STAFRÆN FJÁRSVIK OG SVINDL Í HEIMI GERVIGREINDAR

VERTU VAKANDI OG VERNDAÐU SJÁLFAN ÞIG

Fjársvik og svindl á netinu eru ekki ný af nálinni, en gervigreind (AI) hefur gert þau tæknilega fullkomnari og erfiðara að koma auga á þau. Glæpamenn nota nú fölsuð skilaboð og vefsíður, falska reikninga í nafni þekktra einstaklinga og jafnvel raddir útbúnar af gervigreind eða myndskeið með myndum af fólki sem líkist fulltrúum frá bankanum þínum, vinum þínum eða fjölskyldu þinni til að plata þig.

Þeir hafa oft samband í gegnum samfélagsmiðla, tölvupóst, óvænt símtöl og smáskilaboð sem líta út fyrir að vera eðlileg.

Þú gætir því átt hættu á að verða fyrir fjárhagstjóni, persónuauðkennaþjófnaði og tilfinningalegri vanlíðan vegna þessarar svikastarfsemi. Vertu á varðbergi og fylgdu þessum lykilráðum til að tryggja öryggi þitt:

Vertu á varðbergi gagnvart þekktum fjárhagslegum svikum á netinu og svindli sem knúið er af gervigreind, t.d. eftirhermum, vefveiðum, fjárfestingar- og tryggingarsvindli og jafnvel svikum og svindli sem dulin eru sem rómantísk skilaboð eða álíka. Til að læra meira um mismunandi tegundir svika og svikara sjá blaðsíðu 5, 6 og 7.

Og til að fræðast um svik og svindl sem tengjast sýndareignum skoðaðu sérstakt upplýsingablað um sýndareignasvik og-svindl ( ).

Taktu eftir viðvörunarmerkjum:
Lærðu að þekkja grunsamlega hegðun, skilaboð eða tilboð (sjá blaðsíðu 2);

Verndaðu þig:
Tryggðu öryggi persónuupplýsinga þinna (sjá blaðsíðu 3); og

Þekktu hvað á að gera ef þú verður fórnarlamb svika eða svindls
(sjá blaðsíðu 4).

Viðvörunarmerki

Loforð sem virðist of gott til að vera satt.

Óvænt símtal úr óþekktu símanúmeri.

Brýn beiðni um peninga eða persónulegar upplýsingar, þar á meðal frá einhverjum sem virðist vera fjölskyldumeðlimur, vinur eða jafnvel opinber persóna.

Beiðni um að fá að taka stjórn á tækinu, hlaða niður forriti, skanna QR kóða eða smella á tengil.

Beiðni um persónuupplýsingar eða bankaupplýsingar (t.d. lykilorð, kreditkortanúmer, netbankaskilríki eða öryggiskóða).

Beiðni um greiðslu með órekjanlegum hætti (t.d. sýndareignir, gjafakort, millifærslur eða fyrirfram greidd debitkort).

Grunsamlegt eða rangt netfang eða hlekkur (t.d. stafsetningarvillur í slóðinni eða óvenjuleg netslóð).

Viðhengi af óþekktum uppruna, t.d. .exe, .scr, .zip eða macro-virk Office skrá (.docm, .xlsm).

Lélegt málfar eða sniðmát í opinberu skjali, þó að gervigreind geri svikurum mögulegt að fela þessa galla með skilvirkari hætti en áður.

Vefsíða sem lítur út fyrir að vera fagleg en skortir staðfestar samskiptaupplýsingar eða skráningarupplýsingar fyrirtækisins.

Tónfall eða hrynjandi sem hljómar óvenjulega, skortir hlé og virðist of reiprennandi eða vélræn. Hafðu möguleikann á „raddar klónun“ í huga þó að talgervilsraddir útbúnar með gervigreind geti einnig hljómað mjög eðlilega.

Myndskeið þar sem röddin getur hljómað vélræn eða of flöt, varahreyfingar og andlitstjáning eru mögulega úr takti við ræðu eða það skortir samræmi í bakgrunn, lýsingu og skugga. Þetta eru oft myndbönd framleidd af gervigreind (deepfakes).

Skref til að vernda þig

1 **Aldrei deila persónu- eða bankaupplýsingum:**

Raunveruleg fyrirtæki munu aldrei biðja um PIN-númerin þín, lykilorð, innskráningarupplýsingar eða öryggiskóða með tölvupósti, texta, í gegnum samfélagsmiðla eða síma.

2 **Staldraðu við og hugsaðu áður en þú framkvæmir:**

Ekki flýta þér að senda peninga, deila upplýsingum eða smella á tengla – svindlarar skapa vísvitandi tilfinningu um tímaþröng (t.d. upplýsingatæknivandamál í bankanum þínum, neyðarsímtöl sem tengjast vinum þínum og fjölskyldumeðlimum, ógnandi tal o.s.frv.). Ef einhverjar efasemdir vakna, jafnvel minniháttar, skaltu ekki bregðast við; ljúktu símtalinu og staðfestu uppruna eða auðkenni vandlega.

3 **Athugaðu uppruna/auðkenni vandlega:**

- Gakktu alltaf úr skugga um hvaðan skilaboð, símtöl, tölvupóstar, og tenglar koma – jafnvel ef þeir líta út fyrir að vera raunverulegir, virðast koma frá vini eða fjölskyldu þinni, eða jafnvel opinberri persónu. Hringdu til dæmis eða sendu fjölskyldu þinni og vinum skilaboð með því að nota þekkt númer í gegnum trausta rás; leitaðu að stafsetningarvillum, undarlegum vefslóðum eða öryggisvísum sem vantar (staðfestu t.d. að hlekkur vefsetursins innihaldi „s“ í „HTTPS“ til að ganga úr skugga um að vefsíðan sé örugg og leitaðu að viðbættum eða týndum bókstöfum í nafni fyrirtækisins).

- Ekki opna tengla úr óumbeðnum skilaboðum, settu aðeins upp opinber forrit í gegnum traustar appverslanir (smáforritaverslanir) og ekki skanna óþekkta QR-kóða.

- Sammælstu við fjölskyldu þína um „öruggt orð“- leyniorð sem þú getur notað til að staðfesta auðkenni ef einhver með kunnuglega rödd hringir í þig með brýna beiðni um peninga og segist vera fjölskyldumeðlimur (t.d. foreldrar, systir/bróðir, barn).

- Notaðu staðfestar samskiptaupplýsingar til að ná beint til fyrirtækisins eða einstaklingsins og treystu aldrei á samskiptaupplýsingarnar sem grunaður svikari veitir (leitaðu til dæmis sjálfstætt að nafni fyrirtækisins, notaðu staðfestar viðskiptaskrár eða áður staðfestar samskiptaaðferðir). Svindlarar gætu haldið því fram að þeir séu með leyfi eða hermt eftir vefsíðu raunverulegs fyrirtækis. Gakktu úr skugga um hvort einhverjar viðvaranir hafi verið gefnar út af fjármálaeftirliti í landi þínu eða færðar inn á IOSCO I-SCAN listann (iosco.org/i-scan/). Varðandi þjónustuveitendur sýndareigna, skaltu athuga hvort þeir hafi leyfi á Evrópska efnahagssvæðinu (EES). (athugaðu t.d. ESMA skrána ( ).

4 **Fylgstu með hugsanlegum gervigreindarbrögðum:**

Með þróun gervigreindartækni er svindl að verða meira sannfærandi en nokkru sinni fyrr- jafnvel þó að farið sé eftir bestu öryggisráðum. Ef eitthvað virðist óvenjulegt eða þú finnur eitthvert af viðvörunarmerkjunum sem lýst er hér að ofan skaltu staldra við og endurmeta aðstæður.

5 **Settu aldrei upp fjaraðgangshugbúnað og deildu ekki skjánum þínum:**

Bankar og fjármálastofnanir munu aldrei biðja þig um það.

6 **Haltu tækjum og reikningum öruggum:**

Notaðu sterk og einstök lykilorð, haltu þeim leyndum og forðastu að endurnýta sömu notendanöfn og lykilorð í mismunandi kerfum. Virkjaðu fjölþætta auðkenningu þar sem það er mögulegt. Sjá nokkrar ábendingar um lykilorð hér. ( ). Haltu hugbúnaði og vírusvörnum uppfærðum og virkum.

7 **Vertu varkár þegar boðið er upp á óvænt og tímabundið fjárfestingartækifæri:**

Ef það hljómar of gott til að vera satt, er það líklega ekki satt.

8 **Hugsaðu áður en þú deilir upplýsingum á samfélagsmiðlum:**

Spjallhópar, spjallborð, færslur á samfélagsmiðlum og myndir geta verið verðmætar uppsprettur upplýsinga fyrir svikahrappa. Að sýna of mikið um sjálfan þig eða fjárfestingar þínar getur gert þig að auðveldu skotmarki.

Hvað á að gera þegar þú hefur orðið fórnarlamb svika eða svindls

Stöðvaðu strax allar færslur

Til að koma í veg fyrir frekari millifærslur á grunsamlega reikninga og forðast meira tap. Hættu öllum samskiptum við svindlarana – hunsaðu símtöl þeirra og tölvupóst og lokaðu á sendandann.

Hafðu samband við bankann þinn eða fjármálafyrirtæki

Láttu bankann þinn eða fjármálafyrirtækið vita strax gegnum viðurkenndar samskiptaleiðir til að kanna möguleika á frystingu eða afturköllun viðskipta.

Breyttu lykilorðum þínum á öllum tækjum þínum og forritum/vefsíðum

Svikarar kaupa stolin lykilorð á netinu og reyna að prófa þau á mörgum aðgöngum. Að breyta aðeins einu lykilorði er ekki nóg; Vertu viss um að þú hafir breytt þeim öllum, svo svikarar geti ekki notað lykilorðin aftur.

Tilkynntu og varaðu við

Tilkynntu atvikið til lögreglu og upplýstu tengslanetið þitt (t.d. vini og fjölskyldu) til að auka vitund. Þessar aðgerðir geta hjálpað þér að vernda þig og aðra.

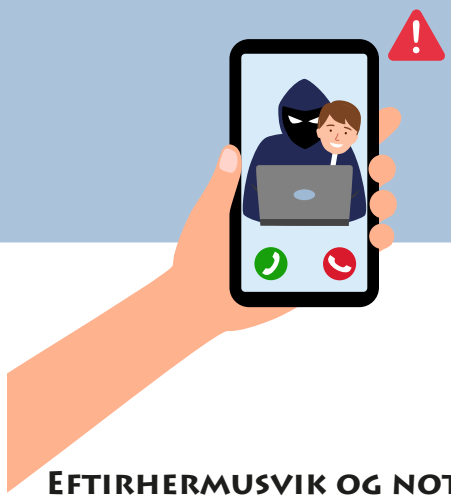
Passaðu þig á svokölluðum „endurheimtarsvikum“

Svikarinn getur haft samband við þig vitandi að þú ert fórnarlamb fyrri svika og sagst vera opinbert yfirvald (t.d. lögregla, skatta- eða fjármálaeftirlit o.s.frv.) og boðist til að endurheimta tapaða peningana þína gegn gjaldi. Þetta er oft önnur tilraun til að svindla á þér. Mundu: að þó að þú hafir verið svikinn einu sinni kemur það ekki í veg fyrir að það verði svindlað á þér aftur.

European Banking Authority, European Insurance and Occupational Pensions Authority, European Securities and Markets Authority, 2025
Luxembourg: Publications Office of the European Union, 2025

PDF ISBN 978-92-9407-280-1 doi:10.2853/1346936 DZ-01-25-168-IS-N

TEGUNDIR STAFRÆNNA FJÁRSVIKA OG SVINDLS MEÐ GERVIGREIND



Eftirhermusvik og notkun djúpfölsunar

Þú færð óvænt símtal frá einhverjum sem segist vera bankinn þinn, opinbert yfirvald (t.d. lögregla, skatta- eða fjármálayfirvald o.s.frv.), dreifingaraðili vátrygginga, upplýsingatæknifyrirtæki eða jafnvel fjölskyldumeðlimur. Sá sem hringir gæti hvatt þig til að flytja peninga til að þeir séu öruggir og vitnað í grunsamlega virkni á reikningnum þínum eða vátryggingarskírteini þínu. Hann getur einnig beðið þig um að gefa upp bankaupplýsingar þínar (t.d. greiðslukortanúmer, innskráningarupplýsingar eða lykilorð), smella á tengil eða setja upp hugbúnað sem á að geta leyst málið fljótt. Sá sem hringir gæti notað falsað númer, sem passar oft við símanúmer bankans þíns til að virðast lögmætur (spoofing).

Svikarar geta notað gervigreind til að útbúa fölsuð myndbönd, myndir eða hljóðbút þar sem hermt er eftir rödd (t.d.fulltrúa banka eða fjölskyldu), andliti (t.d. frægrar persónu) eða hreyfingum. **Þetta er þekkt sem „Deepfake“.**

Hvað gæti gerst:

Með því að vísa til persónulegra upplýsinga og skapa tilfinningu um tímaþröng, blekkir svindlarinn þig til að framkvæma eitthvað sem þú ætlaðir ekki að gera – svo sem að senda peninga á reikninginn sinn, smella á skaðlegan tengil eða setja upp spilliforrit o.fl. í tækinu þínu. Þetta getur gefið svikara beinan aðgang að bankaupplýsingum þínum. Með þessum upplýsingum getur hann breytt lykilorðinu þínu, fengið aðgang að bankareikningnum þínum og stolið peningunum þínum. Mundu að: þótt sá sem hringir hafi persónulegar upplýsingar um þig merkir það ekki að viðkomandi sé áreiðanleg/ur.

Vefveiðar og bragðvísi (e. social engineering)

Þú færð tölvupóst eða skilaboð sem virðast koma frá bankanum þínum eða fjármálafyrirtæki og vara þig við „grunsamlegri virkni“ á reikningnum þínum. Merkið, framsetningin og tungumálið líta fagmannlega út og skilaboðin gætu birst á sama þræði og önnur samtöl frá bankanum þínum. Með skilaboðunum ertu hvattur til að smella á tengil til að staðfesta reikninginn þinn eða endurstilla lykilorðið þitt. Tengillinn leiðir þig á falsaða vefsíðu sem lítur út eins og netbankinn þinn. Án þess að gera þér grein fyrir því slærðu inn upplýsingar þínar á vefsíðu sem er hönnuð til að stela persónulegum upplýsingum þínum.

Svikarar nýta gervigreind til að útbúa sannfærandi vefveiði-skilaboð með því að greina gögn á samfélagsmiðlum til að finna fórnarlömb sín og aðlaga efnið fyrir hvern einstakling.

Hvað gæti gerst:

Svikarinn fær aðgang að bankareikningnum þínum og stelur peningunum þínum eða býr til falsaðan prófíl með persónulegum upplýsingum þínum til að fremja svik.

Fjárfestinga- eða vátryggingasvik

Þú sérð auglýsingu á samfélagsmiðlum eða á vefsetri sem kynnir „fjárfestingartækifæri í takmarkaðan tíma með lítilli áhættu“ eða „afslátt í takmarkaðan tíma“ á tryggingu frá vel þekktu fyrirtæki. Auglýsingin er með mynd af frægum einstaklingi og meðmælum sem eru oft fölsuð. Eftir að þú hefur tjáð áhuga með því að smella á tengil eða fylla út eyðublað er haft samband við þig og þér vísað á vettvang eða skilaboðarás þar sem þú færð faglega ráðgjöf og skjöl. Þú ert hvattur til að fjárfesta með lágri upphæð og í kjölfarið hærri fjárhæðum, eða til að greiða iðgjald inn á það sem virðist vera öruggur reikningur.

Svikarar nota gervigreindarverkfæri til að gera þessar fölsuðu tillögur eða tölvupósta mjög sannfærandi þannig að erfitt er að greina að um svindl sé að ræða. Þeir nota einnig gervigreindarknúna samfélagsmiðlaróbóta til að búa til falsaða aðganga sem eiga í samskiptum við þig, dreifa rangfærslum og líkja eftir raunverulegri hegðun til að öðlast traust og hafa áhrif á ákvarðanir þínar .

Hvað gæti gerst:

Eftir að þú hefur reynt að taka út peningana þína eða gera kröfu hættir tengiliðurinn að svara. Þú uppgötvar að félagið er ekki til eða að tryggingin gildir ekki um atburðinn sem þú hélst að þú værir að tryggja þig gegn. Þú áttar þig síðan á því að þú hefur sent peninga beint til svindlara. Því miður geturðu ekki fengið peningana þína til baka og persónulegar og fjárhagslegar upplýsingar þínar geta verið notaðar til að fremja frekari svik (t.d. undirrita samninga fyrir þína hönd sem gætu leitt til þess að þú tapir enn meiri peningum).

Rómantísk svik og svindl

Það hefur verið haft samband við þig í gegnum samfélagsmiðla, stefnumótaforrit eða með síma/smáskilaboðunum af einhverjum sem þú hefur ekki hitt í raunveruleikanum. Þessi manneskja á við þig tíð, persónuleg og rómantísk samtöl og byggir upp traust með því að nota falska aðganga. Með tímanum færist samtalið í átt að peningum eða fjárhagslegum tækifærum, svo sem sýndareignum þar sem lofað er miklum hagnaði og lítilli áhættu. Viðkomandi biður þig um að millifæra peninga á reikning eða leiðbeinir þér við að setja upp reikning og leggja inn lága fyrstu innborgun til að láta kerfið virðast trúverðugt áður en hann byrjar að hvetja þig til að fjárfesta meira.

Svikarar nota gervigreind til að búa til falska aðganga og finna fórnarlömb á samfélagsmiðlum eða stefnumótaforritum með því að nýta gögn sem þau hafa gert aðgengileg, eða nota spjallmenni til að semja skilaboð.

Hvað gæti gerst:

Svikarinn tekur eins mikið fé og mögulegt er, hættir svo öllum samskiptum og hverfur. Falska fjárfestingavefsíðan eða smáforritið er tekið úr notkun þannig að þú getur ekki fengið aðgang að meintum fjárfestingum þínum. Til viðbótar við fjárhagslegt tjón gætu persónuupplýsingarnar sem þú deildir verið notaðar til að herja á vini þína og fjölskyldu eða til að framkvæma kennisstuld á þér sem getur haft fjárhagslegar eða lagalegar afleiðingar fyrir þig (t.d. gæti svikarinn keypt, tekið lán í þínu nafni eða þú gætir borið ábyrgð á skuldum eða glæpum sem framdir eru í þínu nafni þar til annað hefur verið sannað).

Innkaupasvik

Þú rekst á spennandi tilboð um kaup á netinu. Fyrirtækið sem leggur fram tilboðið fer fram á greiðslu utan þekktra greiðsluvettvanga og segist nota „öruggt greiðslukerfi“ og sendir þér hlekk til að ljúka kaupunum. Tengillinn vísar þér á falsaða auðkennissíðu banka sem líkir eftir raunverulegri vefsíðu bankans og notar vörumerki hans og hönnun, svo þú slærð inn netbankaupplýsingar þínar til að greiða.

Svikarar nota gervigreind til að búa til mjög sannfærandi falskar bankasíður, pöntunarstaðfestingar og reikninga. Gervigreind hjálpar þeim að líkja eftir tóni, vörumerki og stíl alvöru fyrirtækja. Í sumum tilfellum nota þeir gervigreindar-spjallmenni til að svara spurningum og láta samninginn virðast trúverðugri.

Hvað gæti gerst:

Greiðslan í gegnum tengil þriðja aðila fer framhjá vernd markaðarins. Svikarinn fær aðgangsupplýsingar að bankareikningi þínum og stelur peningunum þínum.