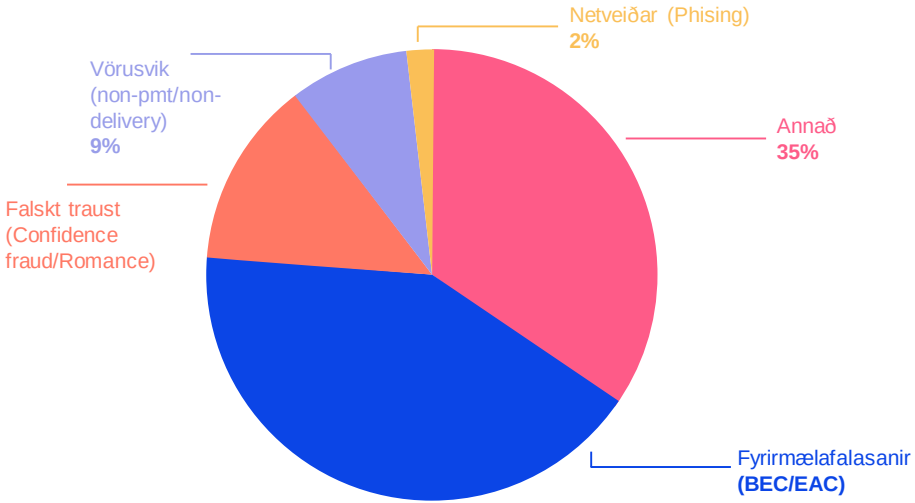
Netöryggi

Tengt fjársvikum

Mikilvægi netöryggis

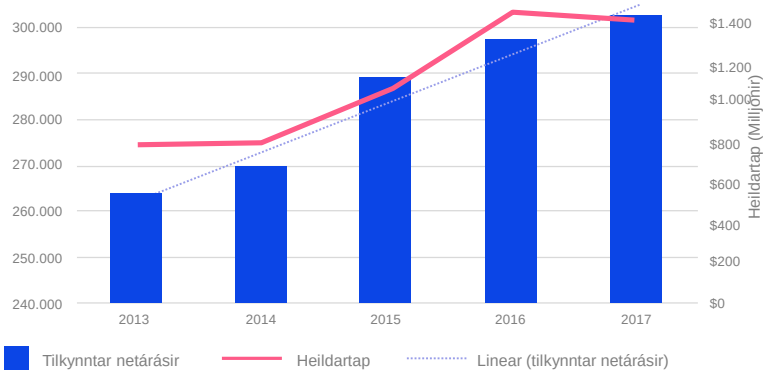
- Mikil aukning í tilraunum til fjársvika í gegnum netið hérlendis
- Netárásirnar eru síbreytilegar og fylgja tækniþróun
- Hætturnar eru til staðar, bæði fyrir einstaklinga og fyrirtæki
- Netöryggi er jafn mikilvægt og aðrar hættur eins og eldvarnir

Gerðir netsvika (top 13)

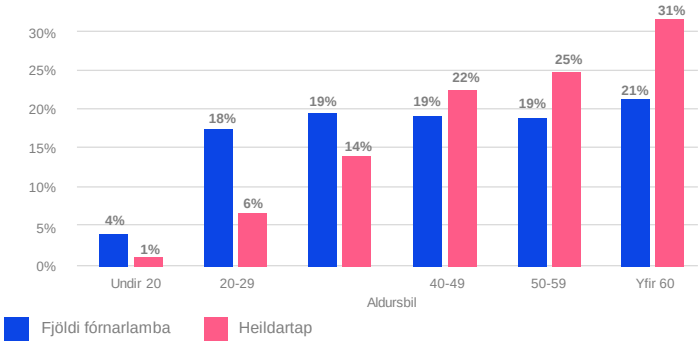


*Gögn líkana tekin frá FBI Internet Crime Complaint Center (IC3, 2017 Report)

Vöxtur í netárásum og heildartapi vegna fjársvika



Skipting eftir aldri (2013–2017)



Fyrirmælafalsanir (Business e-mail compromise)

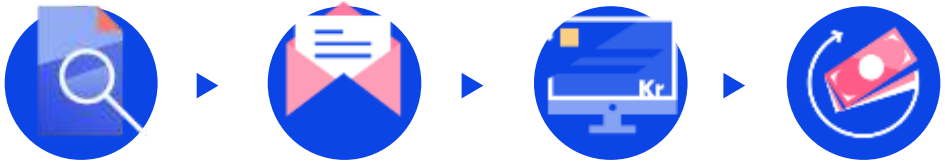
Svikin fara fram með þeim hætti að falsaðir tölvupóstar eru sendir til starfsmanna fyrirtækja, oft undir nafni stjórnenda.

Í póstinum eru fölsk fyrirmæli um að greiðsla skuli framkvæmd með hraði.

Svikahrappar hafa undirbúið sig vel og hafa skipulagt ferlið með þeim hætti að móttakandi fyrirmælanna sjái ekki neinn mun á falsaða póstinum og eðlilegum greiðslufyrirmælum.

Oft eru svikahrappar búnir að finna út hvenær yfirmenn fara t.d. í frí eða eru frá vinnu og senda fölsuðu póstana á því tímabili og í þeirra nafni.

Dæmi um fyrirmælafölsun



Undirbúningur

Svikahrappar leggja mikla vinnu í undirbúning. Finna út hvenær breyting verður í fyrirtækinu t.d. að yfirmaður fer í frí.

Falsaður póstur sendur

Svikahrappur sendir falsaðan post í nafni yfirmanns á starfsmann með fyrirmælum um að framkvæma millifærslu sem fyrst.

Pressa sett á starfsmann

Svikahrappur sendir ítrekun á starfsmann og tekur fram að ekki náist í hann til staðfestingar þar sem hann er í frii.

Millifærsla framkvæmd

Starfsmaður gefur eftir undan pressunni og millifærir á reikning sem kemur í ljós að er í umráði svikahrapps.

Góð ráð til að verjast fyrirmælafölsunum

1. **Fræðsla** – Þekking á einkennum og hættum
2. **Varfærni** – Rýna þarf vel í öll smáatriði
3. **Pressa** – Ekki láta undan pressu og ítrekunum
4. **Símtal** – Greiðslubeiðnir staðfestar með símtali
5. **Birgjar** – Breyttar upplýsingar t.d. Um birgja skulu staðfestar
6. **Samþykktarferli** – Virkja þarf greiðslusamþykktarferli

Vefveiðar (Phishing)

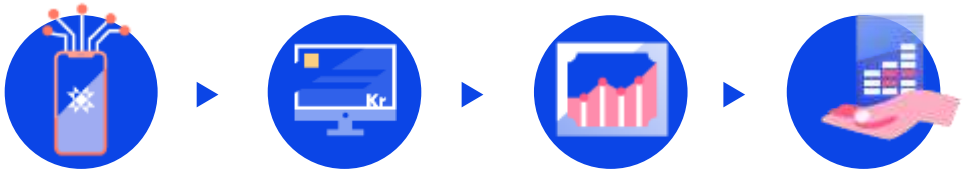
Svikin fara fram með þeim hætti að svikahrappar reyna að blekkja fólk með trúverðugum skilaboðum í tölvupósti eða smáskilaboðum til að smella á slóð, hlaða niður hugbúnaði fjársvikara eða opna viðhengi.

Ef móttakandi skilaboðanna fellur í gildruna, komast svikahrappar yfir upplýsingar á borð við notendanöfn, lykilorð, bankareikningsupplýsingar og leyninúmer.

Skilaboðin eru oft mjög trúverðug og sannfærandi þar sem svikahrappar ýta á eftir móttakanda um mikilvægi aðgerðanna.

Fölsuðu vefsíðurnar, hugbúnaðurinn eða þær leiðir sem svikahrappar nota eru oft mjög líkar þeim þjónustum sem heiðvirð fyrirtæki eða bankar nota, t.d. með eftirlíkingu á vörumerkjum fyrirtækja eða banka.

Dæmi um vefveiðar



Fölsk skilaboð móttekin
Falskur póstur eða smáskilaboð berast sem virðast vera frá heiðvirðu fyrirtæki og móttakandi hvattur til að smella á hlekk

Fölsk vefsíða útfrá hlekk
Móttakandi smellir á hlekkinn sem leiðir hann á falska vefsíðu sem í fyrstu virðist traustverðug

Upplýsingum stolið
Á fölsku vefsíðunni er beðið um viðkvæmar upplýsingar, s.s notendanafn, lykilorð, leyninúmer, kortaupplýsingar eða CVC númer

Upplýsingar notaðar
Á þessu stigi eru svikahrapparnir komnir með skráðar upplýsingar sem þeir nota til að steela fé eða til annars konar svika

Góð ráð til að verjast vefveiðum

Þekkja einkennin – Trúverðug skilaboð
Vefsíðurnar eru falsaðar en virðast trúverðugar t.d. með vörumerki fyrirtækis

Öryggisupplýsingar – Aldrei deila með öðrum
Heiðvirð fyrirtæki biðja ekki um öryggisupplýsingar s.s. lykilorð, PIN eða CVS

Hlekkir – Aldrei slá inn upplýsingar
Vefsíður út frá hlekkjum eru líklega tengdar netsvikum til að komast yfir upplýsingar og gögn

Tveggja þátta auðkenning – Rafræn skilríki
Notast skal við tveggja þátta auðkenningu á öllum tækniþjónustum þar sem það býðst s.s vefpósti og Facebook

Uppfæra kerfi – Hugbúnaðar- og örygisuppfærslur
Allur búnaður, s.s. tölvur, símar, spjaldtölvur, ættu ávallt að vera með nýjustu hugbúnaðar- og öryggisuppfærslur

Lykilorð – Því fleiri, því betra
Nota skal mismunandi lykilorð/PIN fyrir mismunandi þjónustuleiða

Verkferli ef netárás á sér stað

Ef grunur leikur á að netárás hafi átt sér stað skal umsvifalaust grípa til eftirfarandi aðgerða

Aðgerðir ef netárás á sér stað

1

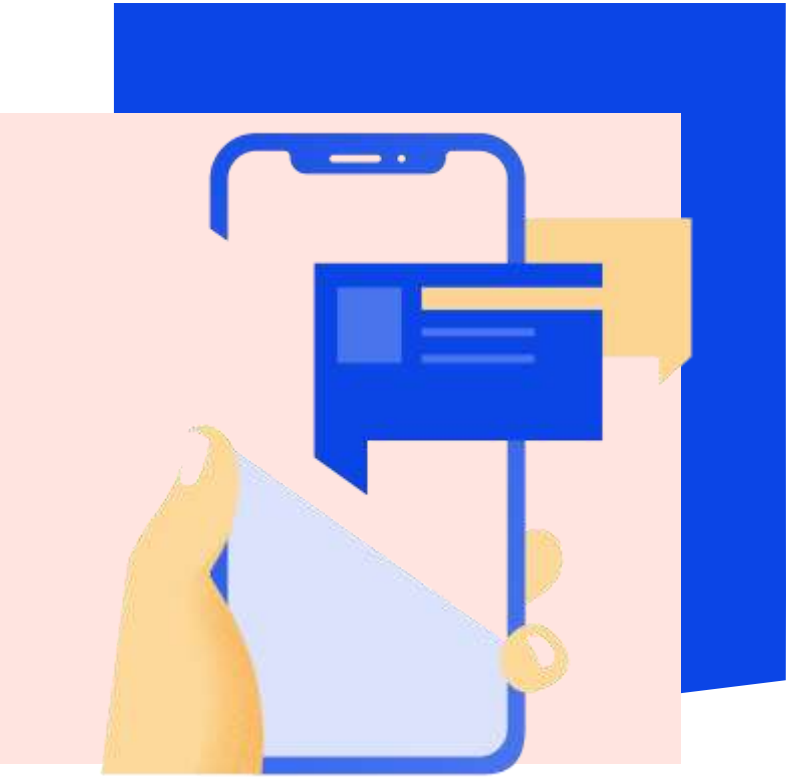
Hafa samband við þinn viðskiptabanka
Ferli fer af stað með yfirvöldum til að stöðva svikin og endurheimta féð

2

Strax skal haft samband við lögreglu
Einnig skal send tilkynning á cybercrime@lrh.is

3

Halda ró og vinna með fagaðilum
Mikilvægt er að allar aðgerðir séu framkvæmdar í samráði við lögreglu, viðskiptabanka og yfirvöld



Gagnlegar vefsíður og upplýsingar

Við mælum með að einstaklingar og fyrirtæki kynni sér vel netöryggi og tryggi þekkingu starfsfólks

Gagnlegar vefsíður:

- Netöryggi.is netoryggi.is
- Lögreglan logreglan.is/fraedsla/internetid
- Samtök fjármálafyrirtækja sff.is/malaflokkar
- Persónuvernd personuvernd.is
- SAFT saft.is
- Enisa enisa.europa.eu

Tengiliðaupplýsingar Arion banka

- Hafðu samband við þinn viðskiptastjóra
- Netfang: arionbanki@arionbanki.is
- Sími: 444 7000

Föllum ekki í gildrurnar