

KONTOEINSTELLUNGEN > ANMELDEN & ENTSPERREN

Login-Schutz für neue Geräte (Februar / März 2025)

Ansicht im Hilfezentrum:
<https://bitwarden.com/help/new-device-verification/>

Login-Schutz für neue Geräte (Februar / März 2025)

Um Ihr Konto sicher zu halten, benötigt Bitwarden ab Februar / März 2025 eine zusätzliche Verifizierung **für Benutzer, die keine zweistufige Anmeldung** verwenden. Nachdem Sie Ihr Bitwarden-Master-Passwort eingegeben haben, werden Sie aufgefordert, einen einmaligen Bestätigungscode einzugeben, der an Ihre Konto-E-Mail gesendet wird, um den Anmeldevorgang abzuschließen, **wenn Sie sich von einem Gerät aus anmelden, bei dem Sie sich zuvor nicht angemeldet haben**. Wenn Sie sich beispielsweise bei einer mobilen App oder einer Browsererweiterung anmelden, die Sie zuvor verwendet haben, erhalten Sie diese Aufforderung nicht.

Die meisten Benutzer werden diese Aufforderung nicht erhalten, es sei denn, sie melden sich häufig bei neuen Geräten an. Diese Überprüfung ist nur für neue Geräte oder nach dem Löschen von Browser-Cookies erforderlich.

Wenn Sie regelmäßig auf Ihre E-Mail zugreifen, sollte das Abrufen des Bestätigungscode einfach sein. Wenn Sie sich zur Verifizierung nicht auf die E-Mail-Adresse Ihres Bitwarden-Kontos verlassen möchten, können Sie eine zweistufige Anmeldung **über eine Authenticator-App**, einen **Hardware Schlüssel** oder eine zweistufige Anmeldung über eine **andere E-Mail-Adresse** einrichten.

Benutzer, die von dieser Änderung betroffen sind, sehen die folgende produktinterne Kommunikation und sollten eine E-Mail erhalten haben, in der sie über die Änderung informiert werden:



Important notice

Bitwarden will send a code to your account email to verify logins from new devices starting in February 2025. [Learn more.](#)

Do you have reliable access to your email, ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ?

- No, I do not
- Yes, I can reliably access my email

Continue

Ankündigung der Verifizierung eines neuen Geräts

Häufig gestellte Fragen

Wann wird dies geschehen?

Diese Änderung tritt ab Februar / März 2025 in Kraft. Diese Seite wird aktualisiert, sobald ein Datum für das Release definiert wurde.

Warum setzt Bitwarden das um?

Bitwarden implementiert diese Änderung, um die Sicherheit für Benutzer zu erhöhen, die keine [zweistufige Anmeldung](#) aktiviert haben. Wenn jemand Zugriff auf dein Passwort erhält, kann er sich ohne sekundäre Verifizierung (den an deine E-Mail-Adresse gesendeten Code) immer noch nicht in dein Konto einloggen. Diese zusätzliche Ebene schützt deine Daten vor Hackern, die oft auf schwache oder exponierte Passwörter abzielen, um unbefugten Zugriff zu erhalten.

Wann werde ich zu dieser Verifizierung aufgefordert?

Sie werden nur dann zu dieser Verifizierung aufgefordert, wenn Sie sich von neuen Geräten aus anmelden. Wenn Sie sich bei einem Gerät anmelden, das Sie zuvor verwendet haben, werden Sie nicht dazu aufgefordert.

Was gilt als neues Gerät?

Ein neues Gerät ist jedes Gerät, mit dem Sie sich bisher nicht bei Ihrem Bitwarden-Konto angemeldet haben. Dies kann ein neues Telefon, Tablet, Computer oder eine Browsererweiterung sein, von der aus du dich noch nie angemeldet hast. Wenn du dich von einem neuen Gerät aus anmeldest, wirst du aufgefordert, deine Identität mit einem einmaligen Code zu verifizieren, der an deine E-Mail-Adresse gesendet wird.

Andere Szenarien, die ein neues Gerät initiieren, sind:

- Durch die Deinstallation und Neuinstallation des Mobilgeräts, der Desktop-App oder der Browsererweiterung wird ein neues Gerät initiiert.
- Durch das Löschen von Browser-Cookies wird ein neues Gerät für die Web-App initiiert, nicht jedoch für Browser-Erweiterungen.

Meine E-Mail-Anmeldeinformationen werden in Bitwarden gespeichert. Werde ich aus Bitwarden ausgesperrt?

E-Mail-Verifizierungs-codes werden nur auf neuen Geräten für Benutzer benötigt, die keine zweistufige Anmeldung aktiviert haben. Diese Eingabeaufforderung wird auf zuvor angemeldeten Geräten nicht angezeigt, und Sie melden sich wie gewohnt mit Ihrer Konto-E-Mail-Adresse und Ihrem Master-Passwort an.

Wenn Sie sich bei einem neuen Gerät anmelden, erhält Ihre Bitwarden-Konto-E-Mail einen einmaligen Bestätigungscode. Wenn Sie Zugriff auf Ihre E-Mail haben, d. h. eine dauerhaft angemeldete E-Mail auf Ihrem Mobiltelefon, können Sie den einmaligen Bestätigungscode abrufen, um sich anzumelden. Sobald Sie sich am neuen Gerät angemeldet haben, werden Sie nicht erneut nach dem Bestätigungscode gefragt.

Wenn Sie sich regelmäßig mit in Bitwarden gespeicherten Anmeldeinformationen in Ihre E-Mail einloggen oder sich nicht auf Ihre E-Mail zur Verifizierung verlassen möchten, sollten Sie eine zweistufige Anmeldung einrichten, die von der Bitwarden-Konto-E-Mail unabhängig ist. Dazu gehören eine Authentifizierungs-App, ein Sicherheitsschlüssel oder eine E-Mail-basierte zweistufige Anmeldung mit einer anderen E-Mail. Wenn eine 2FA-Methode aktiviert ist, wird der Benutzer von der E-Mail-basierten Verifizierung neuer Geräte ausgeschlossen. Benutzer mit 2FA aktiv sollten auch ihren [Bitwarden-Wiederherstellungscodes](#) an einem sicheren Ort aufbewahren.

Wer ist von der E-Mail-basierten Verifizierung neuer Geräte für dieses Konto ausgeschlossen?

Folgende Kategorien von Logins sind ausgeschlossen:

- Benutzer, die eine [zweistufige Anmeldung](#) eingerichtet haben, sind ausgeschlossen.
- Benutzer, die sich mit SSO, einem Passkey oder mit einem API-Schlüssel anmelden, sind ausgeschlossen.

- Selbst gehostete Nutzer sind ausgeschlossen.
- Benutzer, die sich von einem Gerät aus anmelden, auf dem sie sich zuvor angemeldet haben, sind ausgeschlossen.
- Benutzer, die sich von ihrem Bildschirm **Einstellungen** → **Mein Konto** abmelden, sind ausgeschlossen (**Nicht empfohlen**).

Meine Organisation verwendet SSO. Müssen meine Benutzer die Überprüfung neuer Geräte abschließen?

Nein. Benutzer, die sich mit SSO anmelden, werden befreit und nicht aufgefordert, die Anmeldung auf einem neuen Gerät zu bestätigen. Wenn sich ein Benutzer jedoch ohne aktivierte zweistufige Anmeldung mit einem Benutzernamen und einem Passwort anmeldet, ohne SSO zu durchlaufen, wird er aufgefordert, das neue Gerät zu überprüfen.

Ich möchte meine echte E-Mail nicht mit Bitwarden teilen, wie kann ich mein Konto einrichten?

Benutzer, die anonym bleiben möchten, haben mehrere Möglichkeiten:

- Verwenden Sie eine [zweistufige](#) Anmeldeoption, für die keine E-Mail erforderlich ist, einschließlich einer Authentifizierungs-App, eines Sicherheitsschlüssels oder einer E-Mail-basierten zweistufigen Anmeldung mit einer anderen E-Mail.
- Verwenden Sie einen E-Mail-Alias-Weiterleitungsdienst.
- Bitwarden als Selfhost.

Bitwarden ermutigt Benutzer, eine aktive E-Mail zu haben, da Bitwarden wichtige Sicherheitswarnungen wie fehlgeschlagene Anmeldeversuche sendet.

Wenn ich den 2FA-Wiederherstellungscodes auf einem neuen Gerät verwende, weil ich meinen 2FA-Zugriff verloren habe, werde ich dann immer noch dieser neuen Geräteverifizierung unterzogen?

Bitwarden aktualisiert den Ablauf des Wiederherstellungscodes, sodass Sie bei der Übermittlung Ihres Passworts und Ihres Wiederherstellungscodes in der Web-App angemeldet und zu Ihren 2FA-Einstellungen weitergeleitet werden. Wenn Sie befürchten, gesperrt zu werden, sollten Sie diesen Ablauf **nicht** in einem Inkognito-Browser oder auf einem Gerät mit unzuverlässiger Internetverbindung durchführen, um sicherzustellen, dass Sie alle erforderlichen Einrichtungsschritte in dieser angemeldeten Sitzung durchführen können.

Ich möchte mich abmelden! Gibt es eine Option dazu?

Dies bietet zusätzliche Sicherheit für Benutzer, die keine zweistufige Anmeldung aktiviert haben. Benutzer, die keine zweistufige Anmeldung aktiviert haben, sind anfälliger für unbefugten Zugriff durch Angreifer, da Passwörter auf vielfältige Weise kompromittiert werden können, auch wenn sie stark und eindeutig sind. Zu den gängigen Methoden gehören beispielsweise:

- **Phishing-Angriffe:** Cyberkriminelle verwenden irreführende E-Mails oder Websites, um Sie dazu zu bringen, Ihr Passwort preiszugeben.
- **Social Engineering:** Angreifer können versuchen, Sie zu manipulieren oder zu täuschen, um Ihr Passwort durch Telefonanrufe, Texte oder andere Mittel preiszugeben.
- **Passwort-Cracking durch Brute-Force-Angriffe:** Angreifer verwenden automatisierte Tools, um wiederholt zu versuchen, das Passwort zu erraten.
- **Keylogging oder Malware:** Wenn Ihr Gerät mit Malware oder einem Keylogger infiziert ist, können Angreifer jeden Tastendruck – einschließlich Ihres Passworts – ohne Ihr Wissen aufzeichnen.

Selbst wenn Ihr Passwort durch eine der oben genannten Methoden kompromittiert wird, muss der Angreifer bei der Verifizierung eines neuen Geräts immer noch die zweite Verifizierung abrufen, bei der es sich um den einmaligen Code in Ihrer E-Mail handelt. Dies reduziert

die Wahrscheinlichkeit eines unbefugten Zugriffs erheblich.

Die Überprüfung neuer Geräte ist so konzipiert, dass sie weniger aufdringlich ist als die herkömmliche zweistufige Anmeldung. Dies gilt nur, wenn Sie sich von einem Gerät oder Client aus anmelden, das Sie noch nicht verwendet haben. Daher werden die meisten Benutzer diesen zusätzlichen Schritt nicht erleben, da sie sich regelmäßig auf ihren Alltagsgeräten anmelden. Der Verifizierungsprozess verwendet Ihre E-Mail, die viele Leute auf einem Telefon oder Computer offen halten, so dass das Abrufen des Codes schnell und einfach ist.

Benutzer, bei denen einige Herausforderungen auftreten können, tun Folgendes:

- Keine zweistufige Anmeldung aktiviert.
- Speichern Sie ihr E-Mail-Passwort in Bitwarden.
- Deinstallieren und installieren Sie Bitwarden ständig neu.
- Melden Sie sich überall von ihren E-Mails ab.

Nur Benutzer, die all diese Dinge tun und die oben genannten Bedingungen erfüllen, werden mit diesem Sicherheitsupdate Probleme haben. Wenn Benutzer von ihrem Konto ausgeschlossen werden, können sie sich an Customer Success bei Bitwarden wenden.

Wenn Benutzer keine Überprüfung eines neuen Geräts wünschen, wird dringend empfohlen, eine alternative zweistufige Anmeldemethode zu aktivieren (entweder über eine Authentifizierungs-App, einen Hardware Schlüssel oder eine andere E-Mail), um dein Konto zu schützen.

Wenn Benutzer keine Überprüfung des neuen Geräts wünschen, keine alternative zweistufige Anmeldemethode einrichten möchten und **keine Sicherheit für ihr Konto wünschen**, gibt es eine Option zum Abmelden, indem Sie zum Bildschirm **Einstellungen** → **Mein Konto** navigieren und zum Abschnitt Gefahrenzone scrollen. Wir müssen betonen, dass dies **dringend nicht empfohlen** wird, da es dein Konto anfällig für verschiedene Angriffe macht.