

Zwei Faktor Authentifizierung

Was ist die Zwei-Faktor-Authentifizierung?

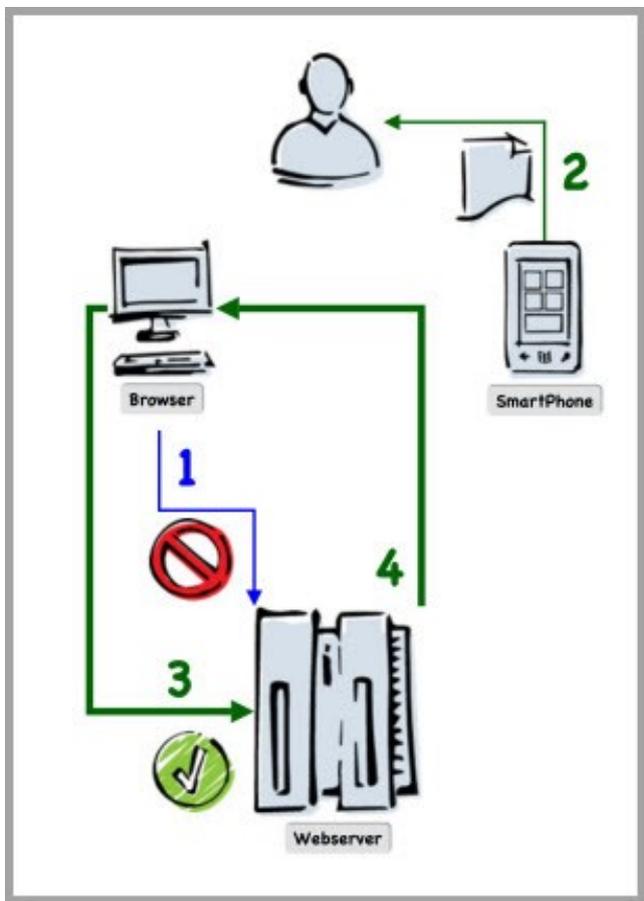
Bei der Zwei-Faktor-Authentifizierung geschieht folgendes: Sie geben wie gewohnt Name und Passwort ein, um sich anzumelden.

Anschliessend fragt Sie der Online-Dienst nach einer – meist sechsstelligen – PIN.

Diese bekommen Sie auf das zu diesem Zweck angemeldete Handy als SMS oder generieren sie via Gratis-App auf Ihrem Smartphone oder Tablet-PC selbst.

Manche Anbieter erlauben auch das Ausdrucken von PIN-Listen – ähnlich zu den alten TAN-Listen Ihrer Bank.

Der sehr wirkungsvolle Schutz der Zwei-Faktor-Authentifizierung besteht darin, dass Ihr Passwort in den Händen eines Hackers für diesen nutzlos ist. Der Angreifer benötigt zusätzlich Ihr Smartphone oder die ausgedruckte Liste, um an den Sicherheitscode zu kommen.



Beispiel Kreditkarten-Abrechnung



Ihre neue Online-Rechnung ist im cardservice bereit

SOS Datenschutz Zum cardservice	
<p>Dies ist eine systemgenerierte Nachricht für ERNST FLURI</p> <p>Es freut uns, dass Sie den cardservice nutzen.</p> <p>Ihre aktuelle Rechnung für Kontonummer *** ***** **** 5087 ist ab sofort im cardservice als PDF-Datei für Sie bereit.</p> <p>Dies ist eine systemgenerierte Nachricht. Bitte antworten Sie nicht auf diese E-Mail. Wenn Sie Kontakt mit unserem Kundendienst wünschen, verwenden Sie bitte unten stehende Kontaktdaten.</p> <p>Freundliche Grüsse Swisscard AECS GmbH</p>	
Sicherheitshinweis	Brauchen Sie Unterstützung?
Swisscard fragt Sie niemals per E-Mail nach vertraulichen Daten wie Karten-PIN oder Zugangsdaten zu card service .	So erreichen Sie uns: https://card-service.swisscard.ch/Swisscard_Consumer/Login.do SOS Alle Kontaktangaben
Impressum	
Swisscard AECS GmbH, Neugasse 18, CH-8810 Horgen SOS Datenschutz Zum cardservice	

Sie erhalten diese Nachricht, weil Sie der elektronischen Kommunikation im Rahmen der card**service** Vertragsbedingungen zugestimmt haben.

Sie sind mit folgender E-Mail-Adresse bei Swisscard registriert:
ernst.fluri@solnet.ch

Um den card**service** nutzen zu können, ist die Hinterlegung einer E-Mail-Adresse zwingend notwendig. Eine Abmeldung ist aus diesem Grund nur mit Verzicht auf die Nutzung von card**service** (über den Kundendienst) möglich.

Credit Cards issued by Swisscard AECS GmbH



Login cardservice

Sie haben bereits einen Benutzernamen und ein Passwort? Bitte jetzt eingeben.

Nach erfolgreicher Eingabe erhalten Sie per SMS eine mTAN an die von Ihnen registrierte Mobiltelefonnummer.

Benutzername

Passwort

Login

[Passwort vergessen?](#)



Login cardservice

Sie haben bereits einen Benutzernamen und ein Passwort? Bitte jetzt eingeben.

Nach erfolgreicher Eingabe erhalten Sie per SMS eine mTAN an die von Ihnen registrierte Mobiltelefonnummer.

Benutzername 

Passwort

Login

[Passwort vergessen?](#)



6-stellige mTAN eingeben

[Sign On](#)

Sie haben eine mTAN per SMS an die von Ihnen registrierte Mobiltelefonnummer erhalten. Bitte geben Sie die sechsstellige mTAN ein.

Neue mTAN anfordern

Sie haben die mTAN versehentlich gelöscht oder nicht erhalten? Dann können Sie eine neue mTAN anfordern.

Wichtig: Mit der Anforderung einer neuen mTAN werden alle vorherigen mTAN sofort ungültig. Sie können nur eine begrenzte Anzahl neuer mTAN anfordern.

Gratis-Apps für die Zwei-Faktor-Authentifizierung:

- **Google Authenticator für Android**
- **Google Authenticator für iOS**
- **Amazon AWS MFA für Android**
- **Microsoft Authenticator für Android**
- **Microsoft Authenticator für iOS**
- **Microsoft Authenticator für Windows Phone**

2-FA ist eine gute Methode, Accounts sicherer zu machen. Aber was, wenn das Handy verschwindet?

von Florian Bodoky 22.05.2018

Das Smartphone verlegt, verloren oder gar gestohlen? Gottseidank gibts ja «Android Lost». Dumm nur, wenn der 2-FA- Sicherheitscode ans besagte Smartphone geschickt wird. Wie Sie sich vor diesem Fall schützen und trotzdem nicht auf 2-FA verzichten müssen:

Methode 1:

Die zweite Nummer

So legen Sie eine Ersatz-Telefonnummer fest



4. Im Bereich Ersatztelefon klicken Sie auf *Telefon hinzufügen*.

5. Tippen Sie die Nummer ein, wählen Sie die Weise, wie Ihnen der Code zugespielt werden soll und klicken Sie auf *Fertig*.

Methode 2:

Back-up-Codes



4. Unter dem Kapitel Back-up-Codes klicken Sie auf *Codes anzeigen*.

5. Es wird eine Liste von 10 Einmalcodes angezeigt. Jeden können Sie nur einmal benutzen. Drucken Sie die Liste aus.

6. Bewahren Sie sie nie beim Smartphone auf, das könnte im Falle eines Diebstahls fatal enden.

So deaktivieren Sie die Zwei-Faktor-Authentifizierung für die Apple-ID

Schritt 1:

Öffnen Sie Ihren Webbrowser am Mac und rufen Sie appleid.apple.com auf.

Schritt 2:

Loggen Sie sich mit Ihrer Apple-ID und Passwort ein. Gegebenenfalls müssen Sie Ihren Browser erst mittels Authentifizierung freigeben.

Schritt 3:

Sie sehen nun Ihren Account. Klicken rechts im Sicherheits-Abschnitt auf „Bearbeiten“

Schritt 4:

Am unteren Ende des Abschnitts sehen Sie, dass die Zwei-Faktor Authentifizierung [eingeschaltet ist](#). Klicken Sie rechts daneben auf „Zwei-Faktor-Authentifizierung deaktivieren“ und bestätigen Sie Ihre Eingabe.

The screenshot shows the Apple ID account page with the following sections:

- PASSWORT**: Zuletzt geändert: 10. Juni 2016. [Passwort ändern ...](#) Fertig
- VERTRAUENSWÜRDIGE TELEFONNUMMERN**: +49. [Telefonnummer hinzufügen ...](#)
- ANWENDUNGSSPEZIFISCHE PASSWÖRTER**: [Passwort erstellen ...](#)
- ZWEI-FAKTOR-AUTHENTIFIZIERUNG**: Ein. Wenn deine Apple-ID zum Anmelden auf einem neuen Gerät oder in einem neuen Browser verwendet wird, sind dein Passwort und ein Bestätigungscode erforderlich. [Weitere Informationen](#) [Zwei-Faktor-Authentifizierung deaktivieren](#)

A red arrow points from the 'Zwei-Faktor-Authentifizierung deaktivieren' link to a confirmation dialog box:

Zwei-Faktor-Authentifizierung deaktivieren?
Wenn du die Zwei-Faktor-Authentifizierung deaktivierst, wird dein Account nur noch durch dein Passwort und deine Sicherheitsfragen geschützt.

[Abbrechen](#) [Zwei-Faktor-Authentifizierung deaktivieren](#)