Published by:	Norwegian National Authority for Investigation and Prosecution of Economic and Environmental Crime (Økokrim)
In cooperation with:	District Prosecutor in Iceland, National Special Crime Unit (NSK) from Denmark, National Fraud Centre (NBC) from Sweden, and National Police board of Finland
Published:	2024
Contact information:	etterretning.okokrim@politiet.no

Photo: iStock

Preface

Due to the escalating threat posed by fraud, police forces from all Nordic countries established a task force in 2023 to combat online fraud. The incidence of reported online fraud schemes is high and continues to rise. This combined with technology that increases fraudsters' chances of success, there is an urgent need for a unified and coordinated Nordic action plan to address this threat.

As a first step, the Nordics have produced a joint threat assessment on online fraud schemes to map the most threatening modus operandi (MO) within online frauds in the Nordics, identifying vulnerabilities and already implemented preventive measures taken in the Nordic countries. This report also provides recommendations as to how the Nordic society as a whole can work together to prevent fraud.

ØKOKRIM

Polisen
Swedish Police

POLITI

POLIISI
POLISEN I FINLAND
Police of Finland

DISTRICT
PROSECUTOR

The continued digitalisation of our working and social life increases the opportunity for fraudsters to commit economic crime. The perpetrators can defraud people, companies, and governmental institutions in the Nordic countries without ever having to be physically present. Furthermore, technology has lowered the barrier for access to the means and knowledge necessary to commit fraud.

Photo generated with AI

Fraud in the Nordics leads to high economic and emotional cost

Fraud is a profit-making engine which finances other criminal activities. In that way fraud works as a driving force for other serious organised crime. Profits from fraud are reinvested in drugs and weapons, and analysis from Sweden demonstrate that there are links between fraud and lethal gun violence.[3]

Close to *260 000* online fraud schemes were reported to the police in the Nordic countries in 2023. The number of online fraud schemes is increasing year by year, as are the amounts of money the fraudsters profit from such activities.

3 Swedish Police - National Fraud Centre, "Lethal Fraud", 2022 - ref no A554.314/2022.

Fraudsters gained an estimated *828 million Euro* from the Nordic inhabitants in 2023.[4] This is a conservative estimate. The unreported cases are likely substantial, as many individuals and companies choose not to report fraud for various reasons.

The impact from fraud on a personal level are also massive. Each year, a substantial number of individuals and companies in the Nordics fall victim to fraud. Some of these victims lose their entire savings, and the guilt and shame they experience after realising they have been manipulated are often immensely painful, leading to isolation. There has also been reports in Denmark about victims committing suicide after they have been defrauded.

4 The numbers provided are estimates based on different methodology. Numbers for Norway and Denmark's is based on estimates from the financial sectors, while Sweden's estimate is based on reports to the police.

Photo: Shutterstock

Top five modus operandi within online fraud

Phishing is a pervasive threat that initiates frauds in the Nordic countries. Phishing campaigns, carried out through emails, SMS (smishing) and phone calls (vishing), often involve requests for money transfers and impersonation of well-known businesses or government entities.

The increased availability of phishing kits sold online allows more criminal networks to be successful in their phishing attacks, regardless of the level of organisation and technical expertise.[5]

Photo: Pngwing

5 Europol, "IOCTA, Europol spotlight – Online fraud schemes: A web of deceit", 2023:11.

Bank scam

Bank scams employ social manipulation to deceive victims into granting fraudsters access to their online bank accounts. The fraudsters often pose as IT-support, police or bank employees, claiming there is an issue with the victim's bank account. They use spoofing techniques – making the caller ID display a legitimate phone number from an organisation like the police or a bank – to convince the victim of their authenticity.[6,7]

Targets:

- Mainly elderly individuals

Severity:

- Large number of cases
- Large economic loss per victim
- High emotional cost for the victim

Threats:

- Nordic organised crime groups

Vulnerabilities:

- Information about victims available in public registers
- Telecom infrastructure

Implemented measures:

- Enhanced cooperation and information sharing among police, banks and telecom infrastructure providers
- Implementation of technical solutions to strengthen the telecom infrastructure and prevent spoofing

6 Europol, "IOCTA, Europol spotlight – Online fraud schemes: A web of deceit", 2023:7.

7 Europol, "Tech support scam infographic", 2021.

Investment fraud – Cryptocurrency

Fraudsters commonly target victims by placing ads on social media, gradually building a trusting relationship, and then persuading them to invest their savings in fraudulent cryptocurrency trading platforms. Criminal networks involved in investment fraud extensively utilise call centres as well. Additionally, dating apps are frequently employed to attract victims.[8]

Targets:

- Often male individuals

Severity:

- Large average economic loss per victim

Threats:

- International organised crime groups

Vulnerabilities:

- Peoples' desire for quick gain
- Easy to create fake websites and false advertisement
- Social media platforms with investment fraud ads

Implemented measures:

- Awareness campaigns

8 Europol, "IOCTA, Europol spotlight – Online fraud schemes: A web of deceit", 2023:8.

Business email compromise (BEC)

Business Email Compromise (BEC fraud) is a form of digital fraud targeting private companies through social engineering techniques. BEC include CEO fraud, where criminals impersonate a company executive to make urgent payment requests, and fake invoice fraud. In fake invoice fraud, fraudsters impersonate business partners and request payments for fictitious invoices, or they may alter legitimate invoices by changing the supplier's bank details. [9]

Targets:

- Companies and organizations

Severity:

- Large average economic loss per victim

Threats:

- Use of a real business from which the false invoices are sent

Vulnerabilities:

- Companies internal routines on internet safety, secure communication, and payments
- Easy access to spoofing and typosquatting tools[10]

Implemented measures:

- Campaigns describing the MO, with examples of good routines for payments, and focus on current trends

9 Europol, "IOCTA, Europol spotlight – Online fraud schemes: A web of deceit", 2023:9.

10 A fake website with almost the same URL as another real and serious website. The fraudsters do this, hoping the victims types the wrong URL and don't realise they landed on the fraudsters' website.

Romance fraud

In romance fraud criminals slowly build a relationship with the victim before they ask for money or bank account/ credit card details. Social media and dating apps are the main tools used to target potential victims.[11]

Targets:

- Middle-aged women, younger men in their 20's and vulnerable groups such as the elderly, the mentally disabled, or the socially isolated

Severity:

- Large average economic loss per victim

Threats:

- International organised crime groups

Vulnerabilities:

- Limited knowledge about the perpetrators
- Difficult to guide victims to prevent further financial losses
- Laws prevent banks from contacting third parties, like relatives of the victim
- Easy for fraudsters to create fake profiles

Implemented measures:

- Various forms of public-awareness campaigns both in national media, social media, documentaries and on police websites.

11 Europol, "What are the signs? Romance scam", 2023:8.

E-commerce fraud: Non-delivery fraud

E-commerce fraud occurs during online customer transactions, commonly in online shopping scenarios. A prevalent subcategory of e-commerce fraud is non-delivery fraud, where fraudsters advertise goods, receive payment, but fail to deliver the purchased items.[12]

Targets:

- Mainly private individuals

Severity:

- A large number of victims, but on average the economic loss is low
- Abuse of legitimate online marketplaces, booking websites and rental sites

Threats:

- The perpetrators are often men aged 20–30, acting independently, and many of whom are repeat offenders

Vulnerabilities:

- Easy to create fake profiles and advertisements
- Difficult to find out who is controlling the account selling an item

Implemented measures:

- Awareness campaigns

12 Europol, "IOCTA – Internet organised crime threat assessment", 2021:30.

Photo: iStock

The perpetrators

Perpetrators of bank scams and certain e-commerce frauds are often young men with Nordic citisenship. They operate across borders within the Nordic countries.

Some fraudsters have connections to criminal groups that are involved in serious drug related crime and violence. The tools and techniques employed are readily accessible and easy to use. This accessibility makes it easy to target a broad segment of the Nordic population.

The perpetrators of online fraud schemes are however often unknown to the Nordic police. The funds are frequently and rapidly transferred abroad through multiple deceptive steps. Given the significant time and resources required to trace these transactions further, authorities often decide not to investigate or pursue the foreign perpetrators.

Implemented preventive measures

The Nordic countries have adopted different preventive measures to fight online fraud schemes. The purpose of this chapter is to share the knowledge and results of these measures.

Enhanced defensive mechanisms to increase customer payment security

Banks and other financial services have increased their defensive mechanisms to increase customer security. In Iceland some banks have made changes related to Google Pay and the functionality of foreign wire payments. The change meant that customers who are abroad cannot manually activate a new Google Pay account on their phones. This type of country blocking helps protect the bank's customers by preventing hackers from accessing their cards and attempting to install Google Pay on another phone outside of Iceland.

Another change made was related to customers' use of foreign telephone payments. Access to phone payments in internet banking was blocked for individuals who had not used them in the last six months. Those individuals needed to contact their bank and have the access re-opened if they intended to use foreign transfers or telephone payments. The goal is to prevent hackers from executing Swift payments and draining the accounts of victims if they gain access to online banking.

Public-Private Partnerships

In all the Nordic countries there is ongoing collaboration between the police, the financial sector and/or the telecom industry.

The public-private partnership between the police and the major banks focuses on combatting money laundering and fraud through strategic planning and

operational working groups. They discuss solutions to identified vulnerabilities, risks and threats.

In Denmark more than 90 public and private organisations work together with the police to combat IT-related economic crime. They also have success with smaller forums, where selected members from the authorities and banks with a certain level of security clearance, can share information.

Spoofing filters in the telecom infrastructure

Finland has had great success implementing technical filters in their telecom infrastructure, making it more difficult for fraudsters to carry out vishing[13] attacks. The telecom operators were also able to find a technical solution to stop spoofed calls from abroad. In order to implement it, operators needed legislative changes.[14]

Norway is currently in the process of implementing technical preventative measures in the telecom infrastructure, however it is too early to evaluate the effect. Similar actions to prevent spoofing in Denmark are also ongoing.

Public information campaigns with varying results

All the Nordic countries have conducted different information and awareness campaigns to enlighten the public about fraud. The results from these are varying. In investment fraud the victim often initiates the fraud themselves, with intent to invest money for profits. Preventive campaigns conducted seems to have had little effect on this MO.

13 Fraudsters call victims to obtain sensitive information, usually by portraying to be someone else.

14 Finish Transport and Communications Agency (TRAFICOM), "Obligations of the Regulation come into effect – up to 200,000 scam calls are prevented per day", Read May 14th 2024.

Decrease in CEO-fraud after awareness campaign in Denmark

In the summer of 2023, the Danish National Center for Economic Cybercrime (NCIK) prevention unit launched a collaboration with national organisations and published various forms of guidance material, such as posters with important advice on CEO-fraud prevention. In the aftermath of this, there was a decline in reports of CEO-fraud. Iceland has also experienced a decrease in CEO-fraud following an awareness campaign on the MO.

Low effect in the Swedish Postcard Initiative

In Sweden, postcards were sent to people over 70 years old (1,2 million people). The primary goal of the Postcard Initiative was to increase awareness about the risks of telephone fraud and to offer pragmatic advice on how to avoid becoming a victim. It was

Photo: Unsplash

supplemented with advertising aimed at the target group (aged 70+) and their relatives. The effect was very low.

Measuring the effectiveness of preventive campaigns can be challenging. The success of such initiatives often depends on precisely targeting specific groups and involving relevant stakeholders. Additionally, communication should provide clear advice on actions recipients should or should not take. However, even with these strategies, it's difficult to attribute a decrease in crime rates solely to the campaign.[15]

15 Niklas Jakobsson & Manne Gerell (2023) "Evaluating the impact of an informational postcard campaign on telephone scams targeting the elderly", Nordic Journal of Criminology, Volume 25, no.1-2024, pp.1-6.

Enhance the public sectors' control of information

Other public sector agencies could significantly increase their efforts to prevent fraud, though they may lack the necessary knowledge to determine precisely where to focus these efforts. In April this year, the Swedish Companies Registration Office (Bolagsverket) became obligated to verify the accuracy of the information in its register. This measure aims to prevent the registration of incorrect information and reduce the risk of companies being exploited in criminal schemes.

Increase the public's internet-skills

Aalto-university in Helsinki is currently working with the Government to launch the "Cyber-citizen-project". The aim is to educate people on navigating safely on the internet and social media platforms. A similar campaign exists in Sweden "Tänk säkert" is a collaboration between Swedish Civil Contingencies (MSB), Swedish Police and the Internet Foundation that aims to increase awareness regarding cyber security issues and how to avoid being scammed online.

Photo: Unsplash

Vulnerabilities

A major vulnerability in online fraud schemes is that humans are susceptible to social manipulation. People's desires to be rich, accepted and loved make them prime targets for fraudsters. Technical tools like spoofing and artificial intelligence enable fraudsters to impersonate well-known institutions or individuals, facilitating easier manipulation.

Law enforcement need to automate and respond quickly

The capacity to act swiftly, prevent and investigate online fraud in the Nordic countries is currently limited. The police need to automate processes to respond quickly and work efficiently. This need is expected to be even more urgent due to current technological trends, such as the development of artificial intelligence, which is likely to exponentially increase the volume, sophistication, and complexity of online fraud.

Trust rather than control – public registers and welfare systems

The Nordic countries' welfare system, social insurance and benefits, taxes, and population registration is highly dependent on a trust-based system. Only a small part of the information people and businesses provide to the public sector is controlled and verified, and it is therefore vulnerable to manipulation.

A significant amount of information about citisens and businesses is publicly available and frequently updated in real time. Perpetrators often use this data to verify names, ages, incomes, and residential addresses or

16 Denmark is currently working with the financial sector on this matter.

Photo: Pixabay

areas. In an increasingly digitalised and automated world, this accessibility leaves the Nordics more exposed to exploitation, for example, enhancing the ability to use spoofing techniques and send bulk SMS messages.

The financial system is exploited

Money is siphoned from the legal economy by exploiting vulnerabilities in the financial system, such as instant payments, the possession of multiple bank accounts, opening bank accounts with

someone else's ID, utilising money mules, and gaining control over remote Banking IDs.

Some banks are developing algorithms designed to detect misuse of accounts by flagging suspicious activities or triggering alarms. In such cases, a bank employee is required to contact the customer to potentially halt unauthorised transactions or freeze the account. Providing banks with more detailed information about the methods of operation is crucial for these systems to effectively reduce risk.

Legal business structure is exploited

In many fraud MOs, the fraudsters use legal businesses to commit the fraud itself, to get credibility which enables fraud, or for the money laundering of the proceeds. In the Nordics, establishing and registering a business, whether as a sole proprietorship or a limited liability company, can be accomplished relatively easily and quickly. When registering a new business, the information provided is usually controlled, but if the company undergoes crucial changes fitted to crime, these changes rarely are monitored and discovered. Based on data from committed frauds, there are indicators that could be used to automate monitoring and serve as early warnings to prevent the exploitations of legal business structures.

Information sharing

The challenge of preventing fraud is exacerbated by the lack of information sharing or obstacles to it. This issue affects the exchange of information between governmental agencies, across the public and the private sectors, and within the private sector itself, both domestically and internationally. Legal boundaries often restrict the ability to share detailed data and personal information related to suspected illegal activities.

The banking sector, in particular, faces legal hurdles that make it difficult to share information, especially in real time. This makes it hard to detect and to stop ongoing fraud. For instance, vulnerable groups such as the elderly and individuals with intellectual disabilities are often targeted by fraudsters. However, banks are legally restricted from contacting third parties about these violations due to existing laws and regulations.[16]

Photo generated with AI

Recommendations

Better analytic tools and automated take-downs

It is a race to keep up with the fraudster's creative methods and shifting modus operandi. The Nordic police are falling behind technologically and do not utilize the information that we receive for analytical purpose. To keep pace, the police need to significantly increase automation across various processes, including information intake, analysis and on knowledge sharing with external parties. This should also extend to cross-border operations, especially within the Nordic countries. Given that many fraudsters operate across borders, police efforts must be similarly expansive.

Legislative changes to improve information sharing

However, in some instances, there is a need for regulatory change on information sharing before automation is possible. There is especially a need for changes in legislation in regards to sharing data and personal information between banks, the telecom sector and the police in cases of suspected illegal activity. Many of the laws are written for an analogue age, but the world, and especially the Nordic region, is highly digitalised.

Better automated monitoring at online banking services

Banks are already stopping a lot of attempted fraud, and their ability to monitor fraud is improving fast. Despite this, a lot of fraudulent transactions do not seem to be flagged by their automated monitoring system. The police and the society as a whole are dependent on the financial institutions priority and ability to constantly develop useful indicators to detect fraud and money laundering. Therefore, it should be established real-time information sharing on trending MOs and perpetrators, both between banks, and between banks and the police.

Increased pressure on tech giants

Tech giants profit from advertisements that promote fraud. A more effective approach to preventing ads for fake investments on social media could involve pressuring tech giants or amending legislation to make them more responsible for the content and ads on their platforms. This would require them to screen ads before publication, rather than removing them later.

Photo: Unsplash

For digital report

ØKOKRIM

Postal address: P.O. Box 2096 Vika, NO-0125 Oslo
Street address: C.J. Hambros plass 2 C, NO-0164 Oslo
Contact: +47 23 29 10 00 / post.okokrim@politiet.no

www.okokrim.no