2025

SVIK OG ÓGNIR

AR!ON
E$CAPE

Samantekt

Á undanförnum árum hafa netsvik aukist verulega og eru í dag orðin ein af sýnilegri öryggisáskorunum íslenskra neytenda. Telja má að meirihluti fullorðinna Íslendinga hafi orðið var við tilraunir til netsvika, hvort það er í formi tölvupósts, smáskilaboða, símhringinga eða annarra leiða, sem undirstrikar hve algeng og markviss slík brotastarfsemi er orðin. Samkvæmt skýrslu Seðlabanka Íslands um umfang svika í greiðsluþjónustu námu heildarsvik á árinu 2024 um einum milljarði króna, sem er talsverð aukning frá fyrri árum.

Þrátt fyrir þessa hröðu og uggvænlegu þróun hefur Arion banki náð góðum árangri í baráttunni gegn netsvikum og dregið verulega úr tjóni viðskiptavina. Frá árinu 2023 hefur tjón vegna netsvika lækkað með hverju ári, og náðist einstakur árangur árið 2025 þegar 98% allra tilrauna til innbrota í netbanka og í smáforrit bankans (e. app) voru stöðvaðar. Þessi árangur byggist á samspili forvirkra svikagreininga, öflugrar fræðslu og markvissra viðbragða starfsfólks bankans.

Þróunin sýnir að netsvik eru sífellt að verða flóknari, persónulegri og hraðari í framkvæmd. Svikarar nýta margvíslegar boðleiðir (t.a.m. smáskilaboð, tölvupóst, símtöl og samfélagsmiðla) og hafa aðlagað aðferðir sínar að hegðun notenda og þeim tækifærum sem skapast í stafrænu umhverfi. Þetta kallar á stöðuga endurskoðun varna og viðvörunarkerfa, fræðslu og þekkingu viðskiptavina þegar kemur að viðvörunarmerkjum netsvika og getu til að bregðast við á réttan hátt.

Á árunum 2023–2025 varð greinileg fjölgun atvika þar sem ógnandi eða óviðeigandi hegðun viðskiptavina skapaði truflun eða óöryggi á starfsstöðvum og kröfðust nokkur alvarleg tilvik aðstoðar öryggisþjónustu eða lögreglu. Þó fyrrgreind mál séu tiltölulega fá miðað við heildarumfang starfseminnar, hefur aukning þeirra áhrif á öryggisupplifun starfsfólks og viðskiptavina og kallar á áframhaldandi eftirfylgni og styrkingu verklags.

Á árunum 2024-2025 jókst auk þess fjöldi mála sem snúa að tryggingasvikum. Það endurspeglar breytt áhættulandslag og aukinn fjölda tilrauna til að sviðsetja tjón. Í framhaldinu var verklag í kringum skráningar slíkra mála styrkt sem hefur bætt yfirsýn, eflt forvarnir og aukið öryggi rekstrarumhverfisins fyrir viðskiptavini.

Inngangur

Netsvik eru orðin ein umfangsmesta glæpastarfsemi í heimi. Þau hófust fyrir alvöru á Íslandi fyrir nokkrum árum og hafa aukist umtalsvert. Mikilvægt er að vera á varðbergi gagnvart ólíkum svikaleiðum og þekkja hvernig megi varast þær.

Tilgangur með skýrslu þessari er að stuðla að auknu gagnsæi, fræðslu og sameiginlegri vitund um þróun svika og ógna. Eitt af gildum Arion banka er að koma hreint fram og með skýrslu þessari veitir bankinn viðskiptavinum, samstarfsaðilum og samfélaginu skýra mynd af þeim áskorunum sem bankinn og fjármálakerfið sem heild stendur frammi fyrir. Markmið Arion banka er að gefa út svika- og ógnaskýrslu árlega til þess að hægt sé að fylgjast með þróun svika og ógna sem og árangri bankans í vörnum gegn slíku.

Skýrslunni er ætlað að vera innsýn inn í þróun netsvika og netógna á undanförnum árum, þá sérstaklega árið 2025. Í skýrslu þessari verður meðal annars farið yfir breytta hegðun svikara árið 2025, þá þróun sem hefur átt sér stað á árunum 2024 og 2025, ógnandi hegðun og skemmdarverk, þróun tryggingasvika á árunum 2024 og 2025 sem og mat á netógnum fyrir árið 2026.

Ljóst er að allir geta lent í netsvikum og er því lykilatriði að geta brugðist rétt og hratt við. Með skýrslunni vonast Arion banki til að efla þekkingu viðskiptavina svo þeir geti sjálfir þekkt hættumerki netsvika og geti stöðvað tilraunir til netsvika.

Breytt hegðun svikara árið 2025

Netógnir hafa almennt aukist á Íslandi undanfarin ár. Arion banki hefur tekið þátt í öflugu og markvissu samstarfi í gegnum NFCERT og CERT-IS sem hefur stuðlað að dýpri þekkingu og auknum skilning á þeim ógnum sem Ísland stendur frammi fyrir.

Á árinu 2025 urðu skýr umskipti í aðferðum svikara. Áður fyrr voru yfirtökusvik (e. account takeover) algengust, þar sem óprúttinn aðili fær aðgang að reikningi viðskiptavinar og framkvæmir greiðslur í hans nafni. Árið 2025 færðust hins vegar svikin yfir í svokallaðar blekkingar (e. scam) þar sem viðskiptavinurinn sjálfur framkvæmir aðgerðina. Þetta felur til dæmis í sér að staðfesta greiðslu, samþykkja kortatengingu eða gefa upp kortaupplýsingar í þeirri trú að um lögmæta beiðni sé að ræða.

Vefveiðiherferðir á árinu urðu einnig meira sannfærandi. Gervigreind var nýtt til að búa til sannfærandi íslenska texta í boðleiðum auk þess sem svikasíður líkja enn betur eftir raunverulegum síðum. Svikaherferðir í nafni Skattsins, Póstsins og fjármálafyrirtækja voru áberandi þar sem útlit og merki fyrirtækjanna voru notuð til að auka trúverðugleika, ásamt því að skilaboð báru með sér þörf á að bregðast fljótt við. Sem dæmi má nefna skattendurgreiðslu, endursendingu pakka eða lokun reikninga. Svikarar nýta sér fjölbreyttar boðleiðir, t.a.m. smáskilaboð, fölsk SMS-skilaboð, tölvupósta, samfélagsmiðla og símhringingar. Þeir hanna samskipti sem kalla fram skjót viðbrögð, byggð á trúverðugleika, ótta eða tilfinningalegum þrýstingi. Þegar viðskiptavinurinn sjálfur framkvæmir aðgerðina er mun erfiðara að greina og stöðva slíkar færslur, enda eru þær sannvottaðar af eiganda reiknings eða korts.

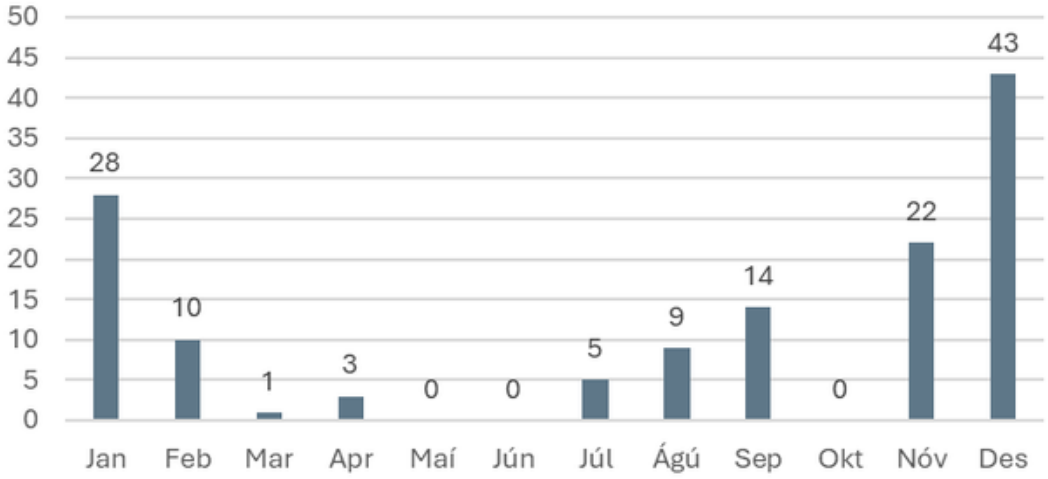
Tafla 1. Dæmi um vefveiðiherferðir

Svikasíður	Herma eftir	Svikaskilaboð í sms eða tölvupósti
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...

Viðbrögð við vefveiðiherferðum

Mikilvægt er að bregðast hratt við þegar nýjar vefveiðiherferðir birtast því þannig er hægt að takmarka tjón viðskiptavina umtalsvert. Fjármálafyrirtækin hjálpast öll að með því að tilkynna svikasíðurnar til NFCERT, CERT-IS og annarra netöryggisfyrirtækja sem geta sett varúðartexta meðan svikasíðan er gerð óvirk. Arion banki lætur sitt ekki eftir liggja en á árinu 2025 hefur bankinn náð miklum árangri í slíkum niðurtökum. Sjá töflu 2 um fjölda vefveiðiherferða tilkynntar af Arion banka.

Tafla 2. Tilkynntar vefveiðiherferðir 2025



Þróun 2024-2025

Á árunum 2024 og 2025 varð veruleg aukning í tilkynntum netsvikum. Tilkynningum til Arion banka fjölgaði nærri því tvöfalt milli ára, sem endurspeglar bæði fjölgun tilfella og aukna vitund almennings og fyrirtækja um mikilvægi þess að tilkynna grunsamleg atvik. Þrátt fyrir þessa miklu fjölgun mála lækkaði heildartjón viðskiptavina á sama tíma, sem bendir til þess að varnir, fræðsla og viðbragðsgeta hafi skilað áþreifanlegum árangri.

Á árinu 2024 voru fjárfestingasvik í rafmyntum stærsti flokkur tilkynntra tjóna. Þessi mál voru áberandi og leiddu oft til verulegs fjárhagstjóns þar sem svikarar beittu blekkingum til að fá fólk til að opna rafmyntaveski eða fjárfesta í fölskum verkefnum. Á árinu 2025 sást markverð breyting á þróuninni, tjón dreifðust á fleiri flokka og aðrar svikategundir urðu áberandi í tölum bankans.

Helstu flokkar tjónsmála árið 2025 voru:

- Nándarsvik (e. physical proximity credential theft) mynda stærsta tjónaflokkinn. Í slíkum málum er svikari kominn yfir tæki eða auðkenningarupplýsingar þolanda og getur því framkvæmt og staðfest greiðslur með búnaði viðkomandi. Slík mál eiga sér oft stað á skemmtistöðum eða í aðstæðum þar sem svikari fylgist með auðkenningu (PIN, rafræn skilríki) áður en tækin eru tekin af viðkomandi aðila.
- Óafhent vörusvik (e. goods·not received) jukust samhliða aukinni netverslun og sérstaklega í kringum stóra verslunardaga. Þar eru fölsuð tilboð notuð til að ná kortaupplýsingum eða seinka afhendingu þar til endurgreiðslufrestur rennur út.
- Falsaðir reikningar og vefveiðar (e. phishing) þar sem notast er við tölvupósta og skilaboð í nafni opinberra eða trúverðugra aðila til að fá fólk til að framkvæma greiðslur eða gefa upp viðkvæmar upplýsingar.

Á árinu 2025 minnkaði tjón vegna yfirtökusvika verulega. Þetta sýnir að varnir gegn slíkum tilfellum hafa skilað miklum árangri og að aðeins litlum hluta svikara hefur tekist að nýta sér aðgang viðskiptavina án þeirra vitundar.

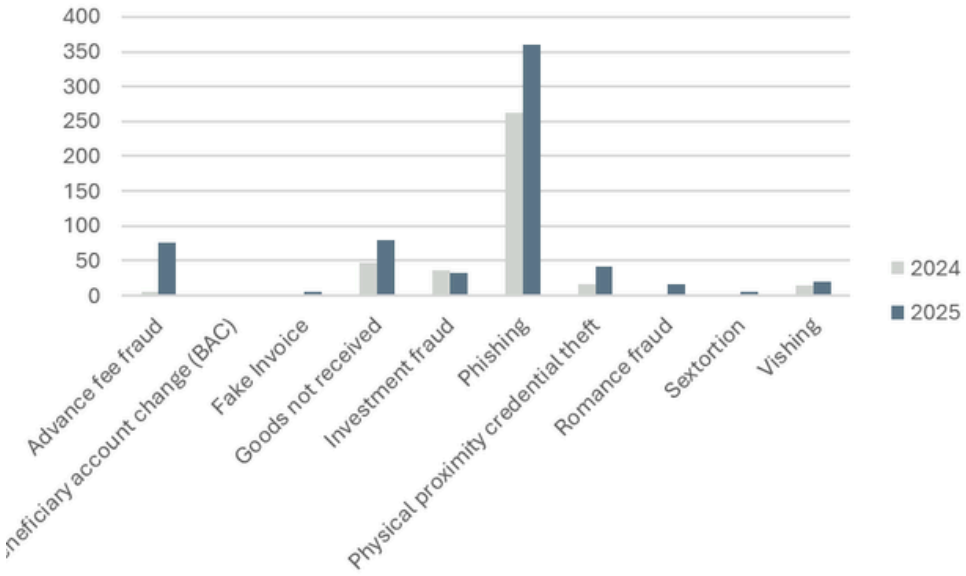
Á sama tíma hefur þróunin orðið sú að blekkingar, félagsleg stjórnun (e. social engineering) og misnotkun á aðgerðum sem viðskiptavinurinn framkvæmir sjálfur eru nú umfangsmeiri og flóknari. Þetta sést m.a. í aukningu nándarsvika, fjölgun tilvika þar sem kort eru tengd í stafrænt veski og fleiri málum þar sem einstaklingar staðfesta sjálfir færslur sem svikarar græða á.

Þróunin milli 2024 og 2025 sýnir því tvö megineinkenni:

- Svikum fjölgar og aðferðir verða fjölbreyttari og persónulegri.
- Varnir bankans draga úr tjóni viðskiptavina, þrátt fyrir aukna virkni svikara.

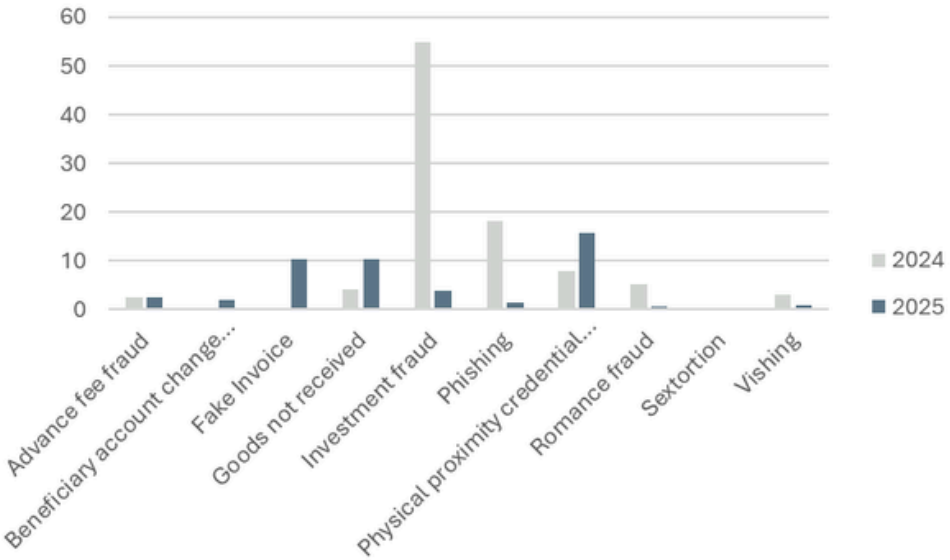
Þetta undirstrikar mikilvægi þess að greina á milli svika þar sem svikari framkvæmir aðgerðina sjálfur og blekkinga þar sem viðskiptavinurinn verður virkur þátttakandi í framkvæmd ólögmætrar færslu.

Tafla 3. Fjöldi netsvikamála eftir svikategund



Tafla 3 sýnir að flokkarnir vefveiðar og vara ekki afhent (e. goods not received) eru svik sem eru hvað algengust og aukast jafnframt á milli ára. Á sama tíma má sjá aukningu í málum sem tengjast nándarsvikum og nýja flokka eins og ástarsvik (e. romance fraud) og sæmdarkúgun (e. sextortion). Sæmdarkúgun eða hótun um að deila viðkvæmum myndum fer vaxandi meðal ungmenna.

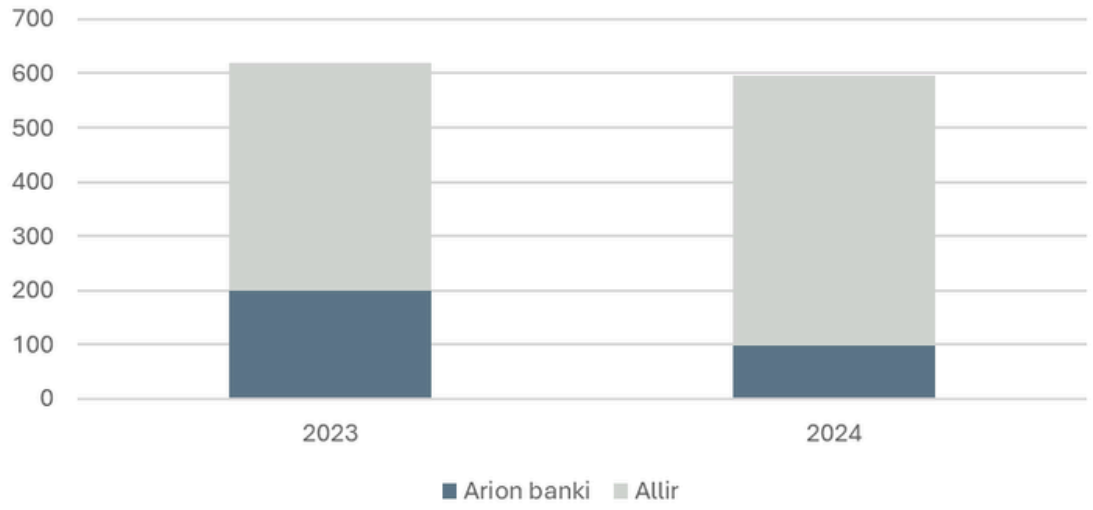
Tafla 4. Heildartjón eftir svikategund í m.kr



Á árinu 2024 var tjón viðskiptavina vegna fjárfestingasvika í rafmyntum mjög mikið, en lækkaði verulega á árinu 2025. Árið 2025 ollu hins vegar nándarsvik mesta tjóninu, sem endurspeglar aukningu í tilvikum þar sem símar og auðkenningartæki eru tekin eða misnotuð.

Tjón vegna óafhentrar vöru og vefveiða var einnig áberandi á tímabilinu. Vert er að benda á að heildartjónsupphæð vegna vefveiða hefur lækkað verulega á sama tíma og tilfellum fjölgar.
Ef bornar eru saman opinberar tölur frá Seðlabanka Íslands um svik í greiðsluþjónustu þá er ljóst að árangur Arion banka er greinilegur en á milli áranna 2023 og 2024 minnkaði tjón viðskiptavina bankans vegna netsvika um helming. Tölur fyrir árið 2025 hafa ekki verið gefnar út.

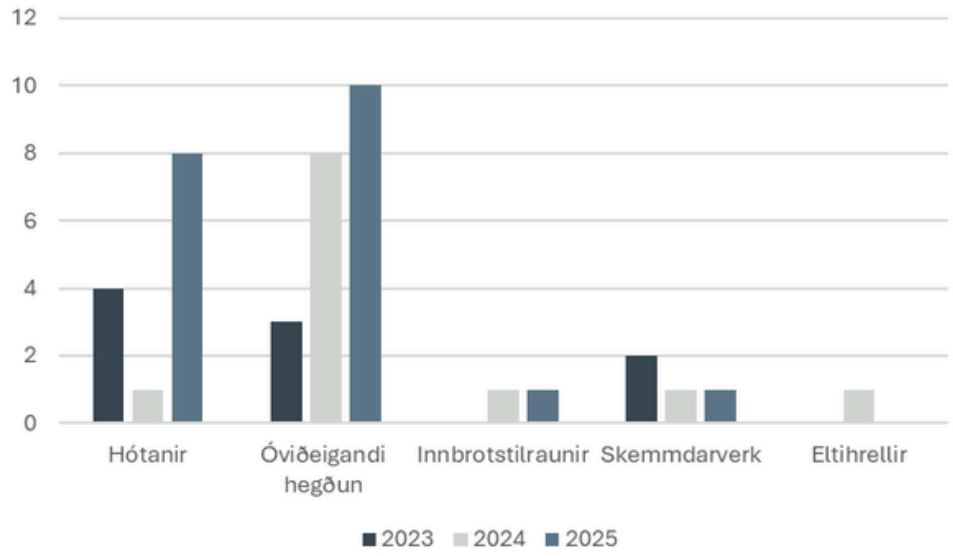
Tafla 5. Þróun heildartjóns í greiðsluþjónustu á Íslandi samanborið við heildartjón viðskiptavina Arion banka



Ógnandi hegðun og skemmdarverk

Talsverð fjölgun hefur verið á atvikum sem tengjast óviðeigandi hegðun viðskiptavina á árunum 2023-2025 þar sem slík hegðun hefur skapað óöryggi eða truflanir á starfsstöðvum bankans.

Tafla 6. Fjöldi öryggismála eftir tegund



Sjá má á töflu 6 að hótunum og óviðeigandi hegðun í garð starfsfólks hefur fjölgað hvað mest milli ára. Slík þróun kallar á áframhaldandi eftirfylgni, markvissa fræðslu og styrkingu öryggisferla til að starfsfólk hafi skýrar leiðbeiningar og rétt verkfæri til að bregðast við þegar hegðun viðskiptavina eða aðstæður eru óvenjulegar, hótandi eða truflandi. Þá eru innbrotstilraunir og skemmdarverk enn tiltölulega fátíð en slík atvik geta verið alvarleg og valdið truflun í daglegri starfsemi.

Ógnandi og óviðeigandi hegðun getur komið fram á margvíslegan hátt og aðstæður geta þróast hratt. Sjá má eftirfarandi dæmi:

- **Viðskiptavinur neitar að yfirgefa útibú:** Viðskiptavinur sýnir óstöðuga og hótandi hegðun og neitar að yfirgefa útibú. Í slíkum tilvikum hefur þurft að kalla til öryggisverði til að vísa viðkomandi út.
- **Óviðeigandi framkoma:** Viðskiptavinur sýnir óviðeigandi framkomu sem endar með ásökunum um þjófnað og hótun um að viðkomandi sendi aðra aðila inn í útibúið til að „kenna starfsfólki lexíu“.
- **Tilraun til að taka út af reikningi annars viðskiptavinar:** Einstaklingur sem getur ekki framkvæmt færslu af reikningi annars aðila verður æstur, ræðst gegn starfsmanni og neitar að yfirgefa útibúið. Kalla þurfti til lögreglu til að vísa viðkomandi út.
- **Ógn og áreiti:** Einstaklingur missir stjórn á sér, slær í hurðir, húsgögn eða áreitir starfsfólk, t.d. með því að ráðast inn í persónulegt rými eða sýna aðra ógnandi hegðun.
- **Eltihrellir:** Einstaklingur mætir reglulega í útibú og beinir óviðeigandi athygli að tilteknum starfsmanni án beinna hótana, en þannig að starfsfólk upplifir aðstæður sem ógn. Málið var metið sem að um eltihrelli væri að ræða.

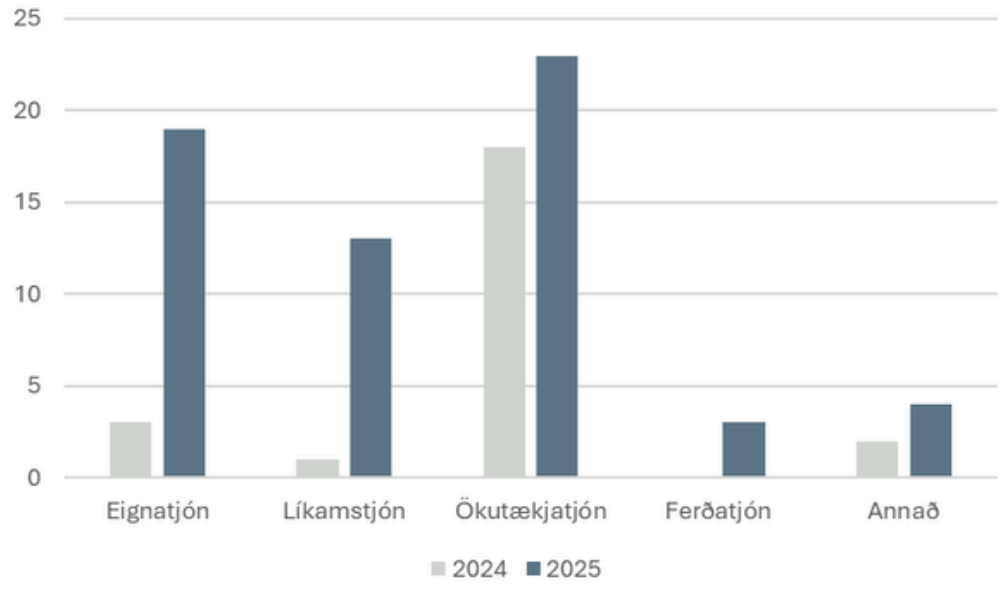
Þróun tryggingasvika árin 2024–2025

Undanfarin misseri hefur orðið veruleg aukning í málum tengdum tryggingasvikum, bæði hvað varðar fjölda tilvika og umfang þeirra. Þessi þróun endurspeglar breytt áhættulandslag á tryggingamarkaði og þá staðreynd að svikatilraunir hafa að jafnaði orðið bæði flóknari og umfangsmeiri.

Í ljósi þeirrar þróunar sem orðið hefur á undanförnum misserum, þar sem bæði fjöldi og umfang mála tengdum tryggingasvikum hefur aukist, hefur Vörður gripið til viðeigandi aðgerða í samræmi við gildandi lög og skilmála. Aðgerðirnar hafa stuðlað að skýrari yfirsýn yfir vafasöm tilvik og markvissara verklagi þegar grunur vaknar um svik. Á sama tíma hefur verið unnið að því að efla verklag og skráningu slíkra mála, sem eykur gagnsæi, styrkir forvarnir og veitir betri heildarmynd af þróun netsvika á tryggingamarkaði.

Með þessum aðgerðum leitast Vörður við að draga úr áhættu vegna tryggingasvika og stuðla að öruggu rekstrarumhverfi fyrir alla viðskiptavini.

Tafla 7. Fjöldi tryggingasvika eftir tegund



Talsverð aukning varð á fjölda skráðra tryggingasvikamála milli ára en slíkt undirstrikar þörfina fyrir árvekni sem og öfluga ferla til þess að hægt sé að bera kennsl á frávik án tafar. Þegar það kemur að tryggingasvikum snúa hefðbundin svik helst að kröfum vegna tjóns án raunverulegs atviks og tilvika þar sem atburðir eru sviðsettir.

Árið 2025 var fjölgun mála þar sem grunur var um fölsun gagna sem gefur til kynna að aðferðir svikara séu síbreytilegar og fjölbreyttar. Á árinu 2025 héldu ökutækjatjón áfram að vera algengasti flokkur svika en þó var fjölgun á málum sem snúa að líkams- og eignatjóni sem gefur til kynna að áhættan dreifi sér á fleiri flokka trygginga nú en áður. Á árinu 2024 voru flest mál fremur einföld og umfangslítil en á árinu 2025 urðu málin fleiri, stærri og flóknari en áður. Snúa málin m.a. að grun um íkveikju, sviðsetningu slysa og innbrota og ferðatjóns en allt eru þetta mál sem krefjast nákvæmrar rannsóknar og ítarlegrar greiningar.

Aukning varð á málum milli ára sem vísa þurfti til lögreglu, sem endurspeglar aukinn alvarleika tryggingasvika og undirstrikar mikilvægi virks samstarfs við yfirvöld þegar grunur vaknar um refsiverða háttsemi. Í því samhengi er tjónagrunnur vátryggingafélaga lykilverkfæri í svikavöktun Varðar þar sem hann styður við greiningu óvenjulegra tjónstilkynninga, svo sem tvíteknar tilkynningar sama tjóns hjá fleiri en einu félagi. Grunnurinn styrkir gæði tjónarannsókna, dregur úr röngum útgreiðslum og eflir samræmda og markvissa nálgun vátryggingafélaga í baráttunni gegn tryggingasvikum, með fullu tilliti til persónuverndar og réttinda viðskiptavina.

Aðgerðir bankans árið 2025

Á árinu 2025 greip Arion banki til umfangsmikilla aðgerða til að vernda viðskiptavini gegn netsvikum. Mikil áhersla var lögð á forvirkar aðgerðir, markvissa upplýsingaöflun og hröð viðbrögð sem leiddu til þess að fjölmörg tilvik voru stöðvuð áður en tjón hlaust af.

Starfsfólk Arion banka hafði samband við viðskiptavini í yfir 5.200 símtölum og náðu til um 4.000 einstaklinga vegna gruns um svik. Í flestum tilfellum var hægt að koma í veg fyrir misnotkun greiðslumiðla vegna þess hve tímanlega var brugðist við og hve markviss samskipti voru við viðskiptavininn. Sú nálgun Arion banka, að vara fólk tafarlaust við óvenjulegri virkni eða hættumerkjum, reyndist ein af áhrifaríkustu vörnunum gegn svikum á árinu.

Arion banki lagði einnig mikla áherslu á fræðslu og vitundarvakningu. Í samstarfi við Sigurstein Másson var herferðin „Sönn svikamál“ sett fram á aðgengilegu og áhrifamiklu formi. Farið var yfir raunveruleg mál sem sýndu greinilega hversu fljótt svik geta þróast og hvernig einstaklingar, óháð aldri eða reynslu, geta orðið aðilar að svikamálum, jafnvel án þess að gera sér grein fyrir því. Niðurstöður herferðarinnar sýndu að skömm og óöryggi eru enn stór hindrun í vegi þess að fólk stígi fram og tilkynni svik. Með herferðinni var sýnt fram á að allir geta lent í svikum og að lykilatriði sé að bregðast rétt og hratt við.

Í framhaldi af fræðsluverkefninu setti bankinn upp flóttaherbergi (e. escape room) með netsvikaþema, þar sem þátttakendur þurftu að setja sig í spor svikara. Markmiðið var að efla skilning á starfsháttum svikahópa með því að láta fólk upplifa hvernig blekkingar eru byggðar upp og hvaða veikleikar eru nýttir. Þátttakendur fengu því tækifæri til að greina hættumerki, læra að hugsa á gagnrýnin hátt og bregðast hratt við aðstæðum sem líkjast raunverulegum svikum.

Einn þátttakandi lýsti því að reynslan hefði hjálpað honum að koma í veg fyrir að fjölskyldumeðlimur lenti í netsvikum skömmu síðar, sem undirstrikar hagnýtt gildi fræðsluverkefnisins.

Aðgerðir Arion banka á árinu endurspegla því tvö meginmarkmið, annars vegar að bregðast hratt við til að stöðva svik áður en tjón verður og hins vegar að efla vitund og þekkingu viðskiptavina til þess að þeir geti sjálfir greint og stöðvað tilraunir til svika.

Samanlagt skiluðu þessar aðgerðir verulegum árangri og drógu úr tjóni þrátt fyrir að svikatilraunum fjölgaði á árinu.

Mat á netógnum fyrir árið 2026

Horfur fyrir árið 2026 benda til þess að netsvik munu halda áfram að þróast hratt og verða sífellt flóknari. Telja verður að vefveiðar verði áfram ein helsta aðferð svikara til að komast í samband við fólk, enda hafa þær sannað sig sem vænlegar til árangurs og auðveldar í framkvæmd. Þessi tegund svika byggir á því að ná athygli viðtakanda í gegnum tölvupóst, smáskilaboð, samfélagsmiðla eða símtöl, og beita svikarar fjölbreyttum blekkingum til að fá einstaklinga til að smella á hlekki, veita upplýsingar eða samþykkja greiðslur. Með aukinni notkun gervigreindar má gera ráð fyrir því að slík skilaboð verði enn trúverðugri og persónulegri og að erfiðara verði að greina þau frá lögmætum samskiptum.

Nándarsvik í formi stolinna síma og greiðslukorta eru einnig líkleg til þess að halda áfram að aukast. Tækniþróun á sviði fjártækni, þar sem greiðslulausnir eru í auknum mæli tengdar snjallsímum, gerir það að verkum að einstaklingar geta nú borið með sér greiðslumöguleika sem áður voru bundnir við posa (e. Point of sale) í verslunum eða netverslanir. Þar að auki eru auknar vísbendingar um að tengdir aðilar sem þekkja til fórnarlambsins geti nýtt sér þessar aðstæður.

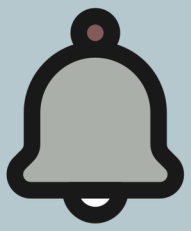
Þá eru til staðar skýr merki um að erlendir svikahópar með tengsl við Austur-Evrópu starfi markvisst á Íslandi. Þeir eru taldir vera hluti af stærri alþjóðlegri starfsemi þar sem hópar eru sendir milli landa til þess að útvíkka svikanet og koma auga á ný tækifæri til að framkvæma svik, þjófnað og fleira. Þó að þeir hópar sem þekktir eru á Norðurlöndunum hafi ekki verið áberandi hér á landi benda gögn og upplýsingar til þess að sambærileg starfsemi eigi sér stað hérlendis og að þessir hópar séu bæði samhæfðir og sérhæfðir í mismunandi tegundum brota. Við slíkar aðstæður er aðeins tímaspursmál hvenær innlendir svikahópar fara að myndast eða koma upp á yfirborðið. Þegar utanaðkomandi aðilar starfa markvisst innanlands verður til þekking, tengsl og aðferðir sem geta smitast yfir í staðbundna starfsemi. Þetta þýðir að innlend þróun gæti fylgt svipuðu mynstri og sést hefur erlendis.

Telja verður að árið 2026 muni einkennast af áframhaldandi aukningu í blekkingum og vefveiðum, frekari fjölgun mála þar sem greiðslur eru framkvæmdar í stafrænum lausnum bundnum við farsíma og vexti skipulagðra svikahópa með tengingar bæði innanlands og utan.

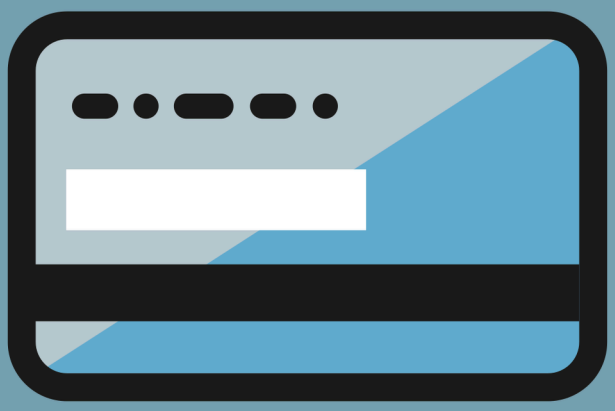
Þær netógnir sem Ísland stendur frammi fyrir eru að stórum hluta sambærilegar því sem aðrar Norðurlandaþjóðir standa frammi fyrir. Viðbúnaðarstig ógna er áfram á vöktuðu stigi og helst stöðugt en skipulagðir glæpahópar eru áfram taldir fela í sér viðvarandi áhættu. Samhliða þessu benda nýlegar greiningar til aukningar í ógnarvirkni sem beinist að Íslandi, sem undirstrikar mikilvægi áframhaldandi árvekni. Helstu ógnir sem snerta Ísland má skipta í nokkra flokka: skipulagða glæpastarfsemi, veikleika tengda birgðakeðju og þjónustuaðilum, netárásir á borð við dreifðar álagsárásir (e. distributed denial of service attack („DDoS“) sem reyna að lama þjónustu, innri áhættur innan fyrirtækja, ógnir tengdar erlendum ríkjum og notkun gervigreindar til að gera blekkingar og vefveiðar trúverðugri. Þá má draga þá ályktun af fyrirliggjandi gögnum og upplýsingum að háþróaðir ógnaraðilar, sem starfa bæði á sviði netglæpa og netnjósna, hafi aukið umsvif sín og beiti aðferðum sem falla undir háþróaða þráláta ógn (e. Advanced Persistent Threat). Slík virkni ber oft einkenni ríkisstuddrar starfsemi fremur en hefðbundinna netglæpahópa og miðar að því að komast inn í kerfi fyrirtækja með markvissum og langvinnum hætti. Telja verður mikilvægt að taka vísbendingum um fyrrgreint alvarlega og meta áhættu í ljósi þess, enda búa slíkir ógnarhópar yfir öflugum verkfærum, tækni og umtalsverðum auðlindum.

Arion banki hefur verið í traustu samstarfi við NFCERT og CERT-IS og hefur samstarfið og markviss upplýsingagjöf því tengt stuðlað að bættri vitund og dýpri skilning á þeirri stöðu sem Ísland stendur frammi fyrir.

Á árinu 2026 mun Arion banki halda þessari vinnu áfram af krafti, leitast eftir að vera leiðandi í svika- og ógnartengdum málum og tryggja öryggi viðskiptavina sinna. Telja má að netógnum muni ekki linna og er því þörf á að hafa skilvirkt eftirlit með slíku sem kallar á áframhaldandi skoðun varna, aukna fræðslu og styrkingu viðbragðskerfa til þess að mæta þeirri þróun sem á sér stað, bæði innanlands sem utan.



2025



ARION
E$CAPE