EUCPN
EUROPEAN CRIME PREVENTION NETWORK

Recommendation paper

CLICK HERE, JUST TRUST ME!

How online fraud works and how to prevent it

EMPACT

Online fraud continues to be a prominent issue in Europe and will remain so for the foreseeable future.

This paper puts forward some broadly applicable concepts and tools to design effective crime prevention initiatives.

Citation
EUCPN (2022). Click here, just trust me!-How online scams work and how to prevent them. Brussels: EUCPN.

Authors/editors
Thomas Van den Berghe, Practice and Policy Officer, EUCPN Secretariat.

Part of the project 'EUCPN Secretariat', February 2023, Brussels
With the financial support of the European Union's Internal Security Fund – Police

Table of contents

Under the hood of fraud schemes 5

The human element 5
Maleficent influencers 5
Taking it one step at a time 6

Prevention initiatives 7

Building blocks 7
Good practices 8

Conclusion 9

Endnotes 10

The paper was written in the context of the EUCPN's cooperation within the European Multidisciplinary Platform Against Criminal Threats (EMPACT) of 2022. This short paper explores the general mechanisms which make online fraud schemes work, puts forward guidelines for prevention initiatives and provides some examples of good practices. Its goal is to provide a solid introduction to and understanding of online fraud schemes, but it does not offer comprehensive guidelines for preventive responses to all online fraud.

We would like to express our special thanks to those who assisted in the creation of this paper, including, but not limited to, the Swedish National Fraud Centre.

Societal changes, such as the COVID-19 crisis and the shift towards a cashless society, also create new opportunities for criminals to reach more victims.

People defrauding others is not a new phenomenon, far from it. Fraud has existed for as long as private property and the ability to communicate have been around.[1] The reach of such scams, however, has increased significantly. The widespread popularity of digital communication technology brought along with it a fresh generation of fraud schemes. These 'cyber-enabled' schemes can spread at an unimaginable speed and target more (potential) victims, all the while allowing criminals to operate in anonymity.[2]

Fraudsters make use of a wide variety of modi operandi (MOs).[3] Different techniques are used, each of which has its own specific characteristics; romance fraud on online dating apps, phishing e-mails with fraudulent links, investment scams involving the latest cryptocurrency and many more. Yet all these different varieties of scams share a single mechanism: social engineering. This is a technique which manipulates human behaviour in order to make people comply with a given demand or give confidential information which they otherwise would not do.[4]

Societal changes, such as the COVID-19 crisis and the shift towards a cashless society, also create new opportunities for criminals to reach more victims. Fraudsters are flexible and eagerly adjust their way of working to increase their chances of success, as they have done in the past. As citizens become more accustomed to using online services such as online banking and web shops, the pool of potential victims grows too.[5] This trend is already clear, given that online fraud becomes more prevalent every year.[6] The likelihood a mass exodus from people's onscreen lives seems rather slim, so it will therefore be necessary to prepare ourselves to combat the types of online fraud.

Under the hood of fraud schemes

The human element

Cybercriminals use a wide variety of techniques to defraud their victims, but they can generally be viewed as forming part of a spectrum. At one end of the spectrum are technology-based approaches. These make use of IT tools such as key loggers, spyware, other types of malware and tools to obtain sensitive information (e.g. passwords, company records or personal data). At the other end of the spectrum, however, criminals target and attempt to influence human action. This includes a wide variety of fraud schemes such as phishing, investment fraud, impersonating friends/authority figures and more. This manipulation is commonly referred to as **social engineering**.[7]

This paper focusses on this human element. Firstly, because the technology based approach generally also tends to exploit a human weakness to infiltrate their IT infrastructure (e.g. attaching fraudulent attachments to an e-mail requesting the recipient to open it and releasing maleficent code when he/she does so). Secondly, focusing on hacking approaches involving a human element has a wider applicability due to their widespread use.

The 'human element' is the weakness that opens the door to online fraud.[8] It is estimated to be involved in over 80% of data breaches around the globe and is considered to be a crucial contributor in many of these.[9] Although it must be noted that 'the human element' encompasses a lot more than simply social engineering, weaknesses such as poor passwords or losing important hardware are not the result of social engineering.

Social engineering works because it (ab)uses the way in which humans process information. Usually, we have two ways of dealing with information. The first one is the 'central route', it requires logic and thought, which analyses incoming information. It is more sceptical and requests additional information to elaborate upon and look for any inconsistencies. The second one, the 'peripheral route', focuses much more closely on the source of information itself and individual/personal reasons to be convinced. If we like the source or if the context in which it is presented is believable, the information coming from it will also thought to be fine and will not be analysed in too much detail.[10] Scammers push their victims onto this second route by abusing the way humans think. This pressures victims, putting them in a position where it is much harder to respond using the central route and apply critical thinking to the situation.[11]

Maleficent influencers

To understand why frauds work, you also have to look at the stories brought to its victims. Only then you can proceed with countering them successfully. Quite a large amount of research has been carried out into this topic and this can be summarised by providing a list of five key elements of fraud.[12]

- **Authority**: Scammers often operate from a position of authority. This could be related to a profession (e.g. police officers) or knowledge (e.g. investment gurus). During their lives, people have been conditioned to respond more submissively to figures of authority.
- **Social Proof**: Humans like to be part of a group, so they tend to follow what others do. If something looks like it is being done by many people, we instinctively assume that it must be safe to do so ourselves, even if that is not actually the case.
- **Liking, Similarity and Deception**: People like people who are like them or who they would want to be. Fraudsters pretend to be a successful investor, a beautiful doctor abroad looking for help/love or simply someone who has the same look/attitudes as us. People subconsciously want the persona to like them.
- **Commitment, Reciprocation and Consistency**: People want to be perceived as consistent and trustworthy. Fraudsters abuse this by giving you a very small favour and requesting something (more difficult from the victim's end) in return. This pressures the victim to comply because 'quid pro quo'. Fraudsters also aim to make you say yes, perhaps to something very simple, before moving on to more substantial requests. If the victim wants to remain to be perceived as helpful, even subconsciously, you must continue to say yes.

- **Distractions**: People like to focus on one thing; something they can win, a risk to avoid or a limited time offer. These distract them from any other signals they might otherwise have perceived and heighten people's emotional state, causing them to ignore illogical fallacies. Fear and greed in particular are influential motivators.

Not all elements are present in all fraud schemes. The elements above are simply ingredients which can be effective in some schemes but not in others. Most frauds limit themselves to one or two of the principles above. By far the most used one is 'Authority' followed by 'Liking, Similarity and Deception'.[13]

Taking it one step at a time

Not just the ingredients of online fraud schemes have similarities. Despite the substantial differences between the many MOs in online fraud schemes, they still share a process at their core. This joint path allows the use of shared frameworks for all online fraud schemes and prevention initiatives aimed at them. One such tool is **Crime Scripting**, which organises the information on the steps criminals take when executing crimes and the requirements to do so.[14]

Making a crime script is a good way to analyse the MOs used in criminal scenarios. It allows you to clearly state the criminal's means, their facilitators and the hot spots where they operate. This information allows you to create more precise and effective prevention and disruption actions. If you know how the fraudsters operate and what information they require, you can more easily craft preventative actions to target them. While this may sound difficult and complex, it really does not have to be.

Yes, crime scripts can be based on deep and profound scientific studies. But experience can also provide a very strong base for crime scripts by bringing together a group of seasoned police officers to discuss their know-how on a specific crime phenomenon.

So how do you write a crime script? First of all, you divide the process of committing a crime into three phases: the preparation phase, the execution phase and the completion phase (which looks at actions taken after the crime).
Then for each phase you make up a timeline/process that includes all of the requirements to execute the crime step by step. The preparation and execution phase vary greatly between the different types of fraud, but the completion phase is more universal.

A simplified example of a preparation phase visualisation of a crime script for Business E-mail Compromise (BEC) fraud would be:

Enter crime scene	Win trust	"The sting"	Concealment measures
Send email to corresponding person within company	Prepared information, corresponding with day to day operations	Use crisis situation – create pressure (time, importance, personal appeal)	Using VPNs
	Use proper lay-out and signature email	Request quick money transfer not following standard procedures	Remain on the move physically
	Use fake phone number in case of check-up OR immediately state that phone contact is not possible		Operate from abroad

Prevention initiatives

Building blocks

Five building blocks can be put forward, which can be used in successful initiatives to prevent online fraud. While these building blocks are not enough by themselves, they can be used as a 'Swiss cheese model' and add imperfect layers of protection forming a solid whole.[15]

The first block sets out to **increase the effort** required and make it more difficult for criminals to execute their scams. In this case, it is important to differentiate between target victims and facilitating victims. Facilitating victims are those who host information and IT infrastructure (e.g. companies) which can be used to defraud the actual target victims, who are targeted for their funds or for other reasons. By focusing on facilitating victims, you can prevent target victims from even being approached. For example, if databases are too difficult to breach, the information they contain cannot be used to target citizens. Many criminals also still use older tools such as the telephone directories. These should not be forgotten, as modern-day solutions to these old problems could be especially effective. Prevention techniques involving access controls that make it harder to access some services should also be used as much as possible by private companies. These can vary from (strong) passwords to two-factor authentication or in some circumstances even background checks for purposes such as gaining access to sensitive databases.

Practitioners should also **increase the risks associated** with committing frauds, in order to strengthen the deterrent effect. Especially the flow of information between public and private entities is crucial. The sharing of knowledge on MOs, prevention measures and enforcement creates a common view of the problems and common ways to tackle them and makes it much more difficult for criminals to operate safely. Many private companies (such as those in the financial sector) already have databases which are interesting as a means of monitoring and keeping track of the situation. Technology can also be a tool to analyse the huge amount of data available. Monitoring the situation to identify high-risk transactions (e.g. to flagged countries or irregular purchases) also enables a proactive approach. This can also circumvent the stigma of being a victim of fraud and still assist users as they do not have to take the initiative. Combating online scams is made more difficult due to complex reporting procedures, varying priorities and the fact that in many cases, people in several countries are involved. It can therefore be difficult to know who to contact initially. A clear and easily accessible point of contact for victims should be provided and clearly communicated, in order to increase the chance of capturing the fraudsters.

Reducing the rewards should also be a focus in prevention initiatives. The 'occupation' of defrauding others should not be an attractive means of obtaining a steady income.

Reducing the rewards should also be a focus in prevention initiatives. The 'occupation' of defrauding others should not be an attractive means of obtaining a steady income.
When catching a criminal, seizing their profits and assets as thoroughly as possible reduces their income. Going after their money laundering infrastructure (e.g. money mules) has a similar effect. Checks into the flow of funds on online selling platforms could have a strong impact on criminal profits (such as services holding on to the money for a certain time before transferring it to the seller).

Reducing provocations is about limiting the likelihood that criminals will be inspired to commit crimes. While there are not many possibilities to do this in the case of online fraud, there is still some potential. By only releasing limited information on the precise MOs used by fraudsters, copycats could be stopped before they even begin.

Finally, preventative initiatives should **remove excuses** from offenders as well. They like to claim their victims will not even know what happened to them. By informing (potential) victims about what is happening and how fraud can be avoided, criminals use an argument to convince themselves. This can take the shape of a pop-up when filling in a bank transaction to a flagged/high risk account, warning victims of the risk, or it may take the form of communication campaigns targeted at high-risk groups, such as people who already have been the victim of frauds before.

Online Fraud is a broad issue. Designing and implementing effective crime prevention initiatives takes time, research and funds.

Good practices

Online Fraud is a broad issue. Designing and implementing effective crime prevention initiatives takes time, research and funds. Fortunately, several examples are already available to use, to serve as inspiration or to adapt depending on your needs.

The **proactive disruption of crypto investment scams** by the Czech Bureau of Criminal Police and Investigation Service is an example of a practice which takes a proactive approach and aims to 'increase the risk' for criminals. The initiative is an offender-focused initiative specifically targeted at suspicious bank accounts and at disrupting criminal profits.
When a victim reports being defrauded, the damage has already been done and the criminals are already erasing their tracks. The Czech police poses as potential victims interested in investing in cryptocurrency to approach criminals themselves. In their contact with the fraudsters, they make them reveal the bank accounts they use. This information is then forwarded to the national anti-money laundering body, which has the authority to investigate the accounts. Whenever any crime or suspicious activity is uncovered, the banks themselves get involved alongside other police units. The cooperation with banks is essential when undertaking combined actions of this type. It was established and maintained because all those involved perceive the relationship to be mutually beneficial.

Project Sunbird is an Australian initiative which can be regarded as focusing on 'increase the effort'. It targets frauds in which victims have to send money to specific West African countries. The project analyses the financial transactions of remittance agencies, financial institutions or banks between Australian territories and five West African countries. This data is analysed and used in several ways. Letters are sent to households suspected of being defrauded and who are sending money to one of the five countries, one when discovering the fraud and a second three months later if payments continue. The letter contains an explanation on why it is sent and encourages them to get in touch with a listed point of contact for more information. The linked bank accounts of identified offenders and potential victims are also potentially blocked if they continue to send funds.
When evaluating the project, 72% of respondents stopped sending money after one letter, and another 50% of those who received a second letter stopped. A small percentage resumed sending funds after initially quitting.[16]

Conclusion

Online fraud continues to be a prominent issue in Europe and will remain so for the foreseeable future. Fortunately, a lot of information is available about how (online) fraud works and how these scams can be prevented. If we want to design effective crime prevention initiatives, using the available intelligence is key. This paper puts forward some general concepts and tools to do precisely this. Several tools that can be implemented in crime prevention initiatives can also serve as a source of inspiration when building new projects or can be implemented within existing ones. Online fraud is characterised by a high degree of flexibility on the part of the offenders, enabling them to adapt to changing circumstances. The information in this paper allows you to develop scientifically backed responses to them in kind.

If you would like to obtain more (academic) information concerning online fraud and additional examples from all over Europe, make sure you read **our toolbox on individual fraud** by clicking here.

If we want to design effective crime prevention initiatives, using the available intelligence is key.

Endnotes

1 K. Crosman, Phone and Television Scams in the Age of the Internet, *Lewis & Clark Law Review* 21:3 (2017), 794.

2 Ibid.; M. Button and C. Cross, Cyber Frauds, Scams and Their Victims, Oxon: Routledge, 794-5, 2017 #39.

3 Europol, European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence, Luxembourg: Publications Office of the European Union, 2021, 60, https://dx.doi.org/10.2813/02362; Europol, Internet Organised Crime Threat Assessment (Iocta) 2021, Luxembourg: Publications Office of the European Union, 2021, 30-2.

4 Europol, European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence, 60; J. Kancherla, Motivational and Psychological Triggers in Social Engineering, Research Paper: Social Science Research Network, 2021, 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3750474#:~:text=Gragg%20(2002)%20extracted%20seven%20psychological,information%20that%20triggers%20strong%20emotions; A. Ferreira, L. Coventry, and G. Lenzini (Eds.), *Principles of Persuasion in Social Engineering and Their Use in Phishing*, ed. T. Tryfonas and I. Askoxylakis, Los Angeles: conference proceedings, 2015, 36, https://link.springer.com/chapter/10.1007/978-3-319-20376-8_4; F. Mouton, L. Leenen, and H.S. Venter, Social Engineering Attack Examples, Templates and Scenarios, *Computers & Security* 59 (2016), https://dx.doi.org/https://doi.org/10.1016/j.cose.2016.03.004; J.-W.H. Bullée, L. Montoya, W. Pieters et al., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks, *Journal of Investigative Psychology and Offender Profiling* 15:1 (2015), 20-1, https://dx.doi.org/https://doi.org/10.1002/jip.1482; X. Luo, R. Brody, A. Seazzu, and S. Burd, Social Engineering: The Neglected Human Factor for Information Security Management, *Information Resources Management Journal* 24:3 (2011), 2.

5 Europol, European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence, 30-2; J.M. Whittaker and M. Button, Understanding Pet Scams: A Case Study of Advance Fee and Non-Delivery Fraud Using Victims' Accounts, *Australian & New Zealand Journal of Criminology* 53:4 (2020), 509-10, https://dx.doi.org/10.1177/0004865820957077.

6 S.N.C.f.C.P. (Brå), Fraud Crime in Sweden: Swedish National Council for Crime Prevention (Brå), 2016, https://bra.se/download/18.7d27ebd916ea64de53037693/1582617820842/2016_9_Fraud_crime_in_Sweden.pdf.

7 Kancherla, Motivational and Psychological Triggers in Social Engineering, 2; M. Allen, Social Engineering a Means to Violate a Computer System: SANS institute, 2021, 4-5, https://sansorg.egnyte.com/dl/Y7NTZsCxKN; ibid., 6-7.

8 Bullée et al., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks, 21{Luo, 2011 #57.}

9 Verizon, Data Breach Investigations Report, 2021, 33, https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf.

10 M.T. Whitty, The Scammers Persuasive Techniques Model - Development of a Stage Model to Explain the Online Dating Romance Scam, *The British Journal of Criminology* 53:4 (2013), 668, https://dx.doi.org/https://doi.org/10.1093/bjc/azt009; J. Teeny, P. Biñol, and R. Petty, *The Elaboration Likelihood Model: Understanding Consumer Attitude Change*, Abingdon: Routledge, 2017, 393-8.

11 Luo et al., Social Engineering: The Neglected Human Factor for Information Security Management, 2; B. Atkins and W. Huang, A Study of Social Engineeringin Online Frauds, *Open Journal of Social Sciences* 1:3 (2013), 23-4, https://dx.doi.org/http://dx.doi.org/10.4236/jss.2013.13004.

12 Ferreira et al., *Principles of Persuasion in Social Engineering and Their Use in Phishing*, 39-40.

13 Bullée et al., On the Anatomy of Social Engineering Attacks - a Literature-Based Dissection of Successful Attacks, 34-5.

14 H. Dehghanniri and H. Borrion, Crime Scripting: A Systematic Review, *European Journal of Criminology* (2019), 2, https://dx.doi.org/10.1177/1477370819850943.

15 D.B. Cornish and R.V. Clarke, Opportunities, Percipators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention, 16 (2003), 41-96.

16 Button and Cross, Cyber Frauds, Scams and Their Victims, 205-8.

Contact details

EUCPN Secretariat
Email: eucpn@ibz.eu
Website: www.eucpn.org

twitter.com/eucpn
facebook.com/eucpn
linkedin.com/company/eucpn