The European Crime Prevention Network: Preventing Individual Fraud in the EU

A Report on a New Toolbox

eucrim
European Law Forum: Prevention • Investigation • Prosecution

Report

Jorne Vanhee

The European Crime Prevention Network (EUCPN) was set up by the Council of the European Union in 2001 (Council Decisions 2001/427/JHA and 2009/902/JHA). For EU Member States, the EUCPN is a first point of contact for crime prevention. The Network collects and disseminates expertise and best practices. The continually evolving thematic focus of the EUCPN reflects the priorities of the EU Policy Cycle, on the one hand, and the EUCPN presidency's priority, on the other. This presidency rotates with that of the Council of the EU.

The EUCPN's output includes toolboxes aimed at local and national practitioners alongside theoretical, research, and policy papers. The toolboxes contain informative studies for practitioners to use, which provide an overview of the problem, present current good practices, and make concrete recommendations for preventive actions. The 13th toolbox in the series published by the EUCPN Secretariat deals with the prevention of individual fraud, after it had been the focal topic of the Bulgarian Presidency in 2018. The following report summarises the main findings on the phenomenon in the EU, best practices, and recommended prevention measures. The full report is available at: <https://eucpn.org/document/toolbox-13-preventing-individual-fraud>.

AUTHOR

Jorne Vanhee
Research officer
European Crime Prevention Network

Published in
2019, Vol. 14(1) eucrim
ISSN: 1862-6947
https://eucrim.eu

Individual fraud means that individual citizens are 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 online forms, with phishing as the most common example. However, it is important to realize that individual fraud has been around for ages. The technological developments of the past decades have allowed these scams to be industrialised on a much larger scale than ever deemed possible. Who has not received a phishing e-mail in his or her life?

Victims actively participate in their victimisation. The offender sets his eyes on the victim's money, but he can only gain access to it by persuading the victim to give him access. The essential tactic used to nudge the victim into this compliant relationship is called **social engineering**. It allows the offender to win the victim's confidence, which 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 "human weaknesses", offenders are capable of activating what is known as the second route of persuasion. The first route requires a great deal of thought and cognitive effort. The second, however, needs no further elaboration and the victim reacts subconsciously. 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 easily allow offenders to exploit them to their own benefit.

Such deceptive tactics are put to use in a wide **variety of scams** (419 scams, granny scams, romance scams, CEO fraud, etc.) – 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 trend involves a combination of new and old technology: the telephone. Vishing or voice phishing combines the advantages of both the internet and the telephone. Making an online phone call entails almost no costs, is harder to trace, and can be made automatically. Using the telephone has additional benefits: people trust it and, due to the more intimate setting, victims are persuaded more readily. It is illustrative of the growing level of sophistication that offenders even hire native speakers to make the phone calls in order to seem as genuine as possible.

Our current understanding of individual fraud is limited however. This crime is characterised by a huge **dark number** as so much of it goes unreported. Victims do not know they have even been victimised, they do not perceive the offence as severe enough, they do not believe reporting will lead to anything, or they simply do not know where to report the offence in the first place. In addition, because of the active role, the victim plays in his own victimisation, feelings of self-blame and embarrassment prevent victims from telling their story. Some scams even have "built-in" anti-reporting mechanisms, as the victims have to undertake illegal actions in the scheme, incriminating themselves in the process. Reporting the scam would feel like 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 recognizing the signs 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 contact their victims randomly or by looking at public registries, but they also share lists among 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 even try to "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 so far. 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; there are some positive effects to be noted especially when delivered in some kind of training format. In essence, these trainings try to close the "knowing-doing" gap to which we referred above. 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 vulnerable position.

During the Bulgarian Presidency, the EUCPN 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. Best practices in this context are awareness-raising campaigns, for which we found good examples in Bulgaria, Sweden, Belgium, and from Europol. The campaigns involve radio spots, posters, flyers, gadgets, etc. that provide useful information to the public and show citizens how to protect themselves from being

harmed. A second set of activities is targeted towards the elderly. Here, more interactive methods are being employed, e.g., in the Czech Republic. The elderly take part in an interactive educational stage play, where they learn about the most common deception schemes and how to react to them. This "live experience" prepares them to react adequately in real-life situations. An evaluation of this project proved the approach to be empowering, as the active group refused phony deals two and a half times more often than a passive control group that did not participate in the play. The third and last category of prevention activities centres on victims. Examples from Australia, the United Kingdom, and Canada showed the need for this type of prevention on this group. There are, unfortunately, few support services for victims of individual fraud – even globally.

Lastly, the EUCPN report on individual fraud drew up several recommendations on how to prevent phone scams. They are based on a workshop with different experts that was organised by the EUCPN Secretariat in August 2018. These **recommendations** are structured according to the five strategies of situational crime prevention.

The first possible strategy is to ***increase the effort*** an offender must expend in order for the scam to succeed. Restricting the publication of and access to phone numbers can already have a major deterrent effect. Another technique involves limiting the amount of phone numbers one person is allowed to possess or at least to link this "ownership" with a bank account or ID number.

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

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

Another strategy is to ***reduce provocations*** that could lead to offending. 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 as some fraudsters will contact identified victims with a deceptive offer to help and retrieve their losses.

The final strategy is to ***remove the excuses***. This is mainly focussed on raising awareness on phone scams and how to protect yourself. The good practices mentioned above are key examples. Awareness campaigns should spread the same message. At best, public-private partnerships and international cooperation need to be established in order to spread a consistent message: *just say no.*

About eucrim

The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union