



Microsoft
Office 365

Informationen zur

Multi-Faktor-Authentifizierung

Mit der Einführung von Microsoft Office 365 müssen wir die Multi-Faktor-Authentifizierung nutzen. Was eine Multi-Faktor-Authentifizierung ist und was mit ihr einhergeht, erfahren Sie hier.

Was ist eine Multi-Faktor Authentifizierung?

Die Multi-Faktor-Authentifizierung ist ein Sicherheitsverfahren, das den Zugriff auf Systeme und Daten besser schützt. **Statt sich nur mit einem Passwort anzumelden, wird ein zusätzlicher Faktor benötigt.** In der MUL-CT nutzen wir als zusätzlichen Faktor die Authentifizierung mittels **Microsoft Authenticator-App**.

Warum ist die Multi-Faktor-Authentifizierung wichtig?

In **52%** der Fälle von Cyberkriminalität versuchten die Angreifer über Phishing, persönliche Informationen wie Passwörter herauszubekommen¹⁾

Durch die Kombination mehrerer Faktoren bei der Anmeldung an Ihrem Microsoft-Konto wird die **Sicherheit** von sensiblen Daten deutlich erhöht. Das heißt, dass selbst wenn ein Hacker Ihr Passwort stiehlt, hat er nicht genug Informationen, um sich unbefugten Zugriff auf Ihre Microsoft-Daten zu verschaffen. Er würde immer noch den zweiten Faktor über die **Microsoft Authenticator-App** benötigen. Da wir in der MUL-CT mit sehr vielen sensiblen Daten arbeiten, ist für die Nutzung von Microsoft Office 365 die **Verwendung der Multi-Faktor-Authentifizierung Pflicht**. Ohne Multi-Faktor-Authentifizierung können Sie also die vielen neuen Funktionen von Microsoft Office 365 leider nicht nutzen.

Was bedeutet das für mich und meinen Arbeitsalltag?

Wenn Sie sich erstmals auf einem **neuen Gerät** bei Ihrem Microsoft-Konto anmelden oder, aus Sicherheitsgründen, **alle 24 Tage** auch auf bereits genutzten Geräten, benötigen Sie zusätzlich die Microsoft Authenticator-App, um Ihre Identität zu bestätigen.

Die Nutzung Ihres privaten Smartphones dafür ist lediglich eine Übergangslösung. An einer langfristigen Lösung arbeiten wir bereits. Auf den nächsten Seiten erfahren Sie, wie Sie die Multi-Faktor-Authentifizierung ganz einfach auf Ihrem Smartphone einrichten können.



Die Microsoft Authenticator-App speichert **keine Unternehmensdaten** auf Ihrem Gerät. Darüber hinaus hat sie **keinen Zugriff auf Ihre privaten Inhalte**, wie Fotos, Nachrichten oder Passwörter. Die App dient ausschließlich zur Bestätigung Ihrer Identität.



Sie wollen mehr über die Multi-Faktor-Authentifizierung erfahren? Dann schauen Sie gern bei den „**Häufig gestellten Fragen (FAQ)**“ vorbei.

Phishing: Täuschungsversuche, sich über gefälschte Webseiten, E-Mails oder Kurznachrichten als vertrauenswürdiger Kommunikationspartner in einer elektronischen Kommunikation auszugeben.

¹⁾ Bitkom e.V. (2024), Bilanz Cyberkriminalität 2023: 7 von 10 Internetnutzern betroffen, <https://www.bitkom.org/Presse/Presseinformation/Bilanz-Cyberkriminalitaet-7-von-10-betroffen>, zuletzt abgerufen am 23.12.2025

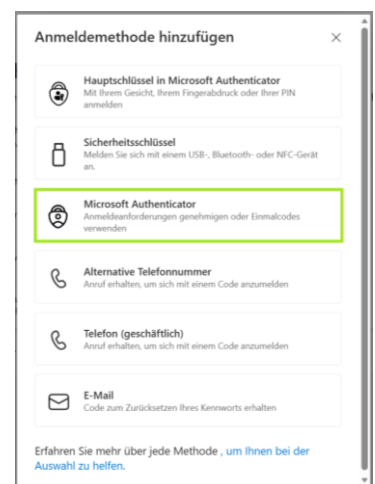
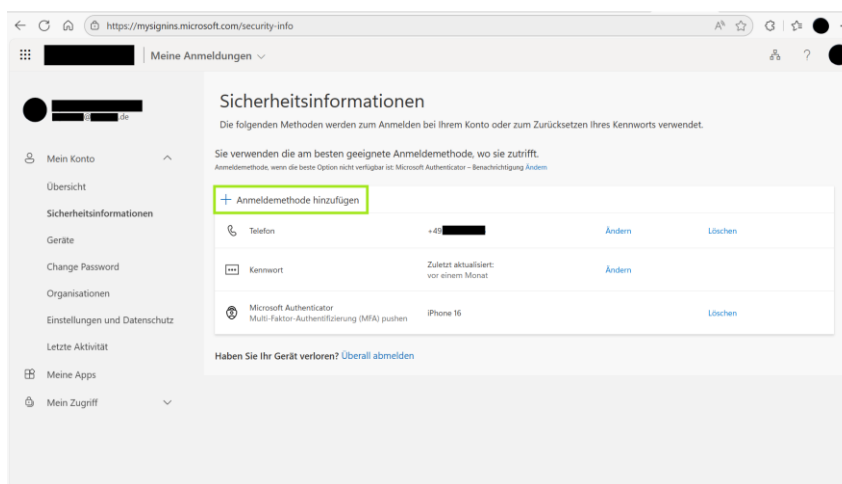


Microsoft
Office 365

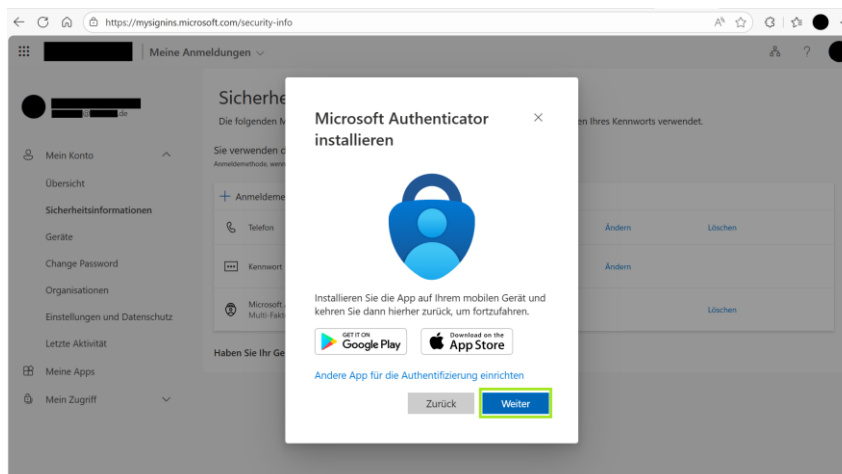
Anleitung zur Einrichtung der *Multi-Faktor-Authentifizierung*

Um die dienstlich bereitgestellten Microsoft-Anwendungen nutzen zu können, müssen Sie für einen höheren Datensicherheit zunächst die Multi Faktor-Authentifizierung einrichten. Hier erfahren Sie, wie das geht.

1. Installieren Sie die **Microsoft Authenticator-App** gratis aus dem Apple App Store oder aus dem Google Play Store auf Ihrem Smartphone.
2. Melden Sie sich mit Ihrem Computer auf der **Sicherheitsinformationsseite** Ihres Microsoft-Kontos an: <https://mysignins.microsoft.com/security-info>.
3. Klicken Sie auf „**+ Anmeldemethode hinzufügen**“ und wählen Sie „**Microsoft Authenticator**“ in dem Menü, welches erscheint.



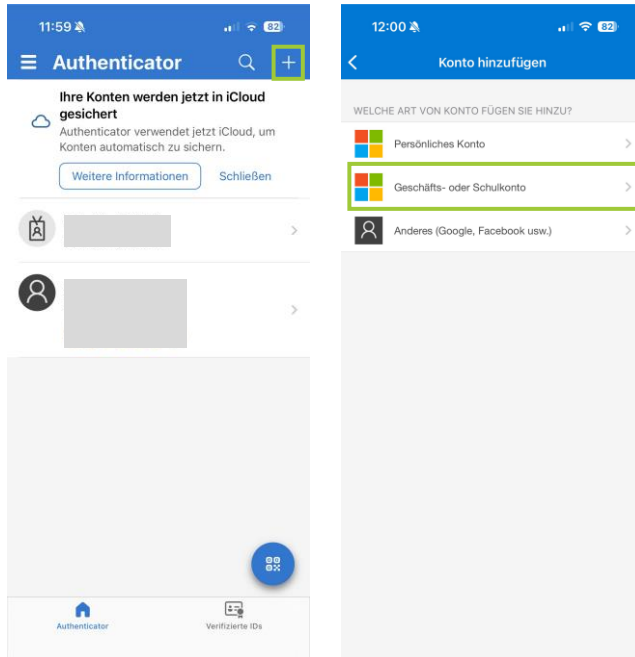
4. Wenn Sie die Authenticator-App bereits installiert haben, klicken Sie auf „**Weiter**“. Nun wird Ihnen ein QR-Code angezeigt.



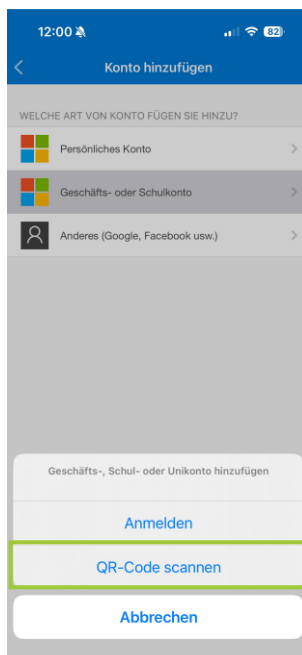


Microsoft
Office 365

5. Öffnen Sie als nächstes die **Microsoft Authenticator-App** auf Ihrem Smartphone und klicken Sie auf das „+“ rechts oben in der Ecke. Wählen Sie **„Geschäfts- oder Schulkonto“**.



6. Klicken Sie dann **„QR-Code scannen“** und scannen Sie den auf Ihrem Computer angezeigten QR-Code ein.





Microsoft
Office 365

7. Nach der erfolgreichen Einrichtung startet ein Test:
Auf Ihrem Computer wird eine **Zahl angezeigt**, die
Sie in der Authenticator-App **auf Ihrem
Smartphone eingeben** müssen.

MUL-CT

Schützen Sie Ihr Konto

Microsoft Authenticator

Probieren wir es aus

Genehmigen Sie die Benachrichtigung, die wir an Ihre App senden, indem Sie die untenstehende Nummer eingeben.

24

Zurück Weiter

[Ich möchte eine andere Methode einrichten.](#)

MUL-CT

Schützen Sie Ihr Konto

Microsoft Authenticator

Benachrichtigung genehmigt

Weiter

[Ich möchte eine andere Methode einrichten.](#)

8. Im letzten Schritt wählen Sie **„Ja, Verwaltung meines Geräts durch meine Organisation zulassen“** und klicken Sie auf **„Ja, alle Apps“**. Damit ist die Einrichtung der Multi-Faktor Authentifizierung abgeschlossen.

Melden Sie sich automatisch bei allen Desktop-Apps und Websites auf diesem Gerät an?

Wenn Sie **Ja, alle Apps** auswählen, geschieht Folgendes:

- Erlauben Sie uns, Ihr Geschäfts-, Schul- oder Unikonto zu verwenden, um Sie bei anderen Desktop-Apps und Websites anzumelden, die Sie auf diesem Gerät verwenden.
- Registrieren Sie dieses Gerät bei Ihrer Organisation, sodass Ihre Organisation Geräteinformationen wie den Namen des Geräts anzeigen kann.

Handelt es sich um ein gemeinsam mit anderen genutztes Gerät? Wenn dies der Fall ist, sollten Sie sich nur bei dieser App anmelden.

Ihre Organisation muss dieses Gerät außerdem verwalten, um auf einige Unternehmensressourcen zuzugreifen. Wenn Sie dies zulassen, kann Ihre IT-Abteilung verschiedene Vorgänge remote ausführen, z. B. das Steuern von Einstellungen, das Installieren von Apps und das Zurücksetzen dieses Geräts.

☐ Verwaltung meines Geräts durch meine Organisation zulassen

[Weitere Informationen](#)

Ja, alle Apps Nein, nur diese App