MAIL BOXES ETC.®

#PeoplePossible

MBE OnLine

Sicherheitsupdate

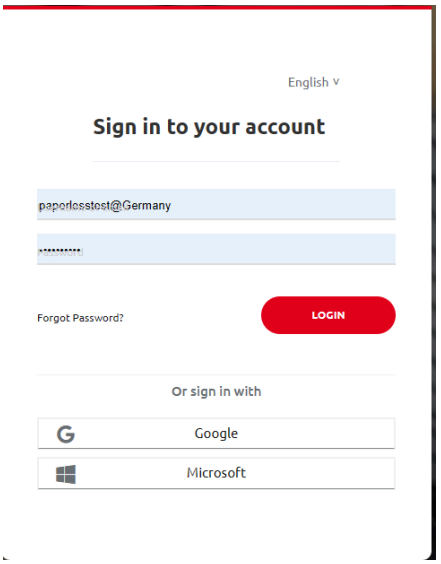
Index

1. Einführung

Moderne Diebstähle haben kaum noch Ähnlichkeit mit Raubüberfällen und Einbrüchen der Vergangenheit. Sie finden mittlerweile im digitalen Bereich statt und erfordern von uns, dass wir uns neben den alten auch neue Sicherheitspraktiken aneignen.

Aus diesem Grund ist ein Update des MBE OnLine-Logins vorgesehen, das neue Sicherheitsfunktionen enthält.

Hierzu gehört eine Aktualisierung des Benutzernamens, ein Zwei-Faktor-Authentifizierungsprozess und die Möglichkeit, sich mit Ihrem Google- oder Microsoft-Konto anzumelden.

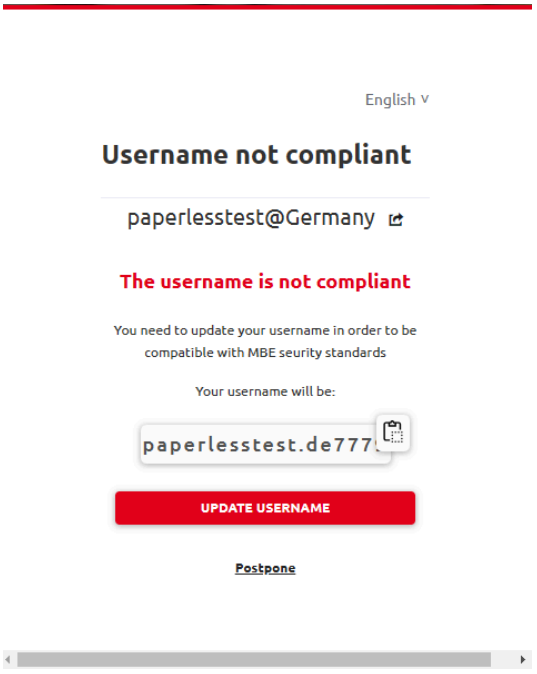


2. Update des Benutzernamens

Wenn Sie versuchen, sich bei Ihrem MBE OnLine-Konto anzumelden, erhalten Sie eine Benachrichtigung, dass Ihr Benutzername nicht kompatibel ist.

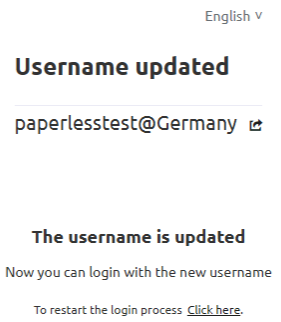
Das bedeutet, dass Ihr Benutzername aktualisiert werden muss, damit er mit den neuen MBE-Sicherheitsstandards kompatibel ist. Unten sehen Sie, wie Ihr neuer Benutzername lautet.

Sie haben auch die Möglichkeit, Ihren neuen Benutzernamen zu kopieren, indem Sie auf das Kopiersymbol neben dem neuen Benutzernamen klicken. Nachdem Sie ihn kopiert haben, klicken Sie auf **BENUTZERNAME AKTUALISIEREN** und Ihr Benutzername wird aktualisiert.



Sie haben auch die Möglichkeit, dieses Update zu verschieben, indem Sie auf **VERSCHIEBEN** klicken. Bedenken Sie, dass Ihr Konto dadurch nicht mehr den neuesten Sicherheitsstandards entspricht.

Sobald Sie auf **BENUTZERNAME AKTUALISIEREN** klicken, erhalten Sie eine Benachrichtigung, dass der Benutzername aktualisiert wurde und Sie sich jetzt anmelden können. Klicken Sie auf **„Hier klicken“,** um sich mit Ihrem neuen Benutzernamen, aber demselben Passwort anzumelden.



Hinweis: Angenommen, Ihr alter Benutzername war design2000@Germany und Sie haben mit der MBE-Center-Nummer DE0001 zu tun.

Ihr neuer Benutzername lautet dann: design2000**.de0001**@Germany.

3. Zwei-Faktor-Authentifizierung

Zwei-Faktor-Authentifizierung (2FA) ist ein Sicherheitsvorgang, bei dem Benutzer zwei unterschiedliche Formen der Identifizierung vorweisen müssen, bevor sie Zugriff auf ein System, eine Anwendung oder ein Konto erhalten. Es fügt eine zusätzliche Schutzebene hinzu, die über einen Benutzernamen und ein Passwort hinausgeht, und erschwert unbefugten Benutzern den Zugriff auf vertrauliche Informationen erheblich.

Vorteile der Zwei-Faktoren-Authentifizierung

1. **Erhöhte Sicherheit**: 2FA verringert das Risiko eines unbefugten Zugriffs erheblich, denn selbst wenn jemand dein Passwort gestohlen hat, kann er ohne den zweiten Faktor nicht auf dein Konto zugreifen.
2. **Schutz vor Phishing**: Selbst wenn ein Passwort durch Phishing kompromittiert wird, benötigt der Angreifer immer noch den zweiten Faktor, um Zugriff zu erhalten.
3. **Reduziertes Risiko eines Identitätsdiebstahls**: Durch Hinzufügen einer zusätzlichen Sicherheitsebene hilft 2FA, Identitätsdiebstahl und nicht autorisierte Transaktionen zu verhindern.
4. **Einhaltung von Vorschriften**: In vielen Branchen ist 2FA erforderlich, um gesetzliche Standards zum Schutz vertraulicher Daten zu erfüllen, beispielsweise im Bank-, Gesundheits- und Regierungssektor.

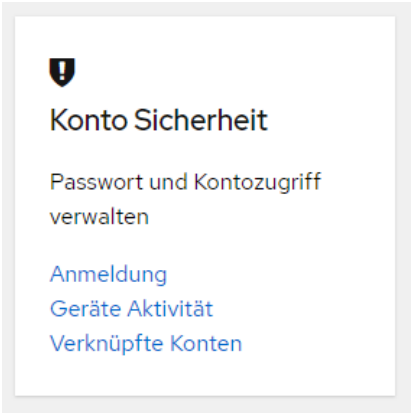
Arten der Zwei-Faktor-Authentifizierung

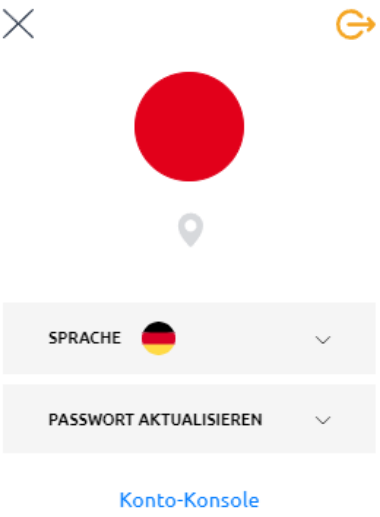
4. **Authenticator Apps**: Apps wie Google Authenticator generieren zeitbasierte Einmalkennwörter (TOTP), die der Benutzer zur Bestätigung seiner Identität eingibt.
5. **E-Mail-basierte Authentifizierung**: Ein Verifizierungscode wird an die registrierte E-Mail-Adresse des Nutzers/der Nutzerin geschickt.

Um die Zwei-Faktor-Authentifizierung zu aktivieren, gehen Sie zu Ihrem Profil und klicken Sie dann auf „Kontokonsole“.

Ein neues Fenster wird geöffnet. Hier können Sie Ihre 2FA aktivieren.

Klicken Sie unter Kontosicherheit auf **Anmelden**

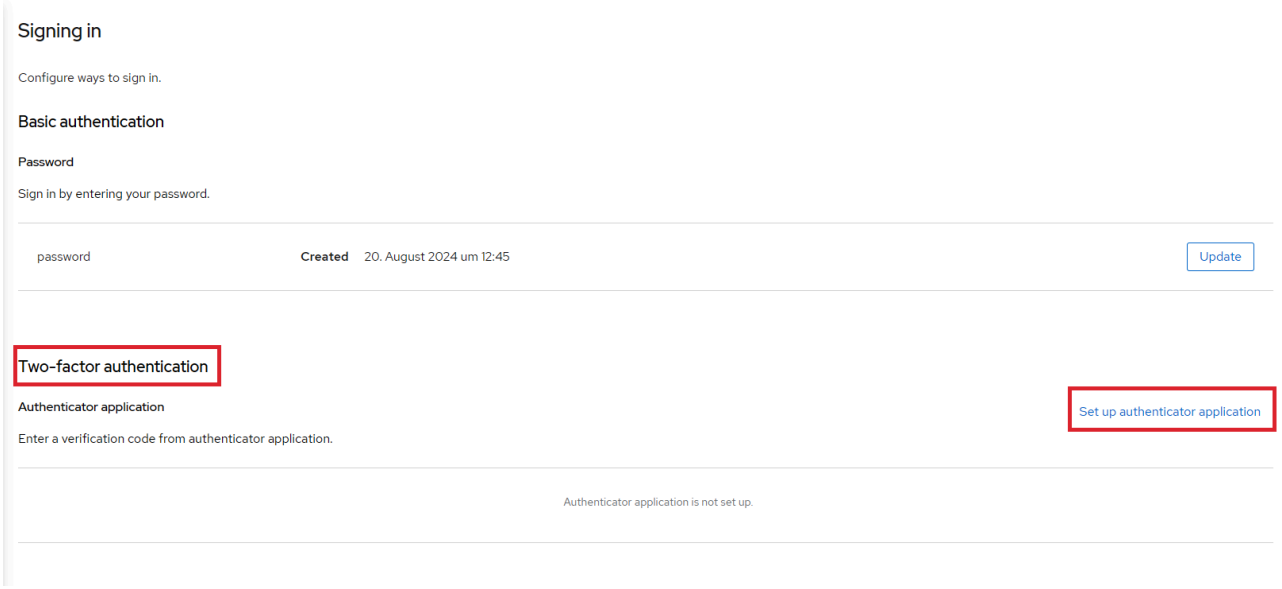




Hier können Sie sehen, wie Sie sich angemeldet haben.

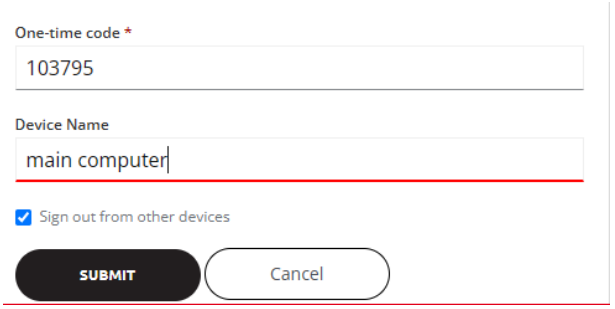
Momentan ist bei Ihnen nur die Basic-Authentifizierung aktiv.

Um die Zwei-Faktor-Authentifizierung zu aktivieren, klicken Sie auf **Authentifikator-Anwendung einrichten**.



Ein neues Fenster wird geöffnet. Es sind 3 Schritte zu befolgen:

1. Installieren Sie eine der folgenden Anwendungen auf Ihrem Mobiltelefon:
    a. Microsoft Authenticator
    b. Google Authenticator
    c. FreeOTP
2. Öffnen Sie die Anwendung und scannen Sie den Barcode:
3. Geben Sie den von der Anwendung bereitgestellten Einmalcode ein und klicken Sie auf „Senden“, um die Einrichtung abzuschließen. Geben Sie einen Gerätenamen an, der Ihnen die Verwaltung Ihrer OTP-Geräte erleichtert.



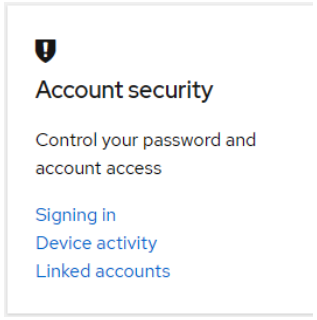
Bitte geben Sie unbedingt einen Namen für Ihr Gerät ein. Die Eingabe von „Test“ oder „123456“ führt zu einem Neustart der Authentifizierung.

Einmal klicken auf **EINREICHEN.** Jetzt sehen Sie, dass die Zwei-Faktor-Authentifizierung aktiv ist und der von Ihnen angegebene Gerätename angezeigt wird.

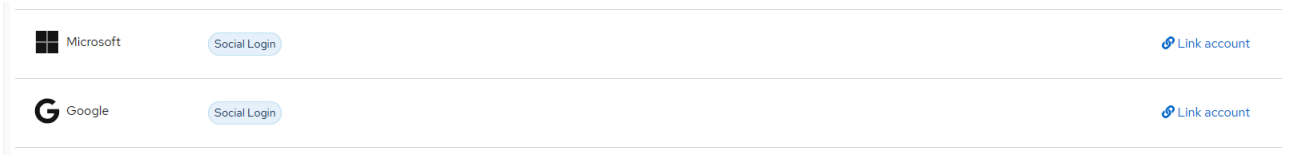
Sie können diese Authentifizierung jederzeit deaktivieren, indem Sie auf **Entfernen**. klicken.

4. Social Login

Unter „Verknüpfte Konten“ haben Sie die Möglichkeit, Ihr Microsoft- oder Google-Konto mit Ihrem MBE OnLine-Konto zu verknüpfen. Dies bedeutet, dass Sie sich anstelle von Benutzername und Kennwort entweder mit Ihrem Microsoft- oder Gmail-Konto anmelden können.



Wenn Sie diese Option aktivieren möchten, klicken Sie auf **Konto verknüpfen.**

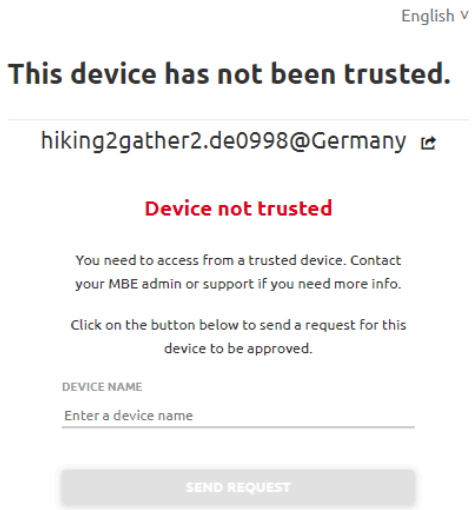


Wenn Sie Google wählen, müssen Sie Ihre Google-E-Mail-Adresse angeben und sich damit anmelden.

Bitte achten Sie darauf, dies nicht zu aktivieren, wenn Sie einen gemeinsam genutzten Computer verwenden, da jeder, der Zugriff auf den Computer hat, dann Zugriff auf Ihr Google-Konto und Ihr MBE OnLine-Konto hat.

5. Vertrauenswürdiges Gerät

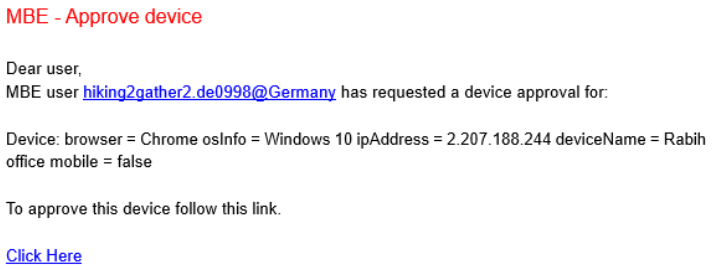
Wie bei vielen anderen Online-Diensten haben Sie die Möglichkeit, bestimmte Geräte, etwa einen Computer oder ein Tablet, zu einer vertrauenswürdigen Liste hinzuzufügen, sodass die Anmeldung von einem anderen Gerät aus genehmigt werden muss. Wenn Sie diesen Dienst aktivieren möchten, müssen Sie sich an Ihr MBE-Center wenden, das ihn dann für Sie aktiviert.



Sobald dies aktiviert ist und Sie versuchen, sich anzumelden, wird eine Seite angezeigt, die darauf hinweist, dass das Gerät nicht vertrauenswürdig ist.

Sie müssen diesem Gerät einen Namen geben und dann auf „Anfrage senden“ klicken. Geben Sie Ihrem Gerät einen Namen, mit dem Sie es leicht identifizieren können.

Sie erhalten dann eine E-Mail. In der E-Mail finden Sie den MBE-Benutzernamen mit dem Computerbetriebssystem, der IP-Adresse und dem Gerätenamen.


MBE - Approve device

Dear user,
MBE user hiking2gather2.de0998@Germany has requested a device approval for:

Device: browser = Chrome osInfo = Windows 10 ipAddress = 2.207.188.244 deviceName = Rabih office mobile = false

To approve this device follow this link.

Click Here

Wenn alles legitim zu sein scheint, klicken Sie auf **„Hier klicken“,** um die Berechtigung zu erteilen und dem neuen Gerät zu vertrauen.

Versuchen Sie dann, sich erneut anzumelden, und es wird funktionieren.

Wenn eine der folgenden Angaben geändert wird, müssen Sie den Prozess für das neue vertrauenswürdige Gerät erneut durchlaufen:

- Browser
- Betriebssystem
- IP-Adresse
- Arbeitsstation

Beispiel: Angenommen, Sie verwenden in Ihrem Büro ein Windows-Tablet, haben den Vorgang durchlaufen und Ihr Tablet gilt nun als vertrauenswürdig. Wenn Sie das Tablet eines Tages mit nach Hause nehmen, erhält es mit Sicherheit eine neue IP-Adresse und wird automatisch zu einem nicht vertrauenswürdigen Gerät.