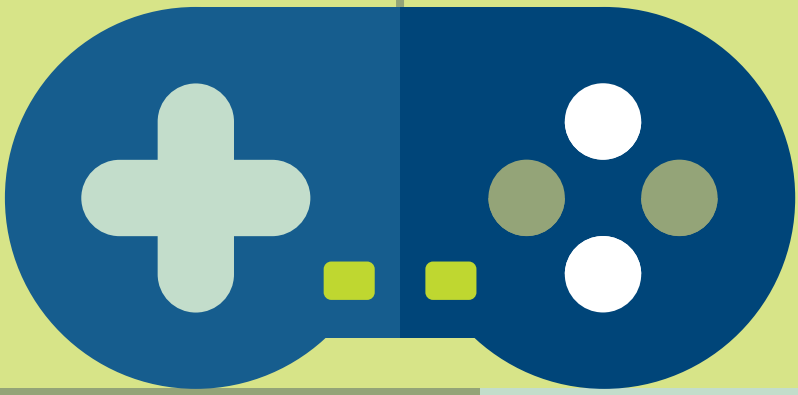
Schritt für Schritt zur Zwei-Faktor-Authentisierung

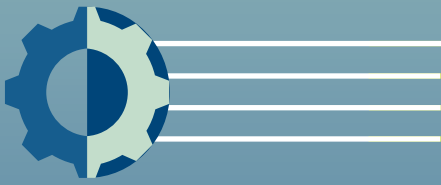
Für Gamingaccounts und Konsolen



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Zwei-Faktor-Authentisierung für Gamingaccounts einrichten



Sobald der Hersteller Ihrer Konsole die Benutzeroberfläche ändert, können sich auch die Schritte im Detail ändern oder Begrifflichkeiten geringfügig abweichen. Das Prinzip der Zwei-Faktor-Authentisierung bleibt dabei aber meist gleich. Sollten diese Anleitungen nicht zu Ihrer Konsole passen, empfehlen wir, dass Sie beim jeweiligen Hersteller nachschauen, um dort möglicherweise eine noch spezifischere Hilfestellung zu finden.

Keine Konsole ohne Benutzerkonto: Für Gamerinnen und Gamer ist der Account notwendig, für Cyberkriminelle umso interessanter. Ob man Opfer einer Phishing-Mail wird oder ein Datenleck das eigene Passwort enthält: Wenn Unbefugte Zugriff zum Account erlangen, können sie ihn zum Beispiel samt Spielfortschritt übernehmen oder die gespeicherten Kreditkartendaten für weitere Käufe nutzen.

Starke Passwörter erschweren es Unbefugten zwar, einen Account zu knacken. Unmöglich machen sie es aber nicht. Eine zusätzliche Absicherung bietet die Zwei-Faktor-Authentisierung. Bei Konsolen sieht sie meist so aus: Wenn eine Nutzerin oder ein Nutzer sich etwa nach dem Kauf einer neuen Konsole in den Account einloggen möchte, fragt die Konsole zuerst nach den Anmeldedaten, oftmals Benutzername und Passwort. Zusätzlich wird ein Code per SMS, E-Mail oder Authenticator App an ein hinterlegtes Smartphone oder Tablet übermittelt. Erst nach der Eingabe der Anmeldedaten und des Codes funktioniert der Login. Ist die Zwei-Faktor-Authentisierung aktiviert, reicht es also nicht, das Passwort zu kennen, um den Account zu knacken.

Nintendo, z.B. Nintendo Switch

Die Zwei-Faktor-Authentisierung heißt bei Nintendo Zweistufen-Authentifizierung oder Zweistufen-Bestätigung. Dabei gehen Sie so vor:

1 Melden Sie sich in den Nintendo-Account-Einstellungen unter *https://accounts.nintendo.com* an. Dafür können Sie einen beliebigen Browser auf einem beliebigen Gerät wie etwa Laptop oder Smartphone nutzen.

2 Gehen Sie zu **Anmelde- und Sicherheitseinstellungen** und anschließend zu **Zweistufen-Bestätigung**. Klicken Sie dort auf **Bearbeiten** und dann auf **Zweistufen-Bestätigung aktivieren**.

3 In manchen Fällen müssen Sie Ihr Passwort oder Ihre E-Mail-Adresse nun erneut bestätigen. Dafür geben Sie das Passwort ein oder lassen einen Bestätigungscode an Ihre E-Mail-Adresse senden.

4 Nach der Eingabe werden Sie aufgefordert, eine Authenticator App auf Ihrem Smartphone oder Tablet zu installieren. Dafür stehen verschiedene kostenlose Apps zur Auswahl.

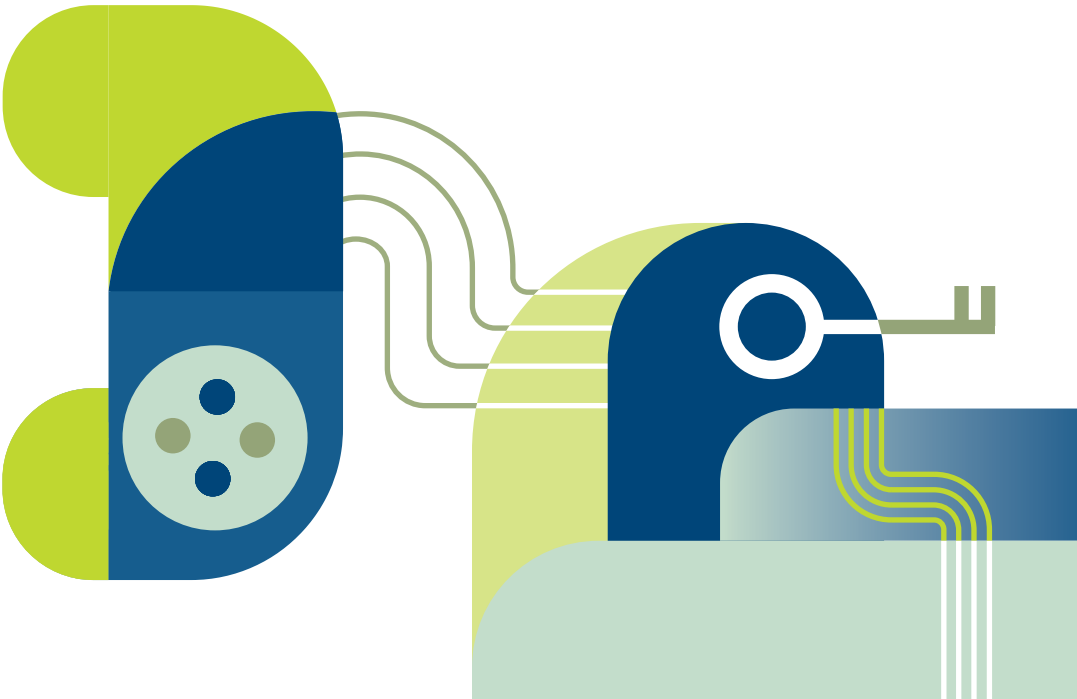
5 In den Nintendo-Account-Einstellungen im Browser wird nun ein QR-Code angezeigt. Scannen Sie ihn mit der Authenticator App ein.

6 Die Authenticator App zeigt jetzt einen Code aus mehreren Ziffern an. Geben Sie diesen in den Nintendo-Account-Einstellungen unter **Bestätigungscode** ein.

7 Sie sehen eine Liste mit sogenannten Backup-Codes. Notieren Sie diese und verwahren Sie die Codes sicher auf. Sollten Sie keinen Zugriff mehr auf die Authenticator App oder das verbundene Gerät haben, können Sie ersatzweise einen dieser Codes nutzen.
Nach dem Login können Sie die Zweistufen-Authentifizierung dann vorübergehend deaktivieren oder zum Beispiel über ein anderes Smartphone neu einrichten.

8 Klicken Sie abschließend auf das Feld **Die Backup-Codes wurden gespeichert** und auf **Ok**.

Übrigens: Die Backup-Codes finden Sie auch zu einem späteren Zeitpunkt noch in den Nintendo-Account-Einstellungen. Klicken Sie dafür auf **Anmelde- und Sicherheitseinstellungen** und dann auf **Zweistufen-Bestätigung**.



Sony, z.B. PlayStation

Die PlayStation spricht in ihren Einstellungen von der zweistufigen Verifizierung. Der erste Schritt hängt davon ab, ob Sie diese in der Konsole oder im Webbrowser aktivieren möchten sowie welches Modell der Konsole Sie nutzen.

1 Aktivieren Sie die zweistufige Verifizierung in Ihren Einstellungen. Je nach Gerät gehen Sie dabei wie folgt vor:

Über den Webbrowser

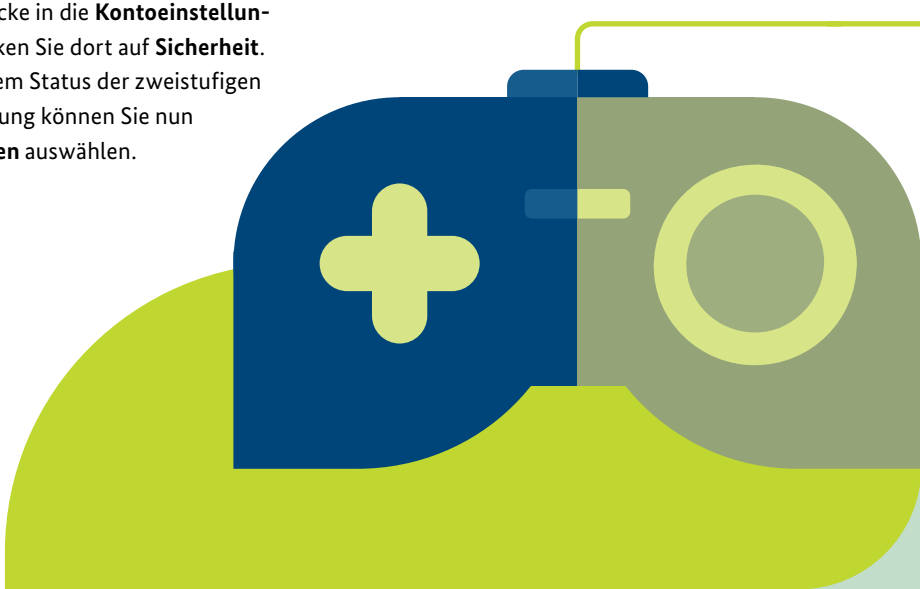
Melden Sie sich unter *https://playstation.com* an. Gehen Sie über Ihren Avatar oder das Smiley-Icon in der rechten oberen Ecke in die **Kontoeinstellungen**. Klicken Sie dort auf **Sicherheit**. Neben dem Status der zweistufigen Verifizierung können Sie nun **Bearbeiten** auswählen.

Über die PlayStation 5

Gehen Sie in die Einstellungen. Dort wählen Sie **Benutzer und Konten**, **Sicherheit** und dann **Zweistufige Verifizierung** aus. Anschließend klicken Sie auf **Aktivieren**.

Über die PlayStation 4

Öffnen Sie die Einstellungen. Klicken Sie auf **Konto-Verwaltung > Kontoinformationen > Sicherheit** und anschließend auf **Zweistufige Verifizierung**. Wählen Sie dort **Aktivieren** aus.



2 Entscheiden Sie, ob der Code per SMS oder an eine Authenticator App verschickt werden soll.

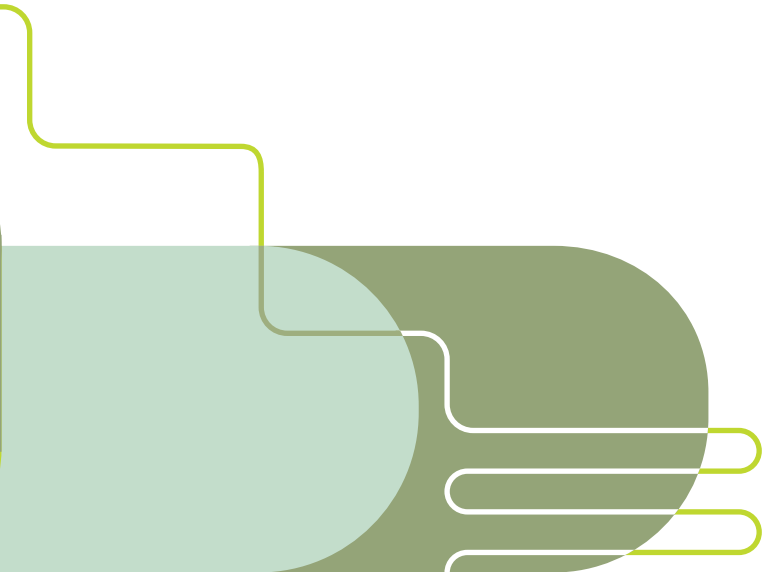
a. Wenn Sie sich für die Zusendung per SMS entscheiden, geben Sie Ihre Mobiltelefonnummer ein. Dann wird Ihnen der Zahlencode zugeschickt.

b. Wenn Sie sich für eine Authenticator App entscheiden, stehen mehrere kostenlose Apps zur Auswahl. Installieren Sie eine solche App auf Ihrem Smartphone oder Tablet. Scannen Sie dann mit der App den in der Konsole oder im Browser angezeigten QR-Code. Alternativ können Sie die angezeigte Nummer eintippen. Dann wird in der App ein Code aus mehreren Zahlen angezeigt.

3 Geben Sie den Zahlencode in der Konsole oder im Browser ein.

4 Anschließend werden Ihnen Ersatzcodes angezeigt. Diese helfen Ihnen weiter, wenn Sie den Zugriff auf das Gerät verlieren, an das die SMS verschickt werden oder auf dem die Authenticator App installiert ist. Bewahren Sie die Ersatzcodes daher sicher auf.

5 Im letzten Schritt bestätigen Sie, dass Sie die Ersatzcodes für die künftige Verwendung gesichert haben, und klicken auf **Ok**.



Microsoft, z.B. Xbox

Um den Xbox-Account zu schützen, sichern Nutzerinnen und Nutzer gleich den gesamten Microsoft-Account ab. Das kann also auch Auswirkungen auf Microsoft-Accounts bei anderen Geräten und Apps haben. Microsoft spricht dabei von einer zweistufigen Überprüfung.

1 Melden Sie sich unter https://account.microsoft.com/security an. Ob Sie dafür beispielsweise Laptop oder Tablet verwenden sowie welchen Browser Sie nutzen, ist egal. Sie befinden sich jetzt in den Microsoft Account-Einstellungen.

2 Öffnen Sie die **Erweiterten Sicherheitsoptionen** und wählen Sie bei der zweistufigen Überprüfung **Aktivieren** aus. Microsoft stellt Ihnen eventuell weitere Fragen u.a. zu den von Ihnen genutzten Geräten, die Sie nun beantworten.

3 Anschließend gelangen Sie zurück in die erweiterten Sicherheitsoptionen. Dort klicken Sie auf **Neue Möglichkeit zur Anmeldung oder Verifizierung hinzufügen**.

Wählen Sie eine der angezeigten Optionen aus: Entweder hinterlegen Sie Ihre Telefonnummer, eine alternative E-Mail-Adresse oder Sie nutzen eine Authenticator App.

a. Wenn Sie sich für die Telefonnummer entscheiden, geben Sie diese ein. Per SMS wird Ihnen ein Verifizierungscode zugeschickt. Geben Sie diesen in den Microsoft Account-Einstellungen ein.

b. Wenn Sie die E-Mail-Adresse auswählen, geben Sie diese ein. Den Verifizierungscode erhalten Sie in Ihrem Postfach und können ihn anschließend in den Microsoft Account-Einstellungen eingeben.

c. Wenn Sie sich für die Authenticator App entscheiden, finden Sie einen Link zum Microsoft Authenticator und einen QR-Code. Laden Sie die App auf Ihrem Smartphone oder Tablet herunter und scannen Sie mit der App den QR-Code ein.

Bei der nächsten Anmeldung wird Ihnen hier der Verifizierungscode zur Eingabe angezeigt.

Übrigens: Microsoft erlaubt es, mehr als nur einen zweiten Faktor anzugeben. Wird das Smartphone gestohlen, kann der Verifizierungscode dann etwa alternativ an die E-Mail-Adresse geschickt werden. So verlieren Nutzerinnen und Nutzer mit aktivierter Zwei-Faktor-Authentisierung nicht den Zugang zu ihrem Account, wenn zum Beispiel ihr Smartphone geklaut wird. Nachdem Sie die Zwei-Faktor-Authentisierung aktiviert haben, klicken Sie erneut auf **Neue Möglichkeit zur Anmeldung oder Verifizierung hinzufügen**, um eine weitere Kontaktmöglichkeit zu hinterlegen.

Kann ich statt Zwei-Faktor-Authentisierung eine PIN einstellen?

Eine PIN ist für viele Spielerinnen und Spieler prinzipiell keine schlechte Idee – etwa für alle, die sich ihren Wohnraum mit anderen Menschen, insbesondere mit Kindern, teilen. So effektiv wie die Zwei-Faktor-Authentisierung ist sie aber nicht.

In der Praxis ist die PIN eine meist kurze Kombination aus Ziffern – im Grunde ähnlich wie ein verkürztes Passwort. Sie wird entweder von der Konsole vorgegeben oder von Spielerinnen und Spielern selbst gewählt. Letztere sind an ihren Konsolen dauerhaft eingeloggt. Beim Starten der Konsole geben Sie also nicht jedes Mal Ihre Anmeldedaten erneut ein – durchaus aber die PIN.

Was eine PIN leisten kann:
Die PIN hilft, wenn sich Unbefugte physischen Zugang zu der Konsole verschaffen. Bei manchen Konsolen lässt sich die PIN daher auch nur als „Kindersicherung“ einstellen. Ist die Konsole zum Beispiel für jüngere Familienmitglieder in Reichweite, können Spielerinnen und Spieler mit einer PIN die gesamte Konsole oder bestimmte Aktivitäten wie etwa Einkäufe vor unerlaubtem oder unbeabsichtigtem Zugriff schützen.

Was eine PIN nicht leisten kann:
Eine PIN schützt ausschließlich vor Fremdzugriffen auf den Account über die jeweilige Konsole. Sie hält also nur jene Kriminelle ab, die etwa in den Wohnraum eindringen und dort die Konsole vorfinden. Unbefugte, die stattdessen das Passwort knacken, können aber dennoch beispielsweise über die Webseite des Herstellers auf den Account zugreifen oder diesen gar übernehmen. Mitunter können sie die PIN dort auch abändern. Als meist kurze Abfolge von ausschließlich Ziffern ist eine PIN außerdem leicht zu knacken. Wer einen Account effektiv schützen möchte, sollte also dennoch die Zwei-Faktor-Authentisierung aktivieren.

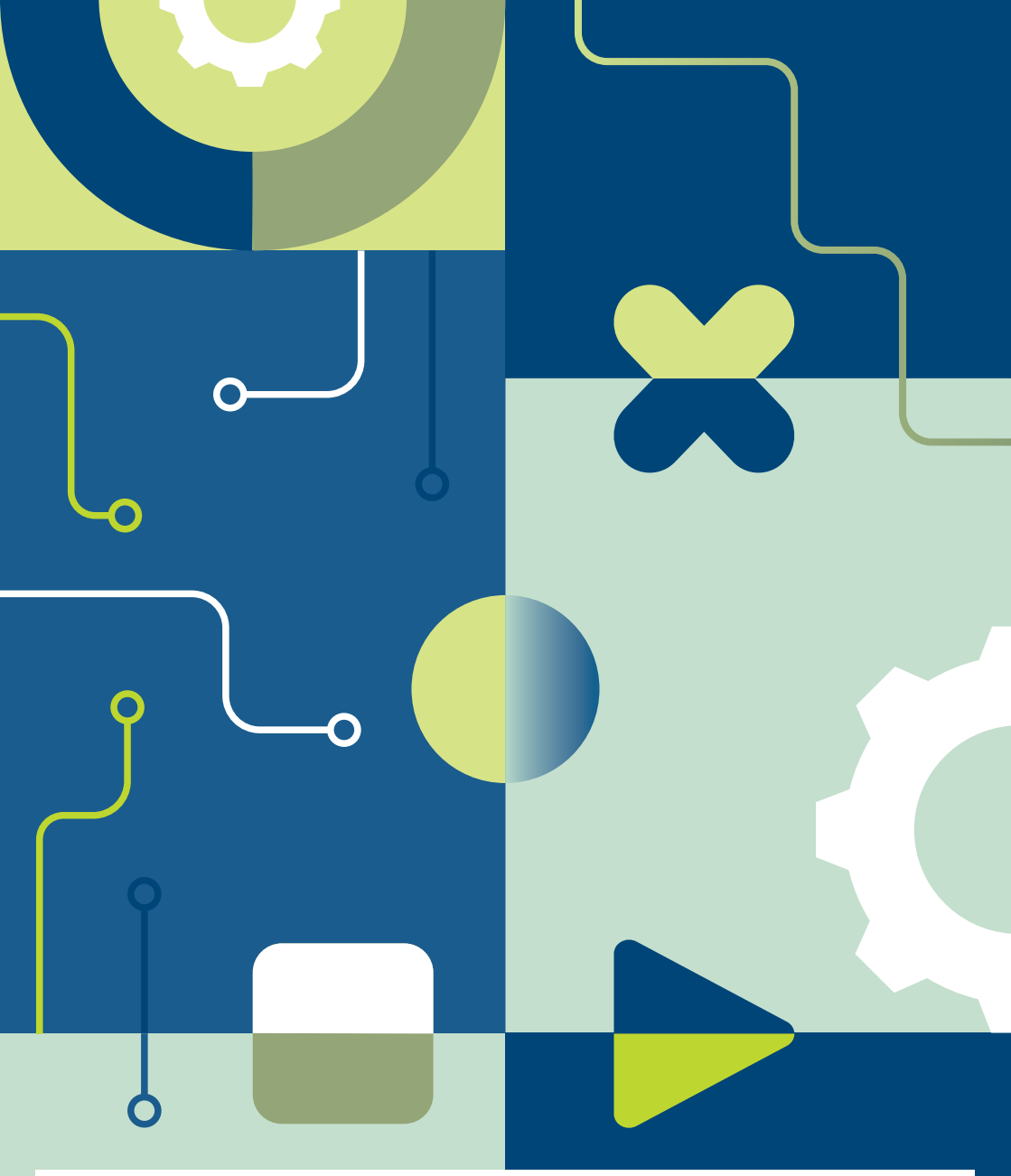
Weitere Informationen

Wegweiser kompakt: 8 Spielregeln für digitale Sicherheit

Gaming – Spielregeln für digitale Sicherheit #accountschutzover9000

Die Sicherheit verzockt – Account mit zweitem Faktor absichern

Zwei-Faktor-Authentisierung



Impressum

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn

Kontakt:
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
Service-Center: +49 (0) 800 274 1000

Artikelnummer: BSI-IFB-23/052