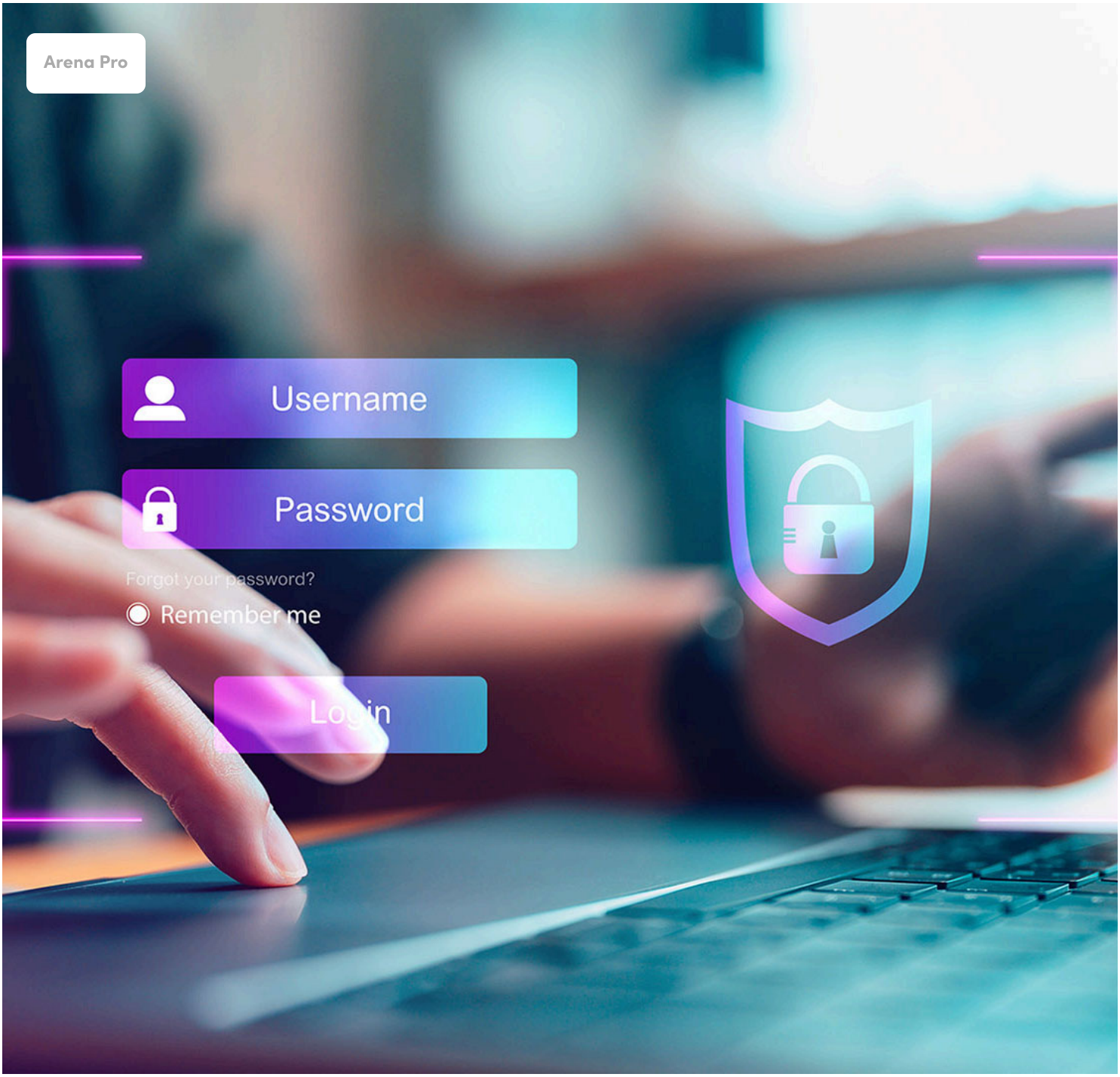

Kuva: Adobe Stock

oppilaitoksissa

Koulutus ja oppiminen Teknologia ja teollisuus

Salasanat ovat arkipäivänen osa tietojärjestelmiä. Tietoturvan kannalta on yhä tärkeää kouluttaa oppilaitosten henkilökuntaa luomaan pitkiä salasanoja ja käyttämään salasananhallintaohjelmia.

12.2.2025
Tuomo Sipola

Salasanojen turvallinen käyttö ja hallinta voivat vaikuttaa sellaisilta perustaidoilta, joihin ei enää tarvitse kiinnittää huomiota. Jos perusasioita ei kuitenkaan pidetä esillä henkilöstölle, voi organisaation tietoturvan yleinen taso heikentyä. Tässä kirjoituksessa tarkastelen salasanojen hallintakäytänteitä oppilaitoksissa pohjaten kokemuksiimme Suomalaisten oppilaitosten valmius kohdata kyberkriisejä -projektissa.

Oppilaitoksissa on käytössä erilaisia tietojärjestelmiä, joiden tarkoitus on tehostaa toimintaa. Järjestelmillä on laaja käyttäjäjoukko, sillä niiden tehtävänä on esimerkiksi:

- säilöä opiskelijarekistereitä,
- opintoihin etenemiseen liittyvää tietoa ja
- välittää viestejä opettajien, oppilaiden tai vanhempien kesken.

Yleinen keino kirjautua sisään tällaisiin järjestelmiin on käyttää käyttäjätunnusta ja salasanaa. Käyttäjätunnusta käytetään tunnistamiseen ja salasanaa todentamiseen. Käyttäjätunnus on usein julkista tietoa, mutta salasanan tulisi olla vain käyttäjän itsensä tiedossa (Adams ym., 1997; Kyberturvallisuuskeskus, n.d.).

Ihminen on usein tietoturvan heikoin lenkki. Vaikka salasanat ovatkin yleinen tapa todentaa käyttäjä, on salasanojen muistaminen vaikeaa. Samaa salasanaa ei saisi käyttää useassa palvelussa. Ur ym. (2016) havaitsivat käyttäjien ymmärtävän, millainen vahvan salasanan tulisi

arvaaminen vaatisi henkilökohtaista tietoa kohteesta.

Havaintoja ammatillisen koulutuksen tilanteesta

Suomalaisten oppilaitosten valmius kohdata kyberkriisejä -projekti on tutkinut ammatillisten oppilaitosten kyberturvariskien luonnetta ja työyhteisöjen valmiutta toimia kyberkriiseissä. Tutkimusryhmämme (Anna-Liisa Ojala, Tuomo Sipola, Karo Saharinen) pyrki laadullisten haastattelujen analyysin kautta kartoittamaan tilannetta ammattikouluissa.

Aineiston perusteella nousi kysymys, että ohjeistetaanko henkilökuntaa enää luomaan turvallisia salasanoja. Tätä asiaa on voitu pitää itsestäänselvyytenä, mutta on liian toiveikasta odottaa taitoja kaikilta työntekijöiltä. Yksi syy huomion vähentymiselle voi olla monivaiheisen tunnistautumisen arkipäiväistyminen, mutta se ei poista salasanojen merkitystä.

Toisaalta havaitsimme myös, että ainakin jotkut käyttäjät hyödyntävät selainten salasananhallintaa, mikä mahdollistaa useiden erilaisten pitkien salasanojen tallentamisen jokaista käytettyä palvelua varten. Sen sijaan organisaatiotason kiinnostus salasanojen hallintaan pitäisi myös saada lisääntymään, jotta ne tarjoaisivat ohjelmistoja ja koulutusta aiheeseen. Ilman organisaation tukea käyttäjät harvoin aktivoituvat tietoturva-asioissa. Kyse on hyödyllisten käytäntöjen jalkauttamisesta henkilöstölle.

Kaksivaiheinen tunnistautuminen

Nykymaailmassa monivaiheinen tunnistautuminen on arkipäivää myös oppilaitoksissa käytettävissä järjestelmissä (ks. Kuva 1). Monivaiheinen tunnistautuminen tarkoittaa, että järjestelmään sisään kirjautuessa käyttäjä joutuu todentamaan itsensä useilla tavoilla tunnuksen ja salasanan lisäksi (Ometov ym., 2018). Tällaisia tapoja ovat esimerkiksi tekstiviestit ja tunnusluvun antavat kännykkäsovellukset. Näistä tosin ensin mainittu ei ole itsessään vahva tunnistautumistapa (Lei ym., 2021).

Kuva 1. Kaksivaiheista tunnistusta vaativaan järjestelmään kirjautuminen joko salasanahallinnan kanssa tai ilman.

On kuitenkin huomattava, että kaksivaiheinen tunnistautuminen ei poista salasanojen huolellisen käytön tarvetta. Ensimmäinen vaihe on salasanan antaminen. Monivaiheisuuden perusajatus on, että jokainen vaihe tehdään turvallisesti, joten salasanoja koskevat käytänteet ovat yhä ajankohtaisia.

Salasanojen hallinta

Kyberturvallisuuskeskuksen (n.d.) määritelmän mukaan salasanojen hallintaan käytettävän sovelluksen avulla voi tallentaa salasanoja yhden pääsalasanan taakse. Tämä mahdollistaa monimutkaisten ja pitkien salasanojen käytön jokaisessa järjestelmässä. Sovelluksen pääsalasanasta täytyy kuitenkin pitää huolta, sillä sen paljastuessa hyökkääjä pääsee käsiksi kaikkiin salasanoihin. Sovelluksia on erilaisia, jotkut tallentavat salasanat pilveen, jolloin niitä voi käyttää eri laitteilla. Toiset taas tallentavat ne käyttäjän tietokoneelle, jolloin ne ovat saatavilla vain sieltä.

Mayer ym. (2022) ovat tutkineet salasananhallintaohjelmistojen käyttöä yliopistossa, ja ehdottavat mm. seuraavia suosituksia organisaatioille:

- Salasananhallintaohjelmistojen tarjoaminen ilmaiseksi johtaa niiden käyttöön.

- Luottamuksen kasvattaminen salasananhallintaohjelmistoja kohtaan.

- Yhteensopivuusongelmien dokumentointi ja niistä eroon pääseminen.

Mitä oppilaitosten tulisi tehdä?

Olisi tärkeää, että salasanojen käyttöön kiinnitettäisiin huomiota henkilökuntaa ohjeistettaessa. Vaikka monivaiheinen tunnistautuminen on käytössä useissa järjestelmissä, toimivat useat niistä kuitenkin pelkän salasanan varassa. Sellaisia ovat esimerkiksi erikseen yhdelle henkilölle hankitut järjestelmät, joita ei ole integroitu kertakirjautumiseen. Tällöin perinteiset salasanakäytänteet ovat yhä välttämättömiä: salasanojen täytyy olla tarpeeksi pitkiä, vaikeasti arvattavia eikä samaa salasanaa saa käyttää useissa palveluissa. Toisaalta pahantahtoiset toimijat voivat hyökätä myös monivaiheista tunnistautumista vaativaan järjestelmään. Tällöin tehtävä helpottuu heikkojen tai pitkään voimassa olleiden yksinkertaisten salasanojen takia. Hyökkääjä voi esimerkiksi lähettää valheellisen kirjautumispyynnön ja asettua palvelun ja käyttäjän väliin, jolloin käyttäjä antaa erheellisesti kirjautumistietonsa hyökkääjälle.

Loppusuosituksina on helppo toistaa se, mitä muutkin ovat havainneet. Esimerkiksi sekä Mänttäri (2020) että Avoine & Leblanc-Albarel (2023) suosittelevat kahta toimenpidettä:

- Salasanojen tulee olla pitkiä. Pituus on tärkein vahvan salasanan tunnusmerkki (ks. esim. Dell'Amico ym., 2010; Bošnjak ym., 2018). Yhdysvaltojen kyber- ja infrastruktuuriturvallisuuden viranomainen suosittelee vähintään 16 merkkiä pitkiä salasanoja (CISA, n.d.).

- Salasananhallintaohjelmat ovat käytettävyydeltään hyvä kompromissi, jotta eri palveluissa käytetään eri salasanoja vaikka käyttäjän tarvitsee muistaa vain yksi pääsalasana (ks. esim. Bonneau ym., 2015).

Ylipäänsä salasanojen tärkeyden esille tuominen oppilaitoksissa lisää käyttäjien ymmärrystä parhaista käytänteistä. Perusteiden kertaaminen Kyberturvallisuuskeskuksen (n.d.) ohjeista on suositeltavaa oppilaitosten henkilökunnalle.

tarkimuksessa tarkastellaan ammatillisten oppilaitosten kyberturvallisten tuotteiden ja oppilaitosyhteisöjen valmiutta toimia kyberkriiseissä ja luodaan alalle harjoittelu- ja toimintasuosituksia.

Lue lisää hankkeesta

Avainsanat:

koulutus kyberturvallisuus kyberturvallisuusosaaminen

Jaa:

Facebook

Twitter

Linkedin

Kirjoittajat:

Vanhempi tutkija
Jyväskylän ammattikorkeakoulu

Olen vanhempi tutkija Jyväskylän ammattikorkeakoulun IT-instituutissa.

Lähteet:

Adams, A., Sasse, M. A. & Lunt, P. (1997). Making passwords secure and usable. Teoksessa Thimbleby, H., O'Conaill, B., Thomas, P.J. (toim.). *People and computers XII: Proceedings of HCI'97* (s. 1–19). Springer. https://doi.org/10.1007/978-1-4471-3601-9_1

Avoine, G. & Leblanc-Albarel, D. (2023). Comment choisir un bon mot de passe ? *The Conversation.* https://hal.science/hal-04349316v1

Bonneau, J., Herley, C., van Oorschot, P. C. & Stajano, F. (2015). Passwords and the evolution of imperfect authentication. *Communications of the ACM, 58*(7), 78–87. https://doi.org/10.1145/2699390

Bošnjak, L., Sreš, J. & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (s. 1161–1166). https://doi.org/10.23919/MIPRO.2018.8400211

CISA. (n.d.). *Require Strong Passwords. Enforcing a password manager protects your business.* Viitattu 24.1.2025. https://www.cisa.gov/secure-our-world/require-strong-passwords

Dell'Amico, M., Michiardi, P. & Roudier, Y. (2010). Password strength: an empirical analysis. *2010 Proceedings IEEE INFOCOM* (s. 1–9). IEEE.

ja hallintaan. Viitattu 24.1.2025 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Salasanat_haltuun.pdf

Lei, Z., Nan, Y., Fratantonio, Y. & Bianchi, A. (2021). On the insecurity of SMS one-time password messages against local attackers in modern mobile devices. *Network and Distributed Systems Security (NDSS) Symposium 2021.* https://dx.doi.org/10.14722/ndss.2021.24212

Mayer, P., Munyendo, C. W., Mazurek, M. L., & Aviv, A. J. (2022). Why users (don't) use password managers at a large educational institution. *31st USENIX Security Symposium (USENIX Security 22)* (s. 1849–1866). Viitattu 24.1.2025. https://www.usenix.org/system/files/sec22-mayer.pdf

Mänttäri, M. (2020). *Moderni salasananhallinta.* [Kandidaatin tutkielma, Tampereen yliopisto]. Trepo. https://urn.fi/URN:NBN:fi:tuni-202005315847

Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1. https://doi.org/10.3390/cryptography2010001

Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N. & Cranor, L. F. (2016). Do Users' Perceptions of Password Security Match Reality? *CHI '16: Proceedings of the 2016 CHI Conference on Human Factors in Computing System* (s. 3748–3760). https://doi.org/10.1145/2858036.2858546

Avainsanat:

koulutus kyberturvallisuus kyberturvallisuusosaaminen

Julkaistu

ISSN 2984-0783

URN
https://urn.fi/urn:nbn:fi:jamk-issn-2984-0783-171

Viittausohje
Sipola, T. (2025). Salasanojen hallinta on yhä ajankohtaista oppilaitoksissa. Jamk Arena Pro. https://urn.fi/urn:nbn:fi:jamk-issn-2984-0783-171

Aiheeseen liittyvää

Kyberturvallisempi Eurooppa: NIS2-direktiivin myötä Suomeen uusi kyberturvallisuuslaki ›

Sote-ammattilaisten kyberturvallisella toiminnalla varmistetaan asiakas- ja potilasturvallisuutta ›

Miten jokainen oppilaitoksen työntekijä voi vahvistaa kyberturvallisuutta? ›

Sairaanhoitajat tarvitsevat tekoälyn lukutaitoa – nyt ›

Jatkuvan kehittämisen menetelmillä kohti tavoiteaikaisia tutkintoja ›

Ihan aamuradion juontajina – kouluttajat sosiaalisen läsnäolon kannattelijoina ›

Takaisin ylös △