Social engineering: The next crime epidemic

Social engineering: The next crime epidemic

Marius Frunza • IntelBlitz • 5 mins read • Feb 18, 2022

The age of social engineers

Lies, romance, manipulation, flamboyant life-styles,... “The Tinder Swindler”, Netflix’s new true crime documentary, paints a harrowing portrait of Simon Leviev, an Israeli con artist, specialised in romance scams. The charismatic fraudster went way beyond the boundaries of romance cons, engineering a complex social network of fake identities and acolytes. How does social engineering work in a highly digitalised society? Are “social engineers” the future of organised crime?

Introduced in the popular culture by Kevin Mitnick[1], the term “social engineering” denotes the use of manipulation of people resulting in disclosing confidential information. The definition provided by Mitnick, states that *“social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology”*.

The initial meaning of social engineering referred to tactics used by fraudsters to obtain credentials of credit cards or online banking access. Usually, the victim received a letter or a phone call from a social engineer, who pretended to be working for a bank or for other institutions. The victim was required to share confidential information or even to send money to a given account. The development of the internet was a catalyst for social engineers. The term phishing was introduced for all the techniques leveraged by

1 In the 1990s Kevin Mitnick was on the FBI’s most wanted list. He was one of the most dangerous hackers, breaking into the networks of major companies (ie. IBM, Nokia, Motorola). After serving a sentence in prison for few years he became a researcher and consultant in cyber-security.

technology for obtaining sensitive information. In the early 2000, email spoofing was the preferred technology, many banks being touched by this fraud.

The range of tools and techniques labelled as social engineering widened over the past decade bolstered by social media and the technology for smartphones. The use of social engineering is not limited anymore to extracting confidential information. Cresting or stealing identities is one of the most recent social engineering tools used by criminals in the sphere of financial crime. Erasing trails or creating misleading information for investigators after a crime is committed is another silo of social engineering. With the quick development of private intelligence agencies, fraudsters are able to hire trained resources for better dissimulating and hiding their crimes.

A resurgence in crimes related to the “social engineering” concept was revealed by the Israeli police. The “social engineers” moved from skimming credit card information towards more profitable frauds against corporations. In 2017, a joint investigation between the FBI and the Israeli law enforcement identified a criminal group that allegedly approached companies, including insurance companies, banks and pension funds abroad. They deployed a very complex and evolved social-engineering crime type under the form of the so–called CEO fraud (described below in this section). The criminals claimed to be senior managers of the targeted companies and approached regular employees of those companies. They used their persuasion techniques and engaged the legitimate employees in financial transactions and entrusted them to transfer large amounts of money to other accounts for various fictitious reasons. The transferred money walked through a few bank accounts mainly located in China and other jurisdictions and finally reached the criminals. Israeli Police revealed that the targeted companies were based in Poland, Finland, India, France and the United States.

The Israeli investigators also revealed that the “social-engineers” were in ties with the Israeli-Arab Hariri crime organisation, one of

Israel's most powerful and dangerous organised crime groups. This pattern was also observed in the Carbon Connection era when criminals from France fled to Israel and then got acquainted with the local organised crime. These alliances were necessary as both groups needed protection from other criminal gangs, services which were obviously offered in exchange for a percentage of the proceeds.

Currently, Israel seems to be the main hub of social-engineering crimes. Two factors contribute to this phenomenon:

a. Israel has a policy of compulsory military service. The young population is trained with respect to military techniques and many see real action in the conflict zones. This constitutes an excellent recruiting pool for organised crime.

b. Israel has a strong education system in technology fields, being the world's top country in terms of technology start-ups related to its population. Israeli firms are the main players in the security software market. Thus, crime also has a recruitment pool of highly competent people.

These two features create a unique environment for the development of social-engineering crimes. The European investigators became aware of the new trend in the underworld cradling from the social engineering universe, especially with the CEO/BEC fraud.

> *" I was one of the first practitioners of social engineering as a hacking technique, and today it is my only tool of use, aside from a smartphone - in a purely white hat sort of way. But if you don't trust me, then ask any reasonably competent social engineer."*
>
> *John McAfee, a British-American computer programmer and businessman.*

Crypto: NFTs seized in a VAT fraud case

Digital assets and VAT fraud

Our Intelblitz issued in June 2021 highlighted the potential misuse of NFTs in VAT fraud. HM Revenue and Customs, the leading British tax authority, announced that three individuals had been arrested in an alleged VAT fraud case that aimed to defraud British taxpayers of 1.4 million GBP. The scam involved over 250 rogue companies.

HMRC has seized three Non-Fungible Tokens (NFT) as part of their investigation. It is not clear yet whether the NFTs continued the underlying of the VTA fraud or they were used to launder the proceeds of crime.

The world on the street: Remmo Clan

Big players in Germany

The Dresden Green Vault heist is one of the biggest burglaries that took place in recent years. A group of well-organised individuals penetrated in November 2019 the Green Vault museum within Dresden Castle and subtracted royal jewellery with an estimated value of over 1 billion euros. The entire operation was orchestrated by the Remmo clan, a criminal organisation that has dominated Germany's underworld for the past two decades.

The Remmos are a large family of Arab descent that relocated from Lebanon in East Germany during the 1980s. The group started to get involved in criminal activities in the early 1990s and rise to power account around 1000 active members, specialised in heists, extortions and drug trafficking. German police indicated amongst the suspects the names of Abdul Majed Remmo and Mohamed Remmo, two prominent members of the crime family.

Know Your Network, AI meets KYC

More insights at schwarzthal.tech

Marius Frunza
marius.frunza@schwarzthal.com

The information and data published in this newsletter were prepared by the market research department of Schwarzthal Tech

Contact

contact@schwarzthal.com
FR: (33) 6 27 29 78 34
UK: (44) 7 95 22 08 734
RU: (44) 7 95 22 08 723

Address

Devonshire House, 582 Honeypot Lane,
Stanmore, England,
HA7 1JS

Social

twitter.com/schwarzthal

linkedin.com/company/schwarzthal-tech