Romanssihuijausten verkossa -podcast kausi 2, jakso 5: Kyberhygienian ABC – tekstivastine

00:00:00
[tangomusiikkia]

00:00:15

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

00:00:29

Janina: Hei tervetuloa taas kuulolle. Täällä ollaan uuden jakson parissa, ja tänään mulla on täällä studiolla kaksi upeaa vierasta. Haluatteko esitellä itsenne?

00:00:40

Laura: Toki toki. Mun nimi on Laura Kankaala. Toimin F-Securella kyberuhkatiedustelun päällikkönä, eli keskityn uhkiin mitä ihmiset kohtaa, kun he elävät elämäänsä internetissä. Ja tota mun tausta on pitkälti tämmöisessä teknisessä tietoturvassa. Oon tehnyt tämmöisenä niinkun tietoturvakonsulttina hakkerointijuttuja: Hakkeroinut yrityksiä, heidän järjestelmiään, prosesseja ynnä muita, ja yrittänyt etsiä haavoittuvuuksia ennen kuin joku ikävämielinen voi sitten käyttää niitä hyväksi. Mutta tosiaan nykyään sitten F-Securella, ja tota toki pitkälti tää mun tausta auttaa myös tässä, että ymmärtää että mitä meistä jokainen kohtaa internetissä, kun me yritetään elää turvallista - tai no jotkut vähän turvattomampaa elämää, mutta kuitenkin niin tota… Niinkun silleen saanut ilon ja kunnian tehdä hyvin niinku monen näköistä ja erilaisia asioita tässä niin kun IT-uralla ja vielä kohdennetusti tietoturva-alalla.

00:01:40

Janina: No niin, mahtavaa että oot täällä ja odotan innolla, että päästään vielä syventymään myös näiden aiheiden pariin, mutta sitten meillä on myös täällä toinen vieras.

00:01:50

Riku: Jes, elikkä Juurikon Riku. Mä toimin Elisalla varautumis- ja resilienssiasioiden kehittäjänä. Tuolla tota… Katsotaan meidän liiketoiminnan jatkuvuuden perään. Ja sitten jos meillä tulee erilaisia häiriötilanteita sun muita, niin miten me voidaan niistä toipua ja ylipäätään ennaltaehkäistä näitä. Ja mulla taas on taustaa tuolta… Mä oon ennen kyberuralle siirtymistä ollut tuolla niin kun fyysisen turvallisuuden puolella ja silleen ihmisten kanssa tekemisissä niin sanotusti, vähän erilaisessa turvallisuusympäristössä. Se on sitten myös ollut itselle semmoinen, kun mä siirryin sinne kyberin puolelle, niin kyberissä myös toimitaan paljon ihmisten kanssa. Ja mä oon myös ollut tekemässä tämmöisiä hyökkäyksiä yrityksiä kohtaan, kuten Laurakin, ja tota… Mun erikoisosaamista siinä on taas ollut tämä niinkun ihmisiin vaikuttaminen. Eli kun tästä huijauksesta nyt puhutaan, niin mä oon tavallaan myös ollut tekemässä näitä huijauksia, niinkun kohdehyökkäyksinä yrityksiä kohtaan…

00:02:50

Laura: Laillisesti!

00:02:51

Riku: Niin kyllä laillisesti, ja näin näihin siis tota tähdennettyihin… Näihin on aina ollut niinku luvat sieltä kohteelta, ja näissä ollaan tehty niinkun koulutusmielessä näitä hyökkäyksiä. Ja ollaan haluttu oppia sitten, ja tunnistaa kehityskohteita näissä yritysten turvallisuusprosesseissa ja näin. Mutta semmoinen niinkun tausta meikäläiselle tähän keskusteluun. Ja sitten toki tää operaattorikulma, että mä toimin siellä... Meillä on tämmöinen niinku ”anti-fraud task force” siellä. Me katsotaan minkälaisia erilaisia huijauksia tuolla verkossa näkyy, ja miten me pystytään viestinnällisin tavoin meidän asiakkaille - ja sit toisaalta mahdollisin teknisin keinoin - reagoimaan erilaisiin huijauksiin. Joihinkin me pystytään tehdä asioita ja jotkut on sitten enemmän tämmöisiä viestinnällisiä keinoja.

00:03:40

Janina: Aivan. Siis ihan todella mahtavaa, että olette molemmat täällä. Teillä on tuollaista niin syvää asiantuntijuutta ja jotenkin mä kuulen, että molemmat kuitenkin sen turvan näkökulmasta myös katsoo tätä asiaa, josta nyt tänään puhutaan. Niin mä haluankin kysyä teiltä molemmilta, että mitä teille tulee niinkun sanasta ”romanssihuijaus” mieleen?

00:04:00

Laura: Kyberrikos.

00:04:03

Riku: Mulle kanssa hyvin vahvasti, että nää romanssihuijaukset nykypäivänä on siirtynyt hyvin pitkälti tonne verkkoon, että tämmöinen ehkä vanha perinteinen, jotenkin suomalainen tuttu Auervaarahan on niinku tämmöinen klassikko romanssihuijari, mistä täällä on jo puhuttu aikaisemmin mahdollisesti ja tota… Mutta nykyään noi Auervaarat on siirtynyt tuonne verkkoon, ja siellä sitten näitä petoksia tehtaillaan mitä enenevissä määrin ja siellä on miljardibisnestä kansainvälisesti.

00:04:16

Janina: Kyllä.

00:04:32

Laura: Niin, se on just tähän Auervaaraan - mä en ihan muista sen detskuja - mutta tässä kun puhutaan nykymaailman näistä romanssihuijauksista - ja nyt vaikka puhutaan huijauksesta, niin tosiaan haluan painottaa että rikos ja petoshan siinä on kyseessä - niin näähän skaalautuu helpommin. Sä voit tehtailla näitä ihan toiselta puolelta maailmaa, että se on ihan eri tavalla läsnä se mahdollisuus meidän elämässä ihan silloin kun me etsitään rakkautta netistä, tai vaikka ei etsitäkään, niin joku voi ihan tosi superhelposti lähestyy meitä just vaikka Facebookin kautta, deittisovelluksen kautta, pelisovelluksen kautta, ihan jonkun… Kerran kuulin, että jonkun liikuntasovelluksen kautta! Niin ja Whatsapp, ja mä meillä on niin paljon kaikkea netissä että…

00:05:20

Riku: Ja kaikki on koko aika netissä.

00:05:21

Laura: Joo. Ja silleen että ei ole semmoista maailmaa enää että ”hei mä en käytä internetiä”, että vaikka olisi vaan lankapuhelinkin niin… No okei, ehkä tämmöisessä voi olla että joku soittaa sinnekin, mutta se lankapuhelin voi tässä tilanteessa suojata jonkun verran. Siis liittyen lähinnä tähän, koska… Tai siis liittyy semmoiseen keskusteluun, kun jotkut ihmiset ajattelee, että kannattaako enää olla internetissä tai että mitä järkeä on olla internetissä, kun siellä on jatkuvasti kaikennäköisiä ongelmia tai yksityisyyden loukkaamista ynnä muuta, niin ei meillä ole sellaista maailmaa varsinaisesti missä me ei tavalla tai toisella olla internetissä.

Että vaikka me ei suoraan itse käytettäisi sitä, niin voi olla että joku muu postaa meistä jotain internettiin, tai sitten kun me mennään julkisella johonkin tai käydään sairaalassa, ostetaan kaupasta jotain, niin meistä jää niinkun dataa jollekin serverille. Että okei, se ei nyt ehkä ihan superpaljon liity näihin romanssinhuijauksiin tässä kohtaa, mut ehkä se mun pointti oli tässä, että joo joku voi soittaa sulle ja tarjota sijoitusneuvoja, mutta ylipäätänsä meidän elämä on jo internetissä, vaikka me ei välttämättä sitä niin kun aina nähdä tai haluttaisi edes.

00:06:22

Riku: Vaikka ei sitä aktiivisesti käytä, niin yritykset joiden palveluita me käytetään, niin käyttää.

00:06:29

Janina: Kyllä. Mites te itse - te olette molemmat alan ammattilaisia - niin oletteko te kohdannut tämmöisiä yrityksiä tai oletteko te huomannut tällaisia tilanteita, missä teitä on yritetty huijata netissä?

00:06:42

Riku: No omalla kohdalla mä ainakin oon vähän niinku harrastanut tällaista, että koska noi huijaritkin kiehtoo mua todella paljon, niin mä haluan oppia niiden toimintatavoista. Ja sitten niinkun miten me pystytään viestimään meidän asiakkaille esimerkiksi että minkälaisia noita toimintatapoja on.

Tässä muutama vuosi sitten oli todella niinkun pinnalla nää tällaiset ”call center” -huijaukset, eli ne soitti yleensä Microsoftina esiintyen. Useimmiten intialaisia soitti ja sanoi, että ”Hello, this is Microsoft calling”, ja sitten siellä kuuluu kuitenkin niinku tämmöinen intialaisen call centerin ääni, ja sitten se tuli suomalaisesta numerosta, mikä nosti tavallaan sen puhelun luotettavuutta siihen verrattuna, että moni on oppinut sen, että ulkomaisiin numeroihin ei kannata vastata. Jollain saattaa olla jopa esto siihen, että ulkomailta ei voi soittaa. Mut sitten kun se tuli suomalaisesta numerosta niin siihen luotettiin, siihen vastattiin ja sitten taas ei osattu ajatella sitä, että okei täällä on kaveri joka puhuu intialaisella korostuksella, sanoo soittavansa Amerikasta ja sitten soittaa suomalaista numerosta ja sanoo että sun kone on hakkeroitu, niin tää oli yksi tämmöinen niinku mitä tuli tosi paljon ja sehän oli semmoinen esimerkki teknisestä estosta, mikä saatiin fiksattua, että ne ei nää pystynyt huijaamaan niitä suomalaisia numeroita.

00:07:59

Laura: Kyllähän tota joo… Ja siis huijauksia ehkä tulee nykyään enemmän vastaan kuin mitä edes jaksaa muistaa, että niitä on niin monenlaisia. Ja sitten monethan niinku saa näitä yrityksiä niinku huijausyrityksiä kohdalleen, mutta ei edes lähde niihin mukaan.

Mutta ehkä tähän liittyen just näihin tämmöisiin romanssihuijauksiin ja rakkauteen tai johonkin tämmöiseen rakkauteen/seksuaalisuuteen liittyviin huijauksiin, niin minulle ja mä tiedän paljon mun niinkuin tuttaville on tullut näitä tämmöisiä ”sugar babe” -huijauksia hiljattain… Tai nyt hiljattain, mutta

tässä niin kun kevään aikana kun tätä äänitetään. Eli tota lähestyy joku tyyppi joka on silleen, että ”Hei, haluatko olla mun sugar babe? Lähetän sulle vaikka 5 tonnia kuussa. Ihan saat kuule niinku treat yourself ja tehdä mitä vaan sillä”. Ja tota se on jännä, kun siis mullekin on tullut näitä ja Instagramissa, missä mulla lukee selkeästi, että mä oon tietoturva-asiantuntija, hakkeri ja tämmöistä, mutta silti ne jaksaa yrittää aina välillä.

00:08:50

Janina: Haastetta!

00:08:51

Riku: Ehkä ne vaan kokeilee, että mikä sun summa olisi, millä lähtee.

00:08:59

Laura: Joo, ja se hauskaa, kun näihin huijauksiin saattaa oikeasti liittyä se, että ne saattaakin lähettää tai niinku feikata että ne lähettää sulle rahaa, ja ne saattaa käyttää tämmöisiä niinku kikkoja hyväksi että ne lähettää sulle rahaa, mutta sitten… Esimerkiksi PayPalin tai jonkun tämmöisen kautta. Mutta sitten niin kun ”disputettaa” sen… Mikä se on suomeksi?

00:09:18

Janina: Joo, eli se otetaan… Siirretään se raha ja se ikään kuin näyttäytyy siellä, mutta sitten vedetään se takaisin.

00:09:27

Laura: Joo, että tota että kyllä nää kikat alkaa myös edistymään, ja haetaan sitä semmoista - mihin niinku Rikukin tuossa viittasi siinä puhelinnumero-keississä - semmoista niinku legitimiteettiä, että haetaan sellaista… Yritetään vakuuttaa ihan eri levelillä ihmiset siitä, että tää on oikeasti totta. Just että lähetetään rahaa, feikataan puhelinnumeroita. Puhelinnumeroiden feikkaus kyllä onnistuu edelleenkin tietyin reunaehdoin - että toki siellä on tullut parannuksia - mutta että kyllä niin kun on paljon tämmöisiä tietoteknisiä- tai ihan siis manipulointikikkoja, mitä näissä kyllä käytetään ihan surutta hyväksi.

00:10:00

Janina: Me ollaan huomattu nyt Nettideittiturvassa se, että yhdistyy romanssihuijaus ja sijoitushuijaus. Oletteko te törmännyt näin?

00:10:11

Riku: Joo, tää on kyllä niinku tuttu ilmiö kyllä.

00:10:14

Laura: Joo, tosi yleinen kyllä. Ja sitten siellä on ne kryptovaluutat yleensä, millä tota sijoitetaan. Ja se on jännä, miten niin kun läpi kyberrikollisuuden tämmöiset… Ja ku puhun nyt kyberrikollisuudesta, niin just tämmöisistä huijauksiin perustuvista kyberrikollisuusksista, niin tosi iso osa niistä on just tämmöisiä sijoitushuijauksia tavalla tai toisella, ja siellä on tyypillisesti se kryptovaluutta sitten. Että se on bitcoin, ethereum… Joskus joku vähän eksoottisempi, dogecoin tai joku tällainen. Ja se syy siihen on se, että se on edelleen helpompi lähettää vaan maailmanlaajuisesti bitcoineja, kuin esimerkiksi rahaa. Siis niinku esimerkiksi euroja ja dollareita.

00:10:52

Riku: Niin ja se on myös sille rikolliselle helppo tapa pysyä anonyyminä, että niitä on huomattavasti paljon vaikeampi jäljittää kun niinku rahasiirtoja ottaa vastaan.

00:10:59

Laura: Niin se se on totta. Joo, se on vaikeampi jäljittää omalla tavallaan. Toki niinku näissä niinku kryptohuijauksissa nykyään on paljon niinku rahanpesuelementtejä ja kaikkea tämmöistä. Ja sinänsä haluan painottaa että että niinku kryptovaluutta ja niinku lohkoketju… Että joo sinänsä niinku siellä ei niinku liiku kenenkään tilinumeroa tai tällaista, mutta se on aina linkitetty jonkun sähköpostiosoitteen, ja jossain kohtaa joku vetää… Niinku muuttaa sen bitcoinin - tyypillisesti bitcoinin tai jonkun muun kryptovaluutan - joksikin toiseksi valuutaksi.

Ja tässä ehkä se isoin kysymys on että missä se muutos tapahtuu, että jos se tapahtuu jossain valtiossa, missä pyritään niin se reguloimaan tai pyritään niinku estämään tällaista huijausta, niin sittenhän siellä voi olla jotain tällaisia kontrolleja. Mutta se vaihto voi tapahtua jossain aivan muualla. Jossain semmoisessa pörssissä, mikä ei esimerkiksi ole Euroopan tai Yhdysvaltojen rajojen sisällä.

00:11:52

Riku: Niin, tai ne ei välttämättä halua luovuttaa tietoja viranomaisille sitten.

00:11:54

Laura: Just näin.

00:11:55

Janina: No kaikki tämä saattaa kuulijoille nyt kuulostaa siltä, että ”okei, että tulee kaikkea tämmöisiä uusia termejä”, niin miten tavallaan jos puhutaan tälleen niinkun Matti Meikäläinen tai Maija Meikäläinen - tasolla näistä niinkun kyberasioista, että on ollaan kuultu tämmöisestä termistä kun ”kyberresilienssi”, että tarvitaanko me jotain… Että mitä ihmiset tarvitsee näiden… Tarvitaanko me niinku uusia taitoja vai miten me niinku osataan suojautua kaikelta tältä?

00:12:20

Riku: Jos mä avaan tästä omasta puolesta, kun tää kyberresilienssi on niinku omalla työpaikalla tosi tosi niinkun lähellä, niin tälleen yhteiskunnallisellahan tasolla tää tarkoittaa niinku sellaista yleistä varautumista ja huoltovarmuutta ja tällaista että meidän yhteiskuntaa ei pystytä lamauttamaan kyberiskujen avulla, ja silleen ylipäätänsä meidän Elisan näkökulmasta esimerkiksi, että verkot toimii ja meillä on sähköä pyörittää meille verkkoja ja toisin päin. Ja sitten yrityksen tasolla se, että niin kun yksittäinen kyberhyökkäys ei pysty lamaannuttamaan koko yrityksen toimintaa, että se pystyssä siitä huolimatta.

Ja sitten taas kun mennään tänne yksilötasolle, niin kun mainitsit, niin mä näkisin itse sen semmoisena niinkun mä ehkä miettisin ”kyberhygienia”-sanaa tavallaan, että niin kun just tämmöistä perus että sulla on salasanat - eri salasanat - eri paikoissa ja sitten tota niinku… No, käytät monivaiheista tunnistautumista. Nää hyvin perinteiset jutut.

Ja ehkä sitten tuohon resilienssin näkökulmaan vielä se, että katsot että sulle niinkun tärkeät tiedot mitä sulla on, niin ne on niin kun jossain varmuuskopioitu vaikka pilvipalvelussa tai sitten… Ihan ehkä tavalliselle käyttäjälle tämmöinen kovalevyn varmuuskopiointi nykypäivänä on vähän ehkä liikaa.

00:13:51

Laura: Joo ja kovalevyt on… Mä just itse asiassa niinku mietin tässä, että ne menee rikki nopeasti!

00:13:56

Riku: Joo, ne kyllä menee, joo! Mutta pilvipalvelut on hyviä.

00:14:00

Laura: Ne on hyviä joo. Mut se jännä toi ”kyberresilienssi” on kyllä aikamoinen sanahirviö, ja ehkä jos miettii että mikä se niinku Wikipedian ”definition” tälle on niin on just se, että miten niinku – sano Riku, jos on väärässä - mutta miten niinku varaudutaan kyberongelmiin, ja miten valmistaudutaan niistä palautumiseen. Tai niinku mietitään, että miten se palautuminen tapahtuu. Meniks oikein?

00:14:09

Riku: Jep. Just näin.

00:14:13

Laura: No niin hyvä. Hänen tittelistään tämän varmistan. Mutta noin. Niin tota että jos mä mietin että mitä se tarkoittaa perusihmisen kannalta - siis nyt niinkun yksilö on ihminen, joka ei välttämättä nyt ole missään työkontekstissa - etenkin tämmöistä huijausmaailmaa, kun… Siis joo nää niinku tekniset toiminnat, että on niinku hyvät salasanat ja monivaiheinen tunnistautuminen ja jollain tavalla joku niinku antivirus-suojaa laitteella, että nää on niinku hyviä juttuja. Mut sitten nää niinku menee tosi semmoiseksi niin kun ”mind gameiksi” nää niinku huijaukset tosi useasti, että kyllä se ehdottomasti se sellainen tietoisuuden lisääminen on tosi tärkeetä.

00:14:53

Laura: Ja koska me ei voida aina kaikille levittää sitä tietoisuutta, niin sitten se, että miten näistä palaudutaan? Koska kyberrikoksiin - etenkin tämmöisiin romanssihuijauksiin tai muunlaisiin tällaisiin huijauksiin, sijoitushuijauksiin ja muihin - siinä ei ainoastaan menetetä ihan hemmetisti rahaa, vaan luottamus teknologiaan, luottamus muihin ihmisiin. Niin edes se semmoinen, että niinku pysähtyy miettimään, että mä voin tehdä tälle asialle jotain - mä voin mennä mun pankkiin, mä voin tehdä rikosilmoituksen - niin ei välttämättä tule kaikille ihan sille ilmiselväksi. Just ehkä niinkun mun semmoinen pieni harmistus näissä on aina siellä, kun puhutaan vähän… Tai me puhutaan puhutaan niinku huijauksista, että puhutaan semmoisesta, että ”äh sulta se nyt vähän huijattiin netissä”, tai että tää on niinku ”juksutettiin” tai niinku silleen…

00:15:35

Riku: Niin että vähän vaan niinku petkutettiin.

00:15:43

Laura: Niin! Kun kyse on kuitenkin siitä, että joku voi menettää koko omaisuutensa. Ja voi menettää luottamuksen just muihin ihmisiin ja teknologiaan, niin mä toivoisin… Että nytkin tässä toki puhutaan huijauksista, koska se on se niin kun termistä mitä käytetään, mutta että haluan alleviivata, että kyse on tosi vakavista ja vakavasti otettavista rikoksista.

00:16:00

Janina: Nimenomaan. Hyvä pointtaus, ja tää on se mitä myös Nettideittiturvassa yritetään lisätä sitä tietoisuutta, että me ei niin kun vedetä näiden huijattujen jalkojen alta mattoa sillä, että me ollaan vaan sillälailla, että ”noh noh”.

00:16:24

Riku: Mulla tuli tuosta resilienssin kulmasta vielä sen niinku se, että sulla on tietoisuus siitä, että netissä on erilaisia ihmisiä. Ja siellä ikävä kyllä korostuu se ihmisyyden ikävä puoli, koska ne on niitä jotka sua todennäköisemmin lähestyy siellä. Siellä on jonkinlainen taka-ajatus. Yleensä jos sulla tulee tuntemattomalta ihmiseltä viesti, niin siellä on tosi harvoin mitään niinku positiivista tarkoitusperää takana. Tavallaan semmoinen vahvuus siinä mielessä, että sä niinkun ymmärrät sen ja hyväksyt sen, että okei ei täällä välttämättä ollut mitään.

00:17:05

Laura: Niin ilman että vaipuu hirveästi epätoivoon, koska mä tiedän sillee… Kun sä vielä… Koska siis loppujen lopuksi tässä surullisinta on just se, että tai siis… Ehdottomasti siis internetissä oikeasti kuka tahansa voi esittää olevansa kuka tahansa ja. Siis oon samaa mieltä Rikun kanssa, että ehdottomasti jokaikinen kohtaaminen internetissä pitää ottaa pienellä semmoisella ”pinch of salt” -varauksella, miten se nyt sanoisi…

Mutta sillä, että kriittisyyttä joo. Mutta että kuitenkin näissä on pointti se, että nää rikolliset haluaa käyttää meidän hyviä ja inhimillisiä piirteitä meitä vastaan. Sitä, että me ollaan herkkiä, että me tunnetaan rakkautta. Me halutaan auttaa. Me halutaan menestyä. Me halutaan niin kun hyviä asioita itselleen ja muille. Ja tää on se ongelma, koska sitten kun me ollaan herkässä tilassa, etenkin näissä romanssihuijauksissa, niin se isku on todella paljon pahempi kuin esimerkiksi että… No riippuu vähän, että jos joku hackaa sun jonkun pelitilin mitä sä et ole hirveästi käyttänyt, niin voi olla että se selviää siitä vähän silleen että joo, se ärsyttää ja niinku aiheuttaa sulle extratyötä, mutta näissä puhutaan sellaisesta…

00:18:16

Riku: Taas piti vaihtaa sähköpostien salasanat ja näin, ja siinä menee pari tuntia.

00:18:18

Laura: Joo, ja sä voit ehkä saada tiliä palautettua, niinku tän käyttäjätilin joskus palautettua. Riippuu ihan palvelusta. Mutta tällaisissa tilanteissa niin nää ei vaan ole mitenkään tietoteknisiä ongelmia, vaan nää on ehdottomasti paljon isompia henkilökohtaisia ongelmia.

00:18:35

Janina: Kyllä. Se tekee tästä niin kun inhimillistä myös tietyllä tavalla, että meissä on tiettyjä semmoisia… Me ei voida mennä pakoon sitä meidän ihmisyyttä myöskään, ja siitä mä jotenkin haluaisin vähän niinku syventääkin tätä keskustelua siihen. Me vähän puhuttiin, avattiin siis näitä manipuloinnin keinoja. Jos puhutaan sosiaalisesta manipuloinnista, mitä nää - jos heistä puhut nyt kyberrikollisina - että mitä he käyttää, niin minkälaisia tavallaan teknologisia apuja heillä on näihin kaikkiin keinoihin, mitä ne hyödyntää?

00:19:01

Laura: No tota… Ihan siis laidasta laitaan, että tässä itse asiassa mulla tuli aikaisemmin jo mieleen, mutta sanon sen nyt tässä kohtaa kun muistui taas mieleen, että ehkä kun mietitään että kyberrikollisia, niin tosi useasti siellä niinkun ajatellaan semmoista niinku hakkeria. Semmoista, että hakkeri pystyy hakkeroimaan mitä vaan ja tekemään mitä vaan. Mutta todellisuus on se, että ne käyttää hyvinkin niinku arkipäiväisiä keinoja. Ne käyttää viestejä. Kuka tahansa meistä osaa lähettää viestejä.

Joissain tilanteissa saatetaan esimerkiksi tehdä jotain nettisivuja, käyttää haittaohjelmia, tämmöisiä asioita, niin riippuu hyvin paljon siitä, että minkälainen taho siellä on taustalla, että kuinka paljon siellä on sitä teknistä osaamista. Mutta sanoisin, että suurimmassa osassa niin se pohjautuu… Sieltä lähetetään viestejä. Ehkä ollaan tehty joku nettisivu, missä feikataan joku just tämmöinen kryptopörssi. Tai sitten pyydetään vaan suoraan niinku laittamaan johonkin tämmöiseen likviditeettipooliin - niinku olemassa olevan palvelun, binancen ynnä muun likviditeettipoolin – rahaa, että käytetään olemassa olevia palveluita. Ja ehkä se korostuu niinku monesti esimerkiksi mun työssä, kun mä tutkin näitä asioita, niin se että mitä nyt on saatavilla, niin se raivaa omalla tavallaan sitä, että mitä rikollisuutta tapahtuu.

Eli just se, että meillä on kryptovaluuttaa. Meillä on kryptovaluuttapörssejä, meillä on likviditeettipooleja ja ynnä muita, mitkä on vähän pitkä konsepti avata. Mutta kuitenkin silleen tämmöisiä sijoitusinstrumentteja näissä niinku olemassa olevissa alustoissa, jotka on siis täysin legitiimejä, että niitä… Ne on siis täysin laillisia yrityksiä ja ne toimii sillä tavalla. Mutta sitten näitä hyväksikäytetään.

Ja nyt ehkä niin kun vahvasti korostuu myös tietysti nää tekoälyn hyväksikäyttömahdollisuudet, eli että miten pystytään esimerkiksi feikkaa olevansa joku muu eli että sä voit vaikka tehdä filttereitä sun puhelinsoittoihin niin, että esiinnyt Tom Cruisena, tai että sinä lähetät kuvia, jotka on tehty täysin tekoälyllä ja feikkaat jonkun muun äänen.

Kaikki tää on niinku nyt jo mahdollista, ja tulee olemaan vaan - kun aika kuluu eteenpäin - niin vaan paremman ja paremman näköistä ja uskottavan näköistä, että tota… Tässäkin toki että osa käyttää tekoälyä, mutta sitten toisaalta on myös se porukka joka vaan sitten niinku esimerkiksi pyörittää jotain niinku tämmöistä bisnestä jossain päin maailmaa, ja sitten vaikka palkkaa malleja soittamaan puheluita niin kun joillekin tyypeille.

00:21:40

Janina: Aivan eli vähän niinku klassisempi tapa.

00:21:42

Riku: Niin kyllä, juu. Joo mä olin mä olin itse tulossa niinkun korostamaan ehkä tätä kulmaa, että he harvoin esiintyy omana itsensä. Toki tää mallin palkkaaminen on yksi vaihtoehto, mutta monesti siellä on nyt semmoinen… Luotu tällaisia niin kun valeprofiileja.

Yleensä tämmöisiä aika perinteisiä, esiinnytään vaikka amerikkalaisena sotilaana tai lääkärinä jossain kriisialueella ja halutaan niin kun luoda tämmöinen hahmo sinne taustalle, mikä yleensä on tämmöinen joka auttaa muita ihmisiä, joka sitten tavallaan saa sen uhrin ajattelemaan, että kun mä autan tätä ihmistä niin mä autan sitä kautta myös niin kun laajempaa yleisöä. Halutaan herättää semmoista niinku myötä myötätuntoa siinä uhrissa, että tota… Se semmoinen valeprofiili on tavallaan todella helppo luoda, tämmöinen hyvinkin uskottava, että sä voit käyttää jonkun olemassa olevia kuvia mitä saa noista julkisista profiileista.

Nykyään onneks noi profiilit on silleen oletuksena lähtökohtaisesti ehkä yksityisempää kuin sanotaan muutama vuosi sitten, kun pystyi käydä raapimassa kenen tahansa kuvat sieltä ja näin, niin… Mutta heillä on toki olemassa tämmöiset kirjastot.

Ja tosiaan tekoälyillakin voi nykyään luoda sitten näitä henkilöllisyyksiä paljon helpommin. Mutta mä sanoisin, että tää on ehkä se huijauksen niinkun ensisijainen teknologian käyttö, tämmöisen taustatarinan ja hahmon luominen, ja sitten sen käyttäminen hyväksi tässä huijauksen alustana.

00:23:05

Laura: Joo, jep. Ja haluan tähän itse asiassa näihin kuvien käyttöön lisätä oman omakohtaisen tarinan. Nimittäin olen kuullut, että esimerkiksi minun kuvia käytetään jossain tai on käytetty jossain Tinderin feikkiprofiilissa, mutta toisaalta siis mulla on julkinen Instagram ja mä oon tiedostanut sen, että mä kuitenkin käyn paljon puhumassa ja oon silleen jonkun verran esillä, että tää on se mahdollisuus että joku joskus tulee näitä käyttämään, että se ei sinänsä tullut mulle yllätyksenä. Mutta että se on hyvä just pitää mielessä, että Instagrammistakin on tosi helppo sitten lataa ne kuvat, että niitä ei voisi niin...

0:23:37

Riku: Niimpä, vaikka kuka vaan voi.

00:23:39

Janina: Se on vähän niinku avoinna oleva albumi, siis semmoinen niinku kotialbumi, jos sinne laittaa ihan kaikkee. Että siitä on kyllä niin kun tavallaan hyvä myös tiedostaa se puoli, että vaikka ei tekisikään julkista työtä, että jakaa sinne omasta elämästään jo paljon kaikkea ja jos se on julkinen, niin kuka tahansa sitä voi käyttää.

Mutta mulle tuli vielä mieleen tuossa kun puhuitte siitä, että nää niinku rikolliset hyödyntää tavallaan aina sitä aikaa, missä me eletään ja mikä silloin on jotenkin nosteessa niinku teknologian puolelta, mutta että myös varmaan kaikki tämmöiset kansainväliset tilanteet niinku sotatilanteet ja muuta… Että sitten hyödynnetään ikään kuin sitä kärsimystä.

00:24:16

Riku: Siinä on just se… Niinkun halutaan tehdä semmoinen taustatarina monesti, joka herättää siinä uhrissa semmoista auttamisen halua.

00:24:25

Janina: Niin.

00:24:26

Riku: Ja sitten se, että kun kun tota… Sanotaan nyt, että sieltä tulee jossain vaiheessa se rahapyyntö, että ”olen vaikka…” ja sitten siellä voi olla tämmöisillä kriisialueella myös vähän tämmöisiä epävakaita olosuhteita, mitkä sitten mahdollistaa jonkun taustatarinan, että ”paikalliset viranomaiset pitävät mua nyt täällä, että mä en pääse lähtemään, tai joku apulähetys voi olla jumissa, että pitää maksaa koko summa, että me saadaan se apulähetys tänne” tai tän tyyppisiä tarinoita.

00:24:52

Laura: Joo. Ja mä muistan siis F-Securella tässä kun tota noin sota alkoi, tai Venäjä hyökkäsi Ukrainaan muutama vuosi sitten, niin me kyllä nähtiin tosi paljon tällaisia huijausviestejä, sähköposteja, joita lähetettiin ympäri maailmaa ja esiinnyttiin ukrainalaisia naisina, jotka hakee seuraa ja hakee apua nimenomaan, ja niinku yritettiin niinku hyötyä tästä konfliktista, että se on ehkä semmoinen nyrkkisääntö mikä mulla on aina kaikessa, että jos on joku iso tapahtuma - nyt puhun ihan niinku positiivistakin tapahtumista, vaikka konsertti tai tota sitten negatiivinen tapahtuma, joku poliittinen konflikti, pandemia, mitä ikinä - niin niiden ympärille aina kerääntyy niitä, jotka yrittää saada sitä rahallista hyötyä huijaamisen ja rikollisuuden avulla, ja se on melkeinpä sääntö kuin poikkeus kyllä.

00:25:44

Riku: Joo, se kyllä näkyy meilläkin niinku vahvasti, että kun meillä on näkyvyyttä, tulee asiakkaat ilmoittaa, että tän tyyppisiä huijauksia on menossa, niin kyllä ne aina näkyy. No just pandemia oli tota iso, ja sitten sodan aikana just tuli erilaisia… No just nää tota että niinkun naiset pyytää tukea, tai sitten että kaikenlaisia ylipäätään huijauksia, että lähettäkää tukirahaa sitten Ukrainan armeijalle tai muuta, jota sitten ei siellä välttämättä ollutkaan. Ainahan nää luo tämmöisiä ilmiöitä.

00:26:07

Janina: Me vähän puhuttiinkin siitä, että ei halua niin kun jotenkin demonisoida tätä verkkotodellisuutta, että koska se on nyt meidän elämää, jokaisen elämää, ja me sielläkin niin kun ollaan meidän arjessa läsnä. Mutta mitkä on tavallaan teidän semmoiset, niin kun top 3 vinkit ja neuvot kuulijoille, niin kuin että miten suojautua romanssihuijauksilta erityisesti?

00:26:36 **Laura:**

Tota… Mä sanoisin että näissä niinku ne… Tai siis mä poistan tän sillä, että nettideittailu on täysin normaalia ja siellä toki tapaa ihmisiä joita sä et ole tavannut ikinä elämässäsi, joskus ne ihmiset saattaa olla toisella puolella maailmaa. Mutta mä sanoisin, että ehdottomasti kannattaa tavata heidät fyysisesti in real life jos vaan kykenee ennen kuin lähettää rahaa, koska jossain tilanteessa voi olla että joku on oikeasti pulassa ja se tarvitsee rahaa. Sekin on ihan fine lähettää ihmiselle, joka on pulassa, rahaa.

Mutta ennen kun sä saat semmoisen hyvän varmuuden siitä, että ihminen on oikeasti olemassa, näyttää siltä, jolta väittää näyttävänsä. Kuulostaa siltä, jolta väittää kuulostavansa. Niin ennen sitä en lähtisi mihinkään.

Ja sitten kaikki tämmöiset sijoitusneuvot. Eli jos et itse hae sijoitusasioita, tai niin kun ole kiinnostunut ja perehtynyt, niin ei kannata mun mielestä ottaa sijoitusvinkkejä vastaan. Etenkään sellaisia joita et ole suoraan pyytänyt keneltäkään, että ne on aina todella niinkun semmoinen vaaran merkki kyllä niinku nyky internetissä.

Ja sitten ehkä viimeisenä toki niinku kaikki nää niinku tekniset keinot, millä suojautua. Just nää vahvat salasanat, monivaiheinen tunnistautuminen, päätelaitteiden suojaaminen just tämmöisellä antivirus-softilla tai tämmöisen päätelaitteiden haittaohjelmaesto-softilla. Koska kyllä mekin ollaan tutkittu näitä esimerkiksi F-Securella ja siellä on käynyt ilmi, että joissain tilanteissa ihan suoraan niinku kalastellaan tietoja. Eli että mennään nettisivulle, missä sitten vaan varastetaan tietoja, tai sitten on käytetty ihan suoraan haittaohjelmia, että ne haittaohjelmat on ollut ehkä hyvin tämmöisiä edistyksellisiä rikosvyyhtejä sitten,

mutta se ei ole mitenkään poissuljettua, etteikö olisi jotain tämmösiä… Öö vähän edistyksen… Tai niinkuin edistyksellisiä teknisiä keinoja, mitä nää voi käyttää näissä romanssihuijauksissa myös valitettavasti apuna.

00:28:30

Janina: Siis pakko kysyä tähän väliin ja avata myös kuulijoille, että mikä on siis haittaohjelma?

00:28:36

Laura: Joo, sori. Haittaohjelma on siis tällainen ohjelmisto, jonka lataat sun puhelimeen. Tyypillisesti esimerkiksi niinku jos puhutaan puhelimesta, niin androidilla on voimakkaampia haittaohjelmia siinä mielessä, että niillä on niinku helpompi varastaa sulta tietoja sieltä sun puhelimelta suoraan. iPhonelle on jonkun verran, mutta tota se on vähän suljetumpi ekosysteemi. Sori, tulee vähän tämmöistä jargonia, mutta tota se niinku…

00:29:11

Janina: Ei haittaa. Tää on hyvä.

00:29:14

Riku: Niitä on vähän harvinaisempaa saada, koska se on se App Storessa.

00:29:19

Laura: Joo, mutta aina välillä sinne luikahtaa. Esimerkiksi näissä eräissä keisseissä, mitä me tutkittiin - toki niinku olemassa olevan niinku materiaalin perusteella, mutta perehdyttiin näihin jonkun verran F-Securella - niin öö oli siis ihan romanssihuijauksia, missä oli saatu haittaohjelmia ihan näihin virallisiin sovelluskauppoihin sisään, eli App Storeen iPhonella ja Play Storeen. Tai riippuu vähän, että mikä puhelin on, mutta kuitenkin saatu sinne huijattua sisään tämmöisiä sijoitussovelluksia niin sanotusti, joilla sitten oikeasti varastettiin vaan niinku tietoja täältä kyseiseltä henkilöltä.

Mutta sen takiahan on just, että haittaohjelmat on hyvin myös mahdollisia näissä tilanteissa, että joku voi käyttää myös sen takia, että haittaohjelmia pystyy tänä päivänä kuka tahansa myös ostamaan. Eli esimerkiksi tämmöisiä haittaohjelmia, joilla voi varastaa tietoja laitteelta, Android-puhelimelta erityisesti, esimerkiksi niinku PC-laitteelta, niin ne on ihan ihan niin kun ostettavaa kamaa tuolla alaverkon myyntipaikoilla.

Että tota en nyt halua liikaa liikaa tässä pelotella, mutta että just että se on hyvä muistaa, että haittaohjelmista ei ehkä nykyään puhuta niin paljon, mutta kyllä ne on jatkuvasti semmoinen staattinen uhka. Ei ne ole kadonneet mihinkään, ja kyllä niinkun silloin kun itsekin tein niinkun sitä niinkun enemmän hakkerointijuttua, niin kyllä meilläkin niitä haittaohjelmia käytettiin siihen, että päästään yrityksiin sisään, ja ihan yksityishenkilöillekin nää haittaohjelmat on edelleen ihan relevantti uhka.

Niin sen takia just että hyvä juttu tässä on se, että meillä on suojauskeinoja sitä vastaan. Ja niitä kannattaa ehdottomasti käyttää, ja kannattaa pitää laitteet ehdottomasti päivitettynä, koska useasti nää haitalliset ohjelmat – haittaohjelmat - käyttää hyväksi sitä, että laitteessa on joku ”pätsäämätön” eli ei päivitetty ominaisuus, missä on joku tietoturva-aukko, ja sitten ne haittaohjelmat voi sitä käyttää hyväkseen, että päästään tekemään ikäviä juttuja laitteella.

00:31:14

Riku: Nää toimii aina tavallaan silleen, että tietoturvatutkijat ja rikolliset myöskin tutkii koko aika tuolla netissä. Kun kuvia, laitteita niin sanotusti, aina välillä niistä löytyy haavoittuvuuksia koodista ja sitten kun niitä löytyy, niin tietoturvatutkijat ilmoittaa niitä sinne yrityksille, jotka sitten korjailee niitä ja sitten ne päivityksen myötä tota korjataan ne haavoittuvuudet, jolloin niitä ei enää pysty hyödyntämään.

Ja no olin tässä just käymässä esimerkiksi isoisän mökillä tässä muutama viikko sitten ja tota sieltä sitten katseltiin vähän modeemeja, ja ne on semmoisia yleisiä tota… Tai siis niinkun internet… Mitä ne nyt on, miksi mä niitä nyt sanon?

00:31:57

Laura: Niin boksit, millä yhdistetään internettiin?

00:31:58

Riku: Niin niin, niin boksit kyllä kyllä. 5G-boksit, SIM-kortti sinne ja sitten wifin kautta nettiin. Esimerkiksi hän ei ollut muistanut päivittää niitä, ja sitten päiviteltiin siellä. Ja ne on semmoinen hyvin yleinen mitkä ihmisiltä saattaa jäädä päivittämättä jos siellä ei ole nää… Jos jotenkin vähän nää tämmöset vanhemmat ei välttämättä ole automaattisten päivitysten piirissä, niin se on semmoinen, mikä kannattaa pitää mielessä.

00:32:26

Janina: Aivan, joo. Mitäs muuta? Tuleeko sulle Riku mieleen tää top 3, miten suojautua?

00:32:33

Riku: Hei no siis joo. Ne oli tosi hyviä mitä Laura sanoi, mutta ehkä mä vielä täsmentäisin tai vähän terottaisin sitä niin kun tietynlaista skeptisyyttä siihen, miten tuntemattomien ihmisten kanssa jutellaan netissä. Ja aina jos tulee vähänkin semmoinen niinku että ”tässä on jotain outoa”…

Ja mä kun itse oon tota puhunut tästä tällaisista sosiaalisen manipuloinnin keinoista, niin sulla on tietynlaisia triggereitä, mitä nää huijarit käyttää. Ja nää on samoja keinoja, mitä ammattimyyjät ja -poliitikot käyttää, ja tota nää on ihan niin kun silleen yliopisto-tutkittua tavaraa ja tota… Heidän tehtävänään on sut saada niin kun myöntymään heidän pyyntöihin, ja siinä käytetään tämmöisiä psykologisia triggereitä niin sanotusti. Saatetaan luoda esimerkiksi jonkinlaista kiireen tuntua. Tai sitten saatetaan vakuutella, että joku muukin on tehnyt näin samoin tai tota… Saatetaan ensin esimerkiksi antaa jonkinlainen lahja, ja sitten sä koet tavallaan tarvetta antaa vastalahjan ja tehdä jotain niin kun vastineeksi.

Niin jos siinä tavallaan tän pyynnön ympärillä, mikä sieltä tulee, niin, jos siihen tulee semmoinen pieni epäilys, että ”onko tässä nyt… Mulla on vähän tämmöinen korostunut tarve, että tässä on nyt vähän jotain outoa. Tämä ei ole tämmöinen ihan luonnollinen juttu, vaan mulla on tämmöinen korostunut tarve tavallaan suostua tuon pyyntöön, että tää on vähän niinku tämmöinen outo…”, niin siinä vaiheessa kannattaa niinku ottaa hetki etäisyyttä siihen pyyntöön. Ehkä kysyä joltain niinkun neuvoa, että ”hei tässä olisi tämmöinen, että vaikuttaako tää sun mielestä jotenkin oudolta?” Koska…

No tässä oli maaliskuussa esimerkiksi hesarissa kerrottiin tästä keissistä, missä oli useaa suomalaisnaista huijattu internetin kautta. Ja tota oltiin kymmeniä ja satojakin tuhansia laitettu rahaa ulkomaille, ja oltiin esiinnytty siis niin kun tota kuuluisina niinkun amerikkalaisena näyttelijänä ja näin. Ja jos he olisi ehkä

kysynyt joltakulta niinkun että onkohan tässä nyt jotain, niinku onko onko tää omituista, niin olisi ehkä saattanut tulla semmoinen skeptisyys siinä kohtaa vastaan.

Mutta mä toki mä ymmärrän, että se on tota… Tässä on ammattihuijarit tota kyseessä, ja he niinkun he juttelee ihmisten kanssa, jotka on haavoittuvassa asemassa, niin se on siinä. On tosi korkea kynnys sitten ottaa tavallaan ulkopuoliselta neuvoa siinä kohtaa. Mutta ehkä omana kantana semmoinen, että jos mä palaan siihen resilienssiin, niin se että pidä semmoinen tietynlainen skeptisyys tuntemattomiin internetissä, vaikka he olisi julkisuuden henkilöitä. Etenkin jos he olisi jotain julkisuuden henkilöitä…

00:35:39

Laura: Etenkin jos minä tulee vastaan Tinderissä… Varokaa.

00:35:41

Riku: Niin niin joo, etenkin jos Laura tulee vastaan. Ja sitten ole valmis kuuntelemaan jotain läheistä. Ja niinku suhtaudu skeptisemmin tuntemattomiin, ja ole niin kun rakkaampi läheisiäsi kohtaan, niin kuuntele läheisiäsi ennemmin.

00:35:57

Laura: Toi on tosi hyvä. Mun mielestä toi, että kuuntele läheisiäsi. Etenkin tämmöisessä tilanteessa mikä on ihan super super jotenkin arkaluontoinen, koska siinä saattaa tulla just sellainen… Ei välttämättä sanota, että sä vaikka… Tää nyt täysin keksitty tarina, mutta sä oot vaikka eronnut 50-vuotias nainen, sulla on aikuisia lapsia, niin ootko sä valmis puhumaan sun lapsien kanssa jotka on ehkä sun lähin niinku semmoinen lähipiiri? Oletko sun… Ootko sä sun lapsien kanssa valmis puhumaan ylipäätänsä sun deittailuelämästä, että nääkin on aika arkaluontoisia.

Mutta ehdottomasti se, että niinku koittaisi niinku rikkoa niitä myös sellaisia näkymättömiä esteitä tämmöisen välillä, että se on okei puhua siitä, että deittailee netissä. Se ei ole mitenkään niinku omituista. Mut just sitten se toinen se kolikon kääntöpuoli on siinä, että siellä on niitä ikäviä tyyppejä, mutta kun me puhutaan siitä ja me ollaan ihan silleen avoimia tän asian kanssa, niin sitten se olisi ehkä turvallisempi keskustella myös sitten läheisten kanssa tai lähestyä niinkun teitä tämä niinku Nettideittiturva-hankkeen tota puolesta, että teidän puoleen kääntyä.

00:37:14

Riku: Kyllä, tähänkin on ammattilaisia auttamassa. Mut me esimerkiksi jutellaan mun äidin kanssa. Se, tota… Hän kyllä tota aina… Hänkin tykkää vedättää tämmöisiä huijareita, niin se aina kertoo mulle, että ”nyt sieltä taas joku pistelee viestiä, ja sitten mä tässä vedättelin sitä tässä, hahaa”.

00:37:31

Janina: Just näin. Eli kerrataan vielä: Elikkä mun mielestä oli tosi hyvä toi, että päivittäkää ne laitteet. Tunsin itsekin piston sydämessäni sillain että en ole päivittänyt omaa iPhoneani, se on siellä aika pitkään huutanut, jaiks. Ja sitten tuota mitäs siinä olikaan muuta… Toi avoimuus ja sitten se jotenkin skeptisyys.

Ja pakko vielä kysyä tämmöinen spesifi kysymys, että miten - jos nyt puhutaan ihan siitä, että nää huijarit on myös tuolla Tinderissä tai muissa deittisovelluksissa - osataanko me tunnistaa niin… Mitä me, miten me osattaisiin tunnistaa niinku siellä sovelluksessa oleva feikkiprofiili?

00:38:04

Riku: No ainakin niinkun miehenä, kun on käyttänyt, niin ne tämmöiset tekoälyllä luodut… Ne on niinku tosi selkeitä, ne nyt huomaa.

00:38:12

Laura: Vielä toistaiseksi ainakin.

00:38:14

Riku: Niin siis joo kyllä. En en toki tiedä, miten tota… Nyt kun tää jakso tulee ulos niin tota onko teknologia kehittynyt niin paljon, että se on vaikea erottaa, mutta tota. Sitten toki se… No, mä palaan tuohon Lauran pointtiin siitä, että niinkun kohdataan kasvotusten, että ennen pitkää niinku jossain vaiheessa sä et voi luottaa siihen videopuheluun tai tämmöiseen, ja jos me nyt ylipäätään mennään tämmöiseen, niin kun rahan käsittelyyn tai jollain tasolla… No, mä olisin skeptinen kaikenlaisista sijoitusneuvoista, vaikka olisi tavannutkin kasvotusten. Mutta niin tota…

00:39:00

Laura: Joo, totta. Sijoita mun firmaan! Joo, toi joo… Koska siis näitä on siis tosi erilaatuisia näitä feikkiprofiileja. On niitä jotka on selvästi silleen, että hei come on, tää on selkeesti feikki, ja toki se myös vaihtelee sitten että kuinka niinku valpas on siinä tilanteessa niinku huomaamaan. Mutta että osa on niinku helpommin huomattavissa, mutta sitten saattaa olla tämmöisiä niinku paljon vaikeammin huomattavissa ja sitten sekin on silleen että omalla tavallaan…

00:39:25

Riku: Niillä voi olla vaikka varastetut kuvat.

00:39:27

Laura: Varastetut kuvat, just. Ja niin kun voi olla, että puhuu todella hyvää suomen kieltä. Voi olla, että puhuu suomen kieltä äidinkielenään tai sitten käyttää - no tekoälyt nyt tässä kohtaa, kun tota tätä äänitetään - niin puhekielessä suomea esimerkiksi edelleen vähän huonosti tuottaa nää kaikki tekoälyt, mitä voi käyttää kääntämiseen, mutta nekin paranee jatkuvasti ja… Että ei se suomen kieli ole mikään semmoinen niinku suojakilpi tai mikään semmoinen antivirus siinä tai tämmöinen palomuuri tässä välissä. Mutta tietyissä tilanteissa se voi auttaa, että jos se on vähän semmoinen, että hän väittää, että hän asuu Suomessa, mutta sitten kuvassa näkyy jotain pilvenpiirtäjiä, jotka eivät ole Kalasataman pilvenpiirtäjiä, taustalla ja puhuu vähän konkkaa suomea, niin sitten siinä saattaa olla tämmöisiä red flageja.

00:40:03

Janina: Niin, kyllä.

00:40:07

Laura: Mut että nää on niin laidasta laitaan sit voi olla nää huijaukset. Ja voihan olla, että joku esiintyy myös ihan omilla kuvillaan, mutta vaikka tekaistulla nimellä. Tai sitten käyttää kuvia jotka on otettu 10 vuotta sitten, jolloin näytti ihan eriltä kun näyttää nykyään. Ja että näissäkin on niinku tosi paljon näitä eri sävyjä sitten, että… Mutta ehkä jos puhutaan just näistä organisoidusta rikollisuudesta, jotka yrittävät systemaattisesti huijata rahaa ihmisiltä, niin ne tosi useasti käyttää näitä tekaistuja profiileja kyllä hyväksi, mistä Riku just puhu.

00:40:37

Riku: Kyllä, ja siellä se lähestyminen ainakin tätä nauhoitusta tehdessä oli vielä useimmiten näiden pikaviestimien, sosiaalisen median kautta ainakin oman tiedon mukaan.

00:40:51

Janina: No hei tähän loppuun vielä… Minkälaisia teknologisia asioita te odotatte, että mitä kehittyy - jos miettii tälleen niinkun positiivisesta näkökulmasta - että minkälaisia niinku asioita te odotatte vaikka tälle vuodelle? Onko jotain sellaisia ”break through”-juttuja?

00:41:11

Riku: Tää on tosi paha ainakin jos miettii nyt niin kun tästä romanssihuijausten näkökulmasta.

00:41:17

Janina: Niin niin, tai ei tarvitse siitäkään. Voi miettiä siis niinkun ihan vaikka omasta työnäkökulmasta myös.

00:41:20

Riku: Niin okei.

00:41:24

Laura: Niin ehkä mä itse näen... Siis nyt puhutaan tietysti paljon tekoälystä ja, tekoälystä kun puhutaan populaarimediassa, niin tosi useasti puhutaan generatiivisesta tekoälystä, jolla voi luoda kuvaa, tekstiä ja videota, mitä ikinä. Mutta tekoäly ylipäätänsä, niin kyllä mä näen että me tehdään - tai siis tässä niinku voin puhua F-Securen puolesta, mutta myös ihan globaalisti - niin tekoäly mahdollistaa kyllä todella paljon myös suojausmekanismeja.

Mistä mä oon ainakin itse innoissani, että me voidaan oikeasti parantaa vielä tätä suojaus-gamea niin sanotusti, että me voidaan tehdä parempia tämmöisiä teknisiä ratkaisuja, jotka oikeasti suojaa sitten ihmisiä erilaisissa tilanteissa. Että se ei ole missään nimessä vaan että tekoälyä - tai tämmöistä generatiivista tekoälyä käytetään ainoastaan rikolliseen käyttöön, vaan kyllä me täällä niinkun pöydän toisella puolella käytetään tekoälyä myös.

00:42:20

Riku: Niin, siellä on puolustuspuolella sitä analytiikkaa ja myös ennustettavuutta, millä me voidaan parantaa meidän puolustusta. Mutta se, mikä tässä meidän alassa on semmoinen, että tää on vähän tämmöistä kilpajuoksua koko aika niinkun että hyökkääjä yleensä tekee sille… Menee silleen, että hyökkääjä tekee jonkunlaisen uuden hyökkäystavan, ja meidän pitää keksiä, miten sitä kohtaan puolustaudutaan. Ja sen sen jälkeen tota sitten hyökkääjä keksii taas jotain uutta, että tota… No tää puhelinnumero-esimerkki, että estetään niinkun numero. Tää olisi niinku, että ulkomailta ei voi esiintyä suomalaisena numerona lähtökohtaisesti, minkä jälkeen hyökkääjät siirty käyttämään tekstiviestejä enemmän.

Nyt me ollaan ruvettu tekemään tota toimenpiteitä tekstiviestien suhteen, jonka jälkeen hyökkääjät siirty sit taas käyttämään Whatsappia ja iMessagea. Ja nää on taas niinku semmoisia mihin operaattorikentällä on vaikeampi mennä. Että tota ne on sitten niinkun siellä niiden yritysten - Applen ja Metan - niinkuin

hallinnassa, että me ei me ei välttämättä päästä sinne ollenkaan. Ja sitten taas pitää niinku keksiä viranomaisten uusia keinoja, että miten sinne päästään sitten vaikuttamaan.

00:43:27

Laura: Joo, kyllä tää on tietysti tosi iso keskustelu, tämmöiset isot ”Big Tech” ja tämmöiset teknologiajätit ja niiden ekosysteemit ja niissä asioiden turvaaminen. Että se on… Ja mä ehdottomasti komppaan tätä Rikun pointtia, että kyllä niinkun nää rikolliset haluaa mennä semmoisiin paikkoihin, missä ne pystyy turvaamaan sitä omaa toimintaansa. Eli just no tekstiviestit edelleenkin on kyllä Suomessakin hyvin niinkun iso tapa, millä huijauksia levitetään. Ei ehkä just näitä niinku romanssihuijauksia niin paljon, mutta sitten kaikkia näitä niinku postia, tulleja, just tällaisia.

Mut just että ollaan vaikka… Sanotaan, että vaikka niinku Tinderissä aloitetaan joku tämmöinen huijaus, että joku lähestyy sua, niin tosi useasti nekin pyytää, että ”hei siirrytäänkö vaikka WhatsAppiin tai Telegramiin”, kun ne tietää että Tinderissä tapahtuu jonkun näköistä moderointia ja siellä voi blokkaa, tai joku voi raportoida tilejä.

00:44:21

Riku: Niin, raportoida, että on epäilyttävää ja sitten niin sitten se koko tili jäädytetään.

00:44:24

Laura: Jep, just näin ja niiden se… Niin ne haluaa siirtyä sieltä sitten muihin kommunikaatiokanaviin, missä ne pystyy ylläpitämään tätä keskustelua. Ja se on ongelma ehdottomasti, koska nää turvaa sitä rikollista toimintaa omalla tavallaan nää tietyt sovellukset.

00:44:53

Riku: Jep, ja sinne taas on lähes mahdotonta mennä sitten niinkun minkään viranomaisen, koska sielläkin on se viestinnän salaisuus sitten, mikä on totta kai itseisarvo.

00:45:02

Laura: On, on. Ja me tarvitaan sitä totta kai. Ja tässä tää on tosi monimutkainen aihe, että ei oo niinku voittajia sinänsä tässä. Mutta onneksi esimerkiksi sitten kun puhutaan nettisivuista ja haittaohjelmista ja tämmöisistä, niin ne on asioita, mitkä niinkun on edelleen tosi isossa roolissa missä tahansa huijauksessa, mitkä on semmoisia asioita, mihin voidaan puuttua ja missä me voidaan tulla väliin vaikka niinkun ehkä… Viranomaistasolla ehdottomasti esimerkiksi ajetaan alas tai otetaan alas haitallisia sivustoja, joissa on just kalastelua, feikkisijoituspalveluita, tai haittaohjelmia levitetään.

Ja sitten esimerkiksi meidän kaltainen yritys voi suoraan laitteella blokkaa näitä sivustoja tai haittaohjelmia ynnä muuta. Että näissäkään ehkä ei ole mitään semmoista yhtä lähestymistapaa, vaan ihan niinku kyberresilienssi yrityksillekin, niin se pitää olla aika monia asioita ja se onkin monia asioita niin, että me voidaan saavuttaa sitten parempi ja turvallisempi internet.

00:45:57

Janina: Kyllä. Tuli vielä tässä yksi juttu mieleen, että miten… Pitäisikö meillä olla sitten semmoisia deittipalveluita, missä pitäisi niinku ihmisen todentaa, että minä olen minä?

00:46:08 **Riku:**

Onhan noissa… Siis tavallaan on nykyään semmoinen, että pitää ottaa selfietä ja useistakin eri kulmasta ja sitten sä saat täpän siihen, että ”verified user”, mutta… En mä jostain syystä enää luottais siihen. Ehkä sen pystyy tekemään tekemään niin kun tota joo…

00:46:28

Laura: Hyödyntää tekoälyä jotenkin.

00:46:30

Janina: Okei, eli sekin on mennyt. Mites että kaikki tämmöiset pankkivarmenteella, onko nekin sit…?

00:46:32

Riku: Ikävä kyllä. Mä en toisaalta sitten taas haluaisi ehkä lähteä itse laittamaan pankkivarmennetta mihinkään deittailusovellukseen.

00:46:38

Laura: Niin, lähtökohtaisesti mä en tiedä niin… Sinänsähän niin kun jos sen saisi silleen miten ne Suomessa toimii ne viranomaispalvelut, niin jotenkin sen…

00:46:46

Riku: Niin sen niinku Suomi.fi-tunnistautumisen kautta? Mutta en tiedä.

00:46:50

Laura: Tai niinku… Niin, niin. Mut mä luulen, että se on tällä hetkellä ehkä teknologinen haaste myös kun puhutaan esimerkiksi Tinder, Bumble, Facebook, Meta… Kaikki ne on kuitenkin jenkkiläisiä yrityksiä, niin se, että lähdettäisiin sitten jotain tuommoista rakentaa, niin se ei ole mitenkään ehkä ihan suoraviivainen teknologisesti ja lainsäädännöllisesti. Mutta voisiko niin tapahtua? En tee lakeja, mutta siis onhan niinku Euroopassa…

00:47:10

Janina: Lainsäätäjät, vink vink.

00:47:11

Laura: Niin jep. Plus että onko sitten ihmisen intressejä käyttää tommoista, että voi olla että ihmiset ei kuitenkaan sitten…

00:47:15

Riku: Niin, niin nostaisiko se sitä kynnystä liikaa sitten, että ei jaksa lähteä tommoiseen?

00:47:18

Laura: Niin. Ja onhan noissa rahaa tietysti, että sitten jonkun pitää koodaa se ja se maksaa se ylläpitäminen. Ja kuka sen sitten… Niinku nyansseja ja tämmöisiä…

00:47:26

Janina: Niin, aivan.

00:47:27

Laura: Voisiko tuommoinen joku olla? Mahdollisesti, mutta että mitä se sitten tarkoittaisi? Miltä se näyttäisi? Ja koska esimerkiksi tää pankkivarmenne-systeemi mikä Suomessa on, on kuitenkin melko uniikki maailmalla katsottuna, että eihän niinkun tää… Me ollaan totuttu, että meillä on se Suomi.fi, ja sitten sä menet Nordea-, OP-, Danske Bank-tunnuksella kirjautumaan… Tai mobiilivarmenteella. Mutta että ei tämmöistä systeemiä ole mitenkään kaikkialla.

00:47:54

Riku: Joo siis me ollaan aika moneen maahan nähden - niinku etenkin Keski-Euroopan maihin - niin aika edellä vielä toistaiseksi.

00:47:54

Laura: Joo, puhumattakaan jenkeissä, että siellä esimerkiksi… No tästä on jokunen vuosi, mutta törmäsin yhteen pankkiin, missä ei ollut esimerkiksi oletusarvoisesti monivaiheista tunnistautumista päällä, niin tota… Että puhutaan niinkun hyvin eri tasoisista asioista.

Ja sitten Suomessa me ollaan jossain kohtaa vaan tehty tämmöinen IT-infrastruktuurillinen päätös, että meillä on pankkivarmenteet, ja pankissa jengi käy varmentamassa itsensä, näyttämässä naamansa ja passinsa, ja sitten sen perusteella voidaan rakentaa tämmöinen tota kirjautumishimmeli sitten erinäköisiin palveluihin.

00:48:36

Janina: Aivan. Hei ihan mahtavaa keskustelua ollut tässä, ja jotenkin niinku olisi ihana jatkaa, mutta mä tiedän, että meidän kuulijat on siellä varmaan jo… En tiedä mitä teette. Toivottavasti te olette vielä kuulolla. Mutta haluaisin tähän vielä niinku… Että kuulijoille, mistä teitä voi niinku löytää että onko teillä jotain niinku… Haluatteko te jakaa jotain somea tai jotain, että jos nää niinku asiat ja ilmiöt kiinnostaa kuulijoita, että mistä teidät löytää?

00:49:04

Laura: No tota Laura Kankaala, allekirjoittanut, on Instagramissa pääasiallisesti, että on joissain muissa someissa, mutta Instagram on se mitä mä käytän joo pääasiallisesti. Ja siellä itse asiassa teen jonkun verran sisältöä liittyen just näihin - aika paljonkin sisältöä - liittyen tietoturvaan ja kyberturvallisuuteen, että en ainoastaan romanssinhuijauksiin, mutta aika laaja-alaisesti silleen näihin IT-ongelmiin.

00:49:27

Riku: Eikö se ollut se YLE:nkin joku yhteistyöprokkis?

00:49:33

Laura: Joo me tehdään... Ollaan nyt tehty jo jonkun aikaa YLE:n kanssa tämmöistä Hakkerin tietoiskut -sarjaa mikä julkaistaan siis…

00:49:37 **Riku:**

Ne on kyllä hyviä. Kyllä mä oon tykännyt.

00:49:39

Laura: Kiitos, kiitos kiitos.

00:49:40

Janina: No niin, menkää sinne katsomaan.

00:49:41

Laura: Joo ja Instagramista tosiaan julkaistaan näitä.

00:49:44

Janina: Joo, noniin. Miten Riku?

00:49:45

Riku: Joo mulla kanssa on insta ehkä se semmoinen aktiivisin kanava, mitä käytän että… Joskus käytti Twitteriä, mutta siihen meni vähän maku kun se lakkasi olemasta Twitter. Sieltä sitten löytää

00:49:53

Laura: Sama, joo.

00:50:00

Janina: Okei. Hei ihan mahtavaa, että olitte vieraina. Kiitos todella paljon vielä kerran.

00:50:03

Laura: Kiitos kutsusta.

00:49:04

Riku: Kiitos samoin, oli oikein mukava olla juttelemassa.

00:50:12

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.