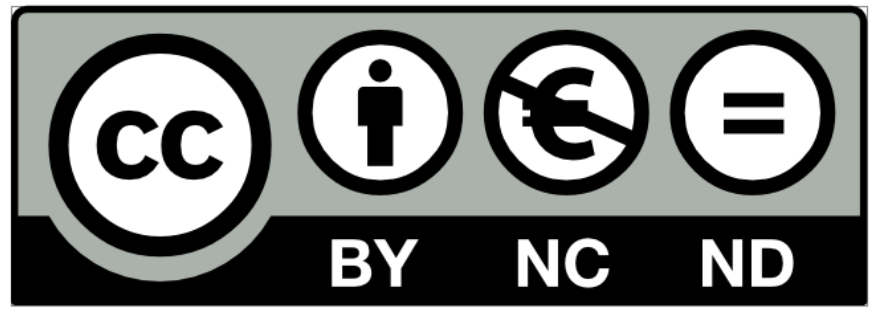
Tarkista ovatko tie-tosi vuotaneet

Peruskäyttäjälle.net

Ohjeen versio 13.1.2019



- ➔ Peruskäyttäjälle.netin Creative Commons-esittely (https://peruskayttajalle.net/tietoja.php#cc)
- ➔ Lisätietoa Creative Commonsista suomeksi (https://creativecommons.fi/)

Sisällysluettelo

1 Johdanto

Erilaiset tietomurrot ja -vuodot ovat nykyään valitettavan yleisiä. Usein murroissa tai vuodoissa joutuu vääriin 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/) on verkkopalvelu, josta voi tarkistaa, ovatko omat tiedot varastettu tai vuotaneet. Palvelusta voi hakea omia tietojaan käyttäjätunnuksen tai sähköpostiosoitteen perusteella.

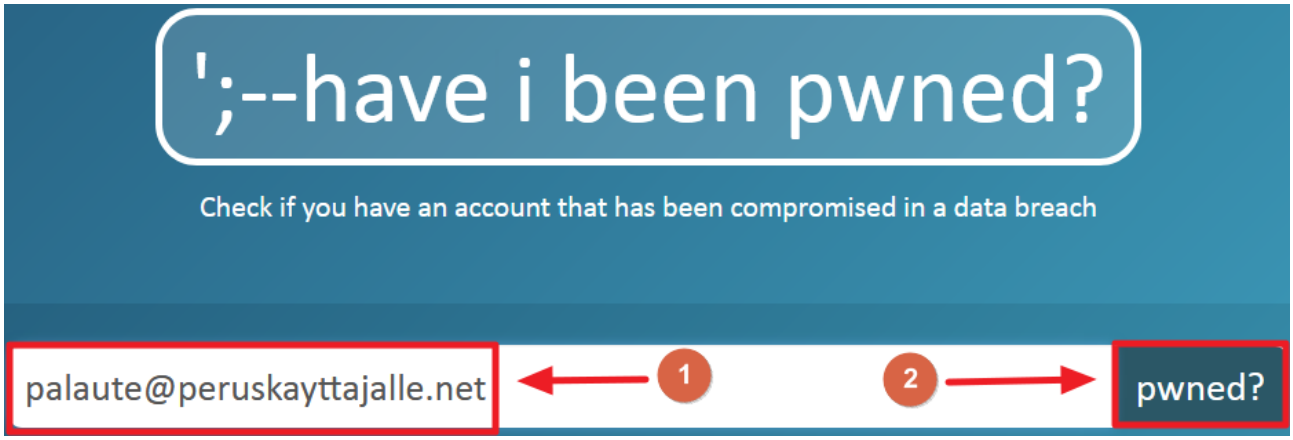
Have I Been Pwned on osoittautunut luotettavaksi verkkopalveluksi. Tässäkin asiassa tulee olla varovainen, koska myös rikolliset ovat pystyttäneet omia vastaavanlaisia verkkopalveluitaan kerätäkseen käyttäjien tietoja.

Tässä ohjeessa käydään läpi omien tietojen etsiminen Have I Been Pwnedissa, sähköpostiilmoituksen 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 tai sähköpostiosoite. Lopuksi napsauta näppäimistön **Enter** -näppäintä tai kentän perässä olevaa tummaa **pwned?** -painiketta. Esimerkissä käytetään sähköpostiosoitetta *palaute@peruskayttajalle.net* (kuva 1).



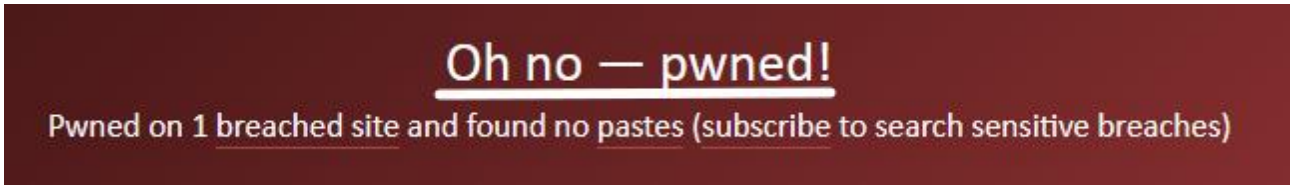
Kuva 1

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

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).

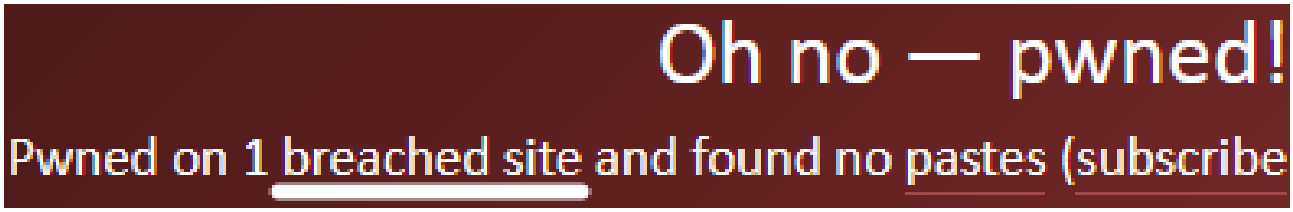
Kuva 2

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*).

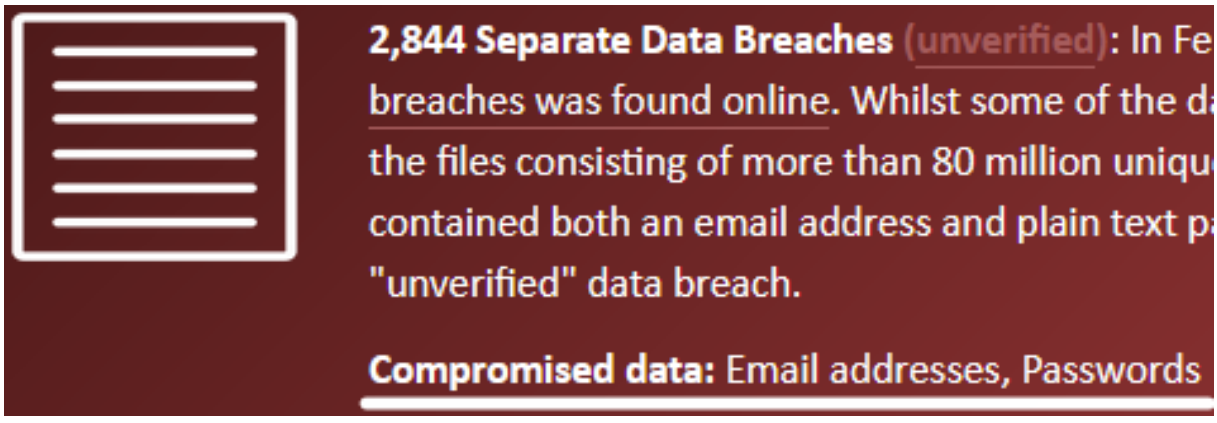


Kuva 4

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.

Kuva 5

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



Kuva 6

Alla on lista osasta vuotaneista tiedoista englanniksi ja suomeksi.

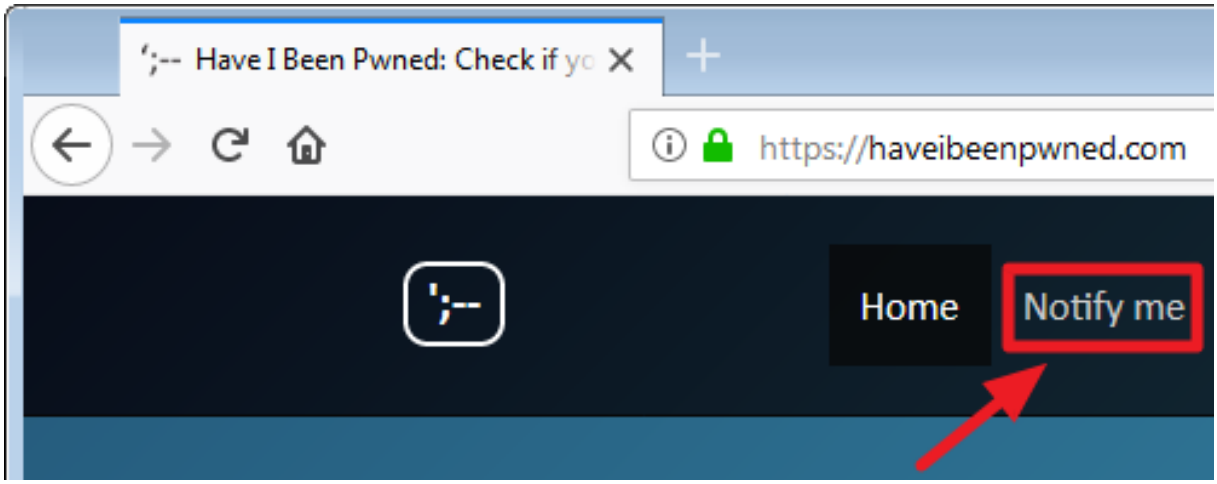
Vuotaneet tiedot englanti–suomi:

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
Usernames	Käyttäjätunnus
Years of birth	Syntymävuosi

3 Sähköposti-ilmoituksen tilaaminen

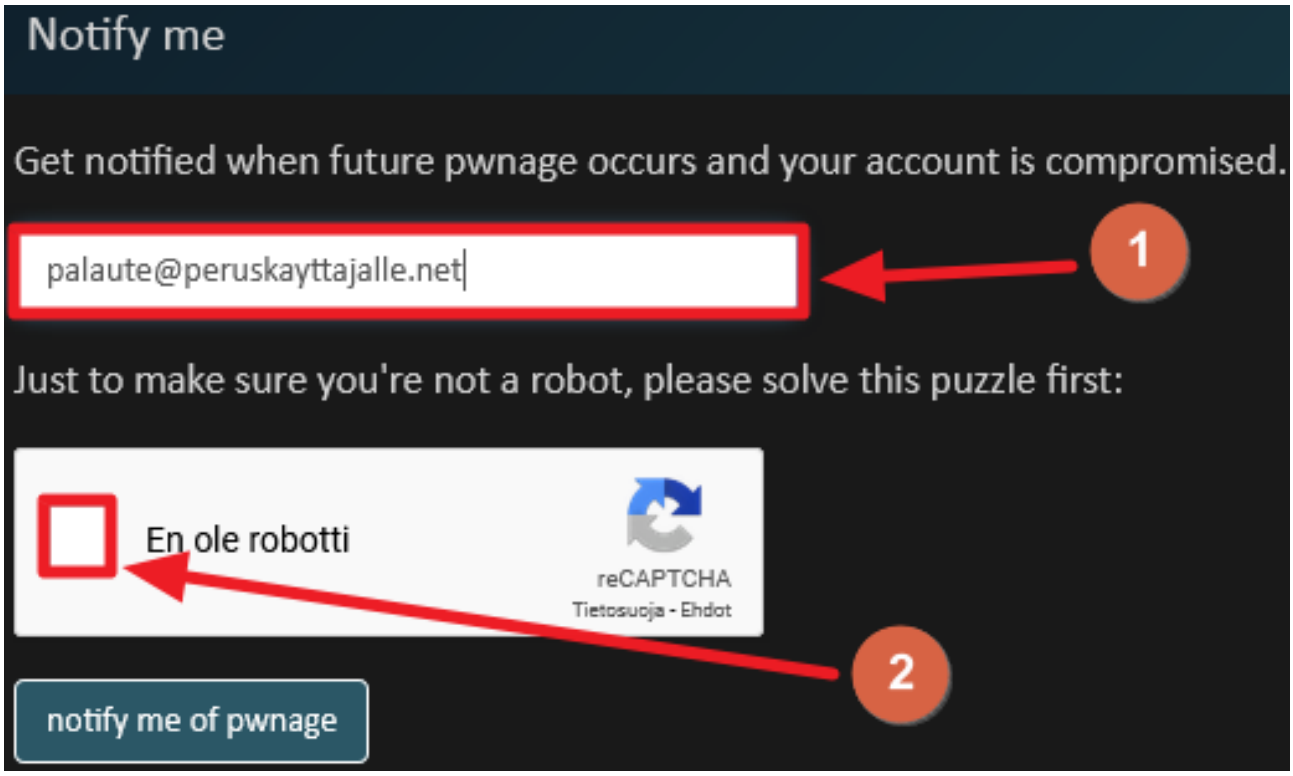
Have I Been Pwnedissa on mahdollista tilata ilmoitus sähköpostiin, jos tietosi ovat vuotaneet. Voit tilata ilmoituksen seuraavasti:

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



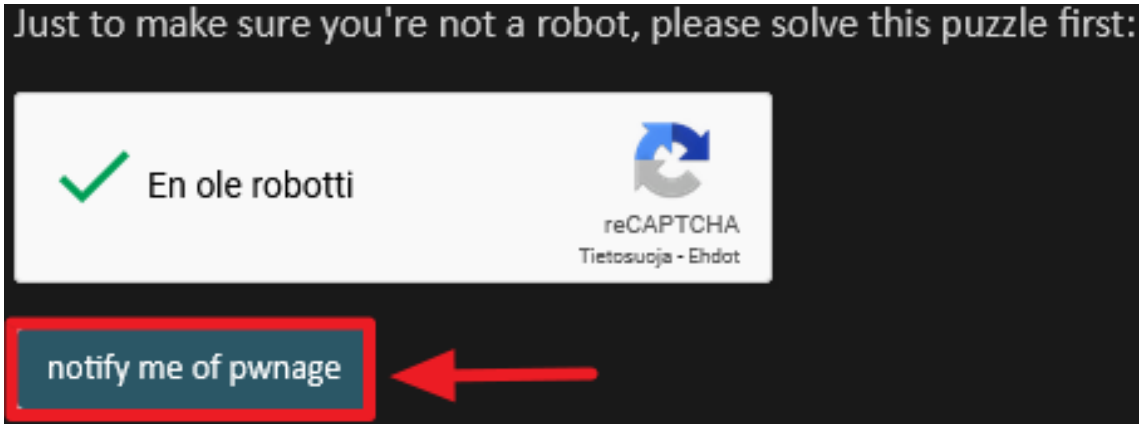
Kuva 7

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.



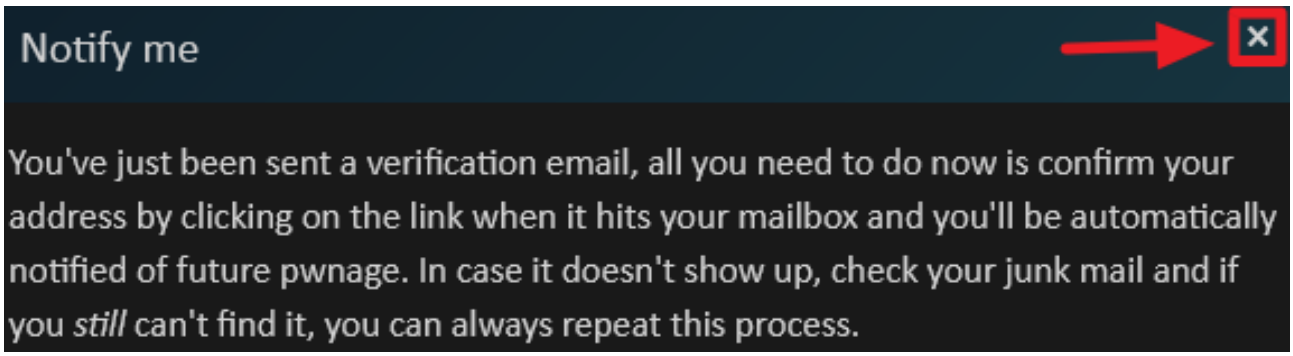
Kuva 8

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

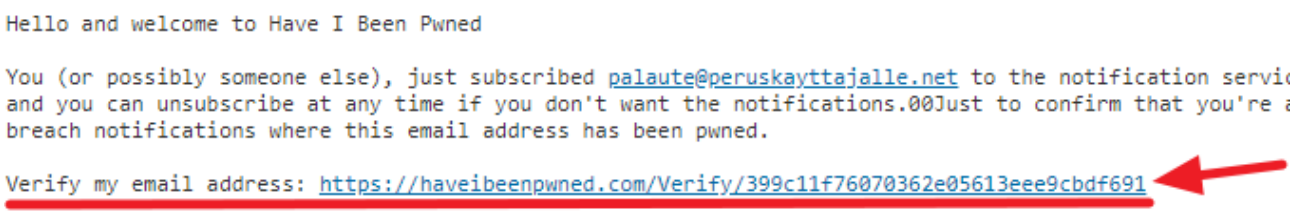
4. Tämän jälkeen avautuu ikkuna, jossa kerrotaan ilmoittamaasi sähköpostiosoitteeseen lähetetyn vahvistusviestin. Voit sulkea ikkunan napsauttamalla oikeassa yläreunassa olevaa vaaleaa rastia (kuva 10).



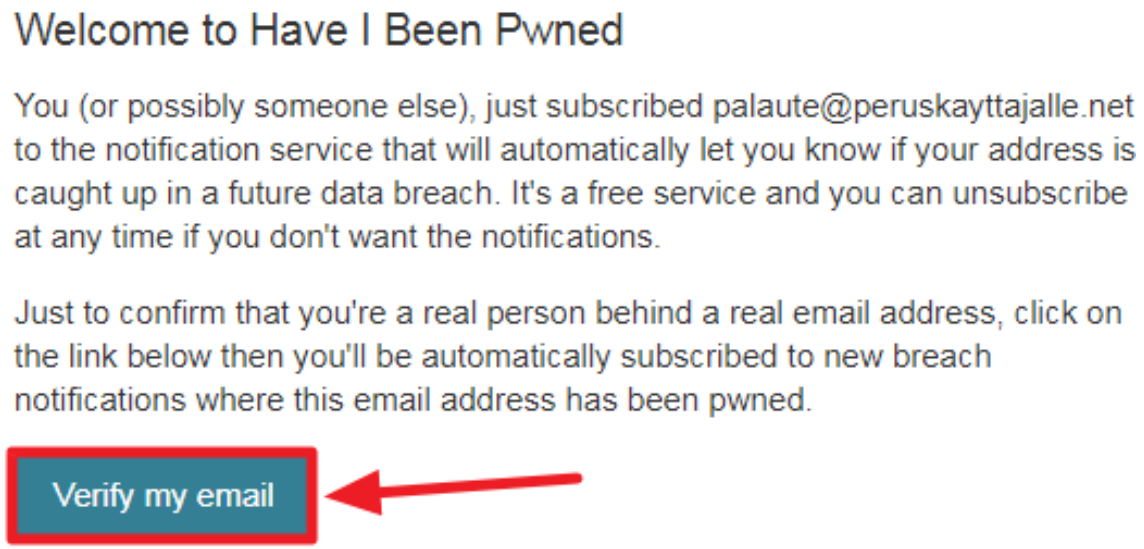
Kuva 10

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).



Kuva 11

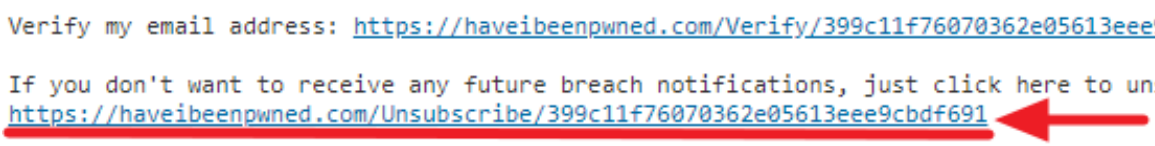


Kuva 12

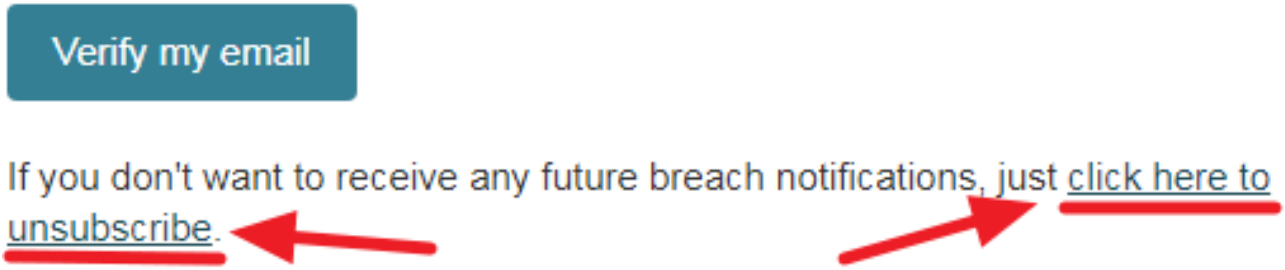
7. Tämän jälkeen nettiselaimeen avautuu sivu, jossa lukee **Verification complete**. Samalla sivulla näkyy, ovatko kyseisen sähköpostiosoitteen tiedot vuotaneet. Ilmoitus on samanlainen kuin kuvissa 2 ja 3 sivulla 4.

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).

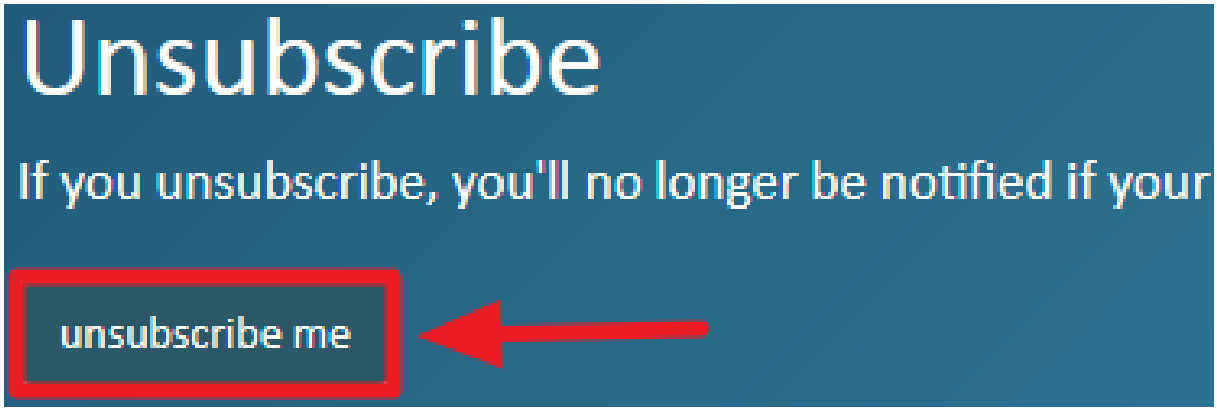


Kuva 13



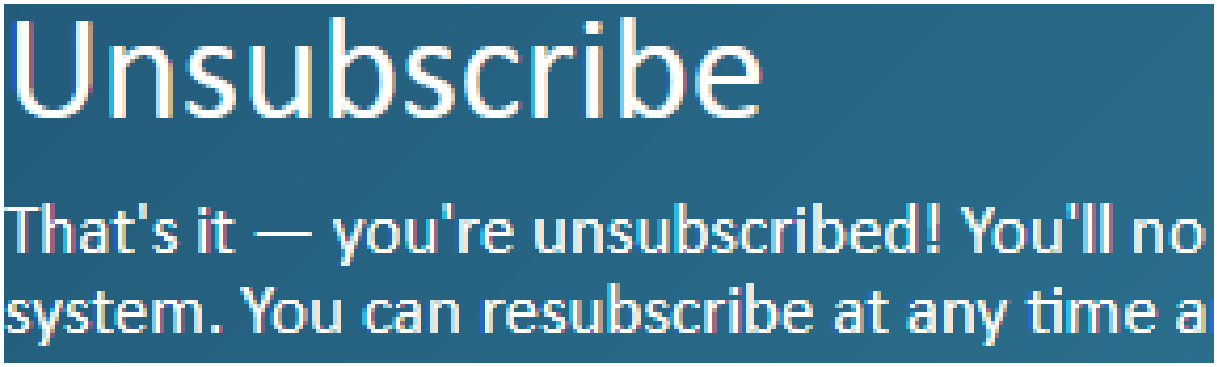
Kuva 14

10. Tämän jälkeen nettiselaimeen 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 koodeista älypuhelimeen asennettaviin ohjelmiin ja tietokoneeseen liitettäviin muistitikkuihin.

Lisätietoa aiheesta löytyy esimerkiksi Googlen kaksivaiheista tunnistautumista esittelevältä nettisivulta (https://www.google.com/intl/fi/landing/2step/) ja Wikipediasta (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 identiteettivarkaat 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 ja Näin voit yrittää välttyä identiteettivarkaudelta, 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).