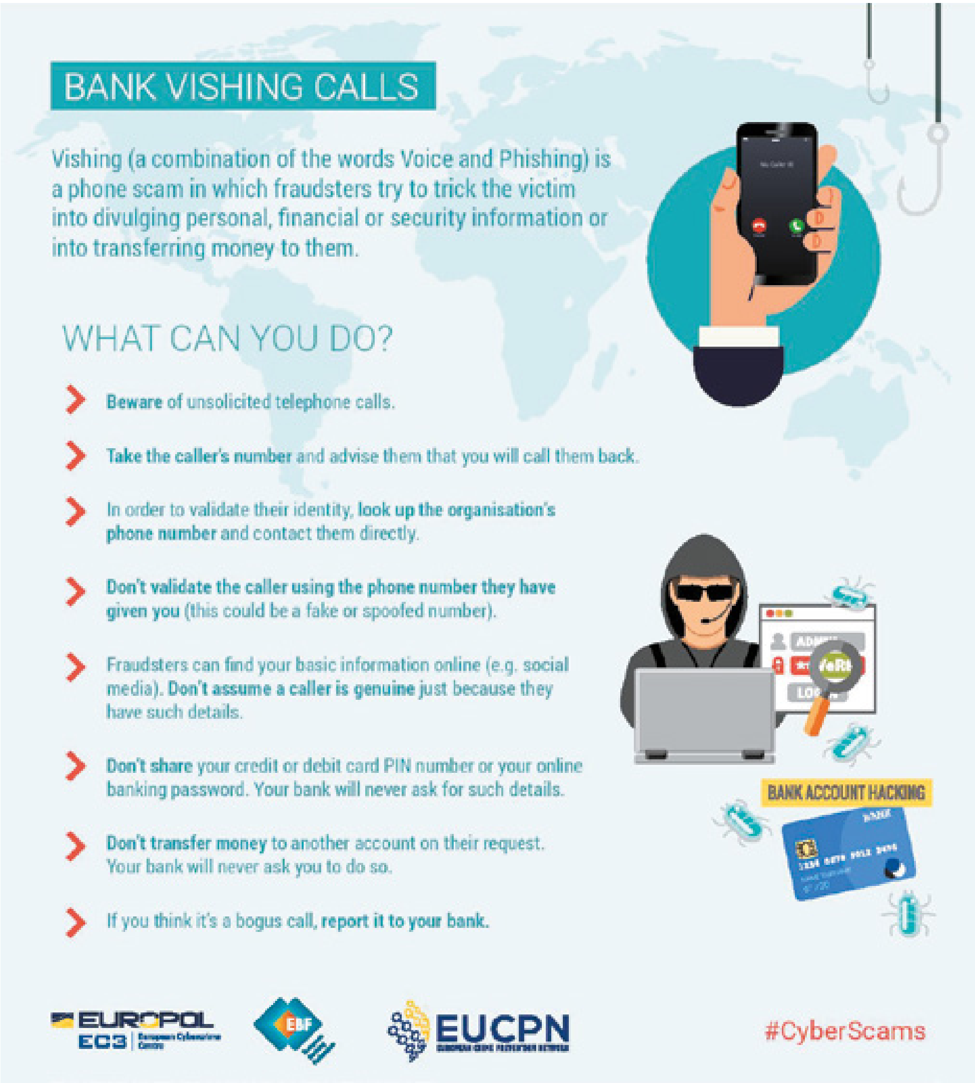
- **Be very careful** about how much personal information you share on social network and dating sites.
- **Always consider the risks.** Scammers are present on the most reputable sites.
- **Go slow** and ask questions.
- **Research** the person's photo and profile to see if the material has been used 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.
- If you agree to meet in person, **tell family and friends** where you are going.
- **Beware of money requests.** Never send money or give credit card details, online account details, or copies of personal documents.
- **Avoid sending them upfront payments.**
- **Don't transfer money** for someone else: money laundering is a criminal offence.

EUROPOL EC3 | European Cybercrime Centre

EBF

EUCPN

#CyberScams



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 ACCOUNT HACKING
ADMIN
LOGIN
BANK
EUROPOL
EC3 European Cybercrime Centre
EBF
EUCPN
EUROPEAN CRIME PREVENTION NETWORK

#CyberScams

Another awareness raising campaign is the anti-phishing campaign that was done by the Belgian Centre for Cybersecurity (CCB). This classical campaign provided information on how to recognise fraudulent emails. The campaign was disseminated through videos, email signatures, banners, posters, but also on a webpage. Besides information and prevention tips, the website also provided a test for the public to see how 'phishingproof' they are. After the test, preventive materials are shown on what steps and actions can be done to further improve security. In addition, people can also send emails they found suspicious to an email address of the CCB. The CCB then checks these emails and links to fraudulent websites and puts these websites on the blacklist of the four main browsers (Internet Explorer, Mozilla Firefox, Google Chrome and Safari). This is done through the EU Phishing Initiative Partnership. Once these websites are on the blacklist, they are blocked for other users. Every day, this CCB mechanism is able to put five websites on the list, which makes for a very interesting crowdfunded prevention mechanism.

The EU anti-Phishing Initiative is a project that is funded by the European Commission and has as its primary goal the disruption of fraudulent websites. The objective is to operationally prevent phishing scams from fooling victims by blocking the websites that are used for this purpose. It is based on a public-private partnership dedicated to fight phishing.

More information:
https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2013_ISEC_AG_INT_4000005246_en

Selective

As was already noted in previous sections, a lot of attention goes to the elderly when it comes to this type of crime. This was already made apparent in the toolbox on crimes targeting the elderly people, which was made under the Slovakian Presidency. A number of projects that entered the European Crime Prevention Award competition that year, focussed on this type of crime targeting the elderly. For example the German project ‘Hello Granny, I need money’, which came in second place, focussed on phone scams involving the grandchild trick. By means of an interactive stage play, elderly are being informed about this crime phenomenon while at the same time the goal is to reduce subjective feelings of insecurity.

Similarly the Czech ‘Nedáme se’ (or ‘We won’t take it’) programme is an interactive educational stage play, in which four types of common deceitful manipulative schemes used against seniors, are performed on stage. These are sales campaigns, selling perfumes on the street, telemarketing and at-senior’s-home selling technique. Besides the actors, a policeman and also the author of the play, psychologist PhDr. Romana Mazalová, appear on the scene. They are entering the play and interact with the audience, thus teaching them new strategies of defence. The play is therefore not only enjoyable, but also becomes a new educational form against so-called “Šmejdi” or fraudsters. In total, one thousand elderly participated in the project. The educational effect of this stage play on the audience was experimentally examined. The results confirmed that the seniors who had seen the play proved to be more successful in defending against fraudulent sellers. The experiment compared 130 seniors who watched the stage play to a control group. A half year after watching the stage play, the experimental group refused a fake deal 2,5 times more often than the group that did not see the play.

NU CREDE TOT CEEA CE ȚI SE SPUNE LA TELEFON!
UN HOȚ AR PUTEA SĂ-ȚI FURE BANII!

Another project that focusses on working with elderly people is the project 'The Price of Friendship' from Romania. The purpose of the project was to reduce the risk for elder people to be victimised, following these objectives: knowing the target group from attitudinal and behavioural perspective, increasing the level of preventive knowledge of elder people and increasing the capacity of self-defense. The target group was composed of people over 60 years old, who are members of local senior clubs. In 2017, a total of 34 preventive information activities were done by the police. The information pointed out the risks associated to age, but also to the prevention of victimisation in case of deceptive schemes, such as fake phoning campaigns. Also, online training courses were given to the elderly. Additionally, a 'senior safety ball' was held to launch a public information campaign.

Besides raising awareness within this target group, an interesting mechanism is implemented in Bulgaria. The Bulgarian fraud section has several good partnerships with private actors, such as the banking sector. More situational in nature, this prevention mechanism introduces a control system when a person older than 50 withdraws a sum of more than 3000 euros. When this happens, the banking clerk will receive a warning upon which he or she can ask some questions to check if the elder is not involved in a manipulative scheme.

Indicated

Another set of prevention activities focusses on people who have already been victimised. Specific interventions are aimed at preventing continued victimisation and falling victim multiple times to different scams. For example, Project Sunbird in Australia, targets financial transactions between Western Australia and some West African countries. The police screen these transactions and list up the illegitimate looking transactions. The victims are then contacted and are explained why the police believes they could be a victim of fraud. When evaluated, 73 percent of the contacted people ceased sending money to these countries (Button & Cross, 2017).

In the United Kingdom, Action Fraud, the national reporting centre for fraud and cybercrime, regularly reports the latest frauds and scams (Button & Cross, 2017). They also direct victims to designated support groups to help those affected by the crime or provide them with the information where they need to report to[5]. This can help to reduce the emotional damage, but also help victims with recovery of lost monies or give advice on how to act in the future, should they be contacted again. Due to the existence of sucker lists (cf. supra), this is a veritable threat.

As was already mentioned, victims suffer from a variety of negative effects due to their victimisation. Among many things, victims have expressed a strong need to simply be listened to and be acknowledged as victim. However, there are –even globally – few support services to these victims. A rare example of such support programme is found in Canada: the Senior Support Unit. By means of a telephone service, staffed with older volunteers and peers, they provide support to fraud victims. They offer advice and warnings, lend an ear and provide reassurance (Cross, 2016). Not only does such an initiative offer support to individual victims, it also helps to raise the level of reporting, which in turn leads to better informed policing and prevention.

3. Preventing phone scams: how can I help you?

The EUCPN Secretariat organised a workshop on the topic of individual fraud. A number of experts came together and discussed their ideas and preventive work in this field. The workshop consisted of three parts. First, the intelligence picture of individual fraud was discussed. This mirrors the first part of this toolbox. Second, different projects were presented and discussed with the group, which is reflected in the section above. Finally, a world café method was organised to draw up recommendations regarding the prevention of phone scams. This way, the experts discussed their recommendations in smaller groups. These were the experts who participated during the workshop:

- Mark Button, University of Portsmouth, United Kingdom
- Michael Will, Europol, AP Furtum
- Simeon Dimchev, Fraud Section in National Police General Directorate, Bulgaria
- Charlotta Mauritzson, National Fraud Centre, Sweden

- Andries Bomans, Centre for Cybersecurity, Belgium
- Constantin Lica, Fight against Fraud Department, Romania
- Aurelian Bocan, General Directorate of Bucharest Police, Romania
- Romana Mazalová, ‘Nedáme se’ project, Czech Republic

We have combined the recommendations following Button’s (2017) example from earlier, and used the five broad strategies from Clarke as a guiding framework. It goes without saying that these do not exclude each other, but can be combined in different projects. As already mentioned, these are:

1. Increasing the effort
2. Increasing the risk
3. Reducing the rewards
4. Reducing provocations
5. Removing excuses

Increasing the effort

The first possible strategy is increasing the effort an offender has to take in order for the crime to succeed. The idea here is that when the efforts are too high, the offender will restrain himself from offending. As was made clear in the first part of this toolbox, offenders can find their potential victims on legitimate lists. Here, organisations openly publish the contact details of people, but people also share their telephone numbers freely and willingly. For example, one can see telephone numbers on Facebook profiles, LinkedIn pages, … Restricting the publication of phone numbers on these lists and social media profiles could already make it more difficult for an offender to contact his victims.

Another way to increase the effort is to restrict the access to the use of telephone numbers. It is extremely easy to purchase a prepaid card or a new telephone number. This allows offenders to keep changing numbers, making it harder for law enforcement to track them. One idea from the workshop was to limit the amount of telephone number per person, by linking it to their bank account or ID number. Thorough cooperation with mobile companies would be advisable here. Not only does this increase the effort for the offender, it also decreases anonymity and increases the risk of being apprehended.

With the rise of online calling, it remains rather easy to contact potential victims and to spoof your location to make it seem legitimate. Increasing use of passwords, encryption and making it nearly impossible to spoof location should also increase the effort the offender has to take in order to contact victims and defraud them.

Scam baiting was also mentioned as a possible tactic, although this is not sufficient in itself. The idea is that policing bodies or other organisation could try to scam the scammers by luring them into useless leads and wasting their time. While they are busy chasing these leads, they cannot scam innocent victims.

Increasing the risk

One key aspect to prevent scams is to know what you are dealing with. Sharing information is of crucial importance here. As scams can be reported to a variety of actors, such as the police, but also private actors, sharing information between the public and private sector is imperative. This would allow for a faster response and better informed preventive measures, thus increasing the risk. As such, other stakeholders than law enforcement need to be involved. Mobile companies, banks, non-profit organisations,… all have their role to play and have important pieces for the information puzzle. This cooperation should not stop at the national borders either. Europol plays a crucial part here as a facilitator for information exchange and cross-border activities. Due to the fact that this type of crime is increasingly international, third countries should also be looked at to share information. This information could also be shared with the general public. If they know what companies offenders claim to represent, they can already be alerted.

Of course, this information needs to be gathered first and victims should be made more aware of the reporting possibilities. For example, awareness raising campaigns could also focus on showing how reporting the crime leads to a successful investigation and adequate solutions. Having a central reporting system for victims, with access to all actors in the field, would also make the process of reporting much easier and lower the threshold for victims to actually take the step to report.

Another strategy to increase the risks is to reduce anonymity. As was mentioned under the rubric ‘increasing the effort’, ICT evolutions have made it possible to spoof the location from where you are calling. This way, the victim could be let to believe she is talking to someone from her country, but instead be talking to someone from abroad. Making it harder to spoof your location, will lead to an increased exposure and risk of being caught. This could be a mechanism for banks for example. They could have voice recognition software and location services to check whether or not this data corresponds with the client’s normal data. Comparing these ‘normal’ characteristics is also something that is used in the example from certain banks in Bulgaria (cf. supra) where the banking clerk is alerted when a person older than 50 wants to withdraw a larger than usual amount of money.

According to the experts of the workshop, awareness campaigns should also explain the risks and sanctions to the offenders in order to deter them. These sanctions should also be heightened to counter the perceived benefits for the offenders. Especially financial penalties are deemed fit in this regard. Together with more specialised training and resources for law enforcement, this crime should be treated as a type of organised crime and punished accordingly.

Reducing the rewards

This third set of measures to prevent phone scams involves reducing the rewards that could be achieved with committing this crime. The main recommendation here is to seize the assets that are being obtained through phone scams. An important step is to monitor the flow of money. The Australian example from earlier shows us exactly what this is about and how effective detecting suspicious transactions can be. The experts expressed the need for an EU wide initiative with banks to adapt this to the European perspective. Another recommendation is to confiscate the equipment and resources that were needed to commit the crime in the first place.

Reducing provocations

During the workshop, no specific recommendations were formulated to reduce provocations. However, following Button (2017), we could state that in some cases it is important not to provide too much information on how the scam has taken place in order to prevent copycats. In addition, it is also known that fraudsters will contact victims with an offer that would make it possible to retrieve their losses for example. Of course, the intention is however to conduct a second scam. Raising awareness on this issue is of crucial importance.

Removing excuses

The last set of recommendations is mainly focussed on raising awareness on phone scams and how to best protect oneself from being harmed. This involves the classical information campaign through a variety of channels such as the radio, television, flyers, … The information that needs to be shared can explain the modus operandi from certain scams, but also on how to defend oneself. This was made clear already with the examples from Romania or the Czech Republic. A stage play for example is an interesting method to teach people how to apply defensive strategies to their own situation. Public-private partnerships are equally important here to spread a preventive message as they are in sharing information to attribute offenders. This is a shared responsibility, which can also be done within community groups or peer groups.

Of course, campaigns need to be evaluated to ensure effectiveness. An important aspect to this is spreading the same message across the different organisations, but also across different countries. The example from Europol (cf. supra) is a good example of this. In addition, it might be a good idea to indeed share information on the variety of scams that exist and explain their modus operandi. However, the message on how to protect yourself, should be constant, in order to be as clear and simple as possible. *Just say no.*

Awareness raising should also focus on the ones that were already victimised. Not only should they be made aware of the risks of falling victim a second time, there is also a clear need for support to these victims. Supportive networks that share information amongst victims and support each other in their losses (financial and emotionally) are noteworthy here. A hotline was also mentioned by the experts to offer the victims the right information and advice.

4. Conclusions

In this second part of the toolbox, we have taken an interest in the prevention of individual fraud. First, some general comments were made based on academic research. Despite the shortage of academic studies on the prevention of individual fraud, we found that the most common prevention tactic is **educating the public** on recognising scams and how to react to them. One study showed a 40% improvement after evaluating training materials that were given to an experimental group. These kinds of evaluations are scarce however and we can only recommend having more research and evaluations on this matter.

Studies also expressed the need to focus on people who already have been victimised. This is due to high levels of repeat victimisation, but also on the dangers of secondary victimisation by peers, family, official bodies,… **Victims** should be supported in their losses and made aware of the dangers of falling victim a second time.

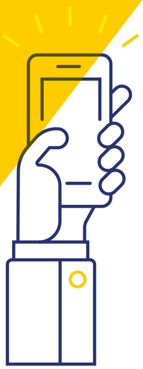
Secondly, we gave an overview of some **good practices** that exist within the Member States. These were categorised according to their target group: universal, selective and indicated prevention activities. In the third part of this toolbox, the reader can find all these projects as well.

Finally, based on a workshop with a variety of European experts, we formulated **recommendations** on how to prevent phone scams. These centred on the five broad strategies of situational crime prevention: increasing the effort, increasing the risk, reducing the rewards, reducing provocations and removing excuses.

Factsheet

PREVENTING PHONE SCAMS

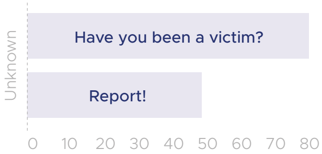
HOW CAN I HELP YOU?



SOCIAL ENGINEERING

Underlying most individual frauds is a technique called social engineering. This is the essential tactic to obtain the trust from victims and to convince them to follow the scam. As such, the victim has a very active part in the fulfilment of the crime, leading to feelings of shame and guilt.

DARK NUMBER



THESE ARE THE STEPS

01 Increase the effort

> Restrict publication of phone numbers
> Stronger password protection and encryption
> Scambaiting

02 Increase the risk

> Share information between all involved partners
> Promote reporting
> Reduce anonymity of the caller

03 Reduce the rewards

> Seize criminal assets
> Monitor money flow

04 Reduce the provocations

> Prevent copycats
> Raise awareness on retrieval scams

05 Remove the excuses

> Raise awareness
> Evaluate campaigns
> Support victims

Want to learn more?
Visit www.eucpn.org

03 PART III: EXAMPLES FROM PRACTICE

"GRANNY SCAM – EVER HEARD OF THAT?" (AT)

©BM.I – Bundeskriminalamt

Short description:
The telephone rings at a victim's ("Granny's") place. Unsuspecting, the victim assumes that the caller is a friend or relative. The victim starts guessing who is calling, utters several different names of family members (in most cases, grandchildren's' or nephews' names), the fraudster picks one and claims to be that person. Later, the caller describes his financial emergency situation and asks the victim for cash. It is not unusual in such cases that victims lose all their savings; often, this loss entails serious emotional distress, even physical ailments.

Crime prevention proves difficult; potential victims are often inaccessible to speeches or campaigns. Bank staff was found to play a crucial role in prevention; so this campaign, in cooperation with Austrian National Bank and Chamber of Commerce, is geared to informing and motivating the general public and bank staff in particular; it includes an information film entitled "The Granny Scam".

Start/duration:

Date of Project Start: 01.04.2015
Public release (press conference): 18.02.2016
On-going: awareness raising with print campaign, based on the video clip produced

Background research:

The sub-department of crime prevention and victim support made an evaluation and status quo of the impact, the modus operandi and the extent of this type of fraud, together with the sub-department of economic crime, sub-department of fraud, forgery and economic crime, and the department of crime analysis at Criminal Intelligence Service Austria.

Budget:

Most costly was the clip (EUR 7,000) funded by Criminal Intelligence Service Austria, and cost of the print campaign (EUR 1,000); aside of that, the press conference was financed by the National Bank; distribution of content was funded jointly by all three stakeholders.

Type of evaluation:

One of the partners of the project – the Austrian National Bank – arranged for a road show; they stopped at all provinces and districts in Austria in the course of summer 2016. Following the tour, staff took the time and stepped into every bank at every city where they had stopped with the road show and questioned bank employees if they had heard about the granny scam, if they had seen the clip and if they knew how to react properly in case they meet a suspect.

For 91% of the employees the granny scam was known and they also knew how to react in case of suspicion. The clip was only known in average by 19%, that is why it was decided to run another campaign with information sheets to promote the modus and the clip again.

Actor conducting evaluation/ timing:

External: the Austrian National Bank

Type of data collection method:

Impact evaluation executed by the Austrian National Bank in 158 banks all over Austria.

Further information:

http://eucpn.org/document/granny-scam

HELLO GRANNY, I NEED MONEY (DE)

Short description:
Elderly people are attractive to fraudsters. One method that has become popular among criminals is the “Grandchild trick fraud”, in which fraudsters pose as relatives of the victim, pretending to be in a desperate situation and in urgent need of money.

The project “Hello Granny, I need money” offers an innovative concept for crime prevention concerning trick fraud. It is an interactive stage play which offers an overview about prevalent techniques and shows up measures to protect oneself from becoming a potential victim. It also reduces the subjective fear towards tricksters and encourages to be more self-confident.

The audience is actively engaged in the performance. Randomly selected audience members take part in the performance as active participants while the actors improvise and react to the input by the audience spontaneously. The background of realistic cases helps to convey the urgency and the entertaining factor ensures a long-lasting impression.

Start/duration:
The project started on 28/03/2012 and is still running.

Background research:
There was a statistical increase of “Grandchild trick frauds”, identified by the PKS (Police Crime Statistics). Striking was the number of cases, as well as the resulting damage.

The number of cases in the federal state Baden-Württemberg increased from 95 (2007), 64 (2008), 143 (2009) up to 311 in 2010.

The financial losses in the federal state Baden-Württemberg increased from 234.890 Euro (2007), 45.870 Euro (2008), 557.900 Euro (2009) to 1.108.131 Euro in 2010.

Budget:
The writing and development of the play happened in voluntary work by Allan Mathiasch, supported by his theatre ensemble and the cooperation partners (police and city). The costs for one performance – including two actors and equipment – total 790-890€, in addition to travel expenses.

Type of evaluation:
Process and impact evaluation.

Actor conducting evaluation/ timing:
External: Theresa Siegler, student at the university of applied sciences in Kehl.

Type of data collection method:
Questionnaire-based survey.

Further information:
https://eucpn.f2w.fedict.be/document/hello-granny-i-need-money

SILVER SURFER (LU)

Short description:
The "Silver Surfer" project is a project by senior citizens for senior citizens. Volunteer senior citizens receive specific training on the creation of awareness about the safe use of the internet. They transfer their knowledge to other senior citizens through conferences, for instance during senior citizens events, at senior citizens' clubs or in senior citizens' associations. "Silver Surfers" work as multipliers.

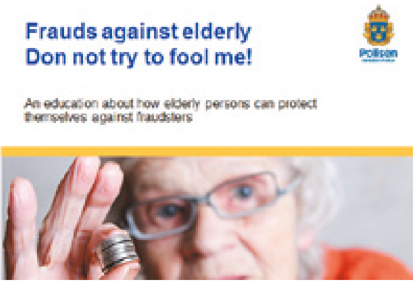
In 2014 the project was created at the initiative of BEE SECURE and is based on collaboration between the Ministry of Family, Integration and the Greater Region of Luxembourg, SECURITYMADEIN.LU, RBS-Center fir Altersfroen and the SenioreSécherheetsBeroder.

Start/duration:
The project started in 2014 and is still running.

Background research:
In 2013 the partner SECURITYMADEIN.LU started a survey during a senior citizens fair. The result showed that the surveyed senior citizens used the PC only to exchange e-mails (94%) or to Skype (32%) with family members. Barely half of them knew about internet frauds. 32% of them have already been victims of phishing attacks, and 12% victims of a ransomware fraud. The same survey was repeated in 2014 at the same fair. The results were comparable and showed that senior citizens were using the internet more often (5% more than in 2013).

Further information:
https://eucpn.org/document/silver-surfer

DO NOT TRY TO FOOL ME (SE)



Frauds against elderly
Don not try to fool me!

Polisen

An education about how elderly persons can protect themselves against fraudsters

Short description:
The project “Do not try to fool me” was created to prevent crimes of fraud against elderly people through increasing awareness about these crimes and make it easier for possible victims to recognise attempts of fraud and to protect themselves against it.

The method that was chosen for the project was to create an information package and a structure for how the material could be used in active meetings where the participants who take part can train for different situations where they could be victims of fraud and how they can act to prevent being the victim of fraud.

The material is supposed to be used at three different meetings and includes a guide for the meeting-leader, three different short films and three different learning-guides. Every occasion includes working with one film and one learning-guide. The material is self-instructing and based on different cases that can be used for discussion and practical exercises.

Start/duration:
The project started officially 16/09/15 and is still running.

Background research:
The national centre against fraud at the Swedish police authority analysed the development of fraud in Sweden and noticed a sharp rise in fraud against elderly people. The deepened analysis showed which modus operandi that was used in these crimes and which fishing-points was used. This analysis was used to create the material and the case-studies in the project-material. The analysis was mainly based on data of crimes reported to the Swedish police.

Budget:
The cost of the project is not specified. Because the project was prioritised all the resources was taken from the ordinary financial framework and therefor was not specified. The police and the organisations produced the films and other materials themselves and through that the costs where kept relatively low.

Type of evaluation:
A process evaluation have not been completed yet but the method will

be evaluated through measuring how many meetings have been completed, and a survey to the individuals that have participated about how they view the project and what changes it have led to concerning their awareness about fraud and what to do to prevent being a victim. The impact evaluation has not been conducted yet but an analysis will be done and the work have started with analysing changes in reported crime of this type and differences regarding completed crimes and attempted crimes.

Further information:
https://eucpn.f2w.fedict.be/document/do-not-try-fool-me

AUSTRIA: THE WATCHLIST INTERNET

Watchlist Internet
Internet-Betrug, Fallen & Fakes im Blick

Short Description

The Watchlist Internet is a project to prevent and to fight against online crime such as fraud and other online traps. Since 2013 the project team researches into fake sites and online fraud cases, with the objective to seriously inform the public at large with news articles on its website. Its unique selling points are continuity and effective search engine optimization. The project also contributes to fighting online crime at large by the network it has established between e-commerce platforms, private banks, governmental bodies and law enforcement agencies in Austria. Essential to the success of the project is also the close cooperation with the online dispute settlement body "Internet Ombudsmann" and with the stakeholders and users of the website, which contribute to reporting cases.

Start/ Duration

The project started on the 3rd of July in 2013 and is still running.

Background Research

There was an analysis of the context by the team of the Internet Ombudsmann.

The noticed rise of Internet fraud cases, stressed the need to raise the efforts in awareness raising. The amount of cases raised by 18 percent in 2012 to the year before. Based on this data, the Watchlist Internet was founded by the Austrian Institute of Applied Telecommunication.

Budget

The Watchlist Internet is funded by the Austrian Federal Ministry of Labour, Social Affairs and Consumer Protection, the Austrian Chamber of Labour, the largest Austrian online market place willhaben.at and the Bank Austria. The yearly costs of the project amount to approximately 65 000 euro/year.

Type of evaluation

There has been an internal process evaluation in August 2014 in the form of an online survey among readers of the Watchlist Internet website. Based on these findings, the project was further shaped, for example using a more easy language with the regard to the older public. No external outcome or impact evaluation has been conducted, but an internal impact evaluation is done on a yearly basis.

Actor conducting evaluation/ timing

Internal: by the project team and an advisory board with public and private stakeholders

Type of data collection method

The annual evaluation is based on Google Analytics, such as user statistics, website visitors, visit duration,…, the feedback from users and funding partners, as well as constantly with checks on whether news about Internet fraud lead to the disappearance of a fake-site.

Links to further information

http://eucpn.org/document/watchlist-internet

FRAUD SECTION BULGARIAN NATIONAL POLICE GENERAL DIRECTORATE (BG)

Short description:

In Bulgaria, an entire 'fraud section' within the National Police General Directorate is dedicated to phone scams. Aside from their reactive police work, they also have the fundamental task of prevention. As part of their work, increasing the population's knowledge and awareness of this crime is done by information campaigns. For example, information leaflets are spread, but also advice is given on a national radio show. Another example from Bulgaria are stickers that are handed out. These stickers have preventive messages and people are asked to stick them to their phone. The idea is that when they are called, they are being remembered to the preventive message because they see the sticker as they pick up the phone.

ANTI-FRAUD MECHANISM FIRST INVESTMENT BANK BULGARIA (BG)

Short description:
This bank in Bulgaria has a mechanism in play to detect and prevent phone fraud cases. When large amounts are being withdrawn that are inconsistent with a set list of criteria from the bank, the clerk is alerted and prompted to check with the client whether or not he or she is being pressured. An algorithm will send a report to the clerk when these criteria seem to point towards a possible phone fraud case. The clerk can then check with the client, according to a 'Phone Fraud Checklist', asking questions for example about the purpose of the withdrawal or by watching the customer's actions.

#CYBERSCAMS (EC3, EUROPOL)

Short description:
Every year the European Cyber Security Month (ECSM) is held in October. This 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. The main goal is to raise awareness, change behaviour and provide resources about how to protect oneself online. Every week there is specific topic and during the third week of the 2018 edition, the European Cybercrime Centre (EC3), the European Banking Federation (EBF) and partners from public and private sectors joined forces to present 'cyber scams' as the theme.

7 common online financial scams are shown on factsheets and are being explained how to avoid them. These materials were spread throughout the EU by means of a social media campaign. After the launch, every scam received one day of highlighting.

Start/duration:
The campaign was officially launched on the 17th of October 2018. The materials will remain available online.

Further information:
https://www.europol.europa.eu/cyberscams

HOW PHISHINGPROOF ARE YOU? (BE)

Short description:
This campaign was launched by the Belgian Centre for Cybersecurity (CCB) during the European Cyber Security Month (ECSM) of 2017. The goal of the campaign was to inform the public on phishing emails and how to recognize them. By disseminating flyers, posters, but also an extensive (social) media campaign, the project claims to have been picked up by approximately 2 million internet users in Belgium.
Aside from this information campaign, the public was also invited to forward suspicious emails to the CCB. By scanning these emails and checking them with sophisticated software, 5 suspicious links are being blocked every day.

Start/duration:
The campaign was officially launched on the 2nd of October 2017. The materials are still available online and the forwarding mechanism is still active.

Further information:
www.safeonweb.be

NEDÁME SE (WE WON'T TAKE IT) (CZ)

Short description:
The "Nedáme se" programme is an interactive educational stage play, in which four types of most common deceitful manipulative techniques, used against seniors, gained their stage versions. These are sales campaigns, selling perfumes on the street, telemarketing and at-senior's-home selling technique. Besides the actors, a policeman, and also the author of the play, psychologist PhDr. Romana Mazalová, Ph.D., appear on the scene. They are entering the play and interact with the audience, thus teaching them new strategies of defence. The play is therefore not only enjoyable, but also becomes a new educational form against so-called "Šmejdi" (crooks). The educational effect on the audience was experimentally examined. The results confirmed that the seniors who had seen the play proved to be more successful in defending against fraud sellers.

Start/duration:
2015

Further information:
https://eucpn.org/document/czech-elderly-dont-swallow-bait

THE PRICE OF FRIENDSHIP (RO)

NU CREDE TOT CEEA CE ȚI SE SPUNE LA TELEFON!
UN HOȚ AR PUTEA SĂ ȚI VREA BANII!

Short description:
The purpose of the project was to reduce the risk for elder people to be victimised, following these objectives: knowing the target group from attitudinal and behavioural perspective, increasing the level of preventive

knowledge of elder people and increasing the capacity of self-defense. The target group was composed of people over 60 years old, who are members of local senior clubs. In 2017, a total of 34 preventive information activities were done by the police. The information pointed out the risks associated to age, but also to the prevention of victimisation in case of deceptive schemes, such as fake phoning campaigns. Also, online training courses were given to the elderly. Additionally, a 'senior safety ball' was held to launch a public information campaign.

Start/duration:
January 2017

Further information:
https://eucpn.org/document/price-friendship-project

SAFETY GUIDE FOR ELDERS (FI)

VANHUSTYÖN KESKUSLIITON KORJAUSNEUVOJAT

Jukka Laakso
jukka.laakso@vtkl.fi
040 502 3807
Korjausneuvonnan päällikkö

Tapio Rokkonen
tapio.rokkonen@vtkl.fi
0400 371 586
Pohjois-Savo

Harri Hietikko
harri.hietikko@vtkl.fi
0400 260 962
Etelä-Pohjanmaa ja Pohjanmaa

Pekka Hulkkonen

Tapio Karhu
tapio.karhu@vtkl.fi
040 516 6738
Pohjois-Pohjanmaa, Kainuu

Ismo Kortman
ismo.kortman@vtkl.fi
0500 651 737
Suur-Savo

Jukka Lampi
jukka.lampi@vtkl.fi
0400 162 494
Sisä-Suomi

Jari Malminen

Tiina Toivonen
tiina.toivonen@tetconsulting.fi
0400 852 727
Satakunta

Voitto Niska
voitto.niska@vtkl.fi
0400 649 199
Pirkka-Häme

Kari Tahvanainen
kari.tahvanainen@vtkl.fi
0500 494 766
Päijät-Häme

Raimo Saarelainen
raimo.saarelainen@vtkl.fi

Short description:
In Finland the Finnish Association for the Welfare of Older People has regional home repair experts who offer older people free advice. They help in situations including where an older person is being persuaded to order an expensive home renovation.
Elderly can contact them regarding:

- Fraudulent sales persons (phone, home visits).
- Renovation and repairs scams (overpriced, unnecessary etc.)
- Advice on **how to act** if sales person pressures for sale
- Advice on **contracts and cancellation** within 2 weeks etc.

'TRICKS AGAINST CHATTER TRICKS' (NL)

Short description:
A senior organisation in the Netherlands created an application for elderly that teaches them the dangers of scams. The app simulates 'scam situations' so the elderly can immediately test their newly learned skills. For example, a simulation of a lottery scam will be shown. The elder can then answer in real life upon which the app will score his answer's level of assertiveness.

ACTION FRAUD (UK)

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Short Description:
Action Fraud is the UK's national reporting centre for fraud and cybercrime where you should report fraud if you have been scammed, defrauded or experienced cybercrime in England, Wales and Northern Ireland. They also direct victims to designated support groups to help those affected by the crime or provide them with the information where they need to report to.

Further information:
https://www.actionfraud.police.uk/

ENDNOTES

[1] Users are for example sent simulated phishing emails to test their vulnerability, at the end of the test, they receive extra information on how to prevent this in the future (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

[2] Here users immediately receive extra information when they click on a false link (Sheng, Holbrook, Kumaragur, Cranor, & Downs, 2010)

[3] Anti-Phishing Phill is a good example of an online game that teaches users good habits to help them avoid phishing attacks. At the end of the training, users recognised fraudulent website better than the control group and more knowledgeable on strategies to prevent them from being victimised (Sheng, et al., 2007).

[4] https://cybersecuritymonth.eu/about-ecsm/whats-ecsm

[5] https://www.actionfraud.police.uk/support-and-prevention/ive-been-a-victim-of-fraud

REFERENCES

Agustina, J. (2015). Understanding Cyber Victimization: Digital Architectures and the Disinhibition Effect. *International Journal of Cyber Criminology, 9*(1), 35-54.

Anderson, K. (2016). *Mass-market consumer fraud: who is most susceptible to becoming a victim?* Washington D.C.: FTC Bureau of Economics.

Atkins, B., & Huang, W. (2013). A study of social engineering in online frauds. *Open Journal of Social Sciences, 1*(3), 23-32.

Barnes, P. (2017). Stock market scams, shell companies, penny shares, boiler rooms and cold calling: the UK experience. *International Journal of Law, Crime and Justice, 48*, 50-64.

Bidgoli, M., & Grossklags, J. (2017). "Hello. this is the IRS calling": a case study on scams, extortion, impersonation, and phone spoofing. *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 57-69). Scottsdale: AZ.

Bullée, J.-W., Montoya, L., Junger, M., & Hartel, P. (2016). Telephone-based social engineering attacks: an experiment testing the success and time decay of an intervention. *Singapore Cyber-Security Conference*, (pp. 107-114). Singapore.

Bullée, J.-W., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2018). On the anatomy of social engineering attacks: a literature-based dissection of successful attacks. *J Investig Psychol offender Profil, 15*, 20-45.

Burgard, A., & Schlembach, C. (2013). Frames of Fraud: a qualitative analysis of the structure and process of victimization on the internet. *International journal of Cyber Criminology, 7*(2), 112-124.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims.* London: Routledge.

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud: literature review.* National Fraud Authority.

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal, 27*(1), 36-54.

Button, M., McNaughton, N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology, 47*(3), 391-408.

Button, M., Tapley, J., & Lewis, C. (2012). The 'fraud justice network' and the infra-structure of support for individual fraud victims in England and Wales. *Criminology and Criminal Justice, 13*(1), 37-61.

Cialdini, R. (2001). *Influence: Sciende and practice.* Boston : Allyn & Bacon.

Cornish, D., & Clarke, R. (2003). Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. *Crime prevention Studies, 16*, 41-96.

Crosman, K. (2017). Phone and Television Scams in the Age of the Internet. *Lewis & Clark L.Rev.*, 21, 791.

Cross, C. (2016). 'I'm anonymous, I'm a voice at the end of the phone': a Canadian case study into the benefits of providing telephone support to fraud victims. *Crime Prevention and Community Safety, 18*, 228-243.

Cross, C., Richards, K., & Smith, R. (2016). The reporting experiences and support needs of victims of online fraud. *Trends & issues in crime and criminal justice, 518*, 1-14.

De Kimpe, L., Walrave, M., Hardyns, W., Pauwels, L., & Ponnet, K. (2018). You've got mail! Explaining individual differences in becoming a phishing target. *Telematics and Informatics, 35*(5), 1277-1287.

EUCPN. (2017). Cyber Safety: A theoretical insight. . In E. Secretariat, *EUCPN Theoretical Paper Series.* Brussels: European Crime Prevention Network.

EUCPN. (2017). Organised Crime Targeting Elderly People: a theoretical overview. In E. Secretariat, *EUCPN Theoretical Paper Series.* Brussels: European Crime Prevention Network.

European Commission. (2017). *Special Eurobarometer 464a: Europeans' attitudes towards cyber security.* Brussels: European Commission.

European Commission. (2018). *Special*

Eurobarometer 462: E-Communications and Digital Single Market. Brussels: European Commission.

Europol. (2014). *Internet organised Crime Threat Assessment.* The Hague: Europol.

Europol. (2016). *Internet Organised Crime Threat Assessment.* The Hague: Europol.

Europol. (2017). *Internet Organised Crime Threat Assessment .* The Hague: Europol.

Europol. (2018). *Internet Organised Crime Threat Assessment.* The Hague: Europol.

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 36-47). Cham: Springer.

Gadhave, U., & Sirsat, S. (2015). Review of Cyber-crimes and their impacts over the society. *international Journal of Electronics, Communication & Soft Computing Science and Engineering*, 357-359.

Harley, D., Grooten, M., Burn, S., & Johnston, C. (2012). My PC has 32,539 errors: how telephone support scams really work. *Virus Conference*, (pp. 1-8).

Jacques, S., & Bonomo, E. (2017). Learning from the Offenders' perspective on crime prevention. In B. Leclerc, & E. Savona, *Crime Prevention in the 21st Century: insightful approaches for crime prevention initiatives* (pp. 9-18). Springer.

Jakobsson, M. (2016). *Understanding Social Engineering based scams.* New York: Springer.

Lab, S. (2010). *Crime prevention: approaches, practices and evaluations.* LexisNexis Group.

Leukfeldt, E., & Stol, W. (2011). De marktplaats-fraudeur ontmaskerd: Internetfraudeurs vergeleken met klassieke fraudeurs. *Secondant, 25*(6), 26-31.

Levi, M. (2008). Organized fraud and organizing frauds: Unpacking research on networks and organization. *Criminology & Criminal Justice, 8*(4), 389-419.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: overview and issues. *Crime, law and social change, 67*, 3-20.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK. *British Journal of Criminology, 48*, 293-318.

Maggi, F. (2010). Are the con artists back? A preliminary analysis of modern phone frauds. *10th IEEE International Conference on Computer and Information Technology*, (pp. 824-831).

Marzuoli, A., Kingravi, H., Dewey, D., & Pindrop, R. (2016). Uncovering the landscap of fraud and spam in the thelephony channel. *15th IEEE international Conference on Machine Learning and Applications*, (pp. 853-858).

Mba, G., Onaolapo, J., Stringhini, G., & Cavallaro, L. (2017). Flipping 419 cybercrime scams: targeting the weak and the vulnerable. *International World Wide Web Conference*, (pp. 1301-1310). Perth.

Mears, D., Reisig, M., Scaggs, S., & Holtfreter, K. (2016). Efforts to reduce consumer fraud victimization among the elderly: the effect of information access on program awareness and contact. *Crime & Delinquency, 62*(9), 1235-1259.

Moreno-Fernández, M., Blanco, F., Garaizar, P., & Matute, H. (2017). Fishing for phsihers. Improving internet users' sensitivity to visual deception cues to prevent electronic fraud. *Computers in Human Behavior, 69*, 421-436.

Murphy, D. R., & Murphy, R. H. (2007). Phishing, Pharming, and Vishing: Fraud in the Internet Age. In T. Fowler, & J. Leigh, *The Telecommunications Review* (pp. 37-45). VA: Noblis.

Ollmann, G. (2007). *The vishing guide.* IBM Global Technology Services.

Petty, R., & Cacioppo, J. (1986). The elaboration likelihood model of persuasion. *Communication and persuasion*, 1-24.

Petty, R., & Cacioppo, J. (2012). *Communication and persuasion: Central and peripheral routes to attitude change.* Springer Science & Business Media.

Rauti, S., & Leppänen, V. (2017). "You have a potential hacker's infection": a study on technical support scams. *IEEE International Conference on Computer and Information Technology*, (pp. 197-203).

Ross, M., Grossmann, I., & Schryer, E. (2014). Contrary to psychological opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on psychological science, 9*(4), 427-442.

Rusch, J. (1999). The "social engineering" of internet fraud. *Internet Society Annual Conference.* Retrieved from http://www. isoc. org/isoc/conferences/inet/99/proceedings/3g/3g_2. htm.

Sheng, S., Holbrook, M., Kumaragur, P., Cranor, L., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Privacy Behaviors*, 373-382.

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Anti-Phishing Phil: The Design and Evaluation of a Game that teaches people not to fall for phish. *Proceedings of the 3rd symposium on Usable privacy and security* (pp. 88-99). ACM.

Singh, L., & Imphal, N. (2018). A survey on phishing and anti-phishing techniques. *International Journal of Computer Science Trends and Technology, 6*(2), 62-68.

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM, 54*(3), 70-75.

Tabron, J. (2016). Linguistic features of phone scams: a qualitative survey. *11th Annual symposium on information assurance*, (pp. 52-58).

Titus, R., & Gover, A. (2001). Personal Fraud: The Victims and the Scams. In F. G., & K. Pease, *Repeat Victimization* (pp. 133-152). New York: Criminal Justice Press.

van de Weijer, S., Leukfeldt, R., & Bernasco, W. (2018). Determinants of reporting cybercrime: a comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, 1-23.

Whitty, M. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665-684.

Whitty, M. (2015). Anatomy of the online dating romance scam. *Security Journal, 28*(4), 443-455.

Whitty, M. (2018). Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking, 21*(2), 105-109.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass marketing scam. *Journal of Experimental Psychology: applied, 24*(2), 196-206.

Wood, S., Liu, P., Hanoch, Y., Xi, P., & Klapatch, L. (2018). Call to claim your prize: perceived benefits and risk drive intention to comply in a mass masketing scam. *Journal of Experimental Psychology: Aplied, 24*(2), 196-206.

Workman, M. (2008). Wisecrackers: a theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the american society for information science and technology, 59*(4), 1-12.

Yeboah-Boateng, E., & Amanor, P. (2014). Phishing, SMishing & Vishing: an assessment of threats against mobile devices. *Journal of Emerging Trends in Computing and Information Sciences, 5*(4), 297-307.

CONTACT DETAILS

EUCPN Secretariat
Phone: +32 2 557 33 30
Email: eucpn@ibz.eu
Website: www.eucpn.org

TWITTER.COM/EUCPN
FACEBOOK.COM/EUCPN
LINKEDIN.COM/COMPANY/EUCPN