

FÜR DEN UNTERRICHT

ACCOUNT-SCHUTZ



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI



AB 1: ACCOUNTS SCHÜTZEN – WARUM UND WIE?

Einführung

Ihr legt einen Sicherheitsgurt an, wenn ihr ins Auto steigt? Ihr schließt die Tür ab, wenn ihr das Haus verlasst? **Der Schutz eurer digitalen Identitäten, also der über euch im Internet hinterlegten persönlichen Daten, ist ebenso wichtig.** Je mehr Onlinedienste wir nutzen, desto mehr geben wir von uns preis. Sich für mehr Sicherheit vorsorglich ein paar Minuten Zeit zu nehmen, lohnt sich. Gehackt werden können z. B. Benutzerkonten bei E-Mail-Anbietern, Streaming-Diensten, Spielen, Online-Shops und mehr. Cyberkriminelle wollen sich illegal fremde Identitäten verschaffen, Inhalte missbrauchen, Daten klauen oder Geld abgreifen. In der Regel geschieht das willkürlich und auf gut Glück und hat nichts mit dir persönlich zu tun. Deshalb müssen wir unsere Accounts schützen.

Olli wird vom Anruf einer Freundin aufgeschreckt: „Hey, was hast du für blödes Zeug auf deinem Kanal gepostet? Ich bin schon von anderen gefragt worden, was mit dir los ist.“ Das schockt Olli, denn er hat heute nichts gepostet. Sein Account ist mit Nutzernamen und Passwort gesichert. Das scheint geknackt worden zu sein. Olli sorgt sich. Denn er hat dieses Passwort auch bei anderen Accounts verwendet.



Macht ein Brainstorming in der Klasse. Tragt zusammen, was ihr schützen müsst, z. B. Adressen und Passwörter. Nennt Gründe, warum es wichtig ist, Accounts zu schützen.



Lest den Text und schaut euch im Anschluss das Video an.



[BSI-Identitätsdiebstahl in Social-Media-Kanal](#)



[YouTube-Video Accountschutz](#)

Bildet zwei Gruppen. Jede Gruppe bearbeitet eine der folgenden Fragen. Tragt die Ergebnisse im Anschluss im Plenum zusammen.

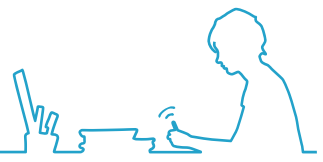
- 1. Notiert, warum man die Kontrolle über einen gehackten Social-Media-Account zurückgewinnen muss und was man tun kann, wenn Unbefugte das Passwort geändert haben.**
- 2. Notiert euch, wie Hacker an Nutzerdaten herankommen könnten.**

PRAXISTIPPS

Passwörter sind eine Möglichkeit, um Accounts zu schützen. Hacker versuchen jedoch, Passwörter herauszufinden, um sich Zugang zum Account zu verschaffen.

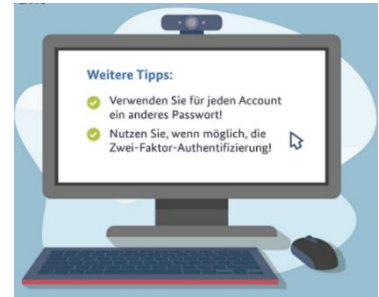
Erschwere Hackern deshalb ihr Handeln weitestmöglich. Nutze nie einfache, sondern immer starke Passwörter, die einem systematischen Durchprobieren stärker standhalten. Bei sogenannten Brut-Force-Angriffen lassen Angreifer ein Computer-Programm alle möglichen Kombinationen von Zeichen, Zahlen und Symbolen in einem Passwort ausprobieren, um das tatsächliche Passwort zu ermitteln. Je mehr Zeichen du verwendest, desto aufwendiger ist das Verfahren.





AB 2: PASSWÖRTER BILDEN UND VERWALTEN

Wer kennt es nicht? Ihr wollt einen Dienst im Internet nur kurz nutzen, und schon wird eine Anmeldung erbeten. Okay, ihr klickt euch zügig durch den Anmeldevorgang, akzeptiert die AGB und dann kommt die Frage nach dem Passwort – mal mit, mal ohne konkrete Vorgaben. Hier sollte immer Sicherheit vor Schnelligkeit gehen!



Schaut euch im Video an, wie ihr starke Passwörter bilden könnt.

multimedia.gsb.bund.de/BSI/Video/220117_BSI_OnlineSchutz_Password_Final_v4.mp4



Stellt die Informationen auf einem Plakat zusammen: Fertigt jeweils zu „kurz & komplex“ und zu „lang & weniger komplex“ eine übersichtliche Skizze an und notiert die Regeln (wie viele und welche Zeichen). Ergänzt Hinweise zu weiteren Themen aus dem Video (voreingestellte Passwörter, Verhalten bei Verdacht auf Hacking).



Findet euch zu zweit zusammen. Jede/r bildet je ein Beispiel für ein komplexes und ein langes Passwort. Überprüft wechselseitig, ob ihr die Regeln richtig eingehalten habt.

Passwortmanager als Helfer

Nur starke Passwörter und für jeden Account ein anderes – das ist sicher. Doch wir haben immer mehrere Online-Accounts und brauchen immer mehrere Passwörter. Sich die zu merken, ist eigentlich unmöglich. Eine gute Hilfe beim Handhaben vieler Passwörter sind Passwortmanager. Denn die helfen nicht nur bei der Verwaltung aller Passwörter, sondern schlagen auch starke Passwörter vor.



Informiert euch im Video über Passwortmanager. Arbeitet auch den Text durch.

multimedia.gsb.bund.de/BSI/Video/Accountschutz_Passwortmanager_720.mp4
[Online-Accounts mit dem Passwortmanager schützen](#)



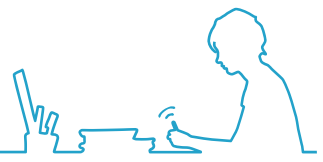
1. Fasst kurz schriftlich zusammen, wie ein Passwortmanager funktioniert.
2. Notiert dazu die wesentlichen Vor- und Nachteile.



PRAXISTIPP

Fest auf einem Gerät installierte Passwortmanager sind sicherer, können aber auch nur auf dem Gerät verwendet werden. In der Regel möchten wir aber von mehreren Geräten, z. B. Laptop und Smartphone, und auch unterwegs auf einen Account zugreifen können. Cloudbasierte Dienste bieten dazu bequeme Synchronisation über alle Geräte. Beides hat Vor- und Nachteile. Entscheidungshilfe gibt dieses Short: <https://www.youtube.com/shorts/sK8pTsuOhuI>





AB 3: PASSKEYS VERSTEHEN UND ANWENDEN

Einführung

Hannah und Olli reden nochmal darüber, dass Ollis Social-Media-Account gehackt wurde.

Hannah: „Hast du eigentlich deinen Social-Media-Account neu gesichert?“

Olli: „Ja. Aber nicht mehr mit Passwort. Sondern mit Passkey. Das nutzt den Fingerabdruck und ist dazu auch als Verfahren noch sicherer.“

Hannah: „Stimmt, biometrische Merkmale können Hacker schwerer nachmachen oder klauen.“

Olli: „Ja, stimmt schon. Aber noch dazu ist auch der technische Ablauf viel sicherer. Bei jedem Anmelden wird beim Anbieter ein öffentlicher Schlüssel und auf meinem Gerät ein privater Schlüssel erzeugt. Davon bekomme ich nichts mit und ich muss auch nichts tun. Nur wenn beide Schlüssel da sind, bekomme ich Zugriff auf mein Benutzerkonto.“



Lest den Text und erläutert die Punkte, die erklären, warum Passkeys sicherer sind als Passwörter. [BSI - Digitale Gewalt - Schafft die Passwörter ab?!](#)



ERSTEINRICHTUNG VON PASSKEY UND NUTZUNG

Das Passkey-Verfahren für Dienste oder Apps braucht eine Ersteinrichtung. Diese ist je nach Webseite oder App etwas anders. Danach läuft die Anmeldung meist in vier Schritten, wie es das Beispiel aus dem zuvor bearbeiteten Text zeigt (Bild aus BSI-Material, siehe obigen Link).



PRAXISTIPP

1. Weil das Passkey-Verfahren wesentlich mehr Sicherheit bringt, solltest du es dir einrichten, wenn es von einem Dienst oder einer App angeboten wird. Dieses Short zeigt dir noch einmal die Vorteile:

<https://www.youtube.com/shorts/74ZMCIUVTis>.



2. Schaue auch nach, ob dein Passwortmanager über einen Passkey aktiviert werden kann, und richte ihn damit ein. Das ist sicherer als mit einem Master-Passwort.

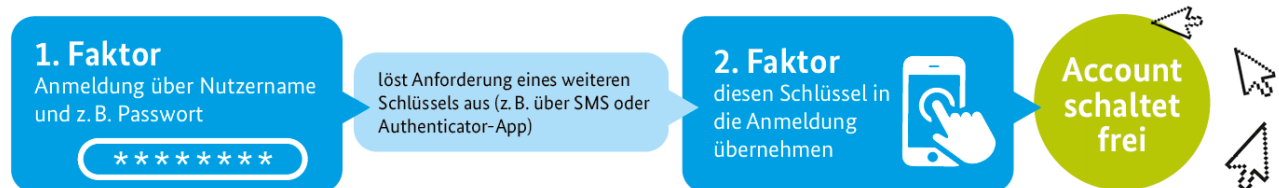


AB 4: MEHR SICHERHEIT DURCH EINEN ZWEITEN FAKTOR

Beispiel

Online-Shopping, E-Mails, Online-Banking oder soziale Netzwerke – um online Dienste und Anwendungen in Anspruch zu nehmen, bei denen viele persönliche Daten hinterlegt werden können, braucht man eine möglichst sichere Form der Authentisierung. Olli hat seine Social-Media-Accounts mit dem Passkey-Verfahren neu eingerichtet, weil das sicherer ist als mit Passwörtern.

Andere sichere Verfahren beruhen darauf, dass der User selbst zwei unterschiedliche Schlüssel verwendet. Sie heißen „2-Wege-Anmeldung“ oder „2-Faktor-Authentisierung“, kurz 2FA. Es gibt sie in zahlreichen Varianten. Einige ergänzen das zuvor eingegebene Passwort um einen zusätzlichen Faktor. Andere ersetzen den vorherigen Login mit Passwort komplett durch eine direkte Kombination zweier Faktoren. Das ist nur möglich, wenn die App dies anbietet. Ihr Grundprinzip:



Für 2FA werden also zwei Schlüssel gebraucht. Das macht die Anmeldung wesentlich sicherer, denn für Hacker ist es viel schwieriger, an zwei Schlüssel heranzukommen als nur an einen.

Die Schlüssel können PINs, Passwörter oder auch biometrische Merkmale sein.

Als zweiter Schlüssel dient meist ein Einmalcode. Noch sicherer wird 2FA, wenn der zweite Faktor über ein zweites Gerät oder eine Authenticator-App übermittelt wird.



Schaut euch für weitere Informationen das Video an. Es zeigt euch, wie 2FA genau funktioniert. Besprecht anschließend in der Klasse, was mit Wissen, Biometrie und Besitz gemeint ist. Nennt dafür jeweils mindestens ein Beispiel.

multimedia.gsb.bund.de/BSI/Video/BSIfB_Animation_Zwei-Faktor-Authentisierung.mp4



WO LÄSST SICH DIE 2FA EINRICHTEN?

Viele, aber nicht alle Dienste und Apps bieten eine Anmeldung mit 2FA an. Die Verfahren sind unterschiedlich. Als zweiter Faktor wird zum Beispiel eine PIN über SMS verschickt oder du kannst eine Authenticator-App verwenden. Auch viele Konsolenspiele und Spiele-Apps können durch 2FA abgesichert werden. Hier kannst du dir eine Broschüre mit Anleitungen für eine Reihe verbreiteter Spieleanbieter herunterladen:

[Schritt für Schritt: Zwei-Faktor-Authentisierung für Gamingaccounts und Konsolen](#)



NACHSTEHENDE BEDINGUNGEN REGELN DIE ZULÄSSIGE NUTZUNG DIESES DOKUMENTS.

- (1) Die Bereitstellung erfolgt unter der Creative Commons Lizenz CC BY abrufbar unter <https://creativecommons.org/licenses/by/4.0/deed.de>, die durch diese Nutzungsbedingungen ergänzt wird.
- (2) Die Inhalte dieses Dokuments dürfen in jedwedem Format oder Medium vervielfältigt und weiterverbreitet werden. Die Inhalte dürfen verändert, ergänzt oder nur in Teilen genutzt werden. Bei der Verwendung dieses Dokuments ist in angemessener Weise (z. B. durch Verlinkung) auf diese Nutzungsbedingungen hinzuweisen.
- (3) Jegliche Verwendung dieses Dokuments darf in keinem Fall den Eindruck einer Zusammenarbeit mit dem BSI oder eines hoheitlichen Internetauftritts erwecken.
- (4) Internet-Seiten und andere Medien, in denen dieses Dokument verwendet wird, dürfen keine strafbaren, gewalttätigen oder sexuellen Inhalte darbieten.
- (5) Die Wiedergabe von abgebildeten Texten und Grafiken dieses Dokuments als Zitat ist ohne Zustimmung des BSI zulässig, soweit Sinn und Zusammenhang gewahrt bleiben. Die Wiedergabe von Aussagen des BSI muss wortgetreu und in Anführungszeichen erfolgen. In allen Fällen ist ein Quellenachweis aufzunehmen.
- (6) Das Logo des BSI enthält mit dem Bundesadler ein Hoheitszeichen, das durch § 124 OWiG und § 145 Abs. 1 Nr. 1 MarkenG geschützt ist und nur mit schriftlicher Zustimmung des BSI verwendet werden darf. Eine Freigabe für die Nutzung von BSI-Inhalten umfasst nicht die Verwendung des BSI-Logos.
- (7) Das BSI übernimmt in Bezug auf die Inhalte dieses Dokuments keine Garantie. Insbesondere wird keine Garantie für die Aktualität, Richtigkeit, Vollständigkeit oder dauerhafte Verfügbarkeit des Dokuments übernommen.
- (8) Die Einräumung von Rechten nach diesen Nutzungsbedingungen erfolgt unter Ausschluss der Gewährleistung (insb. Freiheit des Dokuments von Sach- und Rechtsmängeln, Verwendbarkeit des Dokuments für einen bestimmten Zweck sowie die Vollständigkeit und Korrektheit des Dokuments). Dieser Gewährleistungsausschluss gilt nicht, sofern das BSI einen Mangel arglistig verschweigt oder soweit dem BSI Vorsatz oder grobe Fahrlässigkeit vorzuwerfen ist.
- (9) Das BSI haftet in Bezug auf Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit nur, sofern dem BSI wenigstens Fahrlässigkeit vorzuwerfen ist, für sonstige Schäden nur bei grober Fahrlässigkeit oder Vorsatz, und übernimmt darüber hinaus keine freiwillige Haftung. Die Vorschrift des § 839 BGB bleibt unberührt.

Für Rückfragen steht das Service-Center des BSI (service-center@bsi.bund.de) zur Verfügung.

IMPRESSUM

Herausgeber:

Bundesamt für Sicherheit in der Informationstechnik - BSI

Godesberger Allee 87, 53175 Bonn

E-Mail: service-center@bsi.bund.de

Internet: www.bsi.bund.de

Service-Center: +49 (0) 800 274 1000

Stand: 09/2025

Didaktische Aufbereitung: Eduversum GmbH