

# Mehr Sicherheit für Dein Kundenkonto – Multi-Faktor-Authentifizierung

Multi-Faktor-Authentifizierung (MFA) ist ein Sicherheitsverfahren, das sicherstellt, dass nur berechtigte Personen auf das Kundenkonto zugreifen können. MFA überprüft mehrere unabhängige Merkmale (Faktoren), um die Identität des Nutzers zu bestätigen.

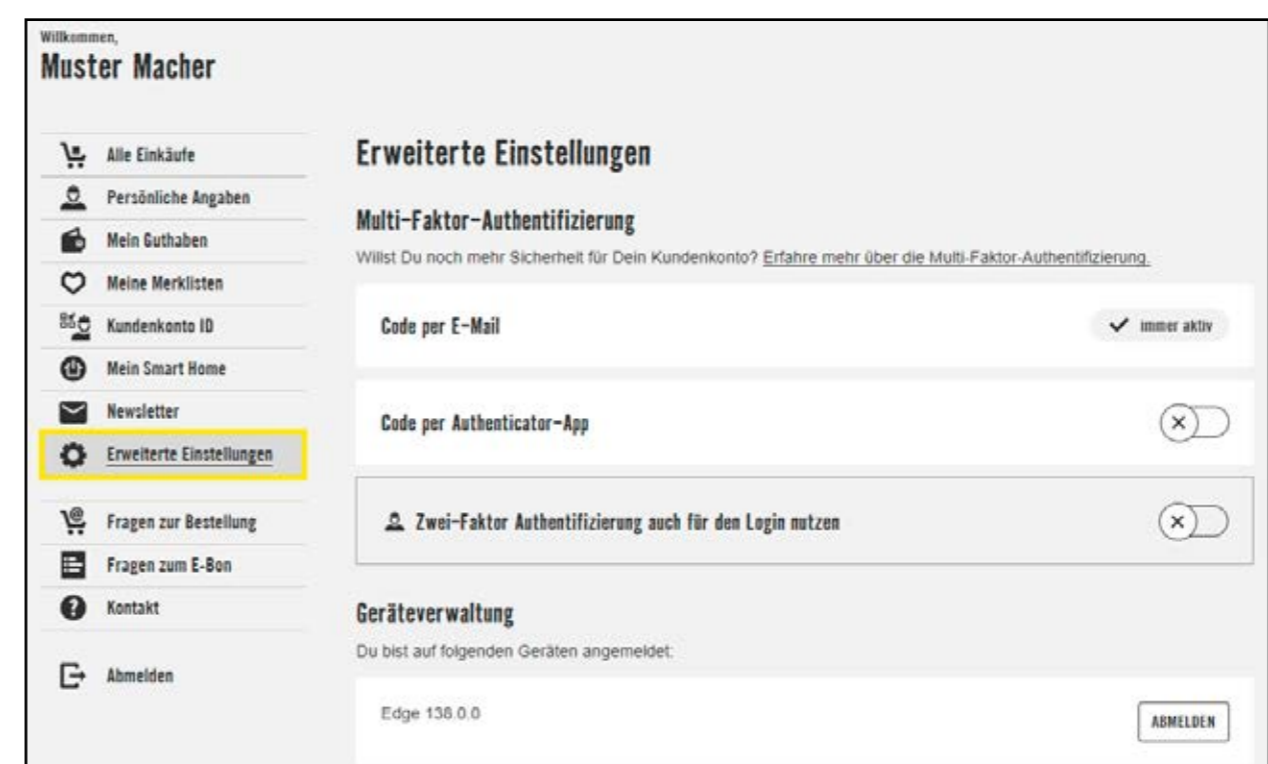
## Anleitung QR-Code mit Authenticator-App

1. Logge Dich in Deinem Kundenkonto ein.
2. Öffne den Bereich „Erweiterte Einstellungen“. (1)
3. Klicke auf den Schieberegler „Code per Authenticator-App“.
4. Nach dem Aktivieren öffnet sich ein neues Fenster (2).
5. Scanne den angezeigten QR-Code mit einer Authenticator-App (z. B. Microsoft Authenticator). Alternativ kannst Du den darunter angezeigten Schlüssel manuell in der Authenticator-App eingeben.
6. Öffne die Authenticator-App und kopiere das dort angezeigte einmalige Passwort (OTP). Achtung, dieses erneuert sich alle 30 Sek.
7. Gib dieses Passwort im entsprechenden Feld im Kundenkonto ein. (2)
8. Klicke auf „MIT KUNDENKONTO VERKNÜPFEN“.
9. Um die Authenticator-App als zusätzliche Sicherheit für den Login zu aktivieren, klicke auf den Schieberegler „Zwei-Faktor-Authentifizierung auch für den Login nutzen“.

Nachdem Du alle Schritte erfolgreich durchgeführt hast, ist die zusätzliche Sicherheitsabfrage hinterlegt.

Beim nächsten Login kannst Du die Authenticator App als zusätzlichen Faktor zur Anmeldung nutzen.

Stell Dir vor, Du möchtest Geld von einem Geldautomaten abheben. Du brauchst dafür Deine Bankkarte (Besitz) und Deine PIN (Wissen). Das ist ein Beispiel für Zwei-Faktor-Authentifizierung, eine Art der Multi-Faktor-Authentifizierung.



(1) Einstellungen im Kundenkonto



(2) Neues Fenster mit QR-Code