SÝNDAREIGNASVIK & -SVINDL

VERTU Á VARÐBERGI OG GÆTTU ÞÍN

Hraður vöxtur sýndareigna og sérkenni þeirra – aðgengi á heimsvísu, hraði, nafnleynd og oft óafturkræf viðskipti – gera þig að skotmarki fyrir netglæpamenn. Svikarar og svindlarar beita háþróuðum aðferðum til að plata þig, svo sem „Ponzi svikum“ (e. Ponzi scheme), fölskum fjárfestingartækifærum, ókeypis tilboðum á samfélagsmiðlum og fölskum skilaboðum. Þeir nota einnig rómantísk fjárfestingarsvik eða líkja eftir sýndareigna-veskisföngum til að spilla færslusögunni í veskinu þínu. Þeir hafa oft samband í gegnum samfélagsmiðla, tölvupóst, óvænt símtöl og skilaboðaforrit sem virðast raunveruleg. Þú gætir átt á hættu á að verða fyrir fjárhagstjóni, auðkennisþjófnaði og tilfinningalegri vanlíðan.

Vertu varkár og fylgdu þessum mikilvægu ráðum til að tryggja öryggi þitt:

Vertu vakandi gagnvart hugsanlegum sýndareignasvikum og -svindli:
til að vita meira um mismunandi tegundir af svikum og svindli (skoðaðu blaðsíðu 5, 6, 7 og 8).

Komdu auga á viðvörunarmerkin:
lærðu að þekkja grunsamlega hegðun, skilaboð eða tilboð (skoðaðu blaðsíðu 2).

Verndaðu þig og eignir þínar:
tryggðu öryggi persónuupplýsinga þinna (skoðaðu blaðsíðu 3).

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

Viðvörunarmerki

Loforð sem virðist of gott til að vera satt.

Óumbeðið tilboð.

Örugg, skjót og mikil ávöxtun.

Þrýstingur um að bregðast skjótt við (t.d. tímabundin tilboð þar sem þrýst er á þig að bregðast strax við).

Beiðni um greiðslu með órekjanlegum hætti (t.d. sýndareignum, gjafakortum, millifærslum eða fyrirframgreiddum debetkortum).

Hvatning til að smella á tengil, skanna QR-kóða eða hlaða niður forriti.

Beiðni um að senda eða deila einkalyklum og fræorðum (listi yfir orð til að fá aðgang að og endurheimta sýndareignaveskið þitt).

Grunsamleg eða röng slóð.

Vörumerki með smávægilegum villum, vefsíða sem hermir eftir útliti vefsíðu raunverulegs fyrirtækis eða lítur faglega út en skortir staðfestar samskiptaupplýsingar, upplýsingar um skráningu fyrirtækis, afrekaskrá eða sannanlega tilvist.

Óþekktur viðskiptavettvangur.

Grunsamlegt viðhengi, sérstaklega .exe, .scr, .zip, eða macro-virk Office-skrá (.docm, .xlsm).

Skref til að vernda þig:

1 Staldraðu við og hugsaðu áður en þú framkvæmir:

Ekki flýta þér að fjárfesta, deila upplýsingum eða smella á tengla – svikarar skapa vísvitandi þá tilfinningu að þú sért í tímaþröng. Ef einhverjar efasemdir eru, jafnvel minniháttar, skaltu ekki framkvæma eða fjárfesta og sannreyndu upprunann vandlega.

2 Sannreyndu uppruna vandlega:

- Sannreyndu alltaf hvaðan skilaboð, símtöl, tölvupóstar, og tenglar koma, jafnvel þó að þeir líti raunverulega út, virðist koma frá vini eða fjölskyldu þinni, eða jafnvel frægum einstaklingi. Leitaðu að stafsetningarvillum, undarlegum vefslóðum eða hvort öryggisvottanir vanti, staðfestu t.d. að hlekkur vefsíðunnar innihaldi „s“ í „HTTPS“ til að ganga úr skugga um að vefsíðan sé örugg og athugaðu hvort einhverjum bókstöfum hafi verið bætt við eða vanti í nafn fyrirtækisins.
- Ekki opna tengla úr óumbeðnum skilaboðum, settu aðeins upp opinber forrit í gegnum traustar smáforritaverslanir og ekki skanna óþekkta QR-kóða.
- Jafnvel þótt tilboð líti út fyrir að vera raunverulegt skaltu alltaf bera það saman við vefsíðu fyrirtækisins eða athuga hvort samfélagsmiðlareikningurinn sé staðfestur (t.d. með opinberum hakamerkjum).
- Notaðu staðfestar samskiptaupplýsingar til að ná beint í fyrirtækið eða einstaklinginn og treystu aldrei á samskiptaupplýsingarnar sem meintur svikahrappur veitir (t.d. leitaðu sjálfstætt að nafni fyrirtækisins, notaðu staðfestar fyrirtækjaskrár). Svikarar gætu haldið því fram að þeir séu með leyfi eða hermt eftir vefsíðu raunverulegs fyrirtækis. Þú getur skoðað hvort þjónustuveitandi sýndareigna hafi leyfi innan ESB með því að skoða ESMA-skrána (↖). Þú getur einnig skoðað vefsíðu fjármálaeftirlits *viðkomandi* ríkis til að sjá hvort einhverjar viðvaranir eða svartir listar hafi verið gefnir út, eða skoðað IOSCO I-SCAN listann (iosco.org/i-scan/).

3 Aldrei deila lykilorðum, einkalyklum eða fræorðum:

Allir sem hafa aðgang að þeim geta náð yfirráðum yfir eignum þínum. Raunveruleg fyrirtæki biðja aldrei um lykilorð eða öryggiskóða með tölvupósti, texta eða síma.

4 Haltu tækjum og einkalyklum öruggum:

Notaðu sterk og einstök lykilorð fyrir hvern sýndareignareikning, haltu lykilorðinu þínu leyndu og forðastu að endurnýta sömu notendanöfn og lykilorð í mismunandi kerfum. Virkjaðu fjölþátta sannvottun þar sem það er mögulegt. Sjá nokkrar ábendingar um lykilorð hér (↖) Haltu hugbúnaði og vírusvörnum uppfærðum og virkum.

5 Sýndu aðgát ef þú færð óvænt fjárfestingartilboð:

Vertu á varðbergi gagnvart fjárfestingum sem lofa mikilli ávöxtun. Ef það hljómar of vel til að vera satt, þá er það líklega svindl.

6 Hugsaðu þig um áður en þú deilir upplýsingum á samfélagsmiðlum:

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

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

Stöðvaðu strax viðskipti

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

Breyttu lykilorðunum þínum í öllum tækjum og forritum/vefsíðum

Svikarar kaupa stolin lykilorð á netinu og reyna að nota þau á marga reikninga. Að breyta aðeins einu lykilorði er ekki nóg; vertu viss um að þú hafir breytt þeim öllum, svo svikarar geti ekki notað þau aftur.

Aftengdu og afturkallaðu aðgang

Afturkallaðu grunsamlegar heimildir í stafræna samningnum þínum sem keyra sjálfkrafa á bálkakeðjunni (snjall-samningur) til að koma í veg fyrir að svindlarar eyði tókum þínum án þíns samþykkis. Mörg veski og bálkakeðjuvafrar bjóða upp á verkfæri sem gera þér kleift að sjá hvaða snjallsamningar veita aðgang að því að eyða tókum þínum. Til að gera það getur þú:

- notað traustan „leyfisskoðara“ sem sannreynir hvort notandi eða bálkakeðju- heimilisfang hafi heimild til að framkvæma aðgerð.
- skoðað skrána yfir veitt samþykki, og
- notað hnappinn „afturkalla“ á vettvanginum sjálfum.

Færðu fjármuni þína

Ef veskið þitt er í hættu skaltu strax flytja það sem eftir er af eignum þínum í nýtt öruggt veski.

Hafðu samband við þjónustuveitanda sýndareigna þinna

Upplýstu sýndareigna þjónustuveitandann þinn eins fljótt og auðið er í gegnum viðurkenndar samskiptaleiðir til að kanna mögulega valkosti. Jafnvel þótt í flestum tilfellum sé ekki hægt að bakfæra viðskipti með bálkakeðju gæti veitandinn samt fryst reikning svikarans (ef hann er á vettvangi veitandans) og fært veskið á svartan lista.

Tilkynntu og varaðu aðra við

Tilkynntu atvikið til lögreglu og láttu tengslanet þitt (t.d. vini og fjölskyldu) vita til að auka vitund. Það er besta leiðin til að vernda þig og aðra.

Varaðu þig á „endurheimtarsvikum“

Svikarinn getur haft samband við þig sem fórnarlamb fyrri svika og þóst vera opinbert yfirvald (t.d. lögregla, skattayfirvöld eða fjármálayfirvöld o.s.frv.) og boðist til að endurheimta tapaða peninga þína gegn gjaldi. Þetta er oft önnur tilraun til að svindla á þér. Mundu: að það að hafa verið svikinn einu sinni kemur ekki í veg fyrir að þú verðir svikinn aftur.

Skoðaðu viðvörun vegna sýndareigna frá sameiginlegu evrópsku eftirlitsstofnununum til að fá frekari upplýsingar um áhættuna sem tengist sýndareignum (↖) og upplýsingablaðið „Sýndareignir útskýrðar: Hvaða þýðingu hefur MiCA fyrir neytendur“ (↖).

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 978-92-9407-274-0 doi:10.2853/0657822 DZ-01-25-162-IS-N

TEGUNDIR SÝNDAREIGNASVIKA

Svikin „Pump-and-dump" eða „Rug pull"

Þú sérð auglýsingu á samfélagsmiðlum eða vefsíðu sem auglýsir „tímabundið fjárfestingartækifæri" í sýndareign þar sem mælt er með því að fjárfesta í nýjum sýndareignatóka eða-verkefni. Eftir að þú hefur sýnt áhuga er haft samband við þig og þér vísað á sýndareignavettvang eða skilaboðarás (t.d. símskeyti, Viber eða WhatsApp). Tengiliður sem virðist trúverðugur hefur samband og lofar skjótum hagnaði eða mikilli ávöxtun ef þú fjárfestir strax. Þú ert hvattur til að fjárfesta með lágri upphæð og síðan þrýst á að þú fjárfestir meira.

Hvað gæti gerst:

Þú uppgötvar að tókinn sem þú fjárfestir í er verðlaus og tengiliðurinn sem þú varst í sambandi við hættir að svara. Þegar þú reynir að taka út peningana þína er vefsíðan ekki lengur til og fyrirtækið er óaðgengilegt. Svikarar hafa blásið upp eða ýkt verðmæti verðlítillar sýndareignar til að auka verðgildi hennar tímabundið (pump), síðan selt eignir sínar (dump), sem veldur því að verðgildið hrynur og fjárfestar sitja eftir með tap. Önnur útfærsla er að þeir loka verkefninu og hverfa á brott með fjármunina (rug pull).

Auðkennisþjófnaður

Eftir að þú hefur sent spurningu á samfélagsmiðil eða vefsíðu um vandamál með sýndareignaveski færðu óvænt einkaskilaboð eða tölvupóst frá einhverjum sem þykist vera traustur aðili (t.d. viðskiptavettvangur fyrir sýndareignir, vörsluaðili sýndareigna, þjónustuaðili á sviði upplýsingatækni eða jafnvel vinur). Einstaklingurinn biður um fræorðin þín (þ.e. röð orða sem tryggja aðgang að stafræna veskinu þínu), lykilorð eða einkalykla (sjálfkrafa myndaður dulkóði sem sannar eignarhald á stafrænum eignum).

Hvað gæti gerst:

Eftir að þú hefur deilt fræorðunum þínum, lykilorðum eða einkalyklum notar svikarinn þá til að stela sýndareignum þínum eða öðrum fjármunum. Hafðu í huga að það að tapa einkalyklum leiðir til varanlegs og óafturkræfs taps á aðgangi að og eignarhaldi á sýndareignum þínum. Ólíkt bankamillifærslum, er nánast ómögulegt að endurheimta fjármuni þegar þeir hafa verið fluttir í formi sýndareigna.

Vefveiðar

Þú færð óvænt skilaboð með tölvupósti, síma, sprettiglugga eða á samfélagsmiðlum sem látið er sem að séu frá þekktum þjónustuveitanda sýndareigna. Með skilaboðunum er þér boðið að skrá þig inn eða hlaða niður nýju forriti. Þú gætir líka fengið tölvupóst sem virðist vera frá sýndareignaveskis forriti þínu þar sem þú ert hvattur til að leysa öryggisvandamál með því að smella á tengil með óstaðfestan uppruna eða með því að uppfæra forritið.

Hvað gæti gerst:

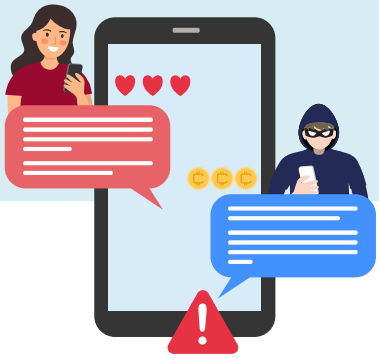
Með því að smella á hlekkinn, hlaða niður forritinu eða skanna QR -kóða setur þú upp spilliforrit sem gerir svikaranum kleift að fá aðgang að upplýsingum og nota þær til að stela sýndareignunum þínum eða fjármunum.

Gjafaleikjasvik

Þú rekst á tilkynningu á samfélagsmiðlum þar sem því er haldið fram að fyrirtæki gefi frá sér sýndareignir í skiptum fyrir litla sýndareignafjárfestingu. Tilkynningin inniheldur myndband eða færslu með myndum af frægum einstaklingi eða vörumerki – oft falsað eða notað án heimildar – sem lofar að „tvöfalda sýndareign þína“ ef þú sendir peninga fyrst. Merkið, útlitið, umsagnirnar og orðalagið sem notað er virðist faglegt og opinbert, sem og vefsíðan sem þér er beint á.

Hvað gæti gerst:

Eftir að hafa sent sýndareign þína færðu ekkert í staðinn og þú hefur tapað sendum peningum. Gjafaleikurinn var svik og færslan eða streymið þar sem líkt var eftir frægu fólki eða fyrirtæki var gert til að blekkja þig.



Rómantísk fjárfestingarsvik

Það hefur verið haft samband við þig í gegnum samfélagsmiðla, stefnumótaforrit eða með síma/smáskilaboðum 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 beinist samtalið að peningum eða fjárhagslegum tækifærum, svo sem sýndareignarfjárfestingum þar sem lofað er miklum hagnaði og lítilli áhættu. Viðkomandi biður þig 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 búa til falska aðganga og nota stolnar myndir eða myndir búnar til með gervigreind til að komast í samband við þig.

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 þurft að taka á þig ábyrgð fyrir skuldum eða glæpum sem framdir eru í þínu nafni þar til annað hefur verið sannað).

Ponzi-kerfið

Þér er boðið að taka þátt í verkefni þar sem lofað er stöðugri og mikilli ávöxtun með sýndareignafjárfestingum, oft studdum með vitnisburðum eða fölskum sögum um velgengni. Áætlunin getur verið kynnt sem fjölþrepa markaðssetning, þar sem þú færð verðlaun ekki aðeins fyrir eigin fjárfestingu heldur einnig með því að fá aðra með. Fyrstu fjárfestarnir virðast fá útborganir, sem hvetur fleiri til að taka þátt og kynna kerfið.

Í raun og veru er engin raunveruleg starfsemi eða hagnaður myndaður. Þess í stað eru peningarnir eingöngu tilkomnir vegna framlags nýrra fjárfesta sem nýttir eru til að greiða ávöxtun til skipuleggjenda kerfisins og fyrstu þátttakenda.

Hvað gæti gerst:

Þegar hægir á nýjum fjárfestingum hrynur kerfið og þú, eins og flestir þátttakendur, tapar peningunum þínum. Skipuleggjendur hverfa, þannig að engin leið er að endurheimta fé. Fjölþrepa markaðssetningin stuðlar að hraðri útbreiðslu svindlsins, þar sem fórnarlömb verða óafvitandi skipuleggjendur.

Tvífara veskisfang sem spillir færslusögunni í veskinu þínu

Eftir að þú hefur átt sýndareignaviðskipti tekur þú eftir nýju veskisfangi (reikningsnúmeri) sem birtist í veskissögu þinni. Þetta veskisfang lítur út eins og það sem þú hefur áður átt viðskipti við. Svindlarar geta látið fölsuð veskisföng birtast í viðskiptasögu þinni með því að senda örlítið magn af sýndareign frá svipuðu veskisfangi í veskið þitt. Þú endar með því að geyma falska veskisfangið sem svikarinn hefur búið til í færslusögu veskisins þíns eða sjálfvirkum tillögum. Svindlarar búa vísvitandi til veskisföng sem líta út fyrir að vera rétt með því að breyta aðeins nokkrum stöfum, oft í miðju veskisfangsins, til að fölsunin uppgötvist ekki.

Hvað gæti gerst:

Þegar þú reynir að senda sýndareign og afritar rangt veskisfang úr veskissögu þinni sendir þú óafvitandi fé í veski svindlarans. Vegna þess að sýndareignarviðskipti eru oft óafturkræf tapast fé þitt í flestum tilvikum varanlega. Þetta svindl byggir á sjónrænum blekkingum og notandavillum og nýtir sér þann vana að afrita og líma veskisföng án nákvæmrar skoðunar.