



TIETO- TURVA- OPAS

**Poliitikoille ja
puolueille**

facebook

Kampanja yksityisyyden suojaamiseksi vaaleissa

Suunnittelu: [ccm.design](#)

Kansikuva: Grisha Bruev

facebook



Yksityisyyden suojaaminen vaaleissa

Me Facebookilla suhtaudumme erittäin vakavasti demokratiaan kohdistuviin uhkiin ja teemme kaikkemme yksityisyyden suojaamiseksi vaaleissa.

Tämän oppaan tarkoituksena on auttaa sinua poliitikkona pitämään Facebook-sivusi ja -tilisi suojattuina. Lisäksi tarjoamme puolueille erityisen yhteydenottokanavan, jotta voimme auttaa nopeasti tietomurtoa epäiltäessä. Nämä toimenpiteet ovat osa Facebookin laajaa vaaleja koskevaa kampanjaa.

Kuva: Grisha Bruev

A photograph of a person with long blonde hair, wearing a dark dress, walking away from the camera on a dirt path through a dense forest. Sunlight filters through the trees, creating a dappled light effect on the path and foliage. The path leads into the distance, flanked by tall evergreen trees.

Kaikkien Facebookin
käyttäjien tietoturva on
meille tärkeää. Facebook-
sivuja ei hakkeroida, mutta
sivujen taustalla olevat
profiilit voivat altistua
uhille. On olemassa
helppoja mutta tehokkaita
toimenpiteitä, joilla voit
suojata tilisi ja tietosi.
Niistä kerromme tässä
oppaassa!

Sivun ylläpitäjien tärkeä rooli tietoturvan varmistamisessa

Tämä opas sisältää vinkkejä puolueiden, poliitikkojen ja julkisuuden henkilöiden Facebook-sivujen ja -profiilien suojaamiseen.

Poliitikot ja puolueet voivat olla vuorovaikutuksessa kansalaisten ja äänestäjiensä kanssa Facebookiin luodun sivun kautta. Kuka tahansa, jolla on Facebook-profiili, voi luoda sivun tai auttaa sen ylläpitämisessä, kunhan kyseiselle henkilölle on myönnetty rooli sivulla. Henkilöt, jotka ovat tykänneet sivusta, näkevät omassa uutisvirrassaan sivun päivityksiä esimerkiksi julkaisujen, kuvien tai videoiden muodossa.

Poliittisesti aktiivisille henkilöille tai organisaatioille kuuluvia sivuja ylläpitää monesti useampi kuin yksi henkilö. Näissä tapauksissa kyse on muustakin kuin yhdestä taustalla olevasta Facebook-profiilista. Siksi kaikkien asianosaisten on hyvä tietää, kuinka tärkeää oman profiilin turvallisuus on. Kaikkien poliittiseen sivuun liitettyjen henkilöiden kaikki turvallisuus- ja yksityisyysasetukset on oltava käytössä.

Kuva: Geran de Klerk, Unsplash

Suojaa sivun ylläpitäjän profili



Suojaa salasanasi ja tilisi

Älä koskaan käytä Facebook-salasanaasi muualla tai jaa salasanasi muille. Kenenkään muun ei pitä tietää salasanasi. Vältä sellaisten henkilökohtaisten tietojen käyttöä, jotka on helppo arvata, kuten nimesi, puhelinnumerosi, syntymäaikasi, sähköpostiosoitteesi tms.

Salasanasi päättelyn pitää olla vaikeaa.

Ota käyttöön ilmoitusviestit tunnistamattomista sisäänkirjautumisista, jotta saat ilmoituksen, jos tilillesi kirjaudutaan uudelta laitteelta.

Käytä kaksivaiheista todennusta tilisi lisäturvallisuustoimintona.

Kirjaudu ulos tililtäsi

Turvallisuus ja sisäänkirjautuminen -asetusten kohdassa "Missä olet sisäänkirjautuneena?" näet luettelon tietokoneista, puhelimista ja tableteista, joilta on vastikään kirjauduttu tilillesi. Jos haluat kirjautua ulos Facebookista toiselta tietokoneelta, puhelimelta tai tablettilta, siirry kohtaan Asetukset ja valitse sitten Turvallisuus ja sisäänkirjautuminen. Kohdassa "Missä olet sisäänkirjautuneena?" voit lopettaa haluamasi istunnot valitsemalla Kirjaudu ulos.

Ota käyttöön ilmoitusviestit tunnistamattomista sisäänkirjautumisista asetusten turvallisuusosiossa. Silloin lähetämme sinulle sähköpostiviestin tai ilmoituksen aina, kun joku kirjautuu tilillesi uudesta sijainnista.

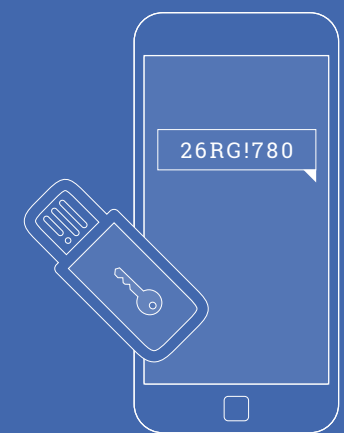
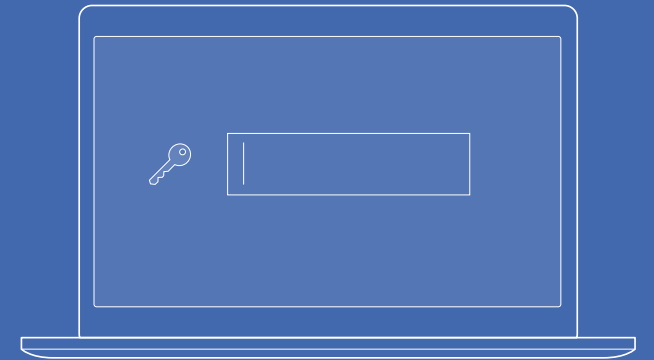
Kaksivaiheinen todennus

MIKÄ SE ON?

Kaksivaiheinen todennus on turvallisuustoiminto, joka salasanana lisäksi auttaa Facebook-tilisi suojaamisessa.

Jos otat käyttöön kaksivaiheisen todennuksen, sinua pyydetään antamaan erityinen turvakoodi tai vahvistamaan sisäänkirjautumisesi joka kerta, kun joku yrittää kirjautua Facebookiin tietokoneelta tai mobiililaitteelta, jota emme tunnista.

- 1 Siirry turvallisuus- ja sisäänkirjautumisasetuksiin klikkaamalla Facebookin oikeassa yläkulmassa olevaa nuolta ja valitsemalla **Asetukset > Turvallisuus ja sisäänkirjautuminen**.
- 2 Vieritä alaspäin kohtaan **Käytä kaksivaiheista todennusta** ja valitse **Muokkaa**.
- 3 Valitse todennustapa, jonka haluat lisätä, ja noudata näytölle tulevia ohjeita.
- 4 Valitse **Valmis**, kun olet valinnut ja ottanut käyttöön todennustavan.



NÄIN SE TOIMII

Turvakoodin voi saada käyttöön monella eri tavalla.

- 1 Voit pyytää kymmentä koodia, jotka voit tulostaa, kirjoittaa muistiin tai tallentaa.
- 2 Jos puhelimeesi tai tablettiisi on asennettu Facebook-sovellus, voit käyttää koodigeneraattoria.
- 3 Voit käyttää ulkoista turva-avainta, joka tukee U2F-protokollaa.



KYBERUHKKA

TOIMINTA, JOHON KANNATTAA KIINNITTÄÄ HUOMIOTA

O n hyvä tietää hakkereiden useimmin käyttämät tavat, joita he kohdistavat poliitikkoihin, ehdokkasiin ja näihin liittyviin henkilöihin. Voit vahvistaa Facebook-tilisi suojausta varmistamalla, että sähköpostitilisi ja verkkosivustot ovat suojattuja. Alla olevilla vinkeillä voit vähentää riskiä, että joku pääsee käsiksi tiliisi.

Jos epäilet, että tilissäsi on jotain vialla, voit ottaa meihin yhteyttä oman puolueesi viestintäosaston kautta.

Tietojenkalastelu



Kohdistetussa tietojenkalastelussa (spear phishing) rikolliset lähettävät räätälöityjä sähköpostiviestejä valikoiduille henkilöille. Näiden viestien tavoitteena on näyttää mahdollisimman aidoilta, mutta ne sisältävät usein haitallisia linkkejä tai tiedostoja.

Tietojenkalastelulla pyritään pääsemään käsiksi tiliisi tai tallentamaan henkilökohtaisia tietojasi sen jälkeen, kun sinut on saatu antamaan kirjautumistietosi tai muita arkaluonteisia tietoja väärennetyllä verkkosivustolla.

Esimerkkinä voidaan mainita räätälöidyt sähköpostiviestit tai viestit, jotka on luotu näyttämään mahdollisimman aidoilta ja joissa väitetään, että tilisi salasana on vaihdettava. Sähköpostiviesti sisältää lyhyen linkin, joka ohjaa väärennetylle sisäänkirjautumissivulle. Jos annat kirjautumistietosi tällä sivulla, hakkerit voivat kirjautua tilillesi ja tehdä muutoksia asetuksiisi, minkä seurauksena et ehkä voi enää käyttää tiliäsi.

Suositus: On tärkeää ymmärtää, että yksityinen sähköpostisi, sosiaalisen median profiilisi ja muut tilisi ovat yhtä houkuttelevia kuin ne, joita käytät työsi puolesta. Noudata samaa varovaisuutta niin yksityisten tiliesi kuin työhösi liittyvien tilien suojaamisessa.

Kuva: Natali9ka

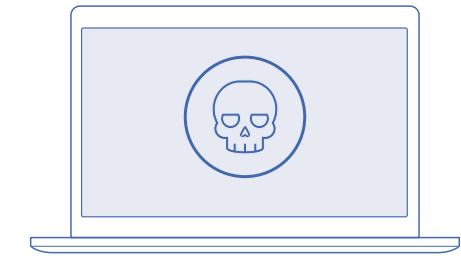
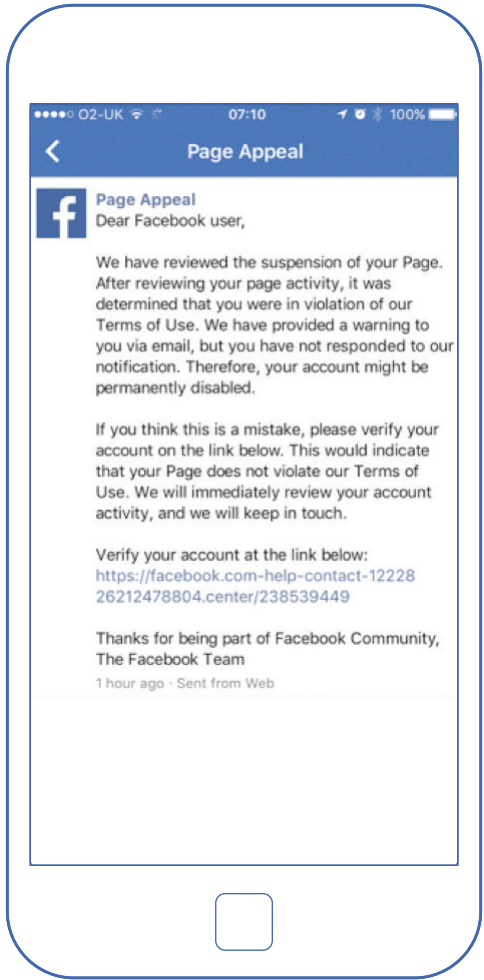
Tietojenkalastelu väärennetyllä Facebook- logolla

Joskus tietojenkalastelulla yritetään vakuuttaa valitut henkilöt siitä, että heidän Facebook-tilinsä tai -sivunsa on suljettu, ja viesti näyttää Facebookin lähettämältä. Näiden toimien tavoitteena on kerätä arkaluonteisia tietoja ohjaamalla valittu henkilö linkin kautta sivulle, joka kerää käyttäjätietoja. Jos hakkerit pääsevät käsiksi kirjautumistietoihisi, he voivat kirjautua tilillesi ja tehdä muutoksia asetuksiisi, minkä seurauksena et ehkä voi enää käyttää tiliäsi.

Facebookia jäljittelevässä tietojenkalastelutoiminnassa käytetään luvatta Facebookin graafista profiilia viestien lähettämiseen tavallisesti Messengerin kautta, mikä lisää vaikutelmaa aidosta ja henkilökohtaisesta ilmoituksesta. Jos viestissä olevaa linkkiä klikataan, tilin suojaus vaarantuu.

Tätä tietojenkalastelumetodia käyttävillä hakkereilla on tavallisesti taloudellinen kannustin, ja he ottavat kohteikseen Facebook-sivuja, joilla on paljon seuraajia. Tämän vuoksi olet poliitikkona kiinnostava kohde.

Suositus: Jos uskot joutuneesi tietojenkalastelun kohteeksi, lähetä sähköpostia Facebookin turvallisuusosastolle osoitteeseen phish@fb.com tai ota yhteyttä puolueesi viestintäosastoon.



Työtoverit kohteina

Digitaalinen turvallisuushuha ei liity ainoastaan sinuun itseesi. Hakkereiden yleinen taktiikka on käyttää samaa lähestymistapaa valitun uhrin työtovereihin voidakseen kerätä mahdollisimman paljon arvokasta tietoa.

Suosituksia: Jaa tietoa turvallisuudesta ja hyvistä käytännöistä työtovereillesi ja kollegoillesi. Organisaation sisäisessä tietoturvallisuuskoulutuksessa pitää korostaa omien tietojen arvoa ja riskiä, että rikolliset yrittävät päästä niihin käsiksi.

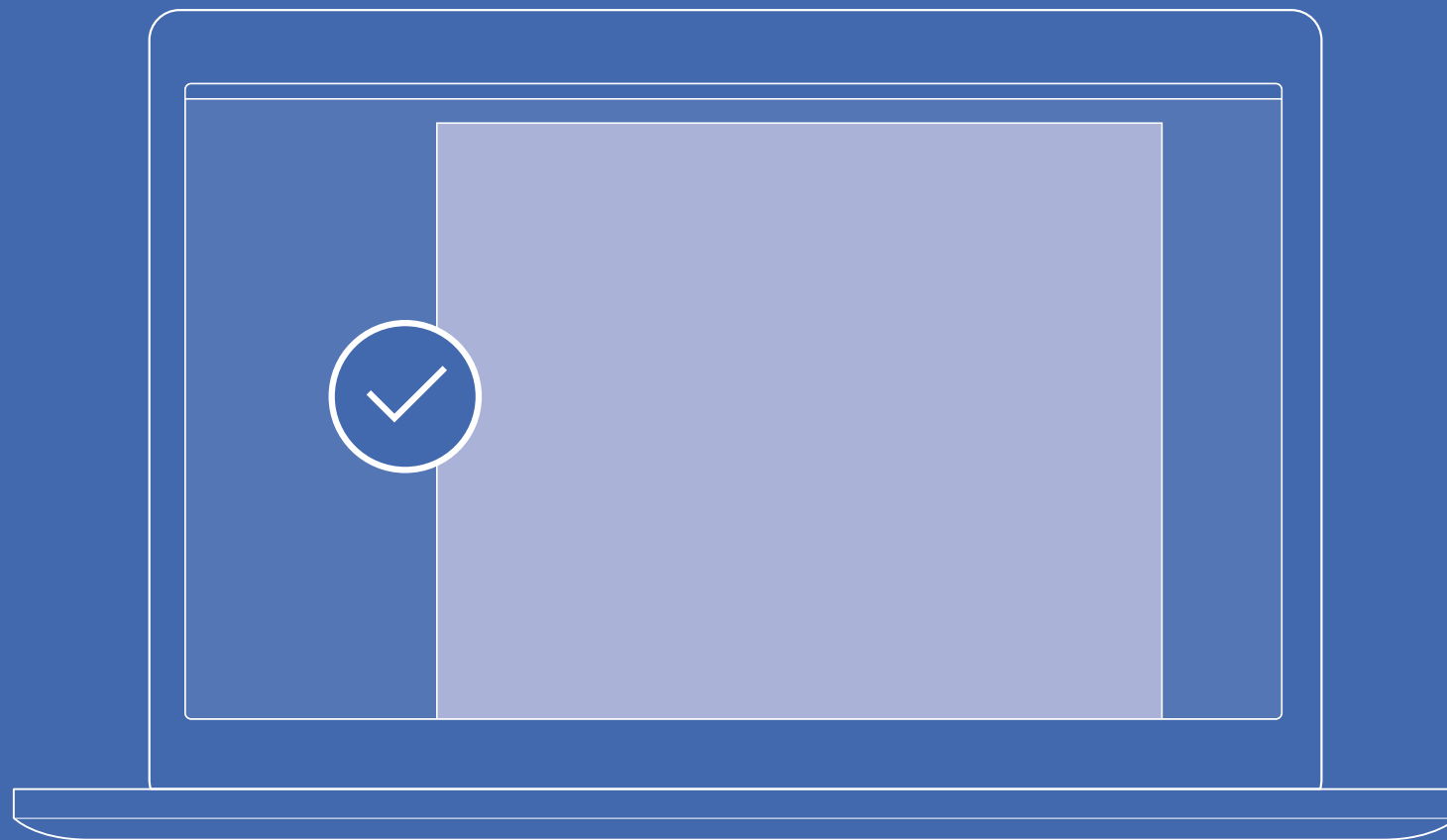
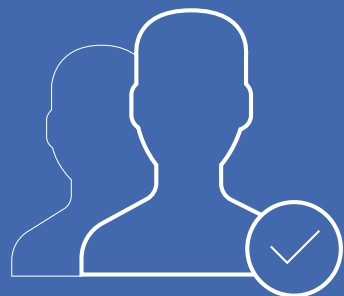
Verkkosivustojen vaarantaminen

Toinen rikollisten käyttämä taktiikka on ”verkkosivustojen strateginen vaarantaminen” saastuttamalla verkkosivut, joilla kohteena olevat henkilöt todennäköisesti vierailevat. Tällaiselle sivulle siirtyminen johtaa haittakoodin lataamiseen yleensä kohteena olevan henkilön verkkoselaimeen. Tätä haittakoodia käytetään sen jälkeen muiden hyökkäysten tekemiseen, kuten uhrin tietojen kopioimiseen tai edelleenjakamiseen. Viime aikoina tämäntyyppinen toiminta on keskittynyt ulkoministeriöiden ja suurlähetystöjen verkkosivuihin.

Suositus: Käytä ainoastaan sellaisia verkkoselaimia, joissa on sisäänrakennetut turvallisuustoiminnot, kuten Google Chromea, ja huolehdi verkkoselaimen ja muiden käyttämiesi ohjelmien jatkuvasta päivittämisestä.

Sivun ylläpitäjien aidot henkilöllisyydet

Facebookissa kaikkien odotetaan käyttävän sitä nimeä, jota he muutoinkin käyttävät. Tätä odotetaan siksi, jotta tietäisit aina, kenen kanssa olet yhteydessä. Kun ihmiset seisovat avoimesti omien mielipiteidensä ja oman toimintansa takana, Facebookista tulee myös mukavampi paikka. Jos saamme selville, etteivät ihmiset käytä oikeita henkilöllisyyksiään, suljemme heidän tilinsä. Kun sivun ylläpitäjät eivät käytä oikeita henkilöllisyyksiään, heidän tilinsä voidaan sulkea eivätkä he enää pääse Facebook-sivulleen.



Vahvistetut sivut

Facebook voi vahvistaa sivuja ja profileja. Sivulla tai profilissa näkyvä sininen vahvistusmerkki tarkoittaa, että Facebook on vahvistanut julkisuuden henkilön tai puolueen sivun tai profilin aitouden.

Sinisen vahvistusmerkin saaminen edellyttää, että sivusi tai profilisi täyttää Facebookin käyttäjäsovimuksen ehdot ja sisältää:

- ① kansikuvan
- ② profilikuvan
- ③ Facebookin ohjeita noudattavan nimen
- ④ tilille julkaistua sisältöä
- ⑤ käyttöön otetun Seuraa-ominaisuuden (koskee ainoastaan profileja).

Mahdollisuus saada sininen vahvistusmerkki perustuu eri tekijöihin, kuten siihen, kuinka hyvin tiliä on täydennetty, miten hyvin se noudattaa sääntöjä ja herättääkö se julkista kiinnostusta.

Voit anoa sinistä vahvistusmerkkiä täyttämällä hakemuslomakkeen. Tarvitsemme kopion viranomaisen myöntämästä kuvallisesta henkilöllisyystodistuksesta (kuten passista, ajokortista tai kansallisesta henkilökortista), jotta voimme vahvistaa pyyntösi. Kehotamme sinua antamaan myös muita tietoja, jotka auttavat meitä pyyntösi tarkistamisessa. Kerro lyhyesti, miksi tilille pitäisi myöntää sininen vahvistusmerkki, ja anna asianmukaiset URL-osoitteet, jotka osoittavat tiliin kohdistuvan julkisen kiinnostuksen.

Hakemuslomake löytyy Facebookin Ohje- ja tukikeskuksesta: **www.facebook.com/help**.

Voit pyytää apua vahvistuksen saamiseen myös puolueesi viestintäosastolta.

Facebookin yhteisönormien tavoitteena on tarjota käyttäjille mahdollisuus ilmaista mielipiteitään kaikille avoimessa ja turvallisessa ympäristössä.

www.facebook.com/communitystandards

Reagoi loukkaavaan sisältöön



ILMOITA LOUKKAAVASTA SISÄLLÖSTÄ

Paras tapa ilmoittaa loukkaavasta sisällöstä tai roskapostista Facebookissa on käyttää ilmiantolinkkiä, joka löytyy julkaisun vierestä.

Tutustumme ilmoitukseen ja ryhdymme tarvittaviin toimenpiteisiin.

Tässä on muutama esimerkki siitä, miten voit ilmoittaa sisällöstä meille:

Ilmianna julkaisu tai kommentti Facebookissa

klikkaamalla kolmea pistettä "..." oikeasta yläkulmasta.

Valitse "Anna palautetta julkaisusta".

Ilmianna viesti

Avaa viesti, jonka haluat ilmiantaa.

Klikkaa oikeassa yläkulmassa olevaa rataskuvaketta.

Valitse "Ilmianna roskaposti tai väärinkäyttö..." ja noudata ohjeita.

Ohjeet muuntyyppisen sisällön ilmiantamiseen löytyvät osoitteesta www.facebook.com/report.



DOKUMENTOI LOUKKAAVA SISÄLTÖ

Jos haluat ilmoittaa laittomasta sisällöstä oikeusviranomaisille, on hyvä ottaa näyttökuvia epätoivotuista toimista.

Jos tunnet olevasi tai joku tuttusi tuntee olevansa välittömässä vaarassa, ota yhteyttä poliisiin.



Julkisuuden henkilöt, kuten päättäjät ja virkamiehet, saavat sekä positiivista että negatiivista huomiota. Siksi on tärkeää ottaa käyttöön Facebookin kaikki turvallisuus- ja yksityisyystoiminnot.

Tärkeitä turvallisuusvinkkejä

Tässä on yhteenvetona joitakin turvallisuusvinkkejä, jotka auttavat tilisi suojaamisessa:

- 1 Suojaa salasanasi.
- 2 Käytä lisäturvallisuustoimintojamme, kuten kaksivaiheista todennusta, sisäänkirjautumisilmoituksia, kertakäyttöistä salasanaa ja luotettuja yhteyshenkilöitä.
- 3 Varmista, että sähköpostitilisi ovat suojattuja.
- 4 Kirjaudu ulos Facebookista, kun käytät muiden ihmisten kanssa jaettua tietokonetta. Jos tämä unohtuu, voit kirjautua ulos tililtäsi myös etänä.
- 5 Käytä tietokoneessasi virustentorjuntaohjelmistoa.
- 6 Mieti ennen kuin klikkaat linkkejä tai lataat sisältöä.

Älä koskaan käytä Facebook-salasanaasi muualla verkossa.

Älä koskaan jaa salasanaasi muille. Sinun on oltava ainoa henkilö, joka tietää salasanan.

Vältä salasanassa omaa nimeäsi tai yleisiä sanoja. Salasanasi arvaamisen pitää olla vaikeaa.

Lisää turvallisuusvinkkejä löytyy Facebookin Ohje- ja tukikeskuksesta: facebook.com/help/keeping-your-account-secure

Turvallisuustarkistus

Facebookin turvallisuustarkistuksen avulla voit tarkistaa tilisi turvallisuuden ja parantaa sitä. Turvallisuustarkistus auttaa sinua:

- 1 kirjautumaan ulos Facebookista sellaisista verkkoselaimista ja sovelluksista, joita et käytä
- 2 saamaan ilmoituksia, kun joku yrittää kirjautua tilillesi tunnistamattomalta tietokoneelta tai mobiililaitteelta
- 3 oppimaan suojaamaan salasanasi.

Turvallisuustarkistus löytyy Facebookin Ohje- ja tukikeskuksesta: facebook.com/help/keeping-your-account-secure

Kuva: Discovod



Apua sinulle poliitikkona vaaleissa

Me Facebookilla suhtaudumme erittäin vakavasti alustamme ja käyttäjiemme tietoturvaan. Olemme vakaasti päättäneet tehdä kaikkemme yksityisyyden suojaamiseksi vaaleissa.

Tukitoiminnon sähköpostiosoite poliitikoille

Jotta voisimme auttaa sinua poliitikkona mahdollisimman nopeasti ongelmatilanteissa, olemme luoneet vaaleja varten erityisen sähköpostiosoitteen.

Ota yhteyttä puolueesi viestintäosastoon, joka auttaa sinua saamaan yhteyden meihin Facebookilla!

Lisätietoja ja linkkejä

www.facebook.com/safety

www.facebook.com/help

www.facebook.com/about/basics

Kuva: Bildagentur Zoonar GmbH

Kampanja yksityisyyden suojaamiseksi vaaleissa

facebook

Kampanja yksityisyyden suojaamiseksi vaaleissa