

Kyberturvallisuus – Henkilökohtaiset tiedot

Arvioitu oppijan taitotaso: aloittelija tai keskitaso

Määritelmä

Henkilötiedot sisältävät kaikki tiedot, jotka voidaan yhdistää henkilöön ja joita voidaan käyttää tunnistamiseen, mukaan lukien:

- Nimi
- Sosiaaliturvatunnus
- ikä
- sukupuoli
- osoite
- puhelinnumero
- kuva

Miksi henkilötietojen suojaaminen on tärkeää

Henkilötietojen suojaaminen on tärkeää ainakin neljästä syystä.

1. Identiteettivarkauksien estäminen
2. Yksityisyyden ja turvallisuuden ylläpitäminen
3. Taloudellisten ja aineellisten menetysten välttämiseksi
4. Maineen säilyttämiseksi

Harjoitus: Suojaamattomat henkilökohtaiset tiedot voivat johtaa monien asioiden menettämiseen. Täydennä alla oleva virke:

Näitä asioita voivat olla: _____, _____, _____, _____, _____, ja _____.

* identiteetti _ yksityisyys _ turvallisuus _ talous _ materiaalit _ maine

Tietoja henkilötietojen tallentamisesta

Euroopan unionissa asetukset, kuten yleinen tietosuojasetus (GDPR), määrittelevät, mitä voidaan tallentaa ja miten. Henkilö voi esimerkiksi antaa ja peruuttaa suostumuksensa tietojen tallentamiseen ja hänellä on oikeus pyytää hänestä tallennettuja tietoja.

Henkilötietojen suojaaminen

Vahva salasana

Vahvalla salasanalla on kaikki seuraavat:

- pituus vähintään 15 merkkiä (enemmän on parempi)
- isot ja pienet kirjaimet



- Numerot
- Erikoismerkkejä
- ei muistuta oikeita sanoja
- Ei samankaltaisuutta aiempien salasanojen kanssa, kun ne vaihdetaan.

Salasanojen hallintaohjelmisto voi säilyttää salasanat, salata ja tallentaa ne turvallisesti. Tämä vapauttaa käyttäjän tarpeesta muistaa kaikki salasanat ja yksinkertaistaa useiden online-tilien hallintaa. (The Cyphere 2023.)

Lisäksi kaksivaiheinen tunnistautuminen (2FA) tai monivaiheinen tunnistautuminen (MFA) voivat tarjota lisäsuojaukskerroksen sitä tukeviin palveluihin (The Cyphere 2023; Australian Signs Directorate 2021). 2FA:ssa tai MFA:ssa, kun käyttäjä kirjautuu palveluun, hänen puhelimeensa lähetetään koodi (yleensä todennusovellukseen tai tekstiviestillä), ja hän syöttää tämän koodin kehoitteeseen, joka tulee näkyviin palvelun kirjautumisnäytön jälkeen.

Harjoitus: Yritä luoda vahva salasana.

Salasanaharjoitus

Turvalliset verkkotavat

Yksi tärkeimmistä asioista on tarkistaa verkkosivun osoite (URL). Tässä on kaksi tärkeintä huomioitavaa asiaa. Ensinnäkin osoite vaikuttaa lailliselta ja kuuluu organisaatiolle tai palveluntarjoajalle (kuten verkkopankille tai kaupalle). Toiseksi osoite alkaa "https" eikä "http"; "S" tarkoittaa suojattua yhteyttä (Norton 2022; The Cyphere 2023).

Toinen vaihe on tarkistaa sivuston salaus vahvistamalla lukkokuvaan läsnäolo selaimen osoiterivin vieressä ja lukemalla salaustiedot napsauttamalla lukkokuvaan.

Kyberhyökkäyksen riskin vähentämiseksi merkittävästi voidaan muistaa (tai tallentaa tiedostoon tai kirjanmerkkiin) kriittisimpien sivustojen, kuten verkkopankeille kuuluvien sivustojen, osoitteet.

On myös tärkeää huomata punaiset liput, jotka osoittavat mahdollisesti vaarallisen verkkosivuston tai jopa mahdollisen hyökkäyksen: ponnahdusikkunat, varoitusviestit ja uudelleenohjaus muille verkkosivustoille (Norton 2022).

Yksi turvatoimenpide on käyttää kertakäyttösähköposteja huolellisesti verkkopalveluissa (The Cyphere 2023).



Varmuuskopiot

On tärkeää varmuuskopioida tiedot säännöllisesti kaikista laitteista (Australian Signs Directorate 2021).

Yhteenveto
Harjoitus: Valitse turvalliset käytännöt henkilötietojen suojaamiseen.
Storing data on a flash drive
Selainhistorian tarkistaminen
Osoiterivin ja vierekkäisten elementtien tarkistaminen
Salasanaluettelon pitäminen tietokoneen lähellä olevalla paperilla
Monimenetelmäisen todennuksen käyttäminen aina kun mahdollista
1,3,5

Seuraava vaihe

[Siirry kyberturvalliseen ohjelmistokehitykseen](#)

References

Australian Signs Directorate. 2021. *Personal Cyber Security: First Steps Guide*. Available at: <https://www.cyber.gov.au/protect-yourself/resources-protect-yourself/personal-security-guides/personal-cyber-security-first-steps>. Accessed 25 June 2024.

Norton. 2022. *Personal cybersecurity resolutions for 2022: A month-to-month guide*. Available at: <https://us.norton.com/blog/privacy/personal-cybersecurity>. Accessed 25 June 2024.

The Cyphere. 2023. *Personal Cybersecurity Best Practices*. Available at: <https://thecyphere.com/blog/personal-cybersecurity-best-practices/>. Accessed 25 June 2024.

