

Ohjeet tilitoimistoille

Kaksivaiheisen tunnistuksen käyttöönotto Fivaldissa viimeistään 22.10.2025



Lyhyesti



Elämme aikakautta, jossa kyberhyökkäykset ovat arkipäivää ja uhka koskettaa meitä kaikkia. **Yksi parhaista keinoista suojata digitaalinen identiteettisi on kaksivaiheinen tunnistus (2FA).**

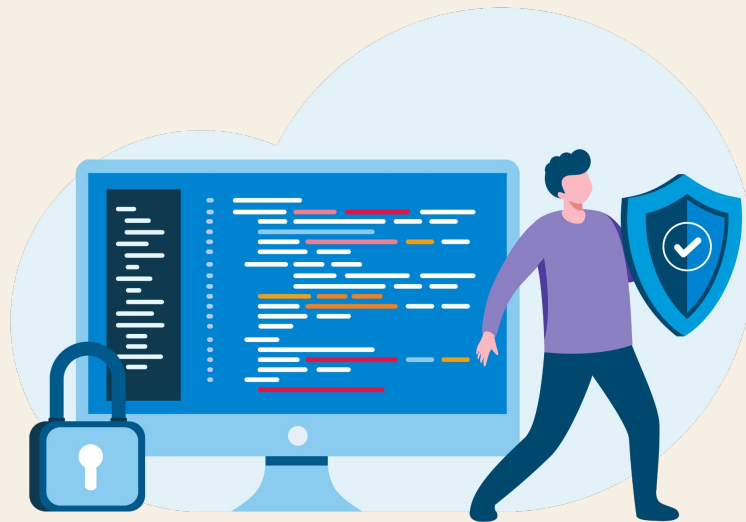
Tämä tehokas lisäsuoja varmistaa, että **tilillesi pääsy vaatii enemmän kuin vain pelkän salasanan.** Käyttämällä kaksivaiheista tunnistusta lisäät rauhaa mieleesi ja vahvan suojakerroksen digitaalisiin tietoihisi.

Lyhyesti

22.10.2025 alkaen kaksivaiheinen tunnistus on pakollinen kaikille, jotka kirjautuvat Fivaldiin Visma Connectin kautta. Fivaldin vanhanmalliset käyttäjätunnukset* poistuvat käytöstä 31.12.2025 mennessä. Tämän jälkeen kirjautuminen Fivaldiin onnistuu vain Visma Connectin kautta.

Tämä koskee kaikkia käyttäjiä, joilla on tunnukset Fivaldiin – **sekä tilitoimiston käyttäjiä että asiakkaitasi.**

Tietoturva on kaikkien käyttäjien vastuulla, joten otathan kaksivaiheisen tunnistautumisen käyttöön jo tänään.



* Jos kirjautut Fivaldiin sähköpostiosoitteella, käytät Connect-kirjautumista. Mikäli käyttäjätunnuksesi on muotoa *yritsoy-matti*, kyseessä on vanhanmallinen käyttäjätunnus-salasana -kirjautuminen.

Mitä tarkoittaa 2FA eli kaksivaiheinen tunnistus?

Kaksivaiheinen tunnistus (2FA) tarkoittaa, että **käytät kahta tunnistautumistapaa kirjautuessasi**. Lisäät siis toisen suojauksen pelkän salasanan lisäksi.

Fivaldissa tämä suojaus tapahtuu Visma Authenticator -sovelluksen kautta.



Miksi suositlemme kaksivaiheisen tunnistuksen käyttöönottoa?

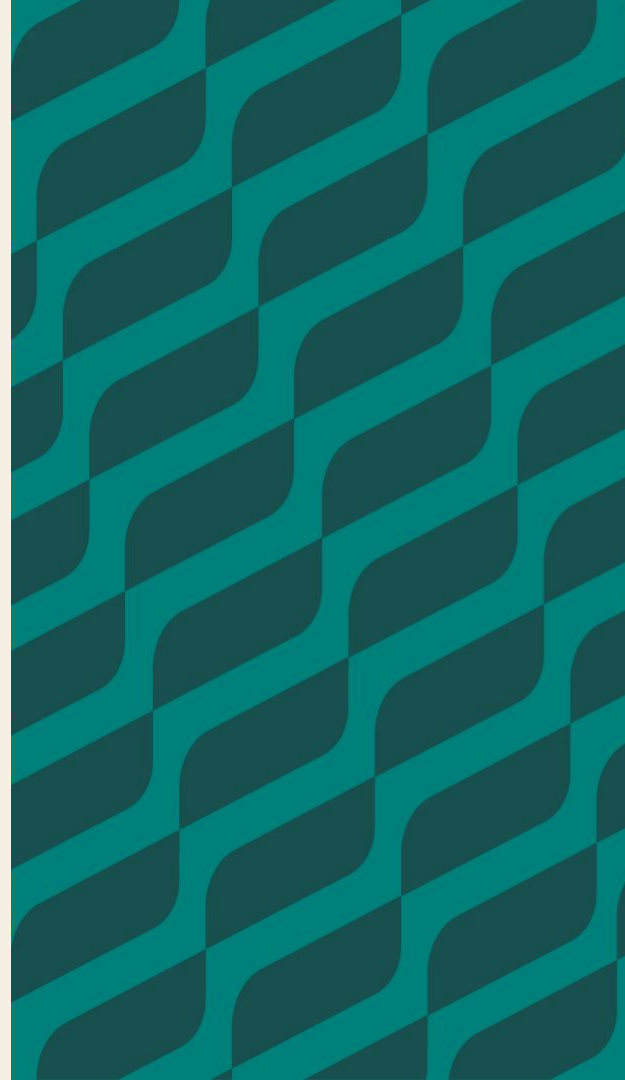
- **Lisäturvaa:** Kaksivaiheinen tunnistus lisää tärkeän suojakerroksen, mikä tekee luvattomasta pääsystä tilillesi huomattavasti vaikeampaa, vaikka salasana joutuisi väärin käsiin. Samalla turvaat myös asiakkaitasi.
- **Rauhallisempi mieli:** Voit olla varmempi tilisi turvallisuudesta tietäen, että olet tehnyt kaiken suositeltavan tilisi turvaamiseksi.
- **Suojaus huijausviesteiltä:** Kaksivaiheinen tunnistus estää tehokkaasti väärinkäytökset ja vähentää tietojenkalasteluyrityksiä, koska pelkkä salasanan tietäminen ei riitä tilille pääsyyn.
- **Tunnistautuminen eri laitteilla:** Kaksivaiheinen tunnistus varmistaa, että vain sinä saat pääsyn tilillesi, vaikka vaihtaisit laitetta. Se varmistaa, että käyttäjä on oikea henkilö riippumatta siitä, miten ja mistä kirjaudut sisään.

Mitä riskejä voi syntyä siitä, jos kaksivaiheinen tunnistus jää käyttämättä?

- **Heikompi suojaus:** Ilman kaksivaiheista tunnistusta tilisi on alttiimpi hakkeroinnille, tietomurroille ja tietojenkalasteluyrityksille.
- **Käyttäjätunnukset voivat olla kauppatavaraa:** Käyttäjätunnuksia, joihin ei ole kytkettynä kaksivaiheista tunnistusta, myydään koko ajan internetin syövereissä rikollisille.
- **Korkeampi riski:** Kaksivaiheisen tunnistuksen puuttuminen voi altistaa liikesalaisuuksia ja henkilötietoja väärin käsiin.
- **Varautuminen tuleviin uhkiin:** Taloushallinto-ohjelmisto on yhä useamman suomalaisen yrityksen liiketoiminnan ytimessä, joten tietoturvaan panostaminen on fiksua varautumista tulevaan.

Tietomurtoja tapahtuu myös taloushallinnon alalla

- Pohjoismaissa on uutisoitu lähiaikoina lukuisia tapauksia, joissa yksittäisen henkilön käyttäjätunnuksen varastaminen esimerkiksi kalastelun kautta on aiheuttanut tietomurron yrityksen järjestelmiin.
- Yleensä nämä olisi voitu estää täysin käyttämällä kaksivaiheista tunnistautumista.
- Lue lisää aiheesta kyberturvallisuuskeskuksen artikkelista: [Näin vältät kyberrikollisten ansat](#)



Onko kaksivaiheinen tunnistus työlästä?

Herääkö ajatus, että ylimääräisen koodin syöttäminen sovelluksesta on liian työlästä?

- Useimmat verkkopalvelut tunnistavat tietokoneesi tai selaimesi ja hyödyntävät sitä toisena tunnistautumismuotona. Siksi koodia ei välttämättä tarvitse syöttää joka kerta kirjautuessasi. Kun koodin syöttö tarvitaan, se vie vain muutaman sekunnin, mutta voi säästää sinut merkittävältä harmilta.
- Halutessasi voit ottaa käyttöön myös push-ilmoitukset. Tällöin riittää, että hyväksyt kirjautumisen puhelimeesi tulevasta ilmoituksesta parilla painalluksella, eikä koodia tarvitse syöttää lainkaan.



Miten kaksivaiheinen tunnistus otetaan käyttöön?

1. Kaksivaiheinen kirjautuminen otetaan käyttöön [Visma Home -sivujen](#) kautta, joihin kirjaudutaan samoilla tunnuksilla kuin Fivaldiin.
2. Kirjauduttuasi siirry **oikeaan yläreunaan** ja avaa nuolesta valikko, josta pääset Omiin tietoihin.
3. Omat tiedot -sivulta löydät otsikon **Salasana & 2FA** – tämän alta voit ottaa kaksivaiheisen tunnistuksen.
4. Sujuvimmin kaksivaiheinen kirjautuminen onnistuu, jos vielä otat käyttöön push-ilmoitukset saman osion alta.
 - [Katso ohjevideo täällä »](#)
 - [Seuraa tukisivun ohjeita täällä »](#)

Miten voin ohjeistaa omia asiakkaitani?

Yrittäjän ohjeet - valmis
PDF-materiaali täällä »

- Kerro kaikille asiakkaillesi, että heidän tulee ottaa kaksivaiheinen tunnistus käyttöönsä vaikka jo tänään, kuitenkin viimeistään 22.10.2025
- Tietoturva on jokaisen käyttäjän vastuulla
- [Täältä löydät valmiin PDF-materiaalin yrittäjille](#), jonka pyydämme sinua jakamaan eteenpäin asiakkaillesi

Vaikutukset kirjautumiseen jatkossa

- **Fivaldiin ei voi kirjautua Visma Connect-tunnuksilla ilman kaksivaiheista tunnistautumista 22.10. Jälkeen.** Mikäli et ole ottanut sitä käyttöön aiemmin, ohjaa kirjautumissivu käyttöönottoon määräpäivänä
- Muuten kirjautuminen Fivaldiin toimii samalla tavalla ja samasta osoitteesta kuten tähänkin asti
- Lisäksi huomioithan, että kaikki Fivaldin omat käyttäjätunnukset* poistuvat käytöstä 31.12.2025 mennessä. Tämän jälkeen kirjautuminen Fivaldiin onnistuu vain Visma Connectin kautta

* Jos kirjaudut Fivaldiin sähköpostiosoitteella, käytät Connect-kirjautumista. Mikäli käyttäjätunnuksesi on muotoa *yritysoy-matti*, kyseessä on vanhanmallinen käyttäjätunnus-salasana -kirjautuminen.

Ongelmatilanne? Ei hätää.

Tarkemmat ohjeet kaksivaiheisen tunnistuksen käyttöönottoon löydät [tukisivuiltamme täältä](#).

Mikäli sinulla on kysyttävää tai tarvitset apua aktivointiin, ota yhteyttä tuki.fivaldi@visma.com



**Tietoturva on jokaisen käyttäjän vastuulla.
Yhdessä voimme varmistaa, että sekä sinun
että asiakkaidesi tilit pysyvät turvassa.**

