

Testaa tietosi digitaalisesta turvallisuudesta! 1/4

On tärkeää olla tietoinen digitaalisista riskeistä ja turvatoimenpiteistä. Tämä kysely on suunniteltu testaamaan ja laajentamaan tietämystäsi digitaalisesta turvallisuudesta. Tämän kyselyn avulla saat myös arvokkaita oivalluksia, joita voit jakaa työssäsä nuorten kanssa.

Ympyröi mielestäsi sopivin vastaus. Oikeat vastaukset selityksineen löydät sivuilta 3–4.

1. Kun keräätte nuorilta henkilötietoja, miten informoitte heitä tietojen käsittelystä?

- A. Emme yleensä informoi erikseen, keräämme vain tarvittavat tiedot.
- B. Kerromme nuorille selkeästi ja ymmärrettävästi, millä perusteella ja mihin heidän tietojaan käytetään ja miten he voivat hallita omia tietojaan.
- C. Informointi tapahtuu vain, jos nuori tai hänen huoltajansa kysyy siitä.

2. Mitä menetelmiä käytätte nuorten tietoturvan varmistamiseen digitaalisissa kommunikaatio-kanavissa?

- A. Opetamme nuoria käyttämään vahvoja salasanoja ja monivaiheista tunnistautumista.
- B. Kaikki keskustelut käydään avoimissa kanavissa, jotta voimme valvoa keskustelujen asianmukaisuutta.
- C. Käytämme vain yhtä, turvalliseksi tiedettyä kommunikaatiokanavaa, ja muita kanavia ei sallita.

3. Kuinka varmistatte, että nuorten henkilötietoja käsittelee vain sellaiset henkilöt, joilla on siihen tarve työnsä puolesta?

- A. Meillä on käytössä yksi yhteinen salasana, joka on kaikkien työntekijöiden tiedossa.
- B. Jokaisella työntekijällä on henkilökohtaiset käyttäjätunnukset ja salasanat, jotka antavat pääsyn vain heidän työtehtäviensä kannalta välttämättömiin tietoihin.
- C. Tiedot säilytetään lukitussa kaapissa, ja avain on kaikkien työntekijöiden yhteisessä käytössä. Tästä ei tarvita erillistä kirjallista mainintaa missään.

4. Miten käsittelette tietosuojaa ja tietoturvaa nuorten kanssa?

- A. Tarjoamme nuorille vuosittaisen työpajan, jossa käsitellään tietosuojaan ja tietoturvaan liittyviä kysymyksiä.
- B. Tietosuoja ja tietoturva on sisällytetty kaikkeen työhömmme, ja keskustelemme siitä säännöllisesti nuorten kanssa.
- C. Oletamme, että nuoret oppivat näistä asioista koulussa ja kotona.

5. Mitä toimintatapoja teillä on tietoturvaloukkauksen varalta?

- A. Käytössä on ylimmän johdon hyväksymä suunnitelma, joka sisältää ennaltaehkäisevät toimenpiteet, seurantajärjestelmät, sekä ohjeet havaitsemisesta, raportoinnista ja vastatoimista tietoturvaloukkauksen sattuessa.
- B. Meillä ei ole erityistä suunnitelmaa, mutta luotamme IT-tiimimme nopeaan reagointiin.
- C. Keskitymme ennaltaehkäisyyn, eikä meillä ole tarvetta suunnitelmalle tietoturvaloukkauksen varalta.

6. Mitä tarkoitetaan nuoren yksityisyyden suojalla?

- A. Se tarkoittaa, että nuorten henkilökohtaiset tiedot, kuten osoite ja puhelinnumero, ovat julkisia tietoja, mutta heidän sähköpostiviestintänsä ja verkkokäyttötymisensä ovat suojattuja.
- B. Se tarkoittaa, että nuorten henkilökohtaisia tietoja, kuten henkilötunnusta ja terveystietoja, suojataan ja niiden käyttö on sallittua vain laillisesti määritellyissä tapauksissa ja asianmukaisin lupamenettelyin.
- C. Se merkitsee, että nuorten henkilökohtaiset tiedot ovat suojattuja, mutta koulut ja viranomaiset voivat jakaa tietoja keskenään ilman nuoren tai huoltajan suostumusta, mikäli se katsotaan nuoren edun mukaiseksi.

7. Miten huolehditte nuorten yksityisyyden suojasta kun viestitte nuorten kanssa?

- A. Käytämme aina salattuja viestintäkanavia ja varmistamme, että keskustelut ovat luottamuksellisia.
- B. Puhumme yksityisyydestä vain, jos nuori itse ottaa sen puheeksi.
- C. Yksityisyysasioita käsitellään vain kasvokkain, ei digitaalisissa kanavissa.

8. Miten informoitte ja keskustellette nuorten kanssa heidän digitaalisista oikeuksistaan?

- A. Oletamme, että nuoret oppivat näistä asioista itse internetissä.
- B. Käymme läpi digitaalisia oikeuksia kun tulee puhetta sosiaalisesta mediasta ja osana nuorten kanssa pidettäviä työpajoja ja ryhmäkeskusteluja.
- C. Sanomme nuorille, että heidän ei tarvitse huolehtia digitaalisista oikeuksista, koska asia ei kosketa nuoria.

8. Miten käsittelette omadatan ja henkilökohtaisten tietojen omistajuutta nuorten kanssa?

- A. Kerromme nuorille, että heidän ei tarvitse murehtia datan omistajuudesta, koska GDPR:n kautta ne on jo hoidettu.
- B. Annamme yleisiä ohjeita internetin käyttöön, mutta emme keskity omodataan tai tietojen omistajuuteen.
- C. Käymme läpi, mitä omodata ja tietojen omistajuus tarkoittavat, ja opetamme nuoria hallinnoimaan omaa dataansa esimerkiksi sosiaalisen median asetusten kautta.

**Katso oikeat
vastaukset selityksineen
seuraavilta sivuilta!**

10. Mitä tarkoitetaan termillä "digitaalinen jalanjälki"?

- A. Digitaalinen jalanjälki tarkoittaa ainoastaan tietoja, jotka käyttäjä tietoisesti jakaa sosiaalisessa mediassa, kuten julkiset päivitykset tai kuvat.
- B. Digitaalinen jalanjälki viittaa kaikkiin jälkiin, jotka jätämme digitaaliseen maailmaan, mukaan lukien tietoisesti ja tiedostamatta jaetut tiedot, kuten selaushistoria, sovellusten käyttö ja sijaintitiedot.
- C. Digitaalinen jalanjälki on ainoastaan virallinen dokumentaatio, kuten verkkopankkitunnukset ja sähköiset asiakirjat, joita yksilö käyttää virallisissa online-transaktioissa.

11. Miten toimitte, jos huomaatte nuorten jakavan valeprofileja tai valheellista tietoa?

- A. Keskustelemme nuoren kanssa kahden kesken ja ohjaamme häntä ymmärtämään tekojensa seuraukset sekä vastuun omasta digitaalisesta jalanjäljestään.
- B. Raportoimme valeprofiilit ja valheellisen tiedon välittömästi alustan ylläpitäjälle ja ohjeistamme muita nuoria välttämään niiden levittämistä.
- C. Emme puutu tilanteeseen, ellei se ole suoraa toimintaamme koskevaa, sillä nuorilla on oikeus yksityisyyteen ja vapaaseen itseilmaisuuksiin verkossa.

12. Mikä seuraavista tilanteista kuvaa tietosuojaloukkausta?

- A. Nuorisotyöntekijä kerää nuorten sosiaalisen median käyttötietoja ilman heidän suostumustaan osana nuorisotutkimusta, jonka tarkoituksena on ymmärtää nuorten online-käyttäytymistä paremmin.
- B. Nuorisotyöntekijä tallentaa nuorten osallistumistiedot turvalliseen järjestelmään, jossa pääsy tietoihin on rajoitettu vain niihin työntekijöihin, joilla on tarve näihin tietoihin osana ohjaustehtäviään.
- C. Nuorisotyöntekijä jakaa anonymisti kerättyjä tietoja nuorten mielipiteistä ja kokemuksista kollegiaalisessa kokouksessa, jossa keskustellaan ohjelmien kehittämisestä, ilman että yksittäisten nuorten tunnistetietoja paljastetaan.

1 B. Henkilötietojen käsittelyn perusteet GDPR:n mukaan

GDPR, General Data Protection Regulation, suomeksi EU:n yleinen tietosuoja-asetus astui voimaan 2016 ja sen soveltaminen alkoi 2018. EU-asetukset ovat sellaisenaan kaikissa jäsenvaltioissa sovellettavaa lainsäädäntöä. GDPR jättää tiettyjä asioita kansallisen liikumavaran piiriin. Niistä säädetään Suomen tietosuojalaissa.

GDPR koskee kaikkia yrityksiä ja organisaatioita, jotka käsittelevät EU-kansalaisten henkilötietoja jos ne toimivat tai tarjoavat palveluitaan EU-alueella. GDPR:n velvoittamista asioista on informoitava rekisteröityä eli sitä, jonka henkilötietoja käsitellään.

2 A. Digitaalisen kommunikaation tietoturva

Vahva salasana ja monivaiheinen tunnistautuminen ovat kaksi keskeistä osaa digitaalisessa turvallisuudessa. Vahva salasana tunnustetaan sen monimutkaisuudesta ja pituudesta. Erikoismerkkien käyttäminen lisää turvallisuutta ja hyvä salasana ei koostu kokonaan tavallisista sanoista tai niiden johdoksista. Monivaiheinen tunnistautuminen (Multi-factor Authentication, MFA) tarkoittaa sitä, että henkilön identiteettiä varmistetaan useampaa eri tunnistautumistapaa käyttämällä.

Monivaiheinen tunnistautuminen lisää ylimääräisen turvakerroksen salasanan päälle. Tämä tarkoittaa, että käyttäjän on esimerkiksi annettava kaksi erilaista todistetta henkilöllisyydestään päästäkseen käsiksi tililleen – kuten salasana ja matkapuhelimeen lähetetty vahvistuskoodi. Tämä menetelmä vähentää merkittävästi luvattoman pääsyn riskiä, koska hyökkääjän on huomattavasti vaikeampaa saada haltuunsa molemmat tunnistautumistekijät samanaikaisesti.

3 B. Pääsynhallinta henkilötietoihin

Henkilötiedot, erityisesti nuorten osalta, ovat arkaluonteisia ja niitä suojataan laeilla, kuten GDPR:llä. Varmistaminen, että vain valtuutetulla henkilökunnalla on pääsy näihin tietoihin, on välttämätöntä näiden lakien noudattamiseksi ja nuorten yksityisyyden suojaamiseksi.

4 B. Tietosuoja ja tietoturvan käsittely nuorten kanssa

Sekä tietosuoja että tietoturva ovat tärkeitä huomioon otettavia asioita datan ja tiedon suojaamiseksi yhä digitalisoituvammassa maailmassa, jossa tietovuotojen ja kyberhyökkäysten riskit jatkuvasti kasvavat. Tietosuoja on perusoikeus, joka keskittyy henkilötietojen suojaamiseen luvattomalta pääsylvä ja käsittelyltä. Kyse on siitä, että varmistetaan henkilökohtaisen tiedon laillinen ja eettinen kerääminen, käyttö ja säilyttäminen, kunnioittaen yksilön yksityisyyttä ja oikeuksia. Tämä kattaa toimenpiteitä, kuten luottamuksellisuuden ylläpitämisen ja lakien, kuten GDPR:n, noudattamisen. Tietoturva on toteutuskeino, joka kattaa kaikenlaisen tiedon (ei vain henkilötietoja) suojaamisen luvattomalta pääsylvä, muokkaukselta, poistamiselta tai varkaudelta. Se sisältää teknisiä ja hallinnollisia toimenpiteitä tiedon eheyden, luottamuksellisuuden ja saatavuuden suojaamiseksi, riippumatta siitä, onko tieto digitaalisessa muodossa tai muussa muodossa.

5 A. Tietoturvaloukkausten ennaltaehkäisy ja reagointi

Tietomurtojen ehkäisemiseksi on tärkeää käyttää vahvaa salakirjoitusta, pitää turvaohjelmat ajan tasalla, kouluttaa henkilökuntaa kyberturvallisuudessa, toteuttaa tiukat pääsynhallintatoimet ja suorittaa säännöllisesti turvallisuustarkastuksia. Nämä askeleet auttavat luomaan turvallisen tietoympäristön.

6 B. Viestintä ja yksityisyys

Yksityisyyden suoja tarkoittaa käsittelijän näkökulmasta henkilötietojen turvallista käsittelyä ja yksilöiden yksityisyyteen liittyvien oikeuksien ylläpitämistä digitaalisella aikakaudella. Se vaatii jatkuvaa valppautta ja päivitettyjä turvatoimia erilaisia uhkia vastaan. Tavoitteena on yksilön vapauden ja autonomian varjeleminen yhä enemmän verkottuneessa maailmassa.

7 A. Viestintä ja yksityisyys

Salatut viestintäkanavat ovat työkaluja digitaalisen viestinnän turvaamiseen, jossa tieto salataan siirron aikana. Tämä tarkoittaa, että vaikka tiedot joutuisivat väärin käsiin tai niitä kuunneltaisiin, sisältö on lukukelvotonta ilman tiettyä purkuavainta. Näitä kanavia käytetään usein herkän tiedon, kuten henkilötietojen ja yrityssalaisuuksien suojaamiseen. Tällaisia kanavia ovat esimerkiksi turvalliset sähköpostipalvelut ja päästä päähän salatut viestisovellukset. Käyttämällä salattuja viestintäkanavia käyttäjät voivat viestiä turvallisesti ja vähentää tietomurron riskiä.

8 B. Nuorten digitaaliset oikeudet

Lasten ja nuorten digitaaliset oikeudet korostavat, kuinka tärkeää on, että nuorisotyöntekijät tunnistavat ja ymmärtävät lasten ja nuorten oikeudet sekä mahdollisuudet digitaalisissa ympäristöissä. Oikeudet edistävät lasten ja nuorten tasa-arvoa ja yksityisyyttä digitaalisessa maailmassa. Ne korostavat turvallisuuden merkitystä, erityisesti haitallisen sisällön, kuten kiusaamisen, väkivallan ja rasmin vastustamisessa. Lisäksi ne korostavat lasten ja nuorten oikeutta saada luotettavaa tietoa ja kehittää medialukutaitoaan. Luovuuden ja itsenäisen luomisen tukeminen on myös keskeinen teema, samoin kuin kansalaisvaikuttaminen ja ymmärrys yhteiskunnallisista muutoksista. Teknologian kehitys vaikuttaa nuorten elämään monin tavoin, ja nuorisotyöntekijöiden on oltava valmiita tukemaan heitä ymmärtämään näitä muutoksia.

9 C. Omadata ja tietojen omistajuus

Omandatan ja datan käytön keskusteleminen nuorten kanssa on tärkeää nuorten tietoisuuden edistämiseksi yksityisyydestä ja turvallisuudesta verkossa. Ymmärtämällä, miten henkilökohtaisia tietoja kerätään ja käytetään, nuoret voivat tehdä tietoisia päätöksiä digitaalisesta jalanjäljestään. Tämä tieto vahvistaa myös heidän kykyään kriittisesti analysoida digitaalista tietoa, mikä on ratkaisevaa valeuutisten aikakaudella. Lisäksi se auttaa heitä ymmärtämään digitaaliset oikeutensa ja eettisen käyttäytymisen merkityksen digitaalisissa ympäristöissä. Tämä oivallus on tärkeä paitsi henkilökohtaiseen suojeluun, myös valmistaa heitä tulevaisuuteen yhä digitalisoituneemassa maailmassa.

10 B. Omadata ja tietojen omistajuus

Digitaalinen jalanjälki sisältää tietoja, jotka kerätään verkkotoiminnan, kuten verkkoselailun, sosiaalisen median, sähköpostin ja verkkokaupankäynnin kautta. Tämä jalanjälki voi koostua sekä aktiivisesti jaetusta tiedosta, kuten sosiaalisen median postauksista, että passiivisesti kerätyistä tiedoista, kuten verkkohistoriasta ja evästeistä. Koska nämä tiedot usein tallennetaan ja niitä voidaan analysoida, on tärkeää olla tietoinen omasta digitaalisesta jalanjäljestään yksityisyyden suojaamiseksi verkossa.

11 B. Valeprofiilit ja valheellinen tieto

Väärän tiedon ja valheellisten profiilien ilmoittaminen verkossa on tärkeää turvallisen ja luotettavan digitaalisen ympäristön ylläpitämiseksi. Vääriä profiileja voidaan käyttää levittämään disinformaatiota, huijauksia tai vahingoittamaan toisten mainetta, mikä voi johtaa vakaviin seurauksiin niin yksilöille kuin yhteiskunnalle laajemminkin. Ilmoittamalla tällaisista profiileista autetaan alustoja tunnistamaan ja poistamaan haitallista sisältöä, mikä suojaa muita käyttäjiä harhaanjohtavalta tai vahingolliselta tiedolta. Lisäksi jokainen ilmoitus auttaa lisäämään tietoisuutta valeuutisten ja disinformaation ongelmasta, mikä on keskeistä digitaalisen lukutaidon ja kriittisen ajattelun edistämisessä verkossa.

12 B. Valeprofiilit ja valheellinen tieto

Tietoturvaloukkaus on tapahtuma, jossa henkilökohtaisia tietoja, tahattomasti tai laittomasti, joutuu menetyksen, varkauden, luvattoman pääsyn, julkistamisen, muuttamisen tai tuhoamisen kohteeksi. Tämä voi merkitä vakavia riskejä asianomaisten henkilöiden yksityisyydelle ja turvallisuudelle ja vaatii nopeita toimenpiteitä vahinkojen rajoittamiseksi. Tällaiset tapahtumat ovat erityisen arkaluonteisia, koska ne koskettavat yksilön perusoikeutta tietosuojan ja yksityisyyteen.

ONNITTELUT!

Olet suorittanut kyselyn ja saanut oikeat vastaukset vahvistaaksesi omaa ymmärrystäsi ja saadaksesi oivalluksia, joita voit jakaa työssäsi nuorten kanssa.