

SICHERHEIT

E-Mails von Bitwarden

Ansicht im Hilfezentrum:

<https://bitwarden.com/help/emails-from-bitwarden/>

E-Mails von Bitwarden

Wie die Verwendung von starken Passwörtern ist das Vermeiden von verdächtigen E-Mails ein wichtiges Werkzeug in Ihrem Online-Sicherheits-Toolkit. Wir empfehlen Ihnen, sich mit diesen [FTC-Richtlinien](#) zum Erkennen und Vermeiden von Phishing vertraut zu machen.

Hier sind einige Richtlinien, die Ihnen helfen können zu bestimmen, ob eine E-Mail-Adresse, die so aussieht, als wäre sie von Bitwarden, legitim ist:

Automatisierte E-Mails

Produktinteraktions-E-Mails

E-Mails wie neue Gerät Warnungen, Einladungen einer [Organisation beizutreten](#) und [Zwei-Schritt-Zugangsdaten-Codes](#) kommen von no-reply@bitwarden.com oder, wenn Sie selbst hosten, einer [konfigurierten Domain](#) wie no-reply@my.domain.com.

Diese E-Mails werden **niemals Anhänge enthalten**. Wenn Sie aufgefordert werden, eine Datei herunterzuladen, melden Sie bitte die E-Mail-Adresse an uns.

Einige dieser E-Mail-Adressen, wie zum Beispiel Einladungen von Organisationen, enthalten Schaltflächen. Überprüfen Sie immer die Gültigkeit des Hyperlinks **bevor Sie darauf klicken**, indem Sie bestätigen, dass er zu <https://vault.bitwarden.com> oder zur selbst gehosteten Domain Ihrer Organisation führt. Wenn Sie die Domain Ihrer Organisation nicht kennen, fragen Sie ein Mitglied Ihres IT-Teams oder einen Administrator.



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.

Einladungsfenster

Zahlungs-E-Mails

Automatisierte Zahlungs-E-Mails für individuelle Premium- und bezahlte Organisation-Abonnements kommen von einer [@stripe.com](mailto:stripe.com) Adresse, wie zum Beispiel invoice+statements+acct_XXXXXXXXXX@stripe.com.

Diese E-Mails **enthalten** Anhänge, insbesondere PDF-Rechnungen und Quittungen.

Opt-in E-Mails

Während Sie im Rahmen der alltäglichen Nutzung von Bitwarden **automatisierte E-Mails** erhalten, könnten Sie auch E-Mails von den folgenden Adressen erhalten, wenn Sie mit verschiedenen Teilen des Bitwarden-Ökosystems interagiert haben:

- Unterstützungsanfragen werden von support@bitwarden.com empfangen.
- Produktankündigungen werden von productupdates@bitwarden.com empfangen.

- Informationen zur Testversion werden von trial@bitwarden.com empfangen.
- Marketingkampagnen werden von marketing@bitwarden.com empfangen.
- E-Mails von Mitgliedern des Bitwarden-Teams werden von @bitwarden.com E-Mail-Adressen empfangen.

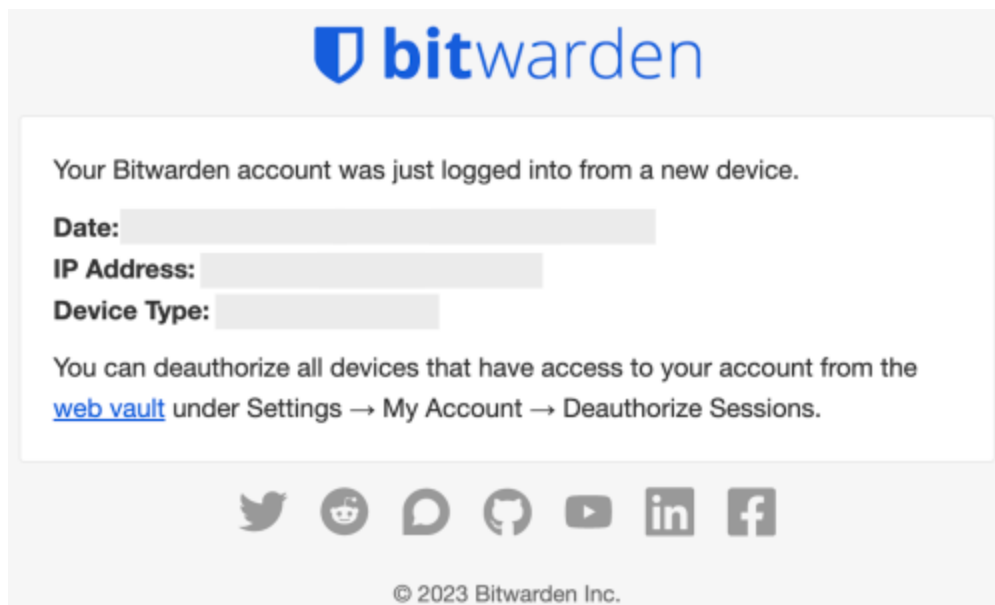
Alarm-E-Mails

Bitwarden wird eine E-Mail-Adresse Alarm für verdächtige Aktivitäten senden, wie zum Beispiel das Anmelden von einem unbekanntem Gerät und fehlgeschlagene Zugangsdaten Versuche von einem unbekanntem Gerät.

Diese E-Mails werden **niemals Anhänge enthalten**. Wenn Sie aufgefordert werden, eine Datei herunterzuladen oder auf einen unbekanntem Link zu klicken, kontaktieren Sie uns bitte.

Neues Gerät angemeldet

Wenn Ihr Konto sich erfolgreich von einem unbekanntem Gerät anmeldet, erhalten Sie eine E-Mail-Adresse mit Informationen über die Zugangsdaten.



Zugangsdaten von unbekanntem Gerät E-Mail-Adresse

Die E-Mail-Adresse wird enthalten:

- Datum
- IP-Adresse
- Gerätetyp

Wenn Sie diese Zugangsdaten nicht erkennen, sehen Sie [hier](#) und ergreifen Sie sofort Maßnahmen, um Ihr Konto zu schützen.

Erkannte fehlgeschlagene Zugangsdaten-Versuche

Wenn mehrere fehlgeschlagene Zugangsdaten-Versuche von einem unbekanntem Gerät auf Ihrem Konto auftreten, wird Bitwarden eine E-Mail senden, um Sie über die fehlgeschlagenen Zugangsdaten-Versuche zu informieren.



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.

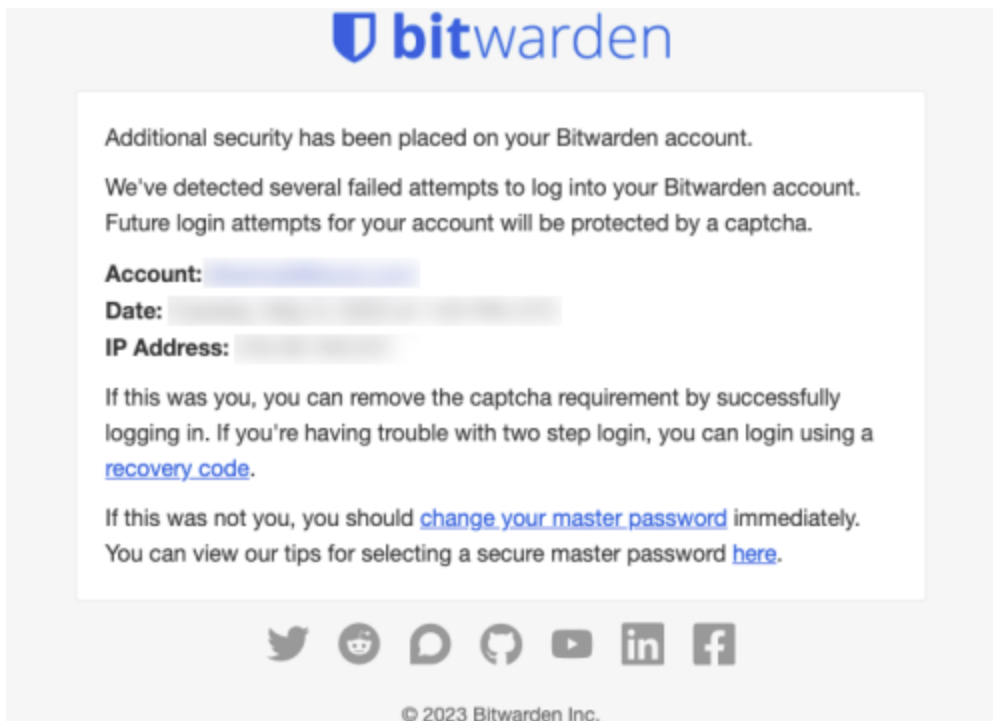


Fehlgeschlagener Zugangsdaten-Versuch E-Mail-Adresse

Als Sicherheitsmaßnahme wird Bitwarden CAPTCHA-Anforderungen auf das Konto setzen. Der Erhalt dieser E-Mail bedeutet nicht, dass auf Ihr Konto zugegriffen wurde, jedoch empfehlen wir, [Ihr Master-Passwort zu ändern](#), wenn Sie diese E-Mail nicht erwartet haben. Für weitere Informationen zu Brute-Force-Angriffen und Maßnahmen, die Sie zum Schutz Ihres Kontos ergreifen können, sehen Sie [hier](#).

Passwort kompromittiert mit aktivem 2FA

Bitwarden wird erkennen, ob während des 2FA-Schritts mehrere fehlgeschlagene Versuche mit den Zugangsdaten aufgetreten sind. Das bedeutet, dass die Zugangsdaten-Versuche den richtigen Benutzernamen und das Master-Passwort verwendet haben, aber die Authentifizierung mit 2FA fehlgeschlagen ist.



Fehlgeschlagene Anmeldeversuche mit 2FA

Das Aktivieren von 2FA auf Ihrem Bitwarden-Konto ist ein wichtiger Schritt, um eine zusätzliche Sicherheitsebene hinzuzufügen. Wenn Ihr Benutzername und Master-Passwort kompromittiert wurden, kann eine aktivierte 2FA immer noch verhindern, dass ein bössartiger Akteur auf Ihr Konto zugreift.

Wenn Sie diese E-Mail-Adresse erhalten, folgen Sie bitte den Anweisungen und [ändern Sie Ihr Master-Passwort](#).

Genehmigung der Anfrage für vertrauenswürdiges Gerät erteilt

Wenn eine Anfrage an einen Administrator einer Organisation, ein [vertrauenswürdiges Gerät hinzuzufügen](#), genehmigt wird, wird dem anfragenden Benutzer eine E-Mail gesendet, die ihn darüber informiert, dass er sich auf diesem Gerät weiter anmelden kann. **Der Benutzer muss innerhalb von 12 Stunden handeln, indem er sich bei dem neuen Gerät anmeldet, sonst läuft die Genehmigung ab.**

Die E-Mail-Adresse wird enthalten:

- Datum
- IP-Adresse
- Gerätetyp