

BEVEILIGING

E-mails van Bitwarden

E-mails van Bitwarden

Net als het gebruik van sterke wachtwoorden is het vermijden van verdachte e-mails een belangrijk hulpmiddel in je online beveiligingstoolkit. We raden je aan vertrouwd te raken met deze [FTC-richtlijnen](#) voor het herkennen en vermijden van phishing.

Hier zijn enkele richtlijnen om je te helpen bepalen of een e-mail die lijkt te komen van Bitwarden legitiem is:

Geautomatiseerde e-mails

E-mails voor productinteractie

E-mails zoals waarschuwingen voor nieuwe apparaten, uitnodigingen om [lid te worden van een organisatie](#) en [inlogcodes in twee stappen](#) komen van no-reply@bitwarden.com of, als je zelf host, een [geconfigureerd domein](#) zoals no-reply@my.domain.com.

Deze e-mails zullen **nooit bijlagen bevatten**. Als je wordt gevraagd een bestand te downloaden, meld de e-mail dan aan ons.

Sommige van deze e-mails, zoals uitnodigingen voor organisaties, bevatten knoppen. Controleer altijd de geldigheid van de hyperlink **voordat je erop klikt** door te bevestigen dat deze leidt naar <https://vault.bitwarden.com> of het zelf gehoste domein van je organisatie. Als je het domein van je organisatie niet kent, vraag het dan aan een lid van je IT-team of een beheerder.



Join My Organization on
Bitwarden and start securing your
passwords!



Join Organization Now

This invitation expires on **Wednesday, May 3, 2023 2:39 PM UTC**

We're here for you!

If you have any questions, search the Bitwarden
Help site or **contact us**.



© 2023 Bitwarden Inc.

Venster Uitnodiging

E-mails voor betalingen

Geautomatiseerde betalingsmails voor individuele premium en betaalde abonnementen voor organisaties komen van een [@stripe.com](#) adres, zoals [invoice+statements+acct_xxxxxxxxxx@stripe.com](#).

Deze e-mails **bevatten** bijlagen, met name PDF-facturen en ontvangstbewijzen.

Opt-in e-mails

Hoewel u [geautomatiseerde e-mails](#) ontvangt als onderdeel van het dagelijkse gebruik van Bitwarden, kunt u ook e-mails ontvangen van de volgende adressen als u interactie hebt gehad met verschillende onderdelen van het Bitwarden ecosysteem:

- Ondersteuningsverzoeken worden ontvangen van [support@bitwarden.com](#).
- Productaankondigingen worden ontvangen van [productupdates@bitwarden.com](#).

- Informatie over de proef zal worden ontvangen van trial@bitwarden.com.
- Marketingcampagnes worden ontvangen van marketing@bitwarden.com.
- E-mails van leden van het Bitwarden-team worden ontvangen van @bitwarden.com e-mailadressen.

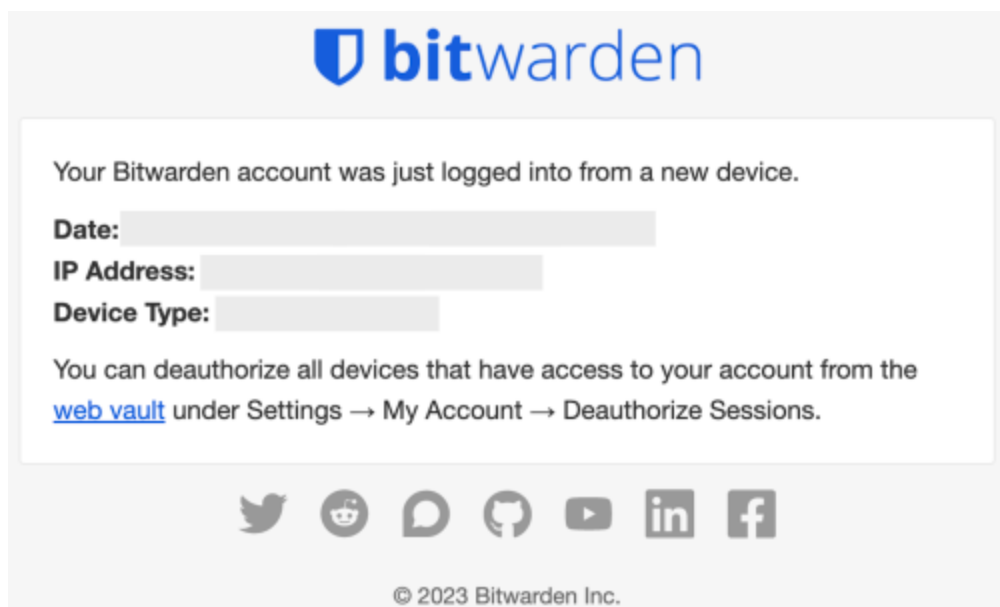
Waarschuwingsmails

Bitwarden stuurt een e-mailwaarschuwing voor verdachte activiteiten zoals inloggen vanaf een onbekend apparaat en mislukte inlogpogingen vanaf een onbekend apparaat.

Deze e-mails zullen **nooit bijlagen bevatten**. Als u wordt gevraagd een bestand te downloaden of op een onbekende koppeling klikt, neem dan contact met ons op.

Nieuw apparaat aangemeld

Als je account succesvol inlogt vanaf een onbekend apparaat, ontvang je een e-mail met informatie over het inloggen.



Inloggen vanaf onbekend apparaat e-mail

De e-mail bevat:

- Datum
- IP-adres
- Type apparaat

Als u deze login niet herkent, kijk dan [hier](#) en neem onmiddellijk maatregelen om uw account te beschermen.

Mislukte aanmeldpogingen gedetecteerd

Als er meerdere mislukte inlogpogingen plaatsvinden op uw account vanaf een onbekend apparaat, stuurt Bitwarden een e-mail om u op de hoogte te stellen van de mislukte inlogpogingen.



Additional security has been placed on your Bitwarden account.

We've detected several failed attempts to log into your Bitwarden account. Future login attempts for your account will be protected by a captcha.

Account: [redacted]

Date: [redacted]

IP Address: [redacted]

If this was you, you can remove the captcha requirement by successfully logging in.

If this was not you, don't worry. The login attempt was not successful and your account has been given additional protection.



E-mail met mislukte aanmeldpogingen

Als veiligheidsmaatregel plaatst Bitwarden CAPTCHA-vereisten op het account. Het ontvangen van deze e-mail betekent niet dat je account is geopend, maar als je deze e-mail niet hebt verwacht, raden we je aan [je hoofdwachtwoord te wijzigen](#). Zie [hier](#) voor meer informatie over brute-force aanvallen en acties die u kunt ondernemen om uw account te beschermen.

Wachtwoord gecompromitteerd met actieve 2FA

Bitwarden detecteert of er meerdere mislukte inlogpogingen zijn geweest tijdens de 2FA-stap. Dit betekent dat de inlogpogingen de juiste gebruikersnaam en hoofdwachtwoord hebben gebruikt, maar dat de verificatie met 2FA is mislukt.



Additional security has been placed on your Bitwarden account.

We've detected several failed attempts to log into your Bitwarden account. Future login attempts for your account will be protected by a captcha.

Account: [redacted]

Date: [redacted]

IP Address: [redacted]

If this was you, you can remove the captcha requirement by successfully logging in. If you're having trouble with two step login, you can login using a [recovery code](#).

If this was not you, you should [change your master password](#) immediately. You can view our tips for selecting a secure master password [here](#).



© 2023 Bitwarden Inc.

Mislukte inlogpogingen met 2FA

Het inschakelen van 2FA op uw Bitwarden account is een belangrijke stap om een extra beveiligingslaag toe te voegen. Als je gebruikersnaam en hoofdwachtwoord gecompromitteerd zijn, kan 2FA nog steeds voorkomen dat een kwaadwillende toegang krijgt tot je account.

Als je deze e-mail ontvangt, volg dan de instructies en [verander je hoofdwachtwoord](#).

Verzoek om vertrouwd apparaat goedgekeurd

Wanneer een verzoek aan een organisatiebeheerder om een [vertrouwd apparaat toe te voegen](#) is goedgekeurd, krijgt de verzoekende gebruiker een e-mail waarin staat dat hij of zij kan blijven inloggen op dat apparaat. **De gebruiker moet binnen 12 uur actie ondernemen door in te loggen op het nieuwe apparaat, anders vervalt de goedkeuring.**

De e-mail bevat:

- Datum
- IP-adres
- Type apparaat