Romanssihuijausten verkossa -podcast kausi 2, jakso 3: Onko romanssihuijaus kyberuhka? – tekstivastine

00:00:00
[tangomusiikkia]

00:00:13
Janina: Tervetuloa Romanssihuijausten verkossa -kakkoskauden pariin. Tällä kaudella syvennytään romanssihuijauksen ilmiöön asiantuntijavieraiden kanssa, ja saadaan käytännön tason suojautumiskeinoja romanssihuijauksilta. Luvassa siis tietoa ja turvataitoja.

00:30:00
Janina: Tänään meillä on täällä vieraana kyberturvallisuuskeskukselta Samuli Könönen, tervetuloa. Millä fiiliksellä oot tänään täällä?

00:00:41
Samuli: Tosi kivaa päästä tänne mukaan keskustelemaan vähän romanssihuijauksista näin niinku kyberturvallisuuden näkökulmasta.

00:00:46
Janina: Just näin. Hei meillä on ollut tässä tapana heti alkuun kysyä kaikilta vierailta, että minkälaisia ajatuksia sana ”romanssihuijaus” sinussa herättää?

00:00:56
Samuli: Heti ekana mulla tulee mieleen ”romanssihuijaus”-sanasta sellainen, että olisiko joku ehkä romanssipetos kuvaavampi. Jos tavallaan huijauksesta voi tulla mieleen, että se on vähän jotenkin vähäpätöisempi - joku niinku jekkuilu tai tällainen - vaikka kyseessä on kuitenkin niinku vakavat rikokset, jotka vaikuttaa tosi isosti uhreihin.

00:01:14
Janina: Siis nimenomaan hyvin kuvattu, että huijauksesta saattaa nimen nimenomaan tulla jotain muitakin mielleyhtymiä kuin se, että on kyseessä niinku oikeasti vakava rikos. Ja poliisihan käyttää termiä rakkauspetos.

00:01:29
Samuli: Joo.

00:01:29
Janina: Mutta sitten tavallaan en tiiä… Ehkä sitten romanssihuijaus on vähän niinku tälleen puhekielessä tai arkikielessä niinku.

00:01:35
Samuli: Niin ja kyllä se huijaus kuitenkin kuvaa sitä, että siinä uhria huijataan.

00:01:38
Janina: Niin, kyllä. Mutta hei ennen kuin mennään syvemmin tähän ilmiöön, niin olisi kivaa nytten kuulijoillekin kertoa vähän lisää siitä, että mistä sä tuut ja mikä sun tehtävä on täällä kyberturvallisuuskeskuksella?

00:01:54
Samuli: Joo. Mä oon tietoturva-asiantuntija Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksessa, ja mä työskentelen siellä meidän CERT-toiminnossa. Voi olla joillekin tuttu, mutta tarkoittaa siis Computer Emergency Response Teamia, ja me käsitellään erilaisia tietoturvaloukkauksia ja autetaan uhreja tapausten selvittämisessä ja jatkotoimenpiteissä.

00:02:16
Janina: Vau mitä työtä ja tosi tärkeetä. Miten pitkään tätä työtä on tehty?

00:02:20
Samuli: No tälleen niinku CERT-toiminta Suomeen on perustettu 2000-luvun alussa, ja se Kyberturvallisuuskeskus sitten varsinaisesti on perustettu vuonna 2014 Suomen ensimmäisen kyberturvallisuusstrategian seurauksena.

00:02:34
Janina: Tosi hienoa ja tosi tärkeetä nimenomaan tässä ajassa, että on tällaista toimintaa.

00:02:38
Samuli: Kyllä.

00:02:40
Janina: Joo. No vielä vähän mennään syvemmälle siihen teidän toimintaan - jos nyt kuulijat vaikka ensimmäistä kertaa kuulee ylipäätänsä tällaisesta toimijasta - niin sä kerroit siitä sun yksikön tehtävistä, mutta mitä muuten niinkun laajemmin sitten silloin 2014, kun tää perustettiin tää keskus, niin mihin… Missä kaikessa te autatte?

00:03:00
Samuli: No se on ihan totta, että me tehdään paljon erilaista työtä. Ja kaikessa meillä on tavoitteena niinku toimiva ja turvallinen digitaalinen yhteiskunta, että meillä on tota… Luottamuksellista ja maksutonta avustamista tietoturvaloukkauksiin. Sen lisäksi on erilaisia yhteistyöhankkeita julkisen ja yksityisen sektorin kanssa, missä edistetään yhteiskunnan tietoturvaa.

00:03:21
Janina: Kyllä. Ja sitä tarvitaan, koska kaikki palvelut on melkeinpä siirtyneet tuonne digimaailmaan. Ja koko ajan maailma niinku tuntuu siirtyvän sinne melkein kaikessa niinku palveluissa ja toiminnoissa niin.

00:03:36
Samuli: Kyllä, maailma muuttuu nopeasti ja kaikkien pitää pysyä mukana. Ja me tuotetaankin paljon tietoa, myös ajankohtaista tietoa kyberturvallisuudesta. Esimerkiksi meidän Kybersää, kuukausittainen katsaus siihen, mikä on tapahtunut, voi olla monille tuttu. Ja sitten meidän verkkosivuilla on paljon erilaisia ohjeita ja oppaita ihan yksittäisille ihmisille ja organisaatioille, että miten voivat parantaa omaa tietoturvan tasoaan. Ja sitten myös toimintaohjeita niinkun tietoturvaloukkaustapauksissa.

00:04:03
Janina: Tosi tärkeetä. Me laitetaan tähän jakson bion kuvaukseen kaikki teidän noi osoitteet, että kuulijat pääsee sitten tarkistamaan vaikka sen Kybersään ja muuta. Toi on kyllä hauska keksintö, toi Kybersää. Mennään sitten jakson aiheeseen. Puhutaan vähän näistä kyberuhista, minkälaisia kyberuhkia on olemassa?

00:04:10
Samuli: Loistavaa. No niitä on tosi paljon erilaisia niinku tuli esille, että kaikki yhteiskunnan toiminnot pikkuhiljaa siirtyy verkkoon. Internetin kautta voi asioida yhä enemmän erilaisissa palveluissa, niin nää niinku uhkatkin lisääntyy. Sitten ne tuolla on vähän erilaisia. Millaisia uhkia kohdistuu niinku yksittäiseen ihmiseen tai sitten organisaatioihin?

Yksi yleisimpiä on erilaiset tietojenkalastelut: Huijaukset, joissa tällaisia viestejä - varmaan kaikki meistä on saanut - missä on vaikka että ”verkkopankissa ongelma, klikkaa tästä” tai joku ”pakettisi toimitus viivästyy, eli klikkaa tästä”, ja sieltä linkin takaa sitten aukeaa sivusto, joka on rikollisten hallussa ja siellä houkutellaan antamaan esimerkiksi verkkopankkitunnukset, joita sitten rikolliset pyrkii hyväksikäyttämään. Nää on valitettavan yleisiä, ja ne on just tätä, että ihmiset on tottunut asioimaan verkossa ja siihen väliin rikollisetkin yrittää sit päästä rahanansainta mielessä.

00:05:15
Janina: Kyllä. Toi on niinkun hyvin konkreettinen ja varmaan aika arkinen esimerkki, että moni kuulija varmaan nyt siellä nyökyttelee tällä hetkellä, että on saanut monenlaisia tekstiviestejä tai niinkun sähköpostiviestejä jonkun toisen ikäänkun organisaation nimellä. Ja sitten kun meidän maailma on niin nopea ja meiltä vaaditaan nopeita reaktioita, niin sitten saattaa olla että on sillee et ei kato niinku tarkemmin ja painaakin jo että ”okei” ja menee eteenpäin.

00:05:31
Samuli: Kyllä, just näin, että niitä lähetetään usein tosi laajalle vastaanottajakunnalle, niin vaikka suurin osa saattaa huomata että ”ei, ei mulla ole tällaista”. Mutta sitten kun sattuu tulemaan just kiireen hetkellä henkilölle, ja nopeasti aamukiireessä vaikka töihin mennessä ni katsoo että ”mikäs tää on” ja ”nopeasti nyt mä selvitän tässä samalla kun mä syön aamupalaa”, niin sitten oikeastaan kuka tahansa voi tällaiseen langeta.

00:06:06
Janina: Nimenomaan toi oli niin hyvä esimerkki, että siis… Ja ehkä just toi, että kuka tahansa meistä voi niihin langeta, koska ne on niin myös taitavasti tehtyjä. Ja siinä nimenomaan sitten hyväksikäytetään tätä kiireisen nykyelämän meininkiä. Kun voi olla, että joskus niinku oikeastikin tulee nopeasti jotain viestejä ihan oikeitakin toimijoilta ja vaaditaan nopeita vastauksia, niin siinä nää rikolliset on kyllä hyvän ikäänkuin kohdan keksineet. Onko romanssihuijaus niinku merkittävä kyberuhka?

00:06:40
Samuli: No romanssihuijaus on tosi hyvä esimerkki tällaisesta verkkorikollisuudesta. Eli siinäkin hyödynnetään tätä, että ihmiset ja heidän toiminta ja elämä siirtyy yhä enemmän internetiin ja siellä sitten käytännössä kuka tahansa maapallon toiselta puolelta voi olla kehen tahansa yhteydessä. Ja sitä nää romanssihuijaritkin hyödyntää, että heille niinku on ihan maailma auki ja kaikki ihmiset kutakuinkin on internetissä tavoitettavissa, niin niinku potentiaalinen uhrien määrä on tosi suuri.

00:07:08
Janina: Nimenomaan. Kun kaikki muutkin asiat ovat siirtyneet sinne niinku verkkoon, niin myös se deittailu on siirtynyt sinne verkkoon. No mitä sä ajattelet näistä romanssihuijauksen niinku tekijöistä, että toimiiko ne jollain tavalla niinku järjestäytyneesti?

00:07:26
Samuli: No varmaan on tosi paljon erilaisia toimijoita, ja varmaan jotkut näitä niinku itsekseenkin tekee.

Mutta kyllä tää niinku ihan globaalina ilmiönä paljon toteutuu järjestäytyneen rikollisuuden kautta. Joko vähän löyhemmin tai sitten tosi tiukastikin järjestäytyneesti, että se on niinkun… Jopa voisi sanoa niinku yritysmallista toimintaa, missä on hierarkiat ja sitä niinkun massamaisesti toteutetaan ja… Joo, on maailmalla myös tapauksia, missä esimerkiksi ihmiskaupan uhreja käytetään siihen, että he niinkun toteuttaa niitä keskusteluja ja romanssihuijauksia, ja sitten joku sen järjestön ylempi porras ehkä kerää ne voitot.

00:08:09
Janina: Aivan, toi oli todellakin konkreettinen esimerkki siitä, että mikä ei meille tässä niin kun näyttäydy välttämättä. Että mitä kaikkea siellä, niinkun romanssihuijarin ikään kuin taustalla on, että hän voi todellisuudessa olla itse myös ihmiskaupan uhri.

00:08:22
Samuli: Kyllä joo, just tää että mistä tahansa päin maapalloa voi olla.

00:08:26
Janina: Just juuri näin. Mitä sä ajattelet, että onko olemassa jotain niin kun tiettyä maata erityisesti, mistä - tai maanosaa - mistä näitä tehdään?

00:08:38
Samuli: No en osaa sanoa suoraan maanosaa, mutta kyllä tässä taas niinku maailmanlaajuisesti tietysti ehkä enemmän matalamman elintason valtioissa näitä toteutetaan. Että usein henkilöt voi olla niinku heikommassa asemassa muutenkin. Ja tää romanssihuijausten toteuttaminen on sitten se keino, millä voi niinkun saada tuloja ja elää elämäänsä, kun ei muita työllistymismahdollisuuksia välttämättä ole tarjolla.

Tai sitten tää voi olla niinku erityisen kannattava tapa hankkia rahaa, ja se myös sitten näkyy siinä, että mihin näitä huijauksia kohdistetaan, niin useimmin ne on korkeamman elintason maat, missä ihmisillä on enemmän varakkuutta, jota sitten huijata.

00:09:20
Janina: Nimenomaan, hyvin tiivistetty. Mitä sä ajattelet, että no vähän puhuttiinkin tuosta, että huijarit valitsee kohdemaansa sen mukaan, että missä on niinku varallisuutta, niin tarkoittaako se sitä, että Pohjoismaat on heille semmoinen niinkun target, joka on tavallaan kaikille tiedossa siellä tekijöille, että…

00:09:44
Samuli: Niin pohjoismaat on niinku hyvinvointivaltioita ja varakkaita valtioita, niin sieltä huijareiden näkökulmasta ehkä nähdään sitä, että täällä ihmisillä, että se ei ole niin pahaa meille, vaikka sitä rahaa menettäiski. Että täällä on muutenkin korkea elintaso ja on ehkä tukiverkostot, sosiaalitukia tällaista, niin se on ihan tällaista… Niinku haastattelututkimuksessa ne tekijät perustellut sitä, että eihän sen väliä niinku rikkaassa maassa elävälle ihmiselle paljon mitään, vaikka mä sitten vähän huijaankin, että kyllä se siellä pärjää silti.

00:10:10
Janina: Toi olikin hyvä pointti, että he tavallaan sillä lailla oikeuttaa sen tekonsa. Että he ajattelee, että kyllä nyt voi siitä muutaman siivun itselleen ottaa, kun siellä on sitä hyvinvointia. Mutta se mitä heille ei sitten näyttäydy on se, että minkälaiseen ikäänkun turbulenssiin nää joutuu sitten nää romanssihuijauksen kokijat.

00:10:33
Samuli: Joo usein nää samat tahot niinku tekee monenlaisia huijauksia, että romanssihuijaus voi olla vaan yksi siellä, niin se on tuossa työkalupakissa ja sitten erilaiset etukäteismaksuhuijaukset verkossa, että on paljon rahaa tulossa, mutta ensin sun pitää vähän lähettää rahaa tänne, niin saattaa toteuttaa samanlaisia näitä samanlaisia… Tai siis erilaisia huijauksia. Ja ei sitten sieltä tekijän näkökulmasta tää romanssihuijaus ei ole kovin erilainen, että kaikesta tulee rahaa, mutta sitten uhrin näkökulmasta tietenkin tällainen tosi yksityinen ja intiimi aihe tai teema, niin tekee siitä huijauksesta niinku erityisen kivuliaan.

00:11:07
Janina: Siis nimenomaan hyvin sanoitettu, että tää on nimenomaan intiimirikos. Ja vaikka nää tekijät ikään kuin oikeuttaa tätä toimintaansa sillä, että ajattelevat että tää nyt menee siinä missä muutkin huijaukset tässä, niin he ei tavoita sitä, että minkälaiseen inhimilliseen kärsimykseen sitten tää kokija joutuu, että kokija joutuu toipumaan pitkään taloudellisesti, mutta myös henkisesti.

00:11:34
Samuli: Kyllä. Sen lisäksi se fyysinen etäisyys, ja vähän niinku internet siinä tekijän ja uhrin välissä, niin entisestään eristää tekijöitä siitä niinku uhrista ja niistä vaikutuksista, mitä tulee.

00:11:46
Janina: Kyllä. miten nää tekijät niinku valitsee nää ikään kuin uhrinsa vai voiko puhua sellaisesta, että he jotenkin etukäteen valitsee tai kalastelee tietoja?

00:11:58
Samuli: No kyllä niitä varmasti esim. sosiaalisessa mediassa kun lähestytään, niin jollain tavalla niitä profiileja valikoidaan mihin ollaan yhteydessä. Mutta todennäköisemmin tässäkin luotetaan niinkun massaan, eli näitä tavallaan ensimmäisiä yhteydenottoja lähetetään varmaan tosi tosi monille, ja sitten sen perusteella miten henkilö vastaa, niin lähdetään ehkä kehittämään sitä huijausta just siihen henkilöön osuvamman hänen profiilissaan ilmi olevien kiinnostuskohteiden ja muiden osalta.

Mutta tää, että kun kyseessä on täällä massainen huijaaminen, niin mä veikkaisin, että sellaista niinku etukäteistä valmistelua ei tehdä niin paljon. Koska sitten jos se henkilö vaikka ei ollenkaan vastaa siihen ensimmäiseen yhteydenottoon, niin se kaikki valmisteluaika on mennyt hukkaan.

00:12:42
Janina: Kyllä, aika on rahaa heille sielläkin.

00:12:46
Samuli: Niin kyllä.

00:12:48
Janina: Minkä takia nää romanssihuijauksen tekijät on niin taitavia teknologisesti?

00:12:53
Samuli: No mä en oikeastaan tiedä, että onko se niin teknologisesti välttämättä taitavia. Että niinku sanoin, niin usein on järjestäytynyttä rikollisuutta taustalla, niin voi olla, että sieltä… Siellä on tietenkin joku osa sitä organisaatiota, joka teknisesti pystyy rakentamaan heille järjestelmät. Mutta sitten se tyyppi, joka näpyttelee niitä viestejä sinne chattiin ja tavallaan toteuttaa sitä huijausta, niin sille henkilölle tärkeimpiä on sitten ehkä niinku sosiaaliset taidot ja tällainen niinku tilanteen lukutaito ja manipulointi, jolla sitten saa sen uhrin uskomaan niitä viestejä.

00:13:26
Janina: Joo, hyvin pilkottu tavallaan tota ajatusta siitä, että siellä on monta henkilöä nimenomaan. Ja ikään kuin he sitten toimii sillä perusteella, että mihinkä heillä on niitä omia taitojaan, ja nimenomaan tuo, että siinä tarvitaan sitä sosiaalista niinku tilannelukutaitoa ja sitä sosiaalista manipulointia.

00:13:46
Samuli: Kyllä. Että kun nää romanssi workshopit ei ole tällaista perinteistä hakkerointia, missä jotain järjestelmää ja ohjelmistokoodia niinku rikotaan, vaan tässä se huijaus kohdistuu ihmiseen ja hänen psykologiaan, inhimillisiin tarpeisiin.

00:14:00
Janina: Just näin. Miten sitten, onko tekoälyä hyödynnetty romanssihuijauksissa? Tiedätkö siitä?

00:14:07
Samuli: No mä en tiedä niinku tapauksista missä sitä olisi hyväksikäytetty tai hyödynnetty romanssihuijauksissa, mutta kyllähän tää niinku tekoäly ja näiden laajojen kielimallien niinku ChatGPT, mitä on viime vuosina tullut esille, niin niiden niinku kehitys on tosi huimaa, ja niinku nopeasti tavallaan saa ideoita, että ”hei tätä mihin kaikkeen tätä voisi hyödyntää”, ja romanssihuijaukset on varmaan yksi potentiaalinen siinä.

Mutta ehkä tällä hetkellä vielä nää teknologiat on kuitenkin sen verran kehitysvaiheessa, että niiden niinku laajempi käyttöönotto on vielä kesken. Ja myös se, että monessa tapauksessa on kuitenkin edullisempaa niinkuin heikossa asemassa olevia ihmisiä käyttää työvoimana kuin sitten että käyttäisi tekoälyä, ja rikollisilla kuitenkin on niinku tavoitteena rahallinen hyötyminen sitten. Miten se kaikista helpointa ja tehokkainta on, niin monessa tapauksessa se tekoälyn käyttöönotto ei ainakaan vielä välttämättä niinku ole heille kannattavaa.

00:14:49
Janina: Aivan, kyllä. Puhutaan vähän lisää tuosta tekoälystä. Haluan avata sitä kuulijoille, eli mitä se tekoäly tarkoitti? Tällanen pieni kysymys.

00:15:12
Samuli: Se on kyllä hyvä kysymys, ja tänä päivänä tota tekoäly-sanaa käytetään tosi paljo tarkottaa tosi eri asioita. Mutta vaikka nää mistä mainitsin, nää laajat kielimallit, ne on ehkä se tänä päivänä kaikista näkyvin niinku tekoälyn osa-alue mitä usein tarkoitetaan, kun puhutaan tekoälystä. Ja nehän on sinällään… Vaikuttaa ihmismäisiltä, kun ne pystyvät tuottamaan tekstiä ja ymmärtämään niille annettua tekstiä. Ja jopa saattaa olla jotain, jotka niinku ääneen puhuu ja heille voi kans äänellä puhua.

Ja en ole näiden laajojen kielimallien asiantuntija, mutta mun ymmärrätääkseni niin ne hyvin pitkälti ennakoi ja yrittää miettiä, että mikä sana voisi tulla tähän seuraavaksi. Ja ne on sitten koulutettu niin isoilla määrillä tekstisisältöä esimerkiksi internetistä, jolloin käytännössä aiheeseen kuin aiheeseen, niin sieltä heidän opetusdatastaan löytyy jonkunlaisia esimerkkejä, joita hyödyntämällä ne sitten pystyy tuottamaan uudelta vaikuttavaa tietoa.

00:16:10
Janina: Joo hyvä hyvä tiivistys. Onko tähän niinkun… Onko tekoälyn tavallaan keksijöille mitään eettistä vastuuta siinä, että jos näitä aletaan hyödyntämään rikollisessa toiminnassa?

00:16:24
Samuli: Niin, tekoäly on teknologia siinä missä muutkin ja on nytten näissä uusimmissa niin jotkut verrannut vaikka sosiaaliseen mediaan tai jopa ydinaseisiin, että uusi tällainen teknologia tuo aina toki jotain vastuuta ja jotain niinkun riskejä siinä missä myös mahdollisuuksia. Ehkä mä näkisin, että tekoälyn suhteen jos miettii, että millä tavalla nyt Euroopan Unionissa ja Yhdysvalloissa on myös lainsäädäntötyötä aloitettu tekoälyn vuoksi, niin osoittaa, että jos vaikka sosiaaliseen mediaan vertaa, niin tää tekoälyn käyttöönotto prosessina niinku ihmiskunnalla kollektiivisesti vaikuttaa menevän enemmän turvallisuus edellä eikä sillä muu ”fast and break things” Facebook-mentaliteetillä.

00:17:06
Janina: Joo. Aivan tuopa oli hyvä kuulla, että siinä on tommoinen lainsäädäntö syntymässä ja sitä niinku viedään eteenpäin. Mitäs sitten, jos vielä jutellaan niin kun siitä, että miten tavallaan tavallinen kuluttaja, niinku somen kuluttaja tai teknologian kuluttaja voi suojautua erilaisilta kyberuhilta?

00:17:31
Samuli: No mä sanoisin, että tässä on niinku muutama sellainen yksinkertainen juttu, että kun ne ottaa haltuun niin sillä pääsee jo tosi pitkälle. Ihan ekana on niinku terve skeptisyys. Tuolla internetissä liikkuu tosi paljon kaikenlaista tietoa. On erilaisia huijauksia, niin kyllä tänä päivänä on vähän se, että kaikkeen pitää suhtautua skeptisesti ja ja niinku miettiä, että mikä tässä on oikeasti takana. Ja sellainenkin vanha viisaus, että jos se on liian hyvää ollakseen totta, niin se ei todennäköisesti ole totta. Ja tää kyllä varsinkin internetissä pätee käytännössä aina.

00:18:05
Janina: Mites sitten kaikki niinkun omien kuvien tai tietojen jakaminen? Onko siihen mitään sellaista kultaista sääntöä, mitä tulisi muistaa?

00:18:15
Samuli: No siinäkin pitää niinku miettiä, että mihin mä näitä kuvia jaan. Että vaikka sosiaalinen media tarjoaa meille tosi hienoja mahdollisuuksia olla yhteydessä meidän ystäviin, ehkä muualla maailmassa jakaa meidän elämää kuvien, videoiden, tekstin kautta. Mutta se on sitten hyvä miettiä, että kenelle niitä jakaa jakaako julkisesti, että kuka tahansa näkee mun profiilista nää kuvat, jaanko mä vaan mun kavereille? No ketä sitten mun kaverilistalla on? Onko mun kaverit sellaisia, jotka mä kaikki oikeasti tunnen, vai onko siellä jotain vähän epämääräisempiäkin tuttuja, mihin ne kuvat saattaa sitten mennä?

Sen lisäksi sitten pitää muistaa se, että vaikka yksityisviestillä joillekin ihmisille kuvia jakaa, niin sitten se henkilö voi niitä myös jakaa eteenpäin, mikä ehkä erityisesti nuorille on sellainen vinkki, että kannattaa miettiä kanssa se, että kenelle haluaa asioitaan jakaa ja kuvia ja niinku tietoa itsestään internetissä.

00:19:08
Janina: Kyllä. Onko jotain keinoa tunnistaa niinku valeprofiili?

00:19:13
Samuli: Sellaista niinku varmaa keinoa ei ole, koska niitä keinojahan myös ne valeprofiilin tekijät tietää ja yrittää tehdä niistä luotettavia. Mutta aika usein somessa, se että tarkastelee vaikka että milloin se profiili on luotu. Ja jos se on tosi uusi, niin se ehkä voi kieliä, että tää on nyt hiljattain tehty, että mitä varten? Sitten vähän muuten että onko sillä profiililla paljon yhteyksiä, kenen kanssa se on ollut yhteyksissä? Ja siitä voi päätellä, että onko tää oikeasti olemassa, tai muuta. Sitten profiilikuvasta voi esim tehdä käänteisen

kuvahaun esimerkiksi Googlen kautta ja sitä kautta katsoa, että onko tää kuva jostain muualta napattu vai? Jos ei löydy mitään tuloksia, silloin se on erityisesti sitä profiilia varten.

00:19:56
Janina: Ja mitäs sitten tavallaan… Voiko nämä valeprofiilin tekijät ostaa niitä seuraajia?

00:20:02
Samuli: No… Tästä mä en tiedä, mutta mäkin oon kuullut sellaisista mahdollisuuksista, että voi ostaa seuraajia. Niissä todennäköisesti on kyseessä se, että joku taho tekee niinku massoittain näitä valeprofiileja, joilla sitten voi tarjota seuraajia maksua vastaan. Näitä sitten sosiaalisen median alustat toki koittaa näitä tällaisia botteja ja muita vaaleja profiileja vastaan taistella, mutta varmaan työnsarkaa riittää.

00:20:29
Janina: Kyllä. Mitä toi botti nyt sitten tarkoittaa? Kun mä oon kuullut monta kertaa, että puhutaan näistä boteista, niin mitä mikä se botti on?

00:20:36
Samuli: Joo, hyvä kysymys koska tää niinku ”botti”-sana ihan huomaamatta täällä siinä lipsahti. Mutta boteilla tarkoitetaan usein niinkun sellaista ohjelmaa, joka automaattisesti toteuttaa jonkunlaista toimintaa. Esimerkiksi sosiaalisessa mediassa tää bottitili voi olla tili, joka automaattisesti tekee tietynlaisia päivityksiä. Ja näitä voi olla ihan niinku hyväntahtoisia botteja, vaikka sometili tämmöiselle säätietobotille, joka joka päivä postaa sinne päivityksen, että ”hei, tänään säätila näyttää tältä”. Mutta sitten niitä botteja voidaan käyttää toki myös niinku pahantahtoisen tarkoitukseen, vaikka väärän informaation levittämiseen.

00:21:15
Janina: Miten tavallaan niinku Kyberturvallisuuskeskusella, että onko nää romanssihuijaukset teille tuttu ilmiö tai oletko sä nähnyt, että ne on jotenkin kasvanut tässä ajan myötä?

00:21:25
Samuli: En osaa sanoa tuosta, että miten ne on kasvanut, mutta meillekin niistä ilmoituksia tulee ihan tasaiseen tahtiin. Usein niissä romanssiksi sekoittuu myös sitten sijoitushuijaukset, nykyään esimerkiksi kryptovaluuttoihin liittyen. Eli ensin saattaa huijari lämmitellä romanttista suhdetta ja sitten sen lisäksi tarjotaan, että ”hei tässä olisi mahtava kryptovaluutan sijoitustilaisuus”, ja todellisuudessa rahat sitten päätyy rikollisten haltuun. Sinänsä romanssihuijaukset ei ole niinku meidän ydinaluetta, koska Suomessa poliisi tutkii rikokset ja selvittää niiden tekijät, mutta me tarjotaan neuvontaa ja apua ja esimerkiksi tän rikosilmoituksen tekoon aina kehotetaan meille ilmoittavia uhreja.

00:22:05
Janina: Hyvä kun nostit vielä ton niinku sijoitushuijauksen tähän vielä, että se on myös jotain mitä me ollaan huomattu, että nää tekijät - romanssihuijauksien tekijät - kyllä hyödyntää sitä, ja nimenomaan näitä kryptovaluuttakeissejä.

00:22:20
Samuli: Kyllä. Nekin on sellainen niinku uusi teknologia, mikä on ihmisille ehkä vähän tuntemattomampi, niin siinä myös sitten huijareilla voi olla enemmän niinku pelivaraa, että minkälaisia väitteitä hän niistä kryptovaluutoista esittää. Kun sitten niinku perinteiset osakemarkkinat tai sijoittaminen on ehkä ihmisille tutumpia ja helpommin sitten tunnistaa sen, että nyt tää vaikuttaa kyllä vähän epäilyttävältä.

00:22:44
Janina: Nimenomaan. Kerrotaan vielä tähän loppuun, että mitä on kryptovaluutat?

00:22:51
Samuli: Joo. No tää on… Taas ei ole mun ykkösasiantuntija aihe, mutta kryptovaluutat on siis tällaiseen lohkoketjuteknologiaan perustuvia elektronisia valuuttoja. Ja se lohkoketju on käytännössä monimutkaisia matemaattisia yhtälöitä, joita tietokoneella lasketaan ja siten sitten siinä ketjussa pystytään varmistamaan, että ne kaikki kuuluu siihen samaan. Ja näiden kryptovaluuttojen niinkun ykkösmyyntivaltti on oikeastaan se, että niitä ei käytännössä kovin helposti pysty jäljittämään jos verrataan muihin valuuttoihin, kuten euroihin ja dollareihin, ja sen takia kryptovaluutat on muutenkin rikollisten suosiossa.

00:23:31
Janina: Kyllä, erittäin hyvä tiivistys vielä siitä ja kuulijoille lisää tietoa. Ennen kuin pistetään nauha poikki, niin haluatko sanoa kuulijoille vielä jotain teidän toiminnasta tai muuten tästä ilmiöstä?

00:23:46
Samuli: No kyllä mä sanoisin sen, että internetissä kun tulee viestejä, tulee jotain tietoa vastaan, joku somepostaus, ihan mitä tahansa, niin sellainen, että mitä vahvempia tunteita itsessä herää - on sitten positiivisia tai negatiivisia, paniikki, ilo - niin tavallaan mitä vahvempia ne tunteet on, niin sitä selvempi merkki se on, että nyt aikalisä. Mistä tässä on kyse, haluaako joku ehkä aiheuttaa mulle paniikkia? Haluaako joku vietellä mua? Ja se on niinku merkki, että nyt pitää miettiä ja vaikka jollekin läheiselle näyttää, että ”hei mitäs mieltä sä oot tästä? Miltä tää sun mielestä näyttää?”, koska sitten yhdessä on helpompi tunnistaa, että joo tää nyt vaikuttaa epäilyttävältä.

00:24:24
Janina: Erittäin hyvä vinkki kaikille kuulijoille ja miksei myös itsellekin. Kiitos Samuli, että olit täällä vieraana.

00:24:28
Samuli: Kiitos. Tää oli oikein mukavaa.

00:24:32
Janina: Kiitos myös kuulijoille, että kuuntelitte tän jakson loppuun asti, ja ihanaa päivän - tai illan tai mikä onkaan se aika, koska tän kuuntelet - niin jatkoa sinne ja ollaan taas kuulolla pian.

00:24:52
Janina: Olet juuri kuunnellut Romanssihuijausten verkossa -podcastin jakson. Koskiko jaksossa käsitellyt asiat sinua? Epäiletkö romanttista viestittelykaveria? Nettideittiturva-tukipalvelut voivat auttaa. Lisää tietoa osoitteesta nettideittiturva.fi. Romanssihuijausten verkossa on Nettideittiturva-hankkeen tuottama podcast. Sosped-säätiön ja Maria Akatemian tuottamaa hanketta rahoittaa STEA.