KYMEN LAAKSON LIITTO

KOULUTUKSELLISIA HARJOITUKSIA

Satamalogistiikan kyberhygienia

Kyberuhkatekijät satamalogistiikan työturvallisuudessa

Projektinumero: 13300047

Tuomas Heikkinen & Vesa Tuomala

2023

XAMK
Kaakkois-Suomen ammattikorkeakoulu

1 JOHDANTO

Tässä julkaisussa tarkastellaan kyberhygieniataitojen testaamista ja informaatiovaikuttamiselta suojautumista. Kyberhygieniataitojen testaamisessa on viisi eri osiota. Testaamisen tarkoitus on auttaa tarkastelemaan jokaisen henkilökohtaisia kyberhygieniataitoja. Osioissa käsitellään salasanaturvallisuutta, huijausten tunnistamista, fyysistä turvallisuutta, etätyöturvallisuutta, ja miten ikävissä kyberturvallisuuden tilanteissa toimitaan.

Julkaisussa käsitellään myös informaatiovaikuttamista ja siltä suojautumista. Informaatiovaikuttamisen osioissa informaatiovaikuttaminen määritetään, sen keinoja esitetään ja kuvataan myös esimerkkejä informaatiovaikuttamisesta. Harjoituksen tavoite on, että jokainen voisi olla paremmin tietoinen siitä, miten jokaiseen meistä saattaa kohdistua vaikutusyrityksiä. Tietoisuuden avulla vaikuttamisyrityksiä vastaan voidaan suojautua.

2 KYBERHYGIENIATAITOJEN TESTAAMINEN

Osio 1: Salasanaturvallisuus

Salasanat, nuo viheliäiset mutta elintärkeät digitaalisen maailman avaimet. Jokaisella meistä on monia salasanoja eri verkkopalveluihin ja sovelluksiin, mutta kuinka usein pysähdymme pohtimaan niiden turvallisuutta? Tässä osiossa pääset testaamaan salasanaturvallisuuden taitojasi.

Osio 2: Huijausten tunnistaminen

Huijaukset ja petokset ovat ikävä osa digitaalista maailmaa, mutta onneksi meillä on keinot tunnistaa ja suojautua niiltä. Tässä osiossa pääset testaamaan huijausten tunnistamisen taitojasi.

Osio 3: Fyysinen turvallisuus

Jokainen työpiste on kuin oma pieni linnakkeensa, ja sen turvallisuus on tärkeää niin sinulle kuin edustamallesi organisaatiolle. Tässä osiossa pääset testaamaan osaamistasi työpisteen ja laitteiden turvallisuudesta.

Osio 4: Etätyöturvallisuus ja tietoturva matkustaessa

Työskentely etänä ja matkustaminen ovat joustavia tapoja hoitaa hommia, mutta samalla ne asettavat meidät uusien tietoturvahaasteiden eteen. Tässä osiossa pääset testaamaan etätyön tietoturvaosaamistasi.

Osio 5: Toiminta ikävässä tilanteessa

Joskus saattaa kohdata tilanteita, joissa kyberturva on uhattuna. Tässä osiossa pääset harjoittelemaan, miten toimit ikävissä tilanteissa.

Osio 1: Salasanaturvallisuus

Salasanat, nuo viheliäiset mutta tärkeät digitaalisen maailman avaimet. Jokaisella meistä on monia salasanoja eri verkkopalveluihin ja sovelluksiin, mutta kuinka usein pysähdymme pohtimaan niiden turvallisuutta? Tässä osiossa pääset testaamaan salasanaturvallisuuden taitojasi.

1. Skenaario: **Salasanan luominen**

Yrityksessänne on käytössä salasanasääntö, jonka mukaan salasanan tulee olla vähintään 12 merkin pituinen ja siinä tulee olla erikoismerkkejä ja numeroita. Minkä salasanan valitset?

a. R@iK4s#5lPs$m2!
b. Fifikani123!
c. Kissakiipesikatollekatsomaangorillaa!1

2. Skenaario: **Sähköposti**

Saat sähköpostiviestin, jonka lähettäjä on yrityksenne IT-tukihenkilö. Hän pyytää sinua salasanasi sähköpostin välityksellä varmistaakseen tilisi turvallisuuden. Mitä teet?

a. En jaa salasanaani sähköpostitse ja ilmoitan asiasta IT-tukeen jotakin toista viestintäkanavaa pitkin.
b. Vastaan viestiin ja jaan salasanani, sillä luotan IT-tukihenkilöön.
c. En reagoi viestiin.

3. Skenaario: **Sama salasana**

Olet huomannut, että käytät samaa salasanaa työpaikan tileissä kuin henkilökohtaisilla tileilläsi. Mitä teet?

a. Jatkat salasanojen käyttöä, koska niiden muistaminen on helppoa, enkä ole ikinä jakanut niitä muille.
b. Päivität kaikki salasanat erilaisiksi työpaikan tileissä ja henkilökohtaisissa tileissäsi.
c. Vaihdat salasanan työpaikan tileihin, mutta jatkat edelleen saman salasanan käyttöä henkilökohtaisissa tileissäsi.

4. Skenaario: **Salasanojen vaihtaminen**

Yrityksessäsi vaaditaan vaihtamaan salasana kolmen kuukauden välein. Sinusta tuntuu, että uusien salasanojen muistaminen aiheuttaa hankaluuksia. Mitä teet?

a. Muutan entistä salasanaani lisäämällä tai vaihtamalla muutaman merkin, jotta se täyttää uuden vaatimuksen, mutta on silti helppo muistaa.
b. Kirjoitan uuden salasanan muistilapulle ja säilytän sitä piilossa työpöytäni laatikossa.
c. Luon uuden vahvan salasanan ja otan käyttöön salasanan hallintaohjelman, joka auttaa minua muistamaan ja luomaan vahvoja salasanoja.

Osio 2: Huijausten tunnistaminen

Huijaukset ja petokset ovat ikävä osa digitaalista maailmaa, mutta onneksi meillä on keinot tunnistaa ja suojautua niiltä. Tässä osiossa pääset testaamaan huijausten tunnistamisen taitojasi.

1. Skenaario: **Tärkeä liitetiedosto**

Olet saanut sähköpostin, jossa väitetään olevan tärkeä liitetiedosto esihenkilöltäsi. Viestissä pyydetään avaamaan liite välittömästi. Miten reagoit?

a. Avaan liitteen heti, koska se tulee esihenkilöltäsi ja vaikuttaa tärkeältä.
b. Epäilen viestin aitoutta ja otan yhteyttä esihenkilöösi varmistaakseni viestin oikeellisuuden.
c. En avaa liitettä, vaan raportoin viestin tietoturvavastaavalle.

2. Skenaario: **Huijauspuhelu**

Saat puhelinsoiton henkilöltä, joka väittää olevansa yrityksen IT-tuen tuen edustaja ja ilmoittaa, että tietokoneesi on saanut viruksen. Hän pyytää päästä etäyhteydellä koneellesi korjatakseen ongelman. Mitä teet?

a. Annan hänelle etäyhteyden tietokoneelleni, koska hän väittää olevansa IT-tuen edustaja.
b. Kysyn häneltä lisätietoja ja pyydän tunnistamaan itsensä ennen kuin teen mitään.
c. Kerron puhelimessa olevalle henkilölle, että otan yhteyttä yrityksen IT-tukeen toista kanavaa pitkin ja suljen puhelun epäilyttävänä.

3. Skenaario: **Epäilyttävä linkki**

Olet saanut työsähköpostin, jossa ilmoitetaan tulevista kesäpäivistä ja ohjeistetaan kiireellisesti ilmoittautumaan tapahtumaan. Viestissä sanotaan, että linkki ohjautuu työpaikan kirjautumissivulle, jonka kautta pääset ilmoittautumaan. Mitä teet?

a. Klikkaan linkkiä heti, koska haluan varmistaa paikkani kesäpäivillä.
b. En klikkaa linkkiä, vaan ilmoitan epäilyttävästä sähköpostista IT-tukeen tai tietoturvavastaavalle.
c. Epäilen linkin aitoutta ja tarkastan huolellisesti linkin osoitteen ja viestin lähettäjän tiedot ennen kuin päätän klikata sitä.

4. Skenaario: **Laskutuspetos**

Saat sähköpostin, joka näyttää olevan yrityksesi toimittajalta. Laskussa oleva tilinumero on kuitenkin erilainen kuin aiemmin käytetty. Mitä teet?

a. Tarkistat toimittajan aikaisemmat laskut ja tilinumerot sekä otat yhteyttä toimittajaan puhelimitse tai muuta kautta varmistaaksesi tilinumeron oikeellisuuden.
b. Maksat laskun heti uudelle tilinumerolle, koska lähettäjä väittää sen olevan päivitetty tili.
c. Ilmoitat asiasta yrityksesi talousosastolle tai vastuulliselle henkilölle, jotta he voivat tutkia tilanteen ennen maksun suorittamista.

Osio 3: Fyysinen turvallisuus

Jokainen työpiste on kuin oma pieni linnakkeensa, ja sen turvallisuus on tärkeää niin sinulle kuin edustamallesi organisaatiolle. Tässä osiossa pääset testaamaan osaamistasi työpisteen ja laitteiden turvallisuudesta.

1. Skenaario: **Työpisteen järjestely**

Työskentelet avokonttorissa, ja työpöytäsi vieressä on useita muita työntekijöitä. Kun poistut työpisteeltäsi kahvitauolle, mitä teet?

a. Jätän tietokoneeni ja muut laitteeni auki ja lukitsematta, koska luotan kollegoihini.
b. Lukitsen tietokoneeni ja piilotan työpöydällä olevat paperit ennen kuin poistun työpisteeltäni.
c. Pyydän kollegoita pitämään silmällä työpisteelläni olevia laitteita, jotta ne eivät katoa.

2. Skenaario: **Epäilyttävä henkilö**

Havaitset henkilön kulkemassa organisaation tiloissa. Hänellä ei ole näkyvää kulkulupaa. Mitä teet?

a. Kysyt henkilöltä, kuka hän on ja mitä hän tekee toimistossa ennen kuin ilmoitat asiasta turvallisuudesta vastaavalle henkilölle.
b. Seuraat henkilön liikkeitä ja tarkkailet tilannetta, ennen kuin päätät, onko hänen käytöksessään syytä huolestua ja ilmoitat siitä turvallisuudesta vastaavalle henkilölle.
c. Ohitat tilanteen, koska et halua sekaantua mahdollisiin vierailijoihin ja uskot, että turvallisuudesta vastaava henkilö hoitaa asian tarvittaessa.

3. Skenaario: **Kadonnut laite**

Huomaat, että kannettava tietokoneesi on kadonnut työmatkan aikana. Et ole varma, oletko unohtanut sen kotiin vai onko se varastettu. Mitä teet?

a. Odotat päivän loppuun asti, jos laite löytyisi jostain ennen kuin teet ilmoituksen kateissa olevasta laitteesta.
b. Teet välittömästi ilmoituksen kadonneesta laitteesta tietoturvatiimille ja esihenkilöllesi.
c. Yrität muistella tarkemmin, missä laitteesi viimeksi oli, ennen kuin teet päätöksen ilmoituksen tekemisestä.

4. Skenaario: **USB-tikku**

Löydät työpöydältäsi USB-tikun, joka ei kuulu sinulle eikä kukaan ole kertonut sen jättämisestä. Mitä teet?

a. Liität USB-tikun tietokoneeseen nähdäksesi, mitä siellä on tallennettuna.
b. Otat USB-tikun mukaasi, jotta voit kysyä muilta työntekijöiltä, onko se heidän ja mitä siinä mahdollisesti on.
c. Jätät USB-tikun huomiotta ja raportoit siitä IT-osastolle tai tietoturvavastaavalle.

Osio 4: Etätyöturvallisuus ja tietoturva matkustaessa

Työskentely etänä ja matkustaminen ovat joustavia tapoja hoitaa hommia, mutta samalla ne asettavat meidät uusien tietoturvahaasteiden eteen. Tässä osiossa pääset testaamaan etätyön tietoturvaosaamistasi.

1. Skenaario: **Julkinen Wi-Fi**

Päätät työskennellä kahvilassa, jossa on julkinen Wi-Fi-verkko. Mitä teet?

a. Käytät julkista Wi-Fi-verkkoa ilman suojattua yhteyttä, koska se on kätevää, etkä tarvitse salasanaa.
b. Käytät kahvilan tarjoamaa suojattua Wi-Fi-verkkoa ja tarkistat, että selaimen osoite alkaa "https://" salatun yhteyden merkiksi.
c. Päätät olla käyttämättä Wi-Fi-verkkoa lainkaan ja jaat yhteyden työpuhelimestasi.

2. Skenaario: **Puhuminen julkisella paikalla**

Olet junassa ja yhtäkkiä puhelimesi soi. Huomaat, että kollegasi soittaa sinulle tärkeästä työasiasta. Keskustelu käsittelee luottamuksellisia asiakastietoja. Miten toimit?

a. Puhut puhelun normaalisti, koska sinulla ei ole muita vaihtoehtoja, mutta yrität puhua niin hiljaa kuin mahdollista.
b. Päätät olla puhumatta luottamuksellisista asioista julkisella paikalla ja sovit kollegan kanssa, että keskustelette myöhemmin.
c. Siirryn keskustelemaan rauhallisempaan paikkaan, jossa ei ole muita kuulolla.

3. Skenaario: **Työlaitteiden käyttäminen**

Olet kotona ja sinun täytyy tehdä kiireellinen työtehtävä, mutta työnantajasi tarjoama työkone ei ole käytettävissä. Harkitset oman kannettavan tietokoneesi käyttämistä.

a. Vältät etätyöskentelyä omalla laitteellasi.
b. Päätät käyttää omaa laitettasi tämän kerran.
c. Otat yhteyttä esihenkilöösi tai IT-tukeen kysyäksesi, onko etätyöskentely omalla laitteellasi sallittua.

4. Skenaario: **Työlaitteiden säilytys**

Pysäköit ravintolan eteen ja menet lounaalle. Sinulla on mukana työtietokone. Miten toimit?

a. Jätät tietokoneen takapenkille ja varmistat, että sitä näe ikkunasta.
b. Laitat tietokoneen takakonttiin lounaan ajaksi ja varmistat, että autosi on lukittu.
c. Otat tietokoneen mukaan ja varmistat sen turvallisen säilytyksen.

Osio 5: Toiminta ikävässä tilanteessa

Joskus saattaa kohdata tilanteita, joissa kyberturva on uhattuna. Tässä osiossa pääset harjoittelemaan, miten toimit ikävissä tilanteissa.

1. Skenaario: **Klikkasin linkkiä**

Olet kiireinen työpäiväsi aikana ja klikkaat sähköpostissa olevaa linkkiä ajattelematta asiaa sen tarkemmin. Linkki vie tutun näköiselle kirjautumissivulle. Heti klikkaamisen jälkeen tajuat, että tämä saattoi olla virhe. Mitä teet?

a. Panikoin hetken, suljen selaimen ja poistan sähköpostin.
b. Ilmoitan huijausviestistä IT-tukeen ja seuraan heidän ohjeitaan.
c. Jatkan työskentelyä normaalisti ja toivon parasta.

2. Skenaario: **Lunnasvaatimus**

Huomaat, että tietokoneellasi on ilmestynyt ilmoitus, jossa kerrotaan, että tietosi on salattu, ja sinulta vaaditaan lunnaita tietojen palauttamiseksi. Mitä teet?

a. Heti maksat lunnasvaatimuksen saadaksesi tiedot takaisin, koska pelkäät menettäväsi tärkeitä tietoja.
b. Yrität itse ratkaista tilanteen ja purkaa salauksen tai palauttaa tietoja varmuuskopioista.
c. Et maksa lunnaita ja otat yhteyttä tietoturvavastaavaan tai IT-tukeen selvittääksesi tilanteen ja mahdolliset toimenpiteet.

3. Skenaario: **Väärä vastaanottaja**

Lähetät vahingossa sähköpostin väärälle vastaanottajalle, sähköpostissa on henkilötietoja. Huomaat virheesi vasta lähettämisen jälkeen. Mitä teet?

a. Raportoit tapahtuneesta IT-tukeen ja tietosuojavastaavalle.
b. Pyydät anteeksi virhettä ja selität väärälle vastaanottajalle tilanteen.
c. Ilmoitat välittömästi vastaanottajalle virheestä ja pyydät häntä poistamaan asiakirjan.

4. Skenaario: **Laitteen häviäminen**

Matkustaessasi huomaat, että työpuhelimesi tai kannettava tietokoneesi on kadonnut. Mitä teet?

a. Päätät, että et voi tehdä mitään laitteen katoamisen vuoksi, ja jatkat matkaasi ilman lisätoimenpiteitä.
b. Ilmoitat välittömästi laitteen katoamisesta esihenkilöllesi tai IT-tuelle ja teet tarvittavat ilmoitukset sekä toimintasuunnitelman laitteen löytämiseksi tai tietojen suojaamiseksi.
c. Oletat, että laitteesi on unohtunut johonkin ja etsit sen vasta palatessasi.

3 INFORMAATIOVAIKUTTAMINEN JA SILTÄ SUOJAUTUMINEN

Mitä informaatiovaikuttaminen tarkoittaa?

Tässä osiossa selitetään, mitä informaatiovaikuttaminen tarkoittaa.

Informaatiovaikuttaminen

Mitä se tarkoittaa?

Informaatiovaikuttaminen tarkoittaa toimintaa, jossa pyritään järjestelmällisesti vaikuttamaan meidän mielipiteisiin sekä meidän käyttäytymiseen. Informaatiovaikuttaminen on siis toimintaa, jonka avulla kohde saadaan toimimaan itselleen haitallisesti ja omia etujaan vastaan. Yleensä informaatiovaikuttamisessa levitetään väärää tai harhaanjohtavaa tietoa.

Mikä sen tavoite on?

Informaatiovaikuttamisen tavoite voi olla esimerkiksi synnyttää vastakkainasettelua ihmisten välille, heikentää meidän turvallisuuden tunnetta tai saada meidät ajattelemaan tietyllä tavalla.

Kolmenlaista haitallista informaatiota

1. **Misinformaatio**
   Tarkoittaa sitä, että henkilö levittää tiedon eteenpäin tiedostamatta, että se on väärennettyä tai valheellista. Voi johtua levittäjän tietämättömyydesta tai siitä, ettei hän jaksa perehtyä asiaan.

2. **Disinformaatio**
   Tarkoittaa sitä, että henkilö levittää tiedon eteenpäin tiedostaen, että se on väärennettyä tai valheellista – tällä on aina jokin tavoite.

3. **Malinformaatio**
   Voidaan kutsua haitalliseksi tiedoksi; tieto on kyllä paikkansa pitävää, mutta sitä käytetään pahantahtoisesti. Voisi ajatella juoruksi, jossa esimerkiksi henkilökohtaisten tietojen avulla aiheutetaan haittaa kohteelle.

Keihin vaikuttamista kohdistetaan?

Vaikuttamista voidaan kohdistaa yksilöihin, yksilöityihin ryhmiin tai suureen yleisöön. Yksilöihin kohdistetaan vaikuttamista esimerkiksi heidän luonteenpiirteiden tai poliittisen näkemyksen pohjalta. Yksilöidyt ryhmät muodostetaan erottavien tekijöiden, kuten iän, koulutuksen tai työpaikan perusteella. Suuri yleisö tarkoittaa vaikuttamista laajempaan joukkoon, jopa koko yhteiskuntaan.

On tärkeä ymmärtää, että vaikuttamista voidaan kohdistaa myös sinuun.

Miksi kannattaa suojautua?

Informaatiovaikuttaminen on monesti hyvin ovelaa ja yleensä emme edes huomaa, että meihin vaikutetaan. Tässä piilee sen haitallisuus. Joku muu kykenee muokkaamaan meidän käytöstämme, mielipiteitämme ja ajatuksiamme ilman, että tiedostamme sitä.

Informaatiovaikuttamiselta kannattaa suojautua, jotta emme toimisi nappuloina jonkun muun pelissä. Suojautumalla myös heikennetään rikollisten ja muiden haitallisten tahojen toiminnan vaikutuksia laajemmin yhteiskunnassa.

Älä siis anna jonkun muun hallita toimintaasi, vaan vahvista omaa ja läheistesi valmiuksia vaikuttamiselle. Ole valppaana ja kyseenalaista se, mitä näet ja kuulet!

Tyypillisiä informaatiovaikuttamisen keinoja

Tässä osiossa tutustutaan tyypillisiin informaatiovaikuttamisen keinoihin. Valtioneuvoston kanslian oppaassa informaatiovaikuttamisen tekniikat jaetaan kuuteen kategoriaan.

Informaatiovaikuttamisen tekniikat:

1. **Verkostojen ja ajatusten hakkerointi**

Tässä informaatiovaikuttaja hyödyntää meidän sosiaalisia suhteitamme. Keinona voi olla esimerkiksi **kaikukammiot**. Kaikukammioissa ihmiset altistuvat sisällölle, joka vahvistaa heidän olemassa olevia näkemyksiä. Niissä jaetaan samanlaisia mielipiteitä ja ne estävät erilaisten mielipiteiden näkemisen.

2. **Harhaanjohtavat henkilöllisyydet**

Tässä informaatiovaikuttaja jäljittelee jotakin luotettavaa tahoa, esimerkiksi ihmistä tai yritystä. Keinona voi olla esimerkiksi **valemediat**. Valemediat ovat aitoja uutissivuja jäljitteleviä väärennettyjä sivuja.

3. **Tekninen manipulointi**

Tässä informaatiovaikuttaja käyttää hyväkseen tekniikkaa. Keinona voi olla esimerkiksi **kuvamanipulaatio**. Kuvamanipulaatio on tekoälyn avulla luotuja huijausvideoita, -kuvaa tai -ääntä.

4. **Pahantahtoinen retoriikka**

Tässä informaatiovaikuttaja vaikuttaa julkiseen keskusteluun. Keinona voi olla esimerkiksi **henkilöön kohdistuva hyökkäys**. Henkilöön kohdistuvassa hyökkäyksessä hyökätään argumentoivaa ihmistä kohtaan. Tavoitteena on pelotella ja hiljentää kohde.

5. **Symboliset teot**

Tässä informaatiovaikuttaja välittää viestin konkreettisten tekojen kautta. Keinona voi olla esimerkiksi **julkiset mielenosoitukset**. Julkisen mielenosoituksen tarkoitus voi olla luoda harhavaikutelma, että asialla on paljon kannatusta vaikkei todellisuudella näin ei olisi.

6. **Disinformaatio**

Käsittelimme aiemmin **disinformaatiota**, siis tiedon välittämistä tiedostaen, että se on virheellistä tai harhaanjohtavaa. Keinona voi olla esimerkiksi valheet. Valheissa julkaistaan virheellistä tietoa sellaisella tavalla, että vastaanottaja uskoo sen todeksi. Voidaan tehdä esimerkiksi tekaistu sähköpostiviesti kohteen nimissä.

Tekniikoita on paljon

Idea ei ole muistaa saatikka ymmärtää jokaista kategoriaa tai keinoa syvällisesti. Idea on, että voitte miettiä voisiko kyse olla informaatiovaikuttamisesta, kun kohtaatte uutta tietoa.

Esimerkkejä informaatiovaikuttamisesta

Tässä osiossa käydään läpi erilaisia esimerkkejä informaatiovaikuttamisesta. Esimerkkien kohdalla tutustutaan myös keskeisiin piirteisiin, jotka osoittavat informaatiovaikuttamista.

Esimerkki 1: Karjalan Liitto – Karjalaiset mahdollisen informaatiovaikuttamisen kohteena

Vuonna 2022 Karjalan Liiton julkaisi tiedotteen, jossa kerrottiin jäseniin kohdistuvista kahdenlaisista viesteistä. Viesteissä haluttiin herättää keskustelua Karjalan palauttamisesta tai itsenäisen Karjalan valtion perustamisesta. Yhteydenottoja on tapahtunut sosiaalisessa mediassa, sähköpostitse ja jopa kasvotusten. Samaan aikaan Venäjällä levitettiin uutisia, joiden mukaan Suomi haluaisi takaisin sodassa menetettyjä alueita.

Karjalan Liitto epäili, että kyse voisi olla informaatiovaikuttamisesta. Liiton mukaan vaikuttamisen tavoitteena voi olla, että vaikuttaja saisi heidät toimimaan itselleen haitallisesti ja omia etujaan vastaan.

Tämä esimerkki havainnollistaa, miten informaatiovaikuttaminen pyrkii manipuloimaan ihmisiä ja vaikuttamaan päätöksentekoon.

Esimerkki 2: Iltalehti – Zelenskyi joutui deepfake-iskun kohteeksi

Ukrainan presidentti Volodymyr Zelenskyistä levitettiin deepfake-videoväärennöstä, eli kuvamanipulaatiota, jossa Zelenskyi käskee joukkoja antautumaan. Todellisuudessa hän ei ollut oikeasti sanonut näin. Kuvamanipulaatiovideolla näytti esiintyvän aidon näköinen Zelenskyi, sillä se manipuloi presidentin kasvoja, eleitä ja suuta. On todennäköistä, että kyseessä oli Venäjän yritys harhauttaa Ukrainan kansalaisia ja muita maita. Vaikka video poistettiin esimerkiksi Facebookista, se levisi kuitenkin Venäjällä suositussa VKontakte- ja Telegram-kanavissa. Zelenskyi itse julkaisi nopeasti kuitenkin videon, jossa hän kiisti deepfake-videon aitouden.

Kuvamanipulaatiovideon voi nähdä esimerkiksi täältä:

Deepfake video of Volodymyr Zelensky surrendering surfaces on social media

Tämä esimerkki osoittaa, miten kuvamanipulaatiot pyrkivät leviämään ja vaikuttamaan poliittisiin tilanteisiin ja kansalaisten mielipiteisiin.

Esimerkki 3: Yle - Britannia käy Twitterissä ennennäkemätöntä propagandakampanjaa Venäjää vastaan

Britannian puolustusministeriö on julkaissut sodan aikana tiedusteluraportteja Twitterissä. Raportit ovat osa Venäjää vastaan kohdistettua informaatiovaikuttamista. Raportit korostavat Venäjän armeijan epäonnistumisia ja Ukrainan armeijan onnistumisia. Ylen toimittaja Sakari Nuuttila toteaa artikkelissa, että Venäjän hallinto hyödyntää sodassa propagandaa, joka perustuu valheisiin ja ristiriitaisiin viesteihin. Britannian tiedusteluraportit taas perustuvat todenmukaisiin faktoihin, mutta esitettävät faktat valikoidaan.

Professori Rory Cormacin mukaan raporttien tavoitteena on haastaa Venäjän versio tapahtumista. Cormac toteaa myös, että Ukraina pitää yllä taistelutahtoa ja lännen tukea valikoivan tiedon avulla. Tällaiselle on professorin mukaan helppo löytää ymmärrystä, kun kansalaiset taistelevat eloonjäämisestä.

Tämä esimerkki osoittaa, miten valtiot voivat käyttää esimerkiksi tiedusteluraportteja informaatiovaikuttamisen työkaluna. Totuuden mukaista tietoa voidaan käyttää valikoiden esimerkiksi vihollisen heikentämiseen tai liittolaisen tukemiseen.

Näin taistelet informaatiovaikuttamista vastaan

Tärkein suojautumiskeino informaatiovaikuttamista vastaan on suhtautua kriittisesti tietoon, jota kohtaamme päivittäin. Seuraavaksi käydään läpi 5 tapaa, joiden avulla voit tarkastella tekstin luotettavuutta.

1. **Tarkastele kokonaisuutta**

Älä tee pelkän otsikon tai lyhyen tekstipätkän perusteella johtopäätöksiä tekstin todellisesta sisällöstä. Viesti tulisi lukea kokonaan läpi ennen kuin siihen otetaan kantaa tai sitä jaetaan eteenpäin. Muista, että julkaisun suosio ei takaa julkaisun luotettavuutta.

2. **Selvitä, kuka tekstin on julkaissut**

Etsi tietoa kirjoittajasta ja julkaisijasta ja arvioi heidän luotettavuutta. Esimerkiksi somessa kannattaa tarkastella ainakin näitä: 1) milloin profiili on julkaistu, 2) onko sisältö käännetty automaattisesti ja 3) julkaistaanko sisältöä epätavallisesti. Tuore profiili, koneella käännetyt tekstit tai outo julkaisutahti saattavat viitata bottitiliin.

Muun median osalta voit pohtia, onko kyseessä tunnettu julkaisija. Ole kuitenkin kriittinen myös tunnettujen julkaisijoiden kohdalla ja tarkista, että tieto on paikkaansa pitävää! Kiinnitä huomiota myös verkko-osoitteeseen (URL). Onko sivusto oikeasti se, mikä se esittää olevansa vai onko osoitteessa esimerkiksi pieni kirjoitusvirhe? Tällöin kyseessä on huijaussivusto.

3. **Arvioi tekstin tavoitetta**

Jokaisella tekstillä on jokin tavoite tai viesti, jota se pyrkii välittämään lukijalle. Pohdi, miksi teksti on julkaistu ja mitä sillä halutaan saada aikaan. Onko teksti esimerkiksi informatiivinen tai argumentoiva? Perustuuko se tunteisiin, mielipiteisiin vai faktoihin? Kiinnitä huomiota myös kuviin: yrittävätkö ne vaikuttaa sinuun jollakin tavalla?

4. **Analysoi sisältöä kriittisesti**

Analysoi tekstin sisältöä kriittisesti. Tarkastele tekstin esittämiä väitteitä ja faktoja, ja varmista niiden paikkansapitävyys. Tarkista ovatko lähteet aitoja tai onko ne irrotettu asiayhteydestään. Älä myöskään automaattisesti luota lähteisiin, koska nekin voivat olla harhaanjohtavia tai virheellisiä. Kriittinen medialukutaito on avainasemassa, kun arvioidaan tiedon luotettavuutta.

5. **Kyseenalaista se, mitä näet**

Älä ota tietoa vastaan sinisilmäisesti, vaan tarkastele sitä aina kriittisesti. On totta, että kattavan taustatutkimuksen tekeminen jokaiselle tekstille vie aikaa ja on haastavaa. Tämän takia informaatiovaikuttaminen on kuitenkin tehokasta. Informaatiovaikuttaja voi hyödyntää tiedon paljoutta ja syöttää harhaanjohtavaa tai manipuloivaa sisältöä tietotulvan sekaan.

Siksi terve epäluuloisuus on tärkeää.

Oikeat vastaukset ”Kyberhygienian testaaminen” -kysymyksiin

Osio 1: Salasanaturvallisuus

1. Skenaario: **Salasanan luominen,** vastaus:
   c) Kissakiipesikatollekatsomaangorillaa!1
2. Skenaario: **Sähköposti,** vastaus:
   a) En jaa salasanaani sähköpostitse ja ilmoitan asiasta IT-tukeen jotakin toista viestintäkanavaa pitkin.
3. Skenaario: **Sama salasana,** vastaus:
   b) Päivität kaikki salasanat erilaisiksi työpaikan tileissä ja henkilökohtaisissa tileissäsi.
4. Skenaario: **Salasanojen vaihtaminen,** vastaus:
   c) Luon uuden vahvan salasanan ja otan käyttöön salasanan hallintaohjelman, joka auttaa minua muistamaan ja luomaan vahvoja salasanoja.

Osio 2: Huijausten tunnistaminen

1. Skenaario: **Tärkeä liitetiedosto,** vastaus:
   b) Epäilen viestin aitoutta ja otan yhteyttä esihenkilööni varmistaakseni viestin oikeellisuuden.
2. Skenaario: **Huijauspuhelu,** vastaus:
   c) Kerron puhelimessa olevalle henkilölle, että otan yhteyttä yrityksen IT-tukeen toista kanavaa pitkin ja suljen puhelun epäilyttävänä.
3. Skenaario: **Epäilyttävä linkki,** vastaus:
   c) Epäilen linkin aitoutta ja tarkastan huolellisesti linkin osoitteen ja viestin lähettäjän tiedot ennen kuin päätän klikata sitä.
4. Skenaario: **Laskutuspetos,** vastaus:
   a) Tarkistat toimittajan aikaisemmat laskut ja tilinumerot sekä otat yhteyttä toimittajaan puhelimitse tai muuta kautta varmistaaksesi tilinumeron oikeellisuuden.

Osio 3: Fyysinen turvallisuus

1. Skenaario: **Työpisteen järjestely,** vastaus:
   b) Lukitsen tietokoneeni ja piilotan työpöydällä olevat paperit ennen kuin poistun työpisteeltäni.
2. Skenaario: **Epäilyttävä henkilö**, vastaus:
   a) Kysyt henkilöltä, kuka hän on ja mitä hän tekee toimistossa ennen kuin ilmoitat asiasta turvallisuudesta vastaavalle henkilölle.
3. Skenaario: **Kadonnut laite,** vastaus:
   b) Teet välittömästi ilmoituksen kadonneesta laitteesta tietoturvatiimille ja esihenkilöllesi.
4. Skenaario: **USB-tikku,** vastaus:
   c) Jätät USB-tikun huomiotta ja raportoit siitä IT-osastolle tai tietoturvavastaavalle.

Osio 4: Etätyöturvallisuus ja tietoturva matkustaessa

1. Skenaario: **Julkinen Wi-Fi**, vastaus:
   c) Päätät olla käyttämättä Wi-Fi-verkkoa lainkaan ja jaat yhteyden työpuhelimestasi.
2. Skenaario: **Puhuminen julkisella paikalla**, vastaus:
   b) Päätät olla puhumatta luottamuksellisista asioista julkisella paikalla ja sovit kollegan kanssa, että keskustelette myöhemmin.

3. Skenaario: **Työlaitteiden käyttäminen,** vastaus:
   a) Vältät etätyöskentelyä omalla laitteellasi.
4. Skenaario: **Työlaitteiden säilytys,** vastaus:
   c) Otat tietokoneen mukaan ja varmistat sen turvallisen säilytyksen.

Osio 5: Toiminta ikävässä tilanteessa

1. Skenaario: **Klikkasin linkkiä,** vastaus:
   b) Ilmoitan huijausviestistä IT-tukeen ja seuraan heidän ohjeitaan.
2. Skenaario: **Lunnasvaatimus,** vastaus:
   c) Et maksa lunnaita ja ryhdy yhteyteen tietoturvavastaavan tai IT-tuen kanssa selvittääksesi tilanteen ja mahdolliset toimenpiteet.
3. Skenaario: **Väärä vastaanottaja,** vastaus:
   a) Raportoit tapahtuneesta IT-tukeen ja tietosuojavastaavalle.
4. Skenaario: **Laitteen häviäminen,** vastaus:
   b) Ilmoitat välittömästi laitteen katoamisesta esihenkilöllesi tai IT-tuelle ja teet tarvittavat ilmoitukset sekä toimintasuunnitelman laitteen löytämiseksi tai tietojen suojaamiseksi.