

# Tarkista ovatko tietosi vuotaneet

[Peruskäyttäjälle.net](https://peruskayttajalle.net)

Ohjeen versio 12.4.2021



Tämä teos on lisensoitu **Creative Commons Nimeä-EiKaupallinen-EiMuutoksia 4.0 Kansainvälinen** -lisenssillä. Tarkastele lisenssiä osoitteessa <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.fi>

Voit jakaa tätä teosta, kunhan mainitset selkeästi sen alkuperäksi ja tekijäksi [Peruskayttajalle.net](http://Peruskayttajalle.net) -sivuston.

- Peruskayttajalle.netin [Creative Commons-esittely](https://peruskayttajalle.net/tietoja.php#cc) (<https://peruskayttajalle.net/tietoja.php#cc>)
- Lisätietoa [Creative Commonsista suomeksi](https://creativecommons.fi/) (<https://creativecommons.fi/>)



# Sisällysluettelo

1	Johdanto.....	3
2	Omien tietojen etsiminen .....	3
3	Sähköposti-ilmoituksen tilaaminen .....	6
4	Toimenpiteet vuoden jälkeen .....	10



# 1 Johdanto

---

Erilaiset tietomurrot ja -vuodot ovat nykyään valitettavan yleisiä. Usein murroissa tai vuodoissa joutuu väriin käsiin tai paljastuu suuri määrä käyttäjien tietoja. Pahimmassa tapauksessa myös salasanat voivat paljastua, jos murron tai vuodon kohde on suojannut ne heikosti tai tallentanut salasanat selväkielisenä eli täysin salaamattomana.

Koska tietomurrot ja -vuodot ovat niin yleisiä, on peruskäyttäjän käytännössä mahdotonta uutisointia seuraamalla pysyä selvillä siitä, ovatko omat tiedot vaarantuneet. Onneksi tähän ongelmaan löytyy helppo ratkaisu.

[Have I Been Pwned](https://haveibeenpwned.com/) (<https://haveibeenpwned.com/>) on verkkopalvelu, josta voi tarkistaa, ovatko omat tiedot varastettu tai vuotaneet. Palvelusta voi hakea omia tietojaan käyttäjätunnuksen, sähköpostiosoitteen tai puhelinnumeron perusteella.

Have I Been Pwned on osoittautunut luotettavaksi verkkopalveluksi. Tässäkin asiassa tulee olla varovainen, koska myös rikolliset ovat pystyttäneet omia vastaavanlaisia verkkopalveluitaan kerätäkseen käyttäjien tietoja.

Tässä ohjeessa käydään läpi omien tietojen etsiminen Have I Been Pwnedissa, sähköposti-ilmoituksen tilaaminen siltä varalta, että omat tiedot vuotavat tulevaisuudessa ja toimenpiteet omien tietojen vuodettua.

## 2 Omien tietojen etsiminen

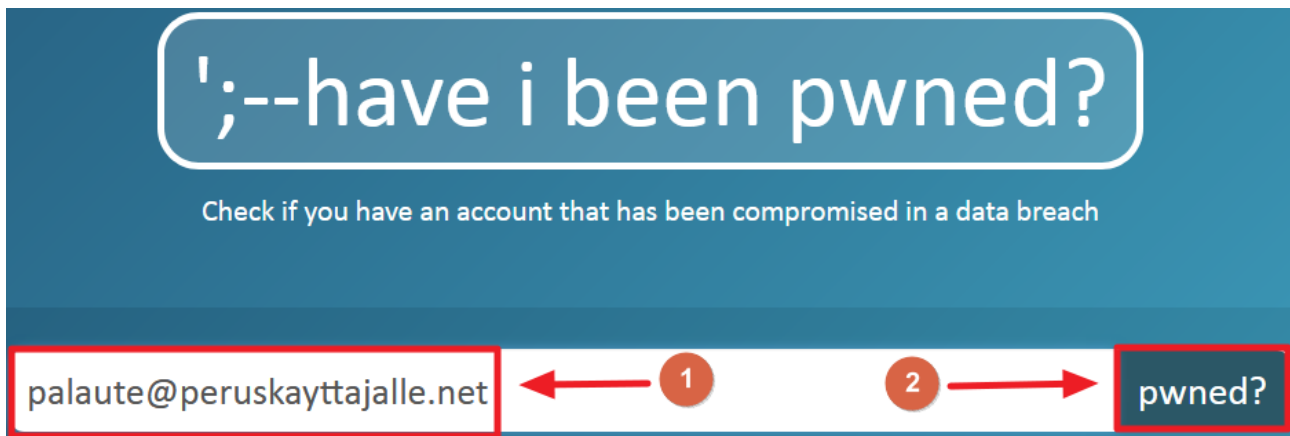
---

Voit etsiä omia tietojasi Have I Been Pwnedissa seuraavasti:

1. Mene osoitteeseen <https://haveibeenpwned.com/>. Kirjoita sivulla olevaan hakukenttään käyttämäsi käyttäjätunnus, sähköpostiosoite tai puhelinnumero. Kirjoita puhelinnumero muodossa 358xxxxxxx, esimerkiksi 3580491234567.

Lopuksi napsauta näppäimistön **Enter** -näppäintä tai kentän perässä olevaa tummaa **pwned?** -painiketta. Esimerkissä käytetään sähköpostiosoitetta *palaute@peruskayttajalle.net* (kuva 1).





Kuva 1

**Huom!** On ehdottomasti suositeltavaa tarkistaa kaikki tärkeimmät käyttämäsi käyttäjätunnukset, sähköpostiosoitteet ja puhelinnumerot.

2. Jos käyttäjätunnusta tai sähköpostiosoitetta ei löydy Have I Been Pwnedista, näkyy sivulla hakukentän alla vihreällä pohjalla teksti *Good news — no pwnage found!* (kuva 2).



Kuva 2

3. Jos käyttäjätunnus tai sähköpostiosoite löytyy Have I Been Pwnedista, näkyy sivulla hakukentän alla punaisella pohjalla teksti *Oh no — pwned!* (kuva 3).



Kuva 3

4. Tekstin alla näkyy tieto siitä, kuinka monesta palvelusta tieto on varastettu tai vuotanut. Esimerkissä kuvassa 4 tieto on varastettu tai vuotanut yhdestä palvelusta (teksti *1 breached site*).



# Oh no — pwned!

## Pwned on 1 breached site and found no pastes (subscribe)


Kuva 4

5. Alempaa sivulta otsikon **Breaches you were pwned in** alta näet, mistä palvelusta tai palveluista tiedot on varastettu ja/tai vuotaneet. Esimerkissä tieto on vuotanut osana suurta tietovuotoa (kuva 5). Jos on tiedossa, mistä palvelusta tiedot ovat vuotaneet, näkyy palvelun nimi tiedoissa.



**Breaches you were pwned in**

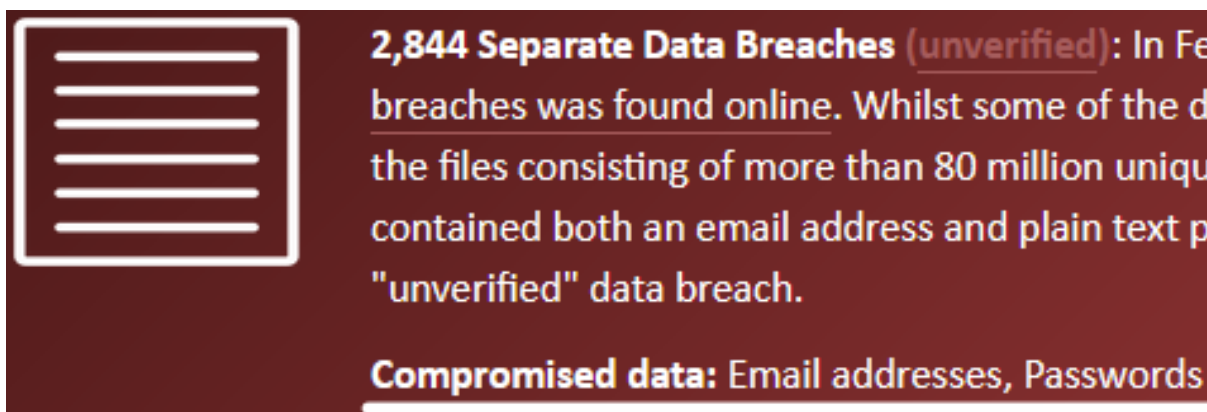
A "breach" is an incident where data has been unintentionally exposed to the public. Using the [1Password password manager](#) helps you ensure all your passwords are strong and unique such that a breach of one service doesn't put your other services at risk.


 **2,844 Separate Data Breaches (unverified):** In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

**Compromised data:** Email addresses, Passwords

Kuva 5

6. Otsikon **Compromised data** jälkeen näkyy lista vuotaneista tiedoista. Esimerkissä tiedoista ovat vuotaneet sähköpostiosoitteet ja salasanat (kuva 6).



 **2,844 Separate Data Breaches (unverified):** In February 2018, a massive collection of almost 3,000 alleged data breaches was found online. Whilst some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently loaded as a single "unverified" data breach.

**Compromised data:** Email addresses, Passwords

Kuva 6

Alla on lista osasta vuotaneista tiedoista englanniksi ja suomeksi.



Vuotaneet tiedot englanti–suomi:

Ages	Ikä
Credit cards	Luottokortin tiedot
Dates of birth	Syntymäaika
Device information	Laitteen tiedot (esim. puhelin)
Email addresses	Sähköpostiosoite
Employers	Työnantaja(t)
Family members' names	Perheenjäsenten nimet
Genders	Sukupuoli
Geographic locations	Sijainti
Historical passwords	Aiemmat salasanat
Homepage URLs	Kotisivun osoite
IP addresses	IP-osoite
Job titles	Titteli (työssä)
Names	Nimi
Password hints	Salasanavihje
Passwords	Salasana
Payment histories	Tiedot maksuista
Phone numbers	Puhelinnumero
Physical addresses	Osoite
Private messages	Yksityisviestit
Relationship statuses	Parisuhdetilanne
Security questions and answers	Turvallisuuskysymykset ja -vastaukset
Sexual orientations	Seksuaalinen suuntautuminen
Social media profiles	Sosiaalisen median profiilit
Spoken languages	Kielitaito
Username	Käyttäjätunnus
Years of birth	Syntymävuosi

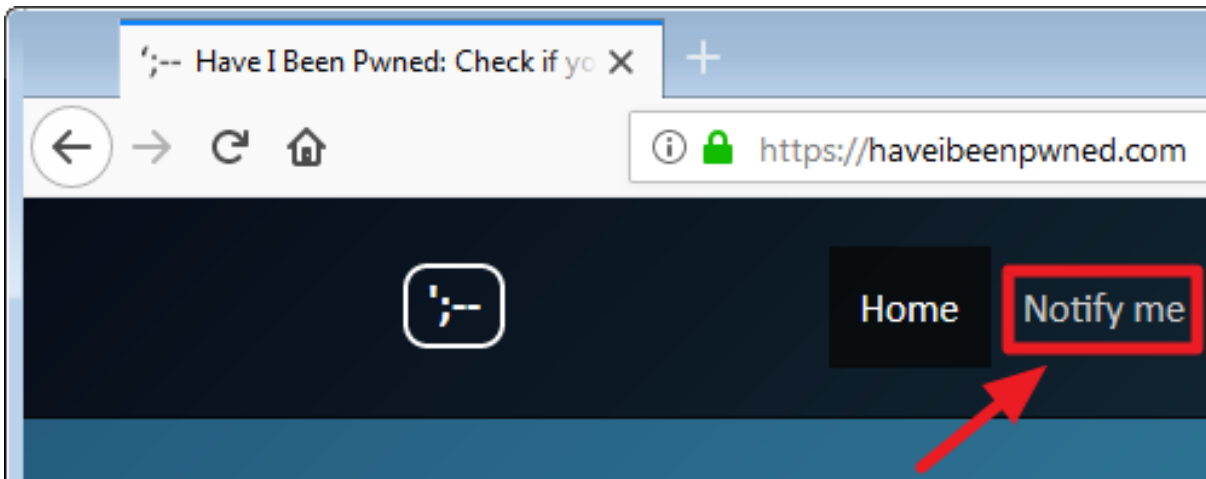
## 3 Sähköposti-ilmoituksen tilaaminen

---

Have I Been Pwnedissa on mahdollista tilata ilmoitus sähköpostiin, jos tietosi ovat vuotaneet. Tällä hetkellä ilmoitusta ei voi tilata puhelinnumeron vuotamisesta. Voit tilata ilmoituksen seuraavasti:

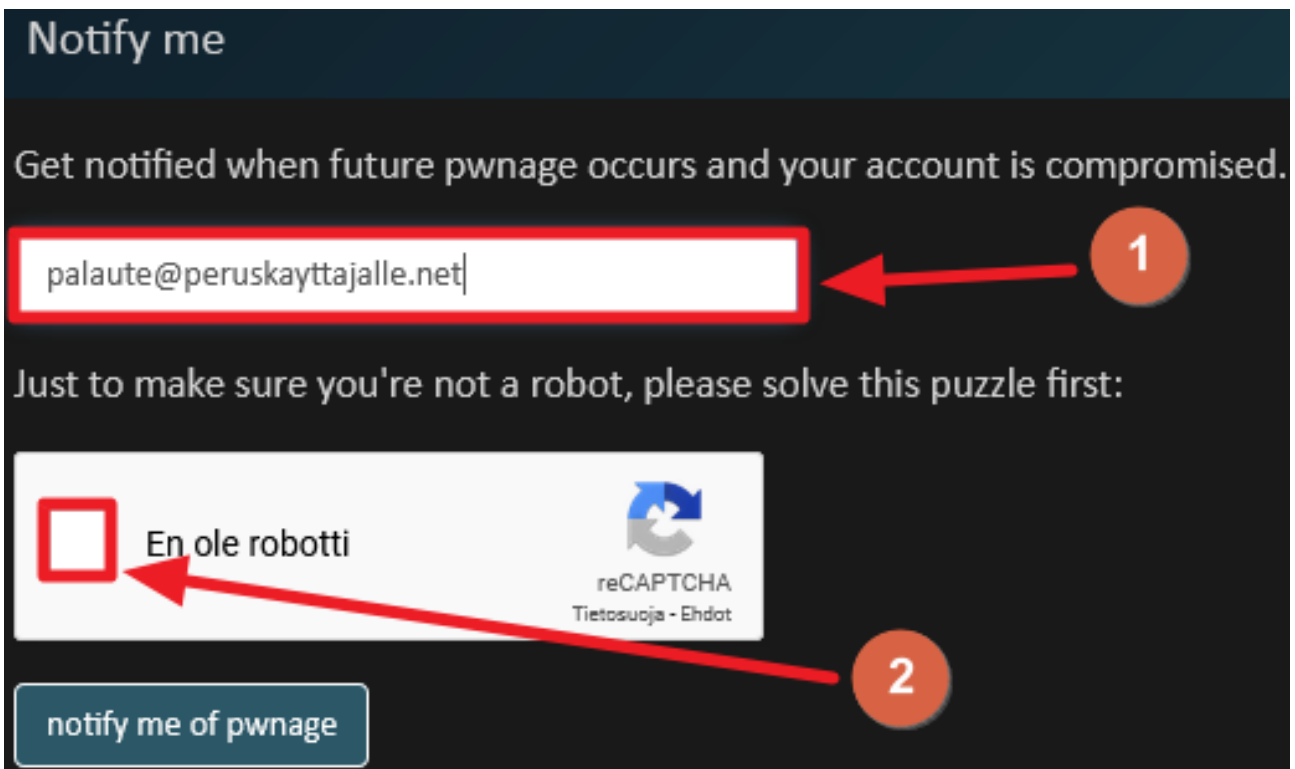
1. Napsauta ikkunan yläreunassa olevaa **Notify me** -linkkiä (kuva 7).





Kuva 7

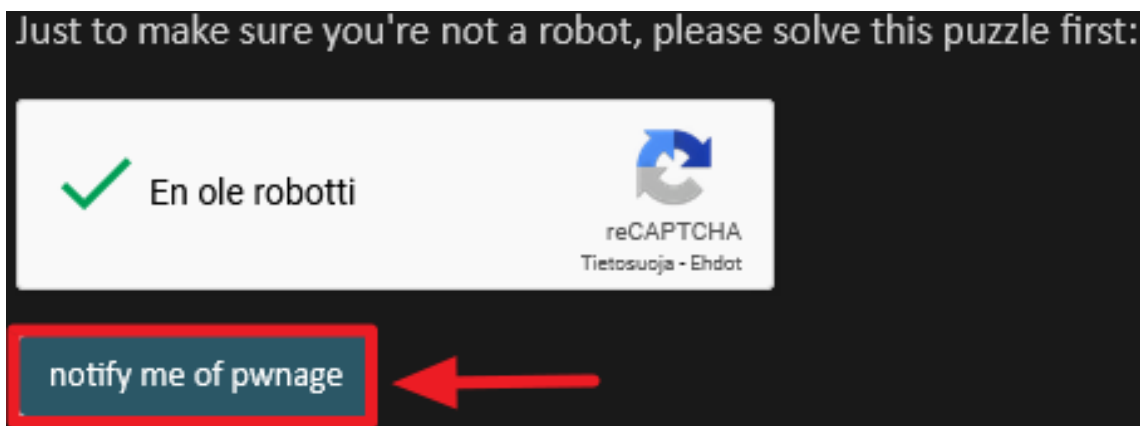
2. Avautuvassa ikkunassa kirjoita kenttään haluamasi sähköpostiosoite ja napsauta rasti ruutuun kohdassa **En ole robotti** (kuva 8). Tämän jälkeen ruudulle avautuu kuviin perustuva varmennus, jolla pitää todistaa lähettäjän olevan ihminen eikä ohjelma. Varmennuksessa on ohjeet siitä, mitkä kuvat pitää valita.



Kuva 8

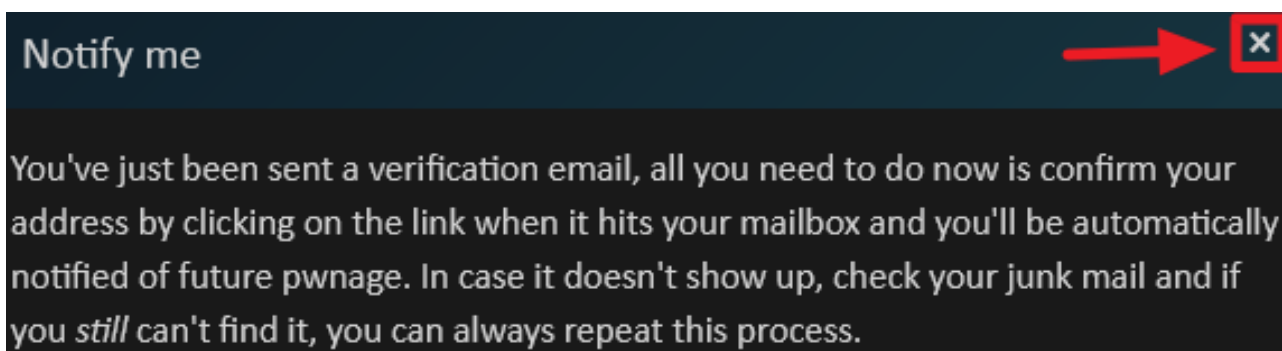
3. Kun varmennus on suoritettu hyväksytysti, näkyy kohdassa **En ole robotti** vihreä "oikein"-merkki. Lopuksi napsauta alareunassa olevaa **notify me of pwnage** -painiketta (kuva 9).





Kuva 9

4. Tämän jälkeen avautuu ikkuna, jossa kerrotaan ilmoittamaasi sähköpostiosoitteeseen lähetetyn vahvistusviestin. Voit sulkea ikkunan napsauttamalla oikeassa yläreunassa olevaa vaaleaa rastia (kuva 10).



Kuva 10

5. Seuraavaksi avaa sähköposti, johon tilasit ilmoituksen. Sähköpostista pitäisi löytyä vahvistusviesti, jonka otsikossa lukee **Confirm your Have I Been Pwned registration**.

6. Vahvistusviestin ulkoasu vaihtelee sen mukaan, näytetäänkö viesti teksti- vai HTML-muodossa. Jos viesti on tekstimuodossa, napsauta viestissä tekstin *Verify my email address* jälkeen olevaa linkkiä (kuva 11). Jos viesti on HTML-muodossa, napsauta **Verify my email** -painiketta (kuva 12).

Hello and welcome to Have I Been Pwned

You (or possibly someone else), just subscribed [palaute@peruskayttajalle.net](mailto:palaute@peruskayttajalle.net) to the notification service and you can unsubscribe at any time if you don't want the notifications. Just to confirm that you're a breach notifications where this email address has been pwned.

Verify my email address: <https://haveibeenpwned.com/Verify/399c11f76070362e05613eee9cbdf691>

Kuva 11



## Welcome to Have I Been Pwned

You (or possibly someone else), just subscribed palaute@peruskayttajalle.net to the notification service that will automatically let you know if your address is caught up in a future data breach. It's a free service and you can unsubscribe at any time if you don't want the notifications.

Just to confirm that you're a real person behind a real email address, click on the link below then you'll be automatically subscribed to new breach notifications where this email address has been pwned.



Kuva 12

7. Tämän jälkeen nettiselaimen avautuu sivu, jossa lukee **Verification complete**. Samalla sivulla näkyy, ovatko kyseisen sähköpostiosoitteen tiedot vuotaneet. Ilmoitus on samanlainen kuin kuvissa 2 ja 3 sivulla 4.

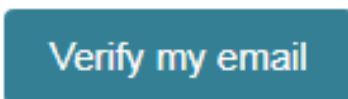
8. Sähköpostiviesti kannattaa säilyttää, koska viestissä olevaa toista linkkiä käyttämällä voit tarvittaessa peruuttaa sähköpostiin tulevan ilmoituksen tietojen vuotamisesta.

9. Peruuttaaksesi sähköposti-ilmoituksen, napsauta tekstimuotoisessa viestissä tekstin *If you don't want to receive any future breach notifications, just click here to unsubscribe* jälkeen olevaa linkkiä (kuva 13). HTML-muotoisessa viestissä napsauta linkkiä **click here to unsubscribe** (kuva 14).

Verify my email address: <https://haveibeenpwned.com/Verify/399c11f76070362e05613eee9cbdf691>

If you don't want to receive any future breach notifications, just click here to unsubscribe: <https://haveibeenpwned.com/Unsubscribe/399c11f76070362e05613eee9cbdf691>

Kuva 13

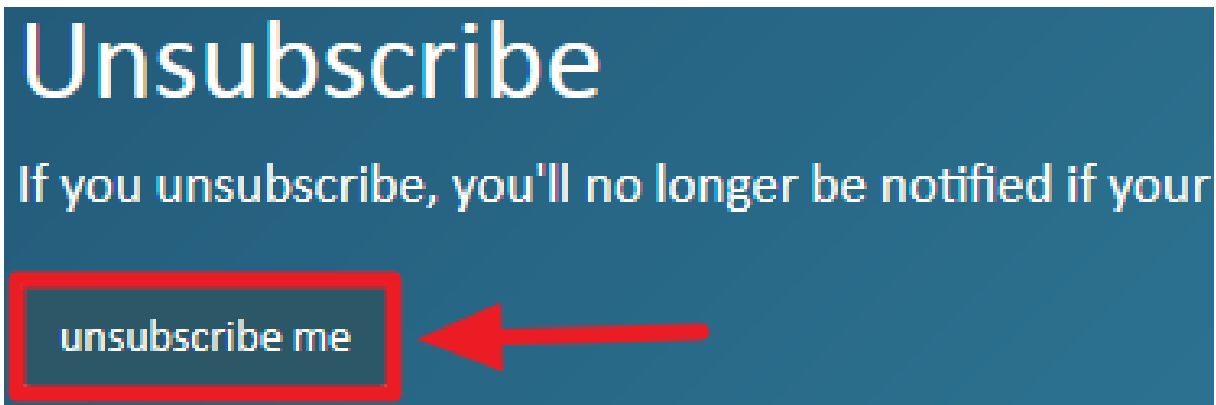


If you don't want to receive any future breach notifications, just click here to unsubscribe.

Kuva 14

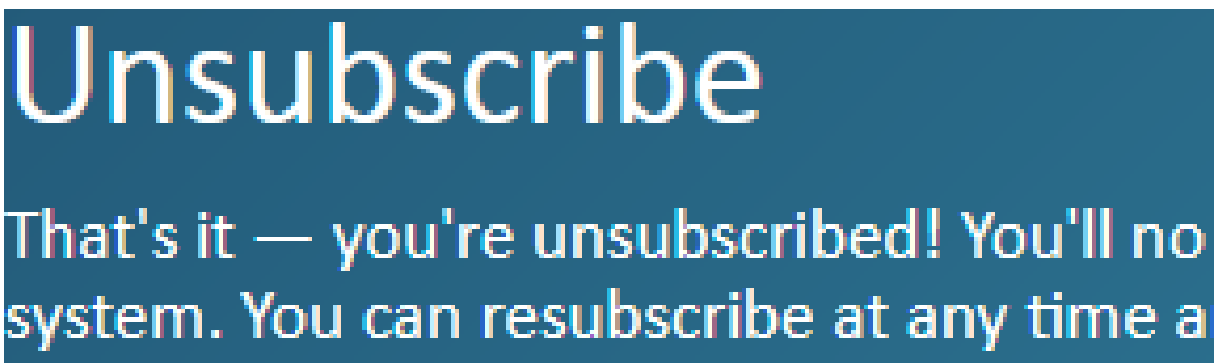


10. Tämän jälkeen nettiselaimen avautuu sivu, jossa lukee **Unsubscribe**. Napsauta sivulla olevaa **unsubscribe me** -painiketta (kuva 15).



Kuva 15

11. Lopuksi avautuu sivu, jossa lukee teksti *That's it — you're unsubscribed!* (kuva 16).



Kuva 16

## 4 Toimenpiteet vuodon jälkeen

---

Tärkein toimenpide tietovuodon tai -murron jälkeen on vaihtaa vuotanut salasana. Tämä on erityisen tärkeää, jos käytät samaa salasanaa eri paikoissa.

Lisäksi on ehdottoman suositeltavaa ottaa käyttöön kaksivaiheinen tunnistautuminen kaikissa verkkopalveluissa, joissa sitä on mahdollista käyttää. Kaksivaiheisesta tunnistautumisesta käytetään myös muita nimiä, kuten kaksivaiheinen vahvistus.

Kaksivaiheisessa tunnistautumisessa verkkopalveluihin annetaan ensin normaalisti käyttäjätunnus ja salasana. Tämän jälkeen kirjautumiseen vaaditaan esimerkiksi tekstiviestillä



saatava koodi. Tällöin kirjautuminen onnistuu vasta, kun verkkopalveluun on annettu oikea koodi.

Eri verkkopalveluiden käyttämät vahvistustavat vaihtelevat tekstiviestillä saatavista koo-  
deista älypuhelimeen asennettaviin ohjelmiin ja tietokoneeseen liitettäviin muistitikkuihin.

Lisätietoa aiheesta löytyy esimerkiksi [Googlen kaksivaiheista tunnistautumista esittelevältä nettisivulta](https://www.google.com/intl/fi/landing/2step/) (<https://www.google.com/intl/fi/landing/2step/>) ja [Wikipediasta](https://fi.wikipedia.org/wiki/Kaksivaiheinen_tunnistautuminen) ([https://fi.wikipedia.org/wiki/Kaksivaiheinen\\_tunnistautuminen](https://fi.wikipedia.org/wiki/Kaksivaiheinen_tunnistautuminen)).

Pahimmassa tapauksessa erilaisia tietoja voi vuotaa niin, että tietoja hyödyntämällä on mahdollista tehdä identiteettivarkaus. Identiteettivarkaudessa henkilö esiintyy toisena henkilönä. Usein identiteettivarkaajat käyttävät väärää henkilöllisyyttä rikollisiin tarkoituksiin.

Uhrin nimissä voidaan esimerkiksi tilata tavaraa tai ottaa pikavippejä. Vuotaneita tietoja voidaan väärinkäyttää myös pelkkään kiusaamiseen.

Yle on kahdessa artikkelissaan ([Identiteettivaras vaanii verkossa](https://yle.fi/uutiset/3-9448910), <https://yle.fi/uutiset/3-9448910> ja [Näin voit yrittää välttää identiteettivarkaudelta](https://yle.fi/uutiset/3-9727894), <https://yle.fi/uutiset/3-9727894>) käsitellyt identiteettivarkauksia ja niiltä suojautumista.

Yksi mahdollinen tapa suojautua osittain identiteettivarkauden seurauksilta on omaehtoinen luottokielto. Usein identiteettivarkaudessa uhrin henkilötietoja hyödynnetään ostamalla luotolla tavaraa, joka sitten myydään eteenpäin. Tällöin uhri joutuu kärsimään seurauksista, kun maksamattomia maksuja aletaan perimään.

Tällaisessa tapauksessa osittaista suojaa antaa omaehtoinen luottokielto. Olen kirjoittanut aiheesta [artikkelin](https://peruskayttajalle.net/artikkelit.php#luottokielto) (<https://peruskayttajalle.net/artikkelit.php#luottokielto>).

