KyberSoTe – kyberkortit

Pelaamalla sote-arjen kyberturvallisuus tutuksi

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

jamk | Jyväskylän ammattikorkeakoulu

LAUREA AMMATTIKORKEAKOULU
University of Applied Sciences

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences

TURKU AMK

KyberSoTe-projekti (2024–2026) on rahoitettu Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030-ohjelmasta.

Kyberkorttipakan hyödyt:

1. **Tietoisuuden lisääminen**: Korttipakka auttaa lisäämään tietoisuutta kyberturvallisuudesta ja sen merkityksestä arjessa. Sen avulla voidaan tuoda tietoisuuteen ajankohtaisia kyberuhkia ja suojautumiskäytäntöjä kaikille työntekijöille.
2. **Keskustelun herättäminen**: Korttien avulla voidaan käydä rakentavia keskusteluja kyberturvallisuudesta, mikä auttaa tunnistamaan ja ennaltaehkäisemään mahdollisia haasteita.
3. **Oppimisen tukeminen**: Korttipakka tarjoaa jatkuvaa oppimista ja muistutuksia tärkeistä kyberturvallisuuskäytännöistä, mikä auttaa pitämään tiedot ja taidot ajan tasalla.
4. **Yhteisöllisyyden vahvistaminen**: Yhteiset keskustelut voivat vahvistaa tiimihenkeä ja yhteisöllisyyttä, mikä on tärkeää organisaation kyberturvallisuuskulttuurin näkökulmasta.
5. **Motivointi ja sitoutuminen**: Korttipakka voi toimia motivaattorina ja sitouttaa työntekijöitä noudattamaan kyberturvallisuuskäytäntöjä, kun he ymmärtävät niiden merkityksen ja kokevat olevansa osa kyberturvallista toimintakulttuuria.

Kyberkorttien käyttötavat:

1. **Osastokokoukset**: Korttipakkaa voidaan hyödyntää osastokokouksissa (tai muissa tiimin kokouksissa) herättämään keskustelua ajankohtaisista kyberturvallisuusteemoista ja jakamaan parhaita käytäntöjä.
2. **Tyhy-päivät**: Tyhy-päivien yhteydessä korttipakka toimii osana koulutushetkeä, jolloin kyberturvallisuusasioita käsitellään rennossa ja osallistavassa ilmapiirissä.
3. **Perehdytys**: Uusien työntekijöiden perehdytyksessä korttipakka on hyödyllinen työkalu, joka auttaa esihenkilöä käymään työntekijän kanssa keskustelua organisaation kyberturvallisuuskäytännöistä.
4. **Säännölliset koulutukset**: Korttipakkaa voidaan käyttää säännöllisissä koulutuksissa ja työpajoissa, joissa käsitellään erilaisia kyberturvallisuusteemoja ja harjoitellaan käytännön skenaarioita.
5. **Itseopiskelu**: Työntekijät voivat käyttää korttipakkaa myös itsenäisesti omien kyberturvallisuustaitojensa kehittämiseen ja ylläpitämiseen.
6. **Kyberkortit ständin materiaalina:** Kyberkortteja voidaan käyttää kyberständillä pelillisenä keskustelun herättäjänä.

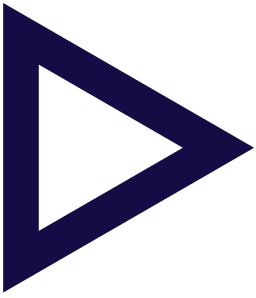
Kenen vastuulla on toteuttaa kyberturvallisuutta sote-alan organisaatioissa? Valitse kaikki oikeat vaihtoehdot.

a) Pelkästään tietohallinnon, koska he hallinnoivat teknisiä järjestelmiä ja verkkoja.

b) Pelkästään johtoryhmän, joka määrittelee organisaation kyberturvallisuusstrategian ja varmistaa tarvittavat resurssit.

c) Jokaisen organisaation työntekijän, inhimilliset virheet ovat yleinen uhka kyberturvallisuudelle.

d) Pelkästään tietoturvapäällikön, joka valvoo ja koordinoi kaikkia kyberturvallisuustoimia.



Oikea vastaus:

c) Jokaisen työntekijän rooli on toteuttaa kyberturvallisuutta käytännössä päivittäisessä työssään ja raportoida mahdollisista uhkista tai poikkeamista.

Sekundaarinen oikea vastaus:
b) Johdon tehtäviin kuuluu mm. kyberriskien-hallintatoimenpiteiden suunnittelu, hyväksyminen ja valvonta. Lain näkökulmasta johto on viimekädessä vastuussa kyberturvallisuudesta.

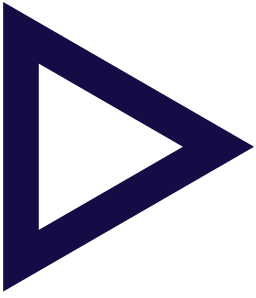
Missä tilanteissa voit antaa käyttäjätunnuksesi ja salasanasi? Valitse kaikki oikeat vaihtoehdot.

a) Tietohallinnon työntekijä pyytää niitä minulta kasvotusten tukipyynnön yhteydessä.

b) Viranomainen pyytää niitä minulta puhelimitse.

c) Opiskelija, jota ohjaan, tarvitsee ne käyttöönsä (koska hänellä ei ole omia tunnuksia).

d) En missään yllä olevista tilanteista.



Oikea vastaus:

d) Omaa käyttäjätunnusta ja salasanaa ei pidä missään tilanteessa paljastaa kenellekään.

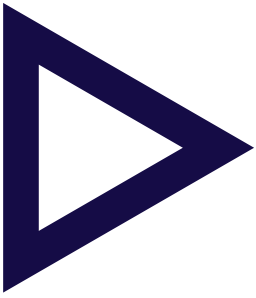
Mitä asioita sinun tulee huomioida kyberturvallisuuden näkökulmasta tehdessäsi etätöitä? Valitse kaikki oikeat vaihtoehdot.

a) Käytä vain organisaatiosi työvälineitä (tietokone, tabletti, puhelin jne.).

b) Työskentele yksityisessä tilassa, jossa ulkopuoliset eivät voi nähdä näyttöäsi tai kuulla keskustelujasi.

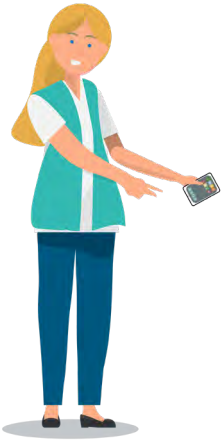
c) Käytä henkilökohtaista sähköpostiasi työasioihin vain, jos et pääse kirjautumaan työsähköpostiisi.

d) Pidä tietokoneesi lukittuna aina, kun poistut työpisteeltäsi.



Oikeat vastaukset:

a, b, d. Etätyökäytänteet voivat aiheuttaa uhkia kyberturvallisuuden näkökulmasta, joten on tärkeä noudattaa organisaation laatimia etätyöohjeita ja näin varmistaa turvallinen tapa toimia myös etätöissä.



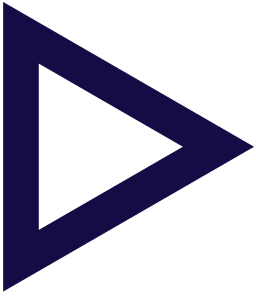
Mitkä alla olevista väittämistä pitävät paikkansa liittyen tekoälysovellusten käyttöön tietoturvallisesti? Valitse kaikki oikeat vaihtoehdot.

a) Tekoälysovelluksen käyttö vaatii aina erillisen lisenssin, joten sitä on tietoturvallista käyttää.

b) Varmista, että käyttämäsi tekoälysovellus on organisaatiosi hyväksymä ja olet perehtynyt organisaatiosi tekoälyn käytön ohjeistuksiin.

c) Tarkista tekoälyn antamat vastaukset, sillä ne voivat sisältää virheellistä tai harhaanjohtavaa tietoa.

d) Voin syöttää tuttuun tekoälysovellukseen arkaluonteisia tai henkilötietoja sisältäviä tietoja.



Oikeat vastaukset:

b, c. Tekoälysovellukset voivat helpottaa olennaisesti työtä, mutta niiden käyttö voi myös aiheuttaa uhkia kyberturvallisuuden näkökulmasta, joten on tärkeää noudattaa organisaation laatimia ohjeita tekoälyn käytön osalta ja näin varmistaa turvallinen tapa toimia.

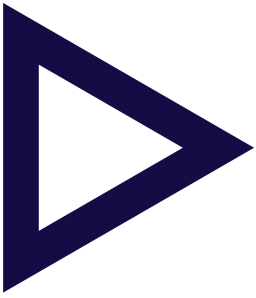
Mitkä alla mainituista ovat tyypillisiä tietojen-kalastelusähköpostin tunnusmerkkejä? Valitse kaikki oikeat vaihtoehdot.

a) Viesti sisältää kiireellisen kehotuksen toimia, kuten ”Tilisi suljetaan, ellet toimi heti!”.

b) Lähettäjän sähköpostiosoite näyttää oudolta tai poikkeaa normaalista.

c) Viestissä on kirjoitusvirheitä tai kömpelöä kieltä.

d) Sinua pyydetään antamaan arkaluonteista tietoa, kuten pankkitietoja tai kirjautumistietoja.



Oikea vastaus:

Kaikki vaihtoehdot ovat oikein. Muista pysähtyä lukiessasi työsähköpostiasi tai tekstiviestejä, älä tee nopeita hätiköityjä päätöksiä. Huom! Tekoälyn nopean kehityksen myötä huijausviestien kielivirheet ovat vähentyneet ja kalasteluviestit saattavat olla todella laadukkaita. Älä siis luota pelkästään viestin hyvään kieliasuun.

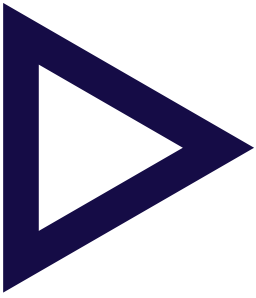
Mitkä ovat terveydenhuoltoalan yleisimpiä kyberuhkia Euroopassa? Valitse kaikki oikeat vaihtoehdot.

a) Palvelunestohyökkäykset.

b) Biotietokantojen manipulointi geneettisen profiloinnin väärentämiseksi.

c) Tietoihin kohdistuvat uhat (tietomurrot ja tietovuodot).

d) Kiristyshaittaohjelmat.



Oikeat vastaukset:

a), c), d) Lähde: Euroopan unionin kyberturvallisuus-virasto ENISA:n vuonna 2023 julkaisema raportti.

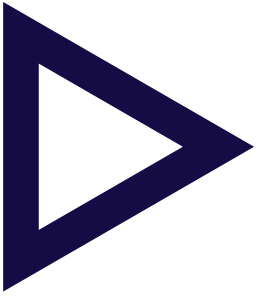
Mikä on palvelunestohyökkäys?

a) Tapa, jolla verkkosivustoja suojataan haittaohjelmilta.

b) Verkkohyökkäys, jossa pyritään estämään verkkosivuston tai verkkopalvelun käyttö.

c) Menetelmä, jolla käyttäjät voivat palauttaa unohtuneen salasanansa.

d) Ohjelmisto, joka analysoi verkkoliikennettä ja parantaa suorituskykyä.



Oikea vastaus:

b). Palvelunestohyökkäyksessä **palvelua kuormitetaan liikaa**, esimerkiksi lähettämällä sille valtava määrä pyyntöjä lyhyessä ajassa. Tällöin palvelu ei ehdi vastata oikeille käyttäjille ja **lakkaa toimimasta tai hidastuu merkittävästi**.

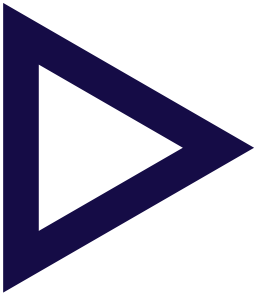
Minkälainen on vahva salasana?
Valitse kaikki oikeat vaihtoehdot.

a) Se sisältää erikoismerkkejä, isoja kirjaimia ja numeroita.

b) Se on vähintään 12 merkkiä pitkä ja vaikea arvata.

c) Se ei ole lause, koska lause voi olla helposti arvattava.

d) Se ei perustu henkilökohtaisiin tietoihin, kuten syntymäpäivään tai lemmikin nimeen.



Oikeat vastaukset:

a), b) ja d). Myös lause on hyvä salasanana ja se on usein helpompi muistaa kuin satunnainen merkkijono. Pituus tekee siitä vahvan. Lauseeseen, kun ujuttaa vielä mukaan, vaikka numeron ja erikoismerkin, niin vahvistaa salasanaa edelleen.

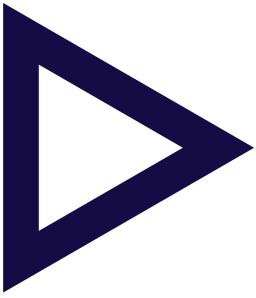
Mitkä seuraavista ovat todennäköisesti tietojenkalastelua (phishing)? Valitse kaikki oikeat vaihtoehdot.

a) Sähköposti, jossa pyydetään kirjautumaan pankkitilille oudon linkin kautta.

b) Viranomaiselta tullut tekstiviesti, jossa pyydetään henkilötietoja.

c) Viesti, jossa tarjotaan ilmainen älypuhelin, jos syötät henkilötietosi.

d) Selaimen ilmoitus, jossa pyydetään tekemään päivitys tietoturvasyistä.



Oikeat vastaukset:

a), b) ja c). Tietojenkalastelu esimerkiksi sähköpostin, tekstiviestin, puhelun tai epäilyttävän verkkosivun kautta on hyvin yleistä, joten kannattaa aina suhtautua hieman skeptisesti, jos jokin kuulostaa liian hyvältä tai sinulta vaaditaan välitöntä nopeaa toimintaa. Jos epäilyksesi heräävät, varmista viestin aitous suoraan lähettäjänä esiintyneeltä taholta käyttämällä virallisia yhteystietoja.

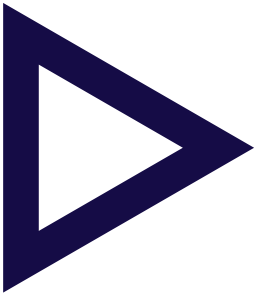
Mikä on kaksivaiheinen tunnistautuminen (2FA)? Valitse kaikki oikeat vaihtoehdot.

a) Kirjautuminen kahdella eri laitteella.

b) Kirjautuminen salasanalla ja erillisellä vahvistuskoodilla.

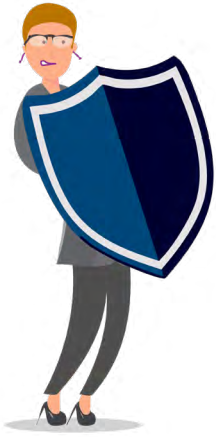
c) Turvatoimi, joka lisää ylimääräisen vahvistusvaiheen kirjautumiseen.

d) Tapa estää tilin luvaton käyttö, vaikka salasana vuotaisi.



Oikeat vastaukset:

b), c) ja d) Monivaiheinen tunnistautuminen (Multi-factor Authentication, MFA) tarkoittaa sitä, että kirjautuessa käytetään kahta tai useampaa tapaa varmistaa, että sinä olet todella itse kirjautumassa. Vaikka ulkopuolinen saisi käsiinsä käyttäjätunnuksesi ja salasanasi, hänen ei ole mahdollista kirjautua tilillesi ilman toista tunnistustapaa, kuten puhelimeesi lähetettyä kertakäyttöistä koodia. Kaksivaiheinen tunnistautuminen (Two-factor Authentication, 2FA) on tyypillisin monivaiheisen tunnistautumisen muoto.



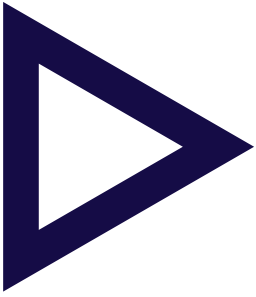
Mikä on VPN:n (Virtual Private Network) tarkoitus? Valitse kaikki oikeat vaihtoehdot.

a) Nopeuttaa internet-yhteyttä.

b) Suojata verkkoliikennettä salaamalla se.

c) Mahdollistaa turvallinen yhteys julkisessa Wi-Fi-verkossa.

d) Piilottaa käyttäjän todellinen IP-osoite*.



Oikeat vastaukset:

b), c) ja d). Ilman VPN-yhteyttä netin käyttösi on vähän kuin postikortti: kuka tahansa matkalla voi lukea sen. VPN tekee siitä kirjekuoren: vain vastaanottaja näkee sisällön.

*IP-osoite (Internet Protocol -osoite) on numerosarja, joka yksilöi laitteen verkossa. Sen avulla tietokoneet ja palvelimet löytävät toisensa ja osaavat lähettää tietoa oikeaan paikkaan.

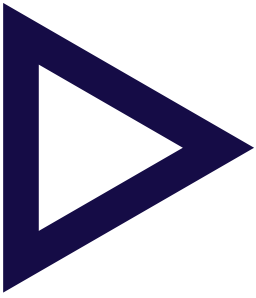
Mikä on deepfake? Valitse kaikki oikeat vaihtoehdot.

a) Tekoälyllä luotu kuva tai video, jossa henkilö näyttää tekevän tai sanovan jotain, mitä hän ei oikeasti ole tehnyt tai sanonut.

b) Moderni haittaohjelma, joka lukitsee tietokoneen.

c) Manipuloitu media, joka voi näyttää aidolta, mutta on väärennös.

d) Teknologia, jota voidaan käyttää sekä viihteessä että huijauksissa.



Oikeat vastaukset:

a), c) ja d). Deepfake-teknologialla tehtävien huijausten ennustetaan yleistyvän tulevaisuudessa. Jo nyt maailmalla tunnetaan tapauksia, joissa työntekijä on deepfake-videon perusteella tehnyt miljoonien eurojen tilinsiirron yrityksen tililtä huijarille luullessaan asioivansa esimerkiksi toimitusjohtajan kanssa.

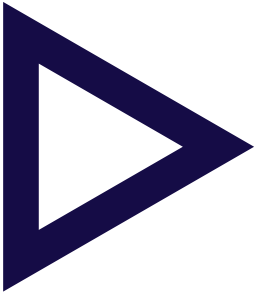
Mikä on NIS2-direktiivi ja miten se liittyy sosiaali- ja terveydenhuoltoalaan? Valitse kaikki oikeat vaihtoehdot.

a) Se on EU:n kyberturvallisuusdirektiivi, joka koskee myös sote-alaa.

b) Se edellyttää, että sote-alan organisaatiot tunnistavat ja hallitsevat kyberriskejä sekä ilmoittavat tietoturvaloukkauksista viranomaisille.

c) Se koskee vain yksityisiä IT-alan yrityksiä, eikä vaikuta julkisiin palveluihin.

d) Se vapauttaa sote-organisaatiot vastuusta, jos tietoturvaloukkaus johtuu alihankkijasta.



Oikeat vastaukset:

a) ja b). Kyberturvallisuuslaki, joka toimeenpanee Suomessa EU:n NIS2-direktiivin, astui voimaan 8.4.2025. Laki määrittää vähimmäisvaatimukset kyberturvallisuuden riskienhallinnan ja poikkeamien raportoinnin osalta useille yhteiskunnan toiminnan kannalta kriittisille toimialoille (kuten terveysala), ja se laajentaa aiemman NIS-direktiivin soveltamisalaa.

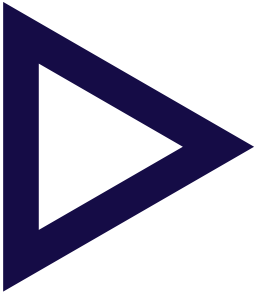
Mitä suoria vaikutuksia kyberhyökkäyksellä voi olla asiakas-/potilasturvallisuuteen?

a) Asiakas- ja potilastiedot eivät ole saatavilla kriittisellä hetkellä, mikä voi vaarantaa hoidon jatkuvuuden.

b) Organisaation sisäiset prosessit voivat hidastua, mikä voi aiheuttaa hallinnollista kuormitusta.

c) Asiakkaat/potilaat voivat menettää luottamuksensa palveluntarjoajaan, mikä voi vaikuttaa hoitoon hakeutumiseen.

d) Tietojärjestelmien käyttöön voi tulla viiveitä, mikä voi vaikuttaa työntekijöiden tehokkuuteen.



Oikea vastaus:

a). vain a-vaihtoehto liittyy suoraan asiakas-/potilasturvallisuuden vaarantumiseen, kun taas muut ovat *epäsuoria tai organisatorisia vaikutuksia*, jotka eivät itsessään vielä vaaranna asiakasta tai potilasta – mutta voivat toki vaikuttaa hoidon laatuun pitkällä aikavälillä.

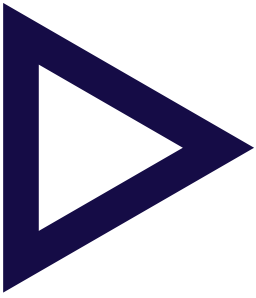
Mitkä seuraavista voivat sisältää haittaohjelman? Valitse kaikki oikeat vaihtoehdot.

a) Excel-taulukko, joka saapuu tuntemattomalta lähettäjältä liitetiedostona.

b) Työterveyden lähettämä sisäinen raportti.

c) Tuntemattoman lähteen tarjoama, ilmaiseksi ladattava sovellus.

d) Sähköpostiviesti, joka sisältää kutsulinkin työpaikan koulutukseen, joka löytyy intrasta.



Oikeat vastaukset:

a) ja c). Haittaohjelma (englanniksi *malware*, lyhenne sanoista *malicious software*) on tahallisesti vahinkoa aiheuttava tietokoneohjelma.

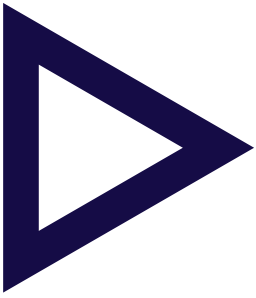
Mikä seuraavista täyttää parhaiten GDPR:n vaatimukset henkilötietojen käsittelyssä?

a) Asiakas antaa suullisen luvan tietojensa tallentamiseen ilman dokumentointia.

b) Tietoja säilytetään rajoittamaton aika varmuuden vuoksi.

c) Henkilötietojen käsittely perustuu lakiin tai kirjalliseen suostumukseen, ja tiedot poistetaan, kun niitä ei enää tarvita.

d) Tietoja voi käyttää vapaasti koulutustarkoituksiin, jos nimi poistetaan.



Oikea vastaus:

c). GDPR (General Data Protection Regulation) on EU:n tietosuoja-asetus, joka säätelee, miten ihmisten henkilötietoja saa kerätä, käsitellä ja säilyttää. Asetus tuli voimaan 25.5.2018 ja koskee kaikkia EU:n alueella toimivia organisaatioita – myös suomalaisia yrityksiä ja viranomaisia.

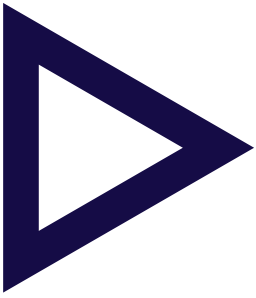
Mitä tarkoittaa “minimointiperiaate” tietosuojassa?

a) Henkilötietoja käsitellään vain, kun asiakas pyytää sitä.

b) Tietoja kerätään ja käsitellään vain siinä laajuudessa kuin on tarpeellista.

c) Käyttäjätunnuksia ja salasanoja ei säilytetä lainkaan.

d) Tallennetaan ainoastaan alle 18-vuotiaiden tiedot.



Oikea vastaus:

b). Minimointiperiaate on yksi keskeinen periaate tietosuojassa, erityisesti GDPR-asetuksessa. Et saa kysyä, tallentaa tai käsitellä ylimääräisiä tietoja, joita et tarvitse. Kerättävien tietojen pitää olla olennaisia, tarpeellisia ja rajoitettuja käyttötarkoitukseen nähden.

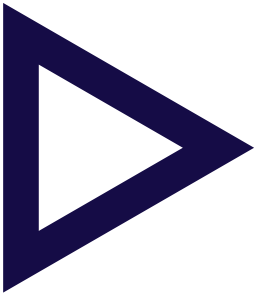
Miksi on tärkeä suojautua kiristyshaittaohjelmilta? Valitse kaikki oikeat vaihtoehdot.

a) Kiristyshaittaohjelmat voivat lamauttaa kokonaisia tietojärjestelmiä ja keskeyttää organisaation toiminnan.

b) Kiristyshaittaohjelmahyökkäys voi johtaa arkaluonteisten tietojen vuotamiseen julkisuuteen.

c) Kiristyshaittaohjelma voi kohdistua yksittäiseen henkilöön, mutta vaikutukset voivat ulottua koko organisaatioon.

d) Kiristyshaittaohjelma voi estää pääsyn kriittiseen tietoon tai tietojärjestelmään.



Oikeat vastaukset:

Kaikki vaihtoehdot ovat oikein. Tunnetuin esimerkki kiristyshaittaohjelmahyökkäyksestä Suomessa on Vastaamon tietomurto. Se on Suomen rikoshistorian suurin yksittäinen rikos asianomistajien määrällä mitattuna. Lokakuussa 2020 paljastuneessa tietomurrossa varastettiin noin 33 000 psykoterapia-asiakkaan henkilö- ja potilastietoja. Tiedoilla kiristettiin rahaa niin Vastaamolta kuin sen asiakkailta, ja tietoja vuodettiin julkisuuteen.

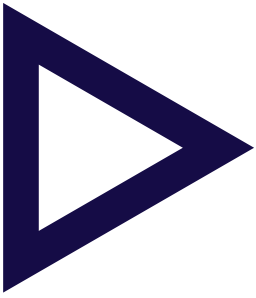
Miksi tietoturvallisesti toimiminen on tärkeää myös työntekijän itsensä kannalta? Valitse kaikki oikeat vaihtoehdot.

a) Tietoturvaloukkaukset voivat johtaa vakaviin seurauksiin, kuten varoituksiin, työsuhteen päättymiseen tai jopa vahingonkorvaustuomioihin, jos työntekijä toimii tahallaan huolimattomasti.

b) Työntekijä käsittelee usein työssään myös omia henkilötietojaan ja tietoturvallinen toiminta estää myös niiden joutumisen vääriin käsiin ja suojaa työntekijää identiteettivarkauksilta.

c) Tietoturvallisesti toimiminen varmistaa, että työntekijä saa automaattisesti korvauksia tietoturvaloukkaustilanteessa.

d) Tietoturvallisesti toimiminen tukee työntekijän ammatillista vastuullisuutta ja eettistä toimintaa.



Oikeat vastaukset:

a), b), d). Turvallinen tapa toimia tuo suojan myös työntekijälle itselleen. On tärkeää, että työntekijänä tunnet oman organisaatiosi tietoturvaohjeet ja ohjeet poikkeustilanteissa toimimiseen.

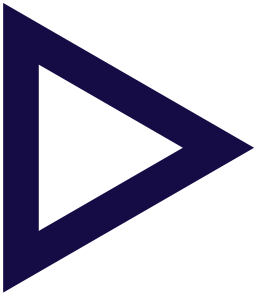
Millaisia vaikutuksia kyberhyökkäyksillä voi olla sosiaali- ja terveysalalla? Valitse kaikki oikeat vaihtoehdot.

a) Kyberhyökkäykset voivat vahvistaa asiakkaiden ja potilaiden sitoutumista hoitoon järjestelmien käyttökatkon jälkeen.

b) Kyberhyökkäyksen seurauksena tiedon saanti voi vaikeutua ja palvelut keskeytyä, mikä voi vaarantaa asiakkaiden ja potilaiden turvallisuuden.

c) Kyberhyökkäykset voivat aiheuttaa suuria välittömiä ja välillisiä kustannuksia organisaatiolle.

d) Kyberhyökkäykset voivat vaikeuttaa organisaation normaalia toimintaa hyökkäyksestä palautumisen aikana.



Oikeat vastaukset:

b), c), d). Kyberhyökkäyksellä voi olla negatiivisia vaikutuksia organisaation maineeseen, talouteen sekä potilaiden ja asiakkaiden luottamukseen ja se voi aiheuttaa mittavia häiriöitä organisaation toimintaan.

Kyberhyökkäykset vaarantavat pahimmillaan myös asiakkaiden ja potilaiden turvallisuuden, jos hoidon kannalta kriittisiä tietoja tai palveluita ei ole saatavilla.

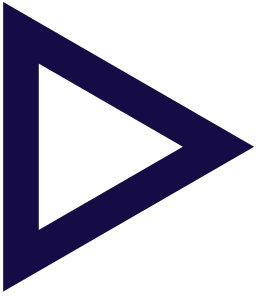
Havaitset tietokoneella työskennellessäsi poikkeavaa toimintaa: ohjelmien avaaminen on selvästi hidastunut, laitteelle on ilmestynyt ohjelmia, joita et ole itse asentanut tai joista ei ole tiedotettu, hiiren kursori liikkuu oudosti tai näytölle ilmestyy epätavallisia ponnahdusikkunoita. Miten toimit? Valitse kaikki oikeat vaihtoehdot.

a) Ilmoitat havainnoistasi IT-tukeen tai esihenkilöllesi organisaation ohjeistusten mukaisesti.

b) Yrität poistaa epäilyttävät ohjelmat itse ja jatkat työskentelyä normaalisti.

c) Oletat kyseessä olevan vain tilapäinen häiriö ja käynnistät koneen uudelleen ilman lisätoimenpiteitä.

d) Kirjaat tekemäsi havainnot ylös mahdollisimman yksityiskohtaisesti mahdollista selvitystyötä varten.



Oikeat vastaukset:

a) ja d). Kuvaillut merkit voivat viitata siihen, että laitteessa on havaittu ulkopuolista kybervaikuttamista, joka voi liittyä esimerkiksi haittaohjelmaan tai koneen luvattomaan etäohjaukseen. Ilmoita havainnoistasi välittömästi eteenpäin organisaatiosi ohjeistusten mukaisesti. On myös tärkeää kirjata havainnot välittömästi ylös mahdollisimman yksityiskohtaisesti, jotta ne eivät unohdu. Yksityiskohdista voi olla paljon apua tilanteen selvittelyssä.

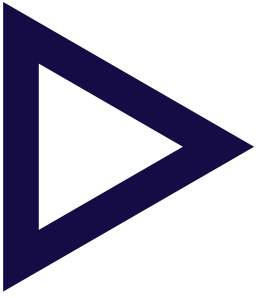
Mitä asioita sinun tulee huomioida kyberturvallisuuden näkökulmasta käyttäessäsi sosiaalista mediaa? Valitse kaikki oikeat vaihtoehdot.

a) Varmistat, että et jaa tietoa, joka sisältää arkaluonteisia henkilötietoja tai organisaatioon liittyviä luottamuksellisia asioita.

b) Suositus on, että käytät samaa salasanaa sosiaalisen median palveluissa kuin työpaikan järjestelmissä, jotta muistat sen helpommin.

c) Huolehdit, että jakamassasi kuvamateriaalissa ei näy taustalla asiakkaita tai heitä koskevia tietoja.

d) Sosiaalisen median (esim. WhatsApp) käyttö työssä on turvallista, kunhan käytät organisaation laitteita.



Oikeat vastaukset:

a) ja c). Ole tarkkana sen suhteen, mitä jaat sosiaalisessa mediassa. Kuvissa ja teksteissä ei saa näkyä mitään, mikä voisi vaarantaa kyberturvallisuuden, tietosuojan tai asiakkaiden yksityisyyden. Verkkoon jaettu sisältö voi levitä laajalle ja sen poistaminen jälkikäteen voi olla vaikeaa tai jopa mahdotonta. Käytä työasioihin liittyvässä viestinnässä vain organisaation hyväksymiä sovelluksia ja ohjelmistoja. Älä käytä samaa salasanaa eri palveluissa.

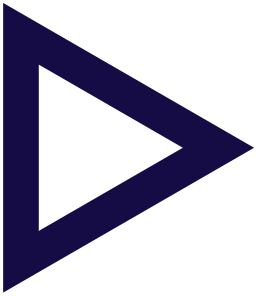
Mitkä seuraavista ovat hyviä turvallisuuskäytäntöjä liittyen työlaitteisiin? Valitse kaikki oikeat vaihtoehdot.

a) Käytät työnantajan tarjoamia laitteita myös henkilökohtaisten asioiden hoitamiseen, koska ne ovat paremmin suojattuja ulkopuolisilta uhkilta.

b) Et jätä työlaitteita valvomatta julkisiin tai lukitsemattomiin tiloihin, jotta ne eivät päädy vääriin käsiin.

c) Poistuessasi tilasta lukitset aina koneesi tai kirjaudut ulos yhteiskäyttökoneilta.

d) Jos laite vaatii päivitystä, lykkäät sitä myöhemmäksi, jotta työsi ei keskeydy.



Oikeat vastaukset:

b) ja c). On tärkeää, että säilytät työlaitteitasi siten, ettei ulkopuolisilla ole pääsyä niihin tai niiden kautta organisaation järjestelmiin ja tietoihin.

Työlaitteet on tarkoitettu työasioihin ja niiden käyttäminen henkilökohtaisiin tarkoituksiin voi altistaa laitteen ja organisaation verkon kyberriskeille.

Hyvä käytäntö on, että asennat päivitykset viipymättä niiden tullessa saataville, vaikka se hetkellisesti keskeyttäisi työn. Päivitykset sisältävät usein tietoturvakorjauksia, jotka suojaavat laitteita uusilta uhkilta.

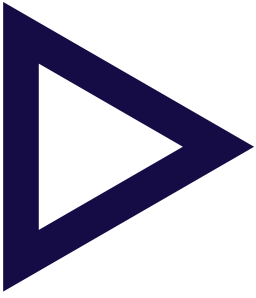
Mitkä seuraavista väittämistä QR-koodeihin liittyvässä tietojenkalastelussa (quishing) pitävät paikkansa? Valitse kaikki oikeat vaihtoehdot.

a) Rikolliset voivat levittää haitallisia QR-koodeja sähköpostitse, sosiaalisessa mediassa tai fyysisinä tarroina.

b) QR-koodin skannaaminen ei koskaan johda haittaohjelman lataamiseen, koska QR-koodit sisältävät vain URL-osoitteita.

c) Lyhennetyt URL-osoitteet QR-koodissa voivat peittää linkin todellisen kohteen, mikä tekee huijauksesta vaikeammin havaittavan.

d) QR-koodilla tehty tietojenkalastelu voi ohittaa perinteiset roskapostisuodattimet, koska suodattimet eivät osaa avata QR-koodeja.



Oikeat vastaukset

a), c) ja d). Käsittele QR-koodia kuten linkkiä: ennen kuin luet QR-koodin sähköpostiviestistäsi, mieti onko viesti aito vai yritetäänkö sinulta huijata tunnuksia tai muita arkaluonteisia tietoja. Kun viet kameran QR-koodin päälle, katso rauhassa koodin linkki ennen kuin klikkaat sitä (jos linkki on epäilyttävä, älä klikkaa). Varo lyhennettyjä linkkejä: jos näyttöön tulee lyhennetty URL-osoite, sinulla ei ole mitään keinoa tietää, minne linkki sinut vie. Esimerkiksi bit.ly alkuinen tai muu erikoinen ja lyhyt linkki voi viedä suoraan huijaussivustolle. Turvallisen suomalaisen verkkosivun URL-osoite alkaa aina https:// ja sisältää suomalaisen .fi-päätteen. Esimerkiksi osoite https://www.traficom.fi on turvallinen, koska se alkaa HTTPS-protokollalla ja päättyy .fi-verkkotunnukseen, joka kuuluu Traficomille.