2025

FRAUD AND THREATS

ARION ESCAPE

Summary

In recent years, there has been a significant increase in online fraud, and it has now become one of the most visible security challenges faced by Icelandic consumers. It is safe to assume that the majority of adults in Iceland have at some point encountered attempted online fraud, whether in the form of e-mails, text messages, phone calls, or other methods, which underscores how common and sophisticated this criminal activity has become. A report produced by the Central Bank of Iceland on the scope of fraud in payment services indicates that total fraud in 2024 amounted to around ISK 1 billion, representing a considerable increase from previous years.

Despite this rapid and worrying development, Arion Bank has achieved strong results in the fight against online fraud and has significantly reduced customer losses. Since 2023, losses due to online fraud have decreased year by year, and exceptional results were achieved in 2025 when 98% of all attempted breaches of the online bank and the Bank's app were prevented. This success is based on a combination of proactive fraud analysis, robust education efforts, and targeted responses by the Bank's employees.

Online fraud is becoming increasingly complex, personalized, and fast in execution. Scammers use various communication channels (such as text messages, e-mail, phone calls, and social media) and have adapted their methods to user behaviour and the opportunities created in the digital environment. This calls for continuous review of defences and warning systems, as well as education and customer awareness regarding signs of online fraud and the ability to respond appropriately.

Between 2023 and 2025, there was a clear increase in incidents where threatening or inappropriate behaviour by customers caused disruption or insecurity at branch locations, and several serious cases required the assistance of security services or the police. Although such cases remain relatively few compared to the overall scale of operations, any increase affects the sense of safety experienced by employees and customers and calls for continued follow-up and strengthening of procedures.

In 2024–2025, the number of cases related to insurance fraud also increased. This reflects a changing risk landscape and a rise in attempts to stage or fabricate losses. In response, procedures regarding the registration of such cases were strengthened, improving oversight, enhancing preventive measures, and increasing the security of the operating environment for customers.

Introduction

Online fraud has become one of the most widespread forms of criminal activity in the world. It began to take hold in Iceland a few years ago and has increased significantly. It is important to stay alert to the different types of fraud and to understand how to protect oneself against them.

The purpose of this report is to promote greater transparency, education, and shared awareness of the development of fraud and threats. One of Arion Bank's core values is to say what we mean, and through this report the Bank is providing customers, partners, and society with a clear picture of the challenges faced by the Bank and the financial system as a whole. Arion Bank aims to publish a fraud and threat report on an annual basis so that it is possible to monitor trends in fraud and threats as well as the Bank's success in defending against them.

This report is intended to provide an insight into trends in online fraud and cyber threats in recent years, particularly in 2025. The report covers changes in scammer behaviour in 2025, developments in 2024 and 2025, threatening behaviour and vandalism, trends in insurance fraud in 2024 and 2025, and an assessment of cyber threats for 2026.

It is clear that anyone can fall victim to online fraud, and therefore the ability to respond correctly and quickly is crucial. With this report, Arion Bank hopes to strengthen customer awareness so that they can recognise the warning signs of online fraud and stop fraud attempts themselves.

Changed behaviour of scammers in 2025

Cyber threats have been on the increase in Iceland in recent years. Arion Bank has participated in strong and targeted collaboration through NFCERT and CERT IS, which has contributed to deeper knowledge and greater understanding of the threats facing Iceland.

In 2025, there was a clear shift in the methods used by scammers. Previously, account takeover fraud was the most common technique, where a cybercriminal gains access to a customer's account and makes payments in their name. In 2025, however, fraud increasingly shifted to scams, in which the customer themselves performs the action. This can include confirming payments, approving a card connection, or providing card details under the belief that the request is legitimate.

Phishing campaigns also became more convincing during the year. Artificial intelligence was used to produce persuasive Icelandic texts across communication channels, and fraudulent websites imitated real ones even more closely. Fraud campaigns carried out in the name of the Icelandic Tax Authority, Iceland Post, and financial institutions were particularly prominent, using the appearance and logos of these organizations to increase credibility. Messages often convey a sense of urgency requiring quick action, for example, tax refunds, package redelivery, or account closures.

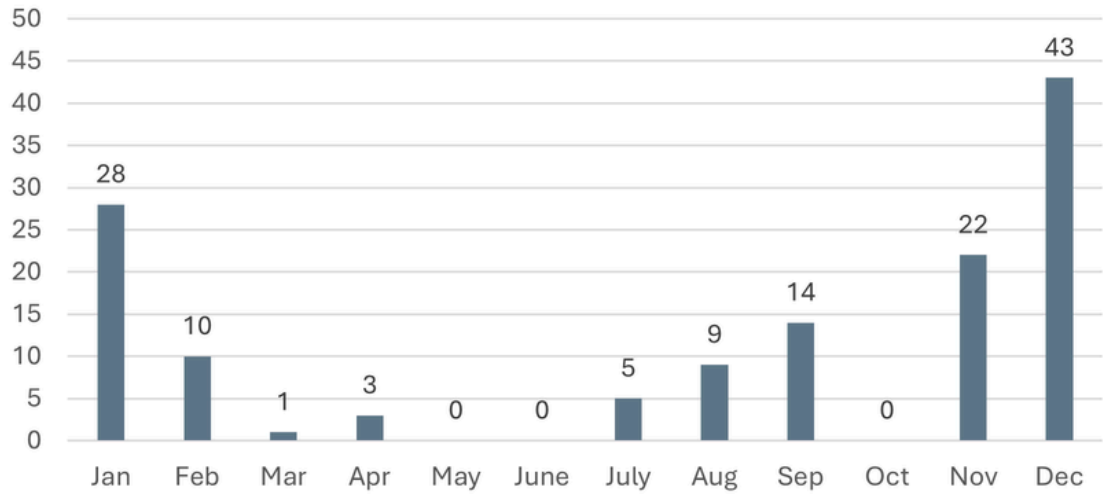
Table 1. Examples of phishing campaigns

Fake websites	Imitates	Fraud messages via text or email
hxxp://arion-is.com	Arion banka	Aðgangurinn þinn að Arion Banki rennur út...
hxxp://rsk-island.web.app	RSK	Til að halda áfram að nota þjónustu island.is...
hxxp://vat-islanksi.web.app	RSK	Endurgreiðsla vegna endurgreiðslu opinberra
hxxp://skaturinn.web.app	RSK	Stjórnsýsluleg tilkynning...
hxxp://postu-info.top/is	Pósturinn	Við reyndum að afhenda pakkann þinn...
hxxp://minnreikningur-is.web.app	RSK	Innheimtumálastofnun Ríkissjóðs Íslands...
hxxps://saktturinn.web.app	RSK	Skattaendurgreiðsla þin fyrir árið 2025....
hxxp://veituuur.web.app	Veitur	Rafmagnsreikningur þinn hefur ekki verið greiddur...

Response to phishing campaigns

It is important to respond quickly when new phishing campaigns emerge, as doing so can significantly limit customer losses. Financial institutions cooperate by reporting fraudulent websites to NFCERT, CERT IS, and other cybersecurity companies that can place warning notices while the fraudulent site is being taken down. Arion Bank also plays its part, and in 2025 the Bank achieved strong results in such takedowns. See Table 2 for the number of phishing campaigns reported by Arion Bank.

Table 2. Reported phishing campaigns in 2025



Trend 2024-2025

In 2024 and 2025, there was a significant increase in reported online fraud. Reports to Arion Bank nearly doubled year over year, reflecting both a rise in the number of incidents and increased public and corporate awareness of the importance of reporting suspicious activity. Despite this sharp rise in reported cases, total customer losses decreased during the same period, indicating that preventative measures, education, and response capabilities have delivered tangible results.

In 2024, cryptocurrency investment fraud was the largest category of reported losses. These cases were prominent and often resulted in substantial financial harm, as scammers used deception to persuade individuals to open cryptocurrency wallets or invest in fake projects. In 2025, a notable shift occurred: losses were distributed across a wider range of fraud types, and other forms of fraud became more prominent in the Bank's data.

The main categories of loss cases in 2025 were:

- Physical proximity credential theft became the largest loss category. In such cases, a scammer obtains access to the victim's device or authentication credentials and can therefore execute and authenticate transactions using the victim's own equipment. These incidents often occur in nightlife venues or situations where the scammer observes the victim's authentication method (PIN, electronic ID) before taking their device.
- Goods-not-received fraud increased alongside the growth of online shopping, especially around major shopping days. Fraudsters use fake offers to obtain card information or delay delivery until the refund window expires.
- Fake invoices and phishing, where e-mails or messages are sent in the name of public authorities or trusted organizations to trick people into making payments or disclosing sensitive information.

In 2025, losses from account takeover fraud decreased significantly. This shows that defences against such incidents have been highly effective, and only a small number of scammers have managed to exploit customer access without their knowledge.

At the same time, the trend shows that scams, social engineering, and misuse of actions performed by the customer themselves have become more extensive and complex. This is reflected, for example, in the increase in physical proximity credential theft, the rise in cases where cards are connected to digital wallets, and more incidents where individuals themselves confirm transactions that scammers profit from.

The trend between 2024 and 2025 therefore shows two main characteristics:

- Fraud is increasing, and the methods are becoming more diverse and more personal.
- The Bank's defences reduce customer losses, despite the increased activity of scammers.

This underscores the importance of distinguishing between fraud where the scammer performs the action themselves, and scams where the customer becomes an active participant in carrying out the unlawful transaction.

Table 3. Number of online fraud cases by fraud type

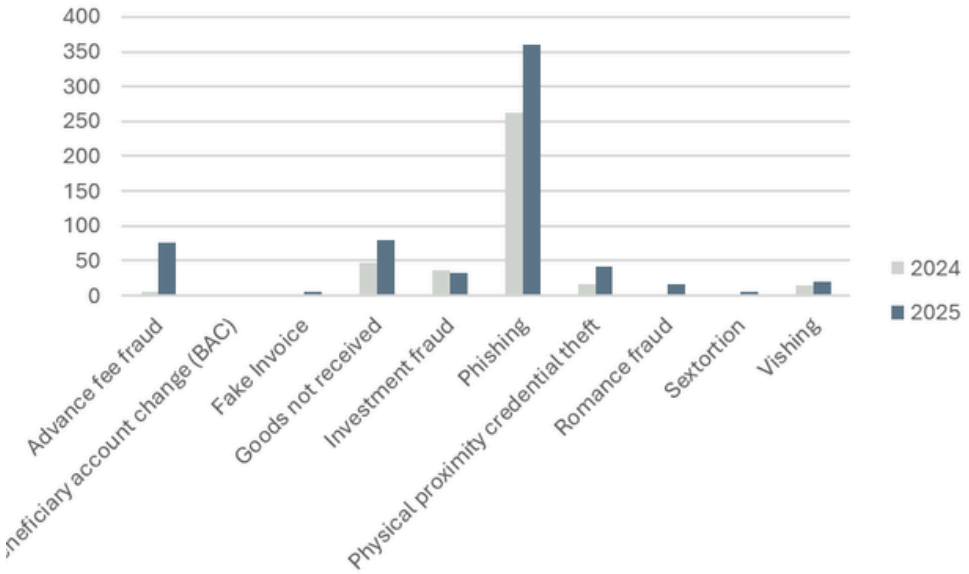
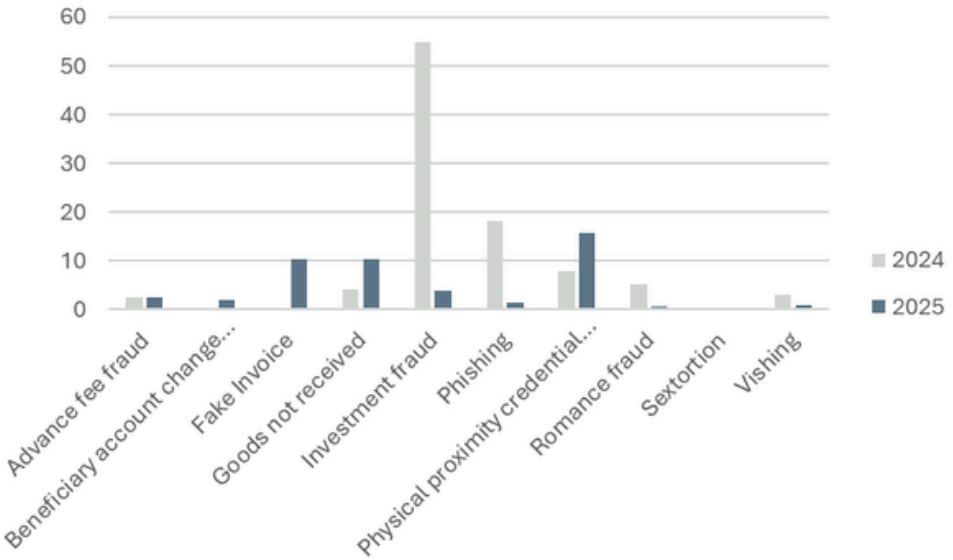


Table 3 shows that the categories phishing and goods not received are the most common types of fraud, and they also increase year over year. At the same time, there has been a rise in cases related to physical proximity credential theft, as well as the appearance of new categories such as romance fraud and sextortion. Sextortion, i.e. threats to share sensitive images, is increasing in frequency among young people.

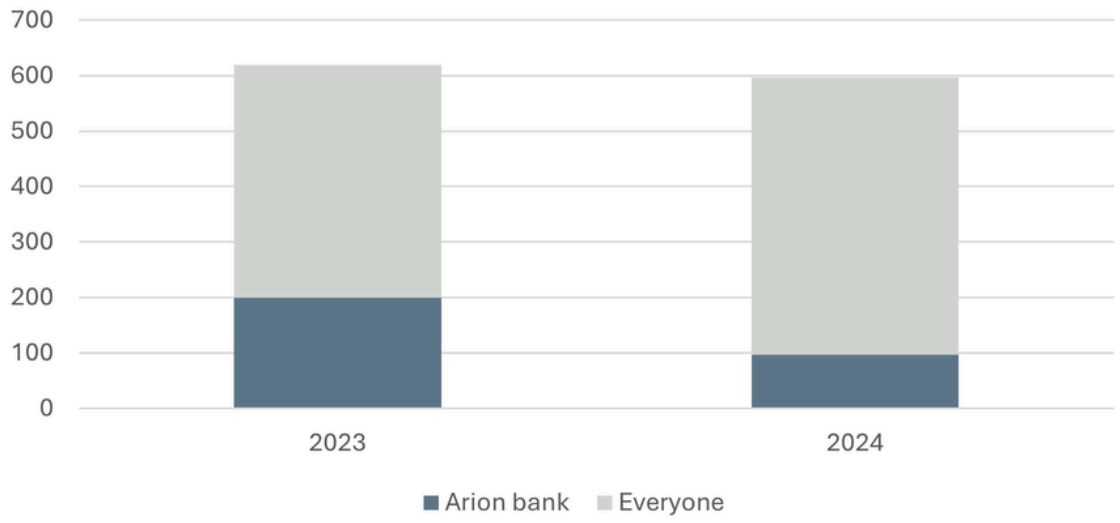
Table 4. Total losses by type of fraud in ISK millions



In 2024, customer losses due to cryptocurrency investment fraud were very high, but they decreased significantly in 2025. In 2025, however, physical proximity credential theft caused the greatest losses, reflecting an increase in cases where phones and authentication devices are taken or misused.

Losses due to goods-not-received fraud and phishing were also prominent during the period. It is worth noting that the total loss amount from phishing has decreased significantly even though the number of cases has increased.
When comparing official figures from the Central Bank of Iceland on fraud in payment services, it is clear that Arion Bank's performance is notable: between 2023 and 2024, customer losses due to online fraud were reduced by half. Figures for 2025 have not yet been published.

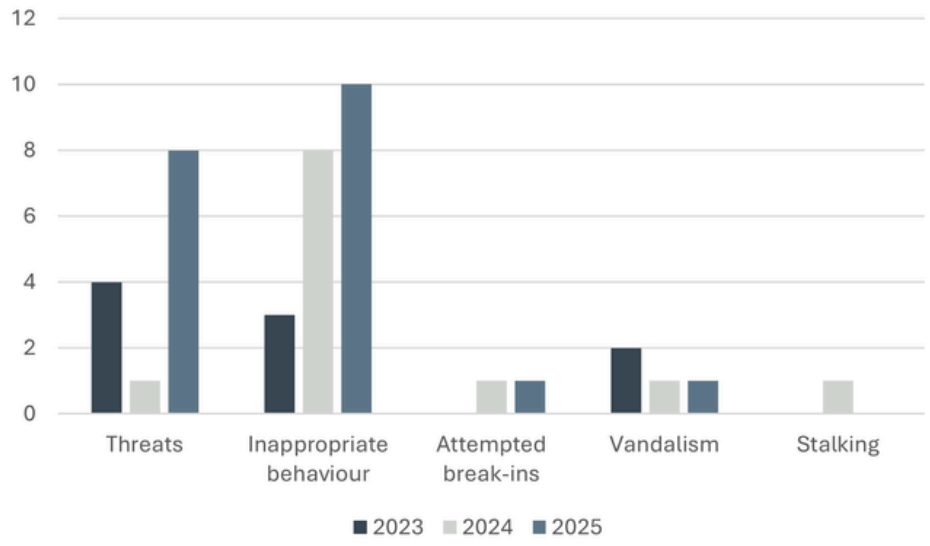
Table 5. Development of total losses in payment services in Iceland compared with total losses of Arion Bank customers



Threatening behaviour and vandalism

There has been a considerable increase in incidents involving inappropriate behaviour by customers between 2023 and 2025, where such behaviour has created insecurity or disruption at the Bank's places of work.

Table 6. Number of security incidents by type



There is a clear increase in threats and inappropriate behaviour toward employees, as shown in Table 6. This development calls for continued follow-up, targeted training, and strengthened security procedures so that employees have clear guidance and the right tools to respond when customer behaviour or circumstances are unusual, threatening, or disruptive. Attempted break-ins and vandalism remain relatively rare, but such incidents can be serious and cause disruption to daily operations.

Threatening and inappropriate behaviour can appear in many forms, and situations can escalate quickly. Examples include:

- **Customer refuses to leave a branch:** A customer displays unstable and threatening behaviour and refuses to leave the premises. In such cases, security personnel have had to be called to escort the individual out.
- **Inappropriate conduct:** A customer behaves inappropriately, eventually accusing employees of theft and threatening to send other people into the branch to "teach the employees a lesson."
- **Attempt to withdraw funds from another customer's account:** An individual who is unable to complete a transaction from someone else's account becomes agitated, confronts a staff member, and refuses to leave the branch. Police intervention was required to escort the individual out.
- **Threats and harassment:** An individual loses control, hits doors or furniture, or harasses staff, for example, by invading their personal space or displaying other threatening behaviour.
- **Stalking:** An individual repeatedly visits a branch and directs inappropriate attention toward a particular staff member, without making direct threats, but in a way that causes staff to feel unsafe. The case was classed as stalking.

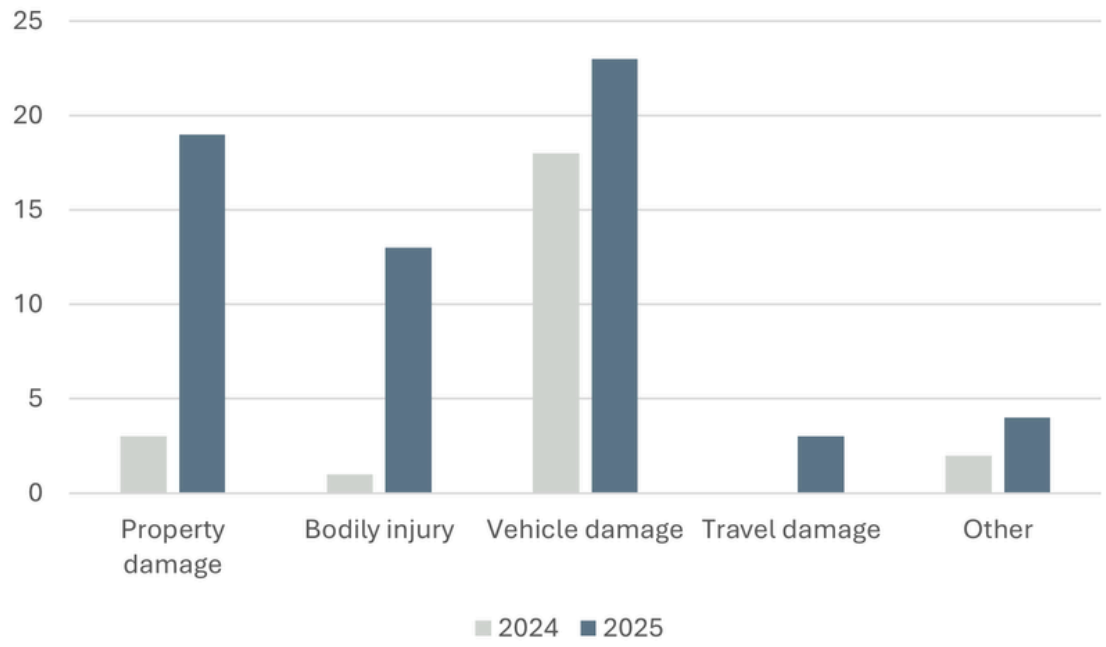
Developments in insurance fraud in 2024–2025

In recent periods, there has been a significant increase in cases related to insurance fraud, both in terms of the number of incidents and their scale. This development reflects a shifting risk landscape in the insurance market and the fact that fraud attempts have generally become both more complex and more extensive.

In light of these developments, where both the number and scale of insurance related fraud cases have increased, Vörður has taken appropriate actions in accordance with applicable laws and conditions. These actions have contributed to a clearer oversight of suspicious cases and more targeted procedures when fraud is suspected. At the same time, efforts have been made to strengthen the processes and documentation of such cases, increasing transparency, reinforcing preventive measures, and providing a better overall picture of online fraud trends in the insurance market.

Through these measures, Vörður seeks to reduce the risks associated with insurance fraud and promote a secure operating environment for all customers.

Table 7. Number of insurance fraud cases by type



There was a considerable increase in the number of recorded insurance fraud cases year over year, which underscores the need for vigilance as well as strong processes to ensure that anomalies can be identified without delay. When it comes to insurance fraud, traditional schemes most often involve claims for losses without any actual incident, or cases where events are staged.

In 2025, there was an increase in cases where document forgery was suspected, indicating that scammers' methods are constantly changing and becoming more diverse. In 2025, vehicle damage claims continued to be the most common fraud category, although there was also an increase in cases relating to personal injury and property damage, suggesting that risk is now spreading across more insurance types than before. In 2024, most cases were relatively simple and small in scope, but in 2025 the cases became more numerous, larger, and more complex. These cases involve, among other things, suspected arson, staged accidents and break-ins, and fraudulent travel insurance claims, all of which require detailed investigation and thorough analysis.

There was an increase year over year in the number of cases that had to be referred to the police, reflecting the growing seriousness of insurance fraud and underscoring the importance of active cooperation with authorities when criminal behaviour is suspected. In this context, the shared claims database of insurance companies is a key tool in Vörður's fraud monitoring, as it supports the detection of unusual claim patterns, such as duplicate claims for the same loss submitted to multiple companies. The database strengthens the quality of claims investigations, reduces incorrect payouts, and enhances a coordinated and targeted approach among insurance companies in the fight against insurance fraud, while fully respecting data protection rules and customer rights.

Action taken by the Bank in 2025

In 2025, Arion Bank implemented extensive measures to protect customers from online fraud. Strong emphasis was placed on proactive actions, targeted intelligence gathering, and rapid response, which led to numerous incidents being stopped before any loss occurred.

Arion Bank staff contacted customers in over 5,200 phone calls, reaching around 4,000 individuals due to suspected fraud. In most cases, misuse of payment instruments was prevented thanks to timely intervention and focused communication with the customer. This approach, promptly alerting people to unusual activity or warning signs, proved to be one of the Bank's most effective defences against fraud during the year.

Arion Bank also placed a strong emphasis on education and raising awareness. In collaboration with filmmaker Sigursteinn Másson, the campaign "Sönn svikamál" ("True Icelandic Fraud Cases") was presented in an accessible and impactful format. The campaign reviewed real cases that clearly demonstrated how quickly fraud can unfold and how individuals, regardless of age or experience, can become involved in fraud schemes without realizing it. The results showed that shame and insecurity remain major barriers preventing people from reporting fraud. The campaign highlighted that anyone can fall victim to fraud, and that the key is to respond correctly and quickly.

After the educational campaign, the Bank set up an escape room with an online fraud theme, where participants had to put themselves in the shoes of a scammer. The goal was to deepen understanding of how fraud groups operate by letting people experience firsthand how deceptive schemes are constructed and which vulnerabilities are exploited. Participants were given the opportunity to identify warning signs, learn to think critically, and respond quickly in situations resembling real world fraud.

One participant noted that the experience helped him prevent a family member from falling victim to online fraud shortly afterward, underscoring the practical value of the educational project.

Arion Bank's actions during the year therefore reflect two main objectives: to respond quickly to stop fraud before losses occur; and to strengthen customer awareness and knowledge so that they can identify and halt fraud attempts themselves.

Taken together, these measures produced significant results and reduced losses despite the increase in fraud attempts during the year.

Assessment of cyber threats for 2026

The outlook for 2026 indicates that online fraud will continue to evolve rapidly and become increasingly complex. Phishing is expected to remain one of the primary methods used by scammers to reach people, as it has proven both effective and easy to carry out. This type of fraud relies on capturing the recipient's attention through e-mails, text messages, social media, or phone calls, and scammers use a variety of deceptive tactics to persuade individuals to click on links, provide information, or approve payments. With increased use of artificial intelligence, such messages are likely to become even more convincing and personalized, making them harder to distinguish from legitimate communication.

Physical proximity credential theft, cases involving stolen phones and payment cards, is also likely to continue increasing. Technological developments in fintech, where payment solutions are increasingly integrated into smartphones, mean that individuals now carry payment capabilities that were once limited to physical point of sale terminals or online checkout systems. Furthermore, there are growing indications that acquaintances or individuals connected to the victim may exploit these circumstances.

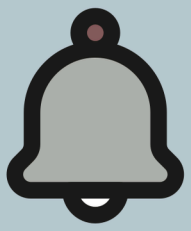
There are also clear indications that foreign fraud groups with links to Eastern Europe are operating systematically in Iceland. They are believed to be part of a larger international network in which groups are moved between countries to expand fraud operations and identify new opportunities to commit fraud, theft, and related crimes. Although the groups known in the Nordic region have not been as visible in Iceland, data and intelligence suggest that comparable activity is taking place here, and that these groups are both coordinated and specialized in different types of offences. In such circumstances, it is only a matter of time before domestic fraud groups begin to form or surface. When external actors operate systematically within a country, knowledge, connections, and methods are developed that can transfer into local criminal activity. This means that domestic trends may follow patterns already seen abroad.

It is expected that 2026 will be characterized by a continued increase in scams and phishing, a further rise in cases where payments are made through mobile-based digital solutions, and the growth of organized fraud groups with links both inside and outside the country.

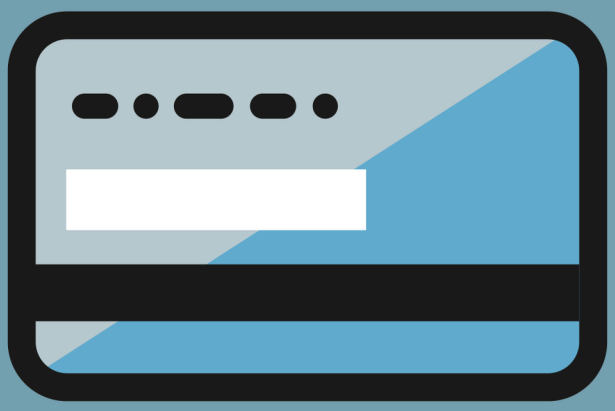
The cyber threats facing Iceland are, for the most part, similar to those faced by other Nordic nations. The threat alert level remains monitored and stable, but organized crime groups continue to present a persistent risk. At the same time, recent analyses indicate an increase in hostile cyber activity targeting Iceland, underscoring the importance of continued vigilance. The main threats facing Iceland can be divided into several categories: organized criminal activity, vulnerabilities related to supply chains and service providers, cyberattacks such as distributed denial of service (DDoS) attacks aimed at disrupting services, internal risks within companies, threats linked to foreign states, and the use of artificial intelligence to make deception and phishing more convincing. Available data and intelligence also suggest that advanced threat actors, operating both in cybercrime and cyber espionage, have increased their activity and are using methods associated with Advanced Persistent Threats. Such activity often bears the hallmarks of state sponsored operations rather than traditional cybercrime groups and aims to infiltrate company systems in a targeted and prolonged manner. It is important to take these indications seriously and assess risks accordingly, as such threat actors possess powerful tools, advanced techniques, and substantial resources.

Arion Bank has maintained strong cooperation with NFCERT and CERT IS, and this collaboration, along with targeted information sharing, has contributed to improved awareness and a deeper understanding of the situation Iceland is facing.

In 2026, Arion Bank will continue this work vigorously, aiming to be a leader in fraud- and threat-related issues and to ensure the security of its customers. Cyber threats are not expected to subside, and therefore effective monitoring is required. This calls for the continued review of defensive measures, increased education, and strengthened response systems in order to meet developments both in Iceland and abroad.



2025



ARION
E$CAPE