

FÜR PÄDAGOGINNEN UND PÄDAGOGEN

ACCOUNT-SCHUTZ



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

Ablauf der Unterrichtseinheit

Phase	Inhalt	Sozial- / Aktionsform
Arbeitsblatt 1 Einführung in Accountschutz und Passwörter (ca. 2,5 U-Std.)	Die Hinführung zum Thema Accountschutz erfolgt durch ein Einführungsbeispiel. Im Anschluss arbeiten die Lernenden heraus, was sie persönlich schützen möchten. Accountschutz wird als Vorbeugung vermittelt, unter Berücksichtigung dessen, wie Hacker an Nutzerdaten gelangen sowie in Anbetracht möglicher Verhaltensmöglichkeiten, wenn Accounts gehackt wurden. Unterscheidung von einfachen und starken Passwörtern und die Ableitung, dass nur starke sowie unterschiedliche Passwörter Sicherheit bieten.	Lesen des Beispiels in Einzelarbeit, Brainstorming, Diskussion im Plenum, Gruppenarbeit, Praxistipps
Arbeitsblatt 2 Starke Passwörter und Passwortmanager (ca. 2 U-Std.)	Vermittlung starker Passwörter, der Strategien „kurz & komplex“ und „lang & weniger komplex“ sowie Regeln zur Bildung starker Passwörter. Kenntnisvermittlung zu Passwortmanagern und Abwägung von Vor- und Nachteilen.	Informationsvideos, Infotext, Einzelarbeit, Paarbeit, Gruppenarbeit, Plenum, Plakaterstellung, Praxistipp
Arbeitsblatt 3 Passkeys verstehen und anwenden (ca. 1,5 U-Std.)	Die Schülerinnen und Schüler lernen beispielhaft Passkeys als Alternative zu Passwörtern kennen. Es werden der prinzipielle Ablauf einer Anmeldung über Passkeys sowie Nutzungsempfehlungen vermittelt.	Einführungsbeispiel, Infotext, Paarbeit, Prinzip-Skizze, Informationsvideo, Praxistipps
Arbeitsblatt 4 Mehr Sicherheit durch 2FA (ca. 2 U-Std.)	Vermittlung, dass eine Anmeldung mit zwei Schlüsseln die Sicherheit erhöht und eine Darstellung des Prinzips der „Zwei- Faktor-Authentisierung“. Exemplarisch gibt es in der BSI-Broschüre „Schritt für Schritt: Zwei-Faktor- Authentisierung für Gamingaccounts und Konsolen“ ergänzende Infos, wie das Verfahren bei verschiedenen Konsolen konkreter abläuft.	Einführungsbeispiel, Prinzip- Skizze, Informationsvideo, Einrichtungsanleitungen (aus Link), Praxistipps, Einzelarbeit, Paarbeit

Hintergrundinformationen zum Thema der Einheit und Lösungshinweise zu den Aufgaben

Einordnung der Unterrichtseinheit

Sie legen einen Sicherheitsgurt an, wenn Sie ins Auto steigen? Sie schließen die Tür ab, wenn Sie das Haus verlassen? Der Schutz Ihrer digitalen Identität, also der über Sie 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. Das gilt nicht nur für Sie, sondern auch für Ihre Schülerinnen und Schüler.

Der **Accountschutz** ist in der Gesamtheit der Schutzmaßnahmen **zentraler Baustein** und ebenso wichtig wie der grundlegende Schutz des Smartphones (Thema 1) und die Maßnahmen gegen Phishing und Schadsoftware (Thema 2). Alle drei Unterrichtseinheiten sind grundsätzlich singulär nutzbar und erfordern keine speziellen Vorkenntnisse. Lernende werden aber davon profitieren, wenn sie sich zuvor mit grundlegenden Schutzmaßnahmen für Smartphones befasst haben.

Ein erstes Ziel der Unterrichtseinheit ist es, den Lernenden verständlich zu machen, dass Unbefugte, die sich Zugang zu fremden Benutzerkonten für illegale Zwecke verschaffen möchten,

- zum einen an Informationen und persönlichen Daten interessiert sind und
- zum anderen in Anwendungen und Accounts gelangen möchten.

Da interessiert zum Beispiel, wer mit wem fest befreundet ist, um dann mit dem/der Betreffenden als vermeintliche/r Freund/in Kontakt aufzunehmen. Mit zunehmendem Alter haben die Lernenden verschiedene Accounts, nehmen am Geschäftsleben teil und müssen dann z. B. auch Nutzerkonten von Spielen, Kundenkontos im Onlinehandel oder natürlich Bankkonten schützen.

Das Einloggen mit Benutzernamen und Passwort wird oft als lästig empfunden und nur stiefmütterlich behandelt. Deshalb setzt der Einstieg in die konkreten Verfahren zum Accountschutz beim Thema Passwörter an, indem vermittelt wird, wie starke Passwörter gebildet werden. Aber auch starke Passwörter sind nicht völlig sicher, sondern können zum Beispiel bei unsicheren Verbindungen oder mittels Phishing abgefangen werden. Deshalb behandelt die Unterrichtseinheit für mehr Schutz als weiterentwickelte, sicherere Verfahren Passkeys und die Zwei-Faktor-Authentisierung. Sie sollten immer genutzt werden, wenn sie vom Diensteanbieter angeboten werden.

Zu den einzelnen Arbeitsblättern

Arbeitsblatt 1: Account schützen – warum und wie?

Als Einführung in das Thema dient ein Beispiel aus der Lebenswelt der Zielgruppe. Für die Lernenden, die die vorherigen Einheiten bearbeitet haben, ist es eine anknüpfende Wiederholung, für Lernende ohne Vorkenntnisse eine hinführende Einleitung. Thematisiert wird ein gehackter und danach missbrauchter Social-Media-Account. Im Plenum kann, ohne Maßnahmen vorwegzunehmen, beispielsweise über die Frage diskutiert werden, an welcher Stelle der Schutz nicht ausreichend war.

Als Aufgabe folgt ein Brainstorming. Die Schülerinnen und Schüler reflektieren, welche Bereiche sie schützen möchten, und benennen diese konkret. Sie überlegen auch, warum ihre Daten schützenswert sind und besprechen, was passieren kann, wenn jemand auf den eigenen Account zugreift. Der so hergestellte **persönliche Bezug zum Thema** ist **motivierend** und die zu entwickelnde Liste gibt erste Hinweise darauf, wo es notwendig ist, den eigenen Accountschutz zu verbessern.

Natürlich müssen auch weitere Accounts geschützt werden, um persönliche und sensible Inhalte abzusichern. Beim Brainstorming sollten Problembereiche benannt, aber nicht unmittelbare Probleme Einzelner ungewollt aufgedeckt werden. Als mögliche Impulse können außerdem folgende Aussagen dienen:

- „Ich will nicht, dass jemand peinliche Bilder oder Nachrichten von mir postet.“
- „Ich will nicht, dass meine Freunde glauben, ich hätte sie beleidigt oder blockiert, wenn das gar nicht von mir kommt.“

- „Ich habe mir Skins, Add-Ons und Musik gekauft – ich will nicht, dass dies jemand klaut.“
- „Ich will nicht, dass jemand in meinem Namen betrügt und ich dann Ärger bekomme.“
- „Jemand könnte meine Freunde anschreiben und sie um Geld bitten – als ob ich das wäre.“
- „Ich will nicht, dass mein Account gehackt wird und dann weg ist. Ich habe meine ganzen Erinnerungen, also Fotos, Videos und Chats da drauf.“
- „Ich habe viel Zeit in meinen Spielstand gesteckt. Wenn der Account gehackt wird, ist das alles weg.“
- „Ich will nicht, dass jemand über meinen E-Mail-Account Passwörter anderer Accounts zurücksetzt und mich damit aus meinen eigenen Profilen ausschließt.“

Im Anschluss werden die Beispiele in Kategorien geclustert, wie z. B. Privatsphäre, persönliche Angaben, Fakes und ihre Folgen, Betrug und Geldverlust und ggf. weitere. Hier kann evtl. auch ergänzend auf den Missbrauch von Kreditkartendaten eingegangen werden.

Nach der Auswertung des Brainstormings erhalten die Schülerinnen und Schüler einen Informations-Input, der mithilfe eines Textes und eines Videos des BSI erfolgt. Damit wird das Thema weitergeführt und die Lernenden erfahren auch, was zu tun ist, wenn ein Account gehackt wurde. Sie sollen Schaden schnell abwenden und wissen, was im Notfall zu tun ist. In diesem Kontext sollte grundlegend auf Passwörter eingegangen und die Unterscheidung von einfachen und starken Passwörtern deutlich gemacht werden. Der abschließende Praxistipp bekräftigt die Handlungsaufforderung, immer nur starke Passwörter und für jeden Account ein eigenes zu verwenden.

Neben der Vermittlung des Inhalts ist angestrebt, die Kompetenz zu stärken, sich aus Informationsmaterial wesentliches und zum Handeln notwendiges Wissen zu erschließen. Als spielerische Wiederholung wichtiger Grundbegriffe bietet sich als Ergänzung auch noch das folgende Kreuzworträtsel an:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/accountschutz_node.html



Wichtig ist der Hinweis, dass **jeder Account ein eigenes Passwort** braucht. Das kann nochmals an Beispielen klar gemacht werden – zum Beispiel: Ein User nutzt für alle Online-Spiele und Social-Media-Accounts ein einziges Passwort. Das gibt er an einen Mitspieler weiter, damit er etwas ausprobieren kann. Dieser probiert es spaßeshalber auch auf anderen Anwendungen aus und hat somit uneingeschränkten Zugriff.

Arbeitsblatt 2: Passwörter bilden und verwalten

Wer kennt es nicht? Wir wollen einen Dienst im Internet nur kurz nutzen und schon wird eine Anmeldung erbeten. Okay, man klickt sich zügig durch den Anmeldevorgang, akzeptiert die AGBs und dann kommt die Frage nach dem Passwort – mal mit, mal ohne konkrete Vorgaben. Hier sollte immer Sicherheit vor Schnelligkeit gehen! Wie im Arbeitsblatt ausgeführt, nutzen Hacker vollautomatisches Ausprobieren von Zeichenkombinationen, so genannte Brut-Force-Angriffe. Um dem zu begegnen, brauchen wir starke Passwörter.

Die **Definition starker Passwörter** erfolgt über die **Regeln zu ihrer Bildung**. Sie werden in der Lerneinheit über ein Video vermittelt. Es benennt **zwei Strategien**:

- Kürzere, komplexere Passwörter bestehen aus mindestens acht Zeichen und verwenden vier verschiedene Zeichenarten (Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen).
- Längere, dafür weniger komplexe Passwörter haben 25 Zeichen und zwei Zeichenarten.

Diese Regeln erarbeiten sich die Lernenden aus dem Video des BSI und erstellen dazu ein Plakat. Es folgt eine Übung, bei der jede/r Lernende konkret starke Passwörter bildet.

Anschließend wird die Funktionsweise von **Passwortmanagern** vorgestellt und es werden deren Vor- und Nachteile mithilfe eines weiteren Videos und eines Arbeitstextes erarbeitet. Die Schülerinnen und Schüler informieren sich über gerätebezogene und cloudbasierte Passwortmanager und sehen sich dazu ein YouTube-Short an. Der Inhalt sollte im Anschluss besprochen werden.

Arbeitsblatt 3: Passkeys verstehen und anwenden

Wie oben in der Einleitung schon ausgeführt, sind Passwörter nie völlig sicher. Lernenden dies zu vermitteln, macht sie für **umfassenden Accountschutz** aufgeschlossen.

Sicherer, zugleich einfach und als erste Wahl zu empfehlen, ist das Passkey-Verfahren. Es kann eingerichtet werden, wenn ein Diensteanbieter es anbietet. Kurz umrissen funktioniert es wie folgt: Bei der Einrichtung wird ein Schlüsselpaar erzeugt. Ein (öffentlicher) Schlüssel verbleibt beim Anbieter, der zweite (private) im Gerät des Users. Bei jedem Einloggen sendet der Diensteanbieter eine dynamische Anfrage („Challenge“), die über Abgleich des Schlüsselpaars geprüft, signiert und nach Authentifizierung des Users (meist durch ein biometrisches Merkmal, z. B. Fingerabdruck, oder über eine PIN) bestätigt wird. Der Datenaustausch ist dabei verschlüsselt. Der Komfort liegt in der einfachen Nutzung sowie in der Sicherheit in der Abfrage- und Verschlüsselungstechnik, bei der keine persönlichen Daten versendet werden.

Sie finden eine ausführlichere, verständliche Darstellung im Podcast „Update verfügbar #40: Passkey statt Passwort – was steckt dahinter?“

<https://www.youtube.com/watch?v=m0J40Xczj14&t=1s>



Die Lernenden erarbeiten das Verfahren anhand eines Infotextes vom BSI. Sie erhalten darin noch weiterführende Informationen zum Thema.

Ziel ist es, den Lernenden zu vermitteln, dass Passkeys ein sehr sicheres Verfahren bieten, das sie immer einrichten sollten, wenn ein Diensteanbieter es anbietet. Dazu sollen sie den Ablauf einer Anmeldung mittels Passkey kennenlernen, der im Arbeitsblatt in einer Prinzipskizze dargestellt wird.

Auch lohnt es sich zu prüfen, ob man einen Passwortmanager besser mit einem Master-Passwort oder mit einem Passkey absichert.

Arbeitsblatt 4: Mehr Sicherheit durch 2FA

Wo keine Passkeys angeboten werden, ist Accountschutz über starke Passwörter in Verbindung mit einer **Zwei-Faktor-Authentisierung** eine Alternative, die eingerichtet werden sollte. Diensteanbieter stellen sie in verschiedenen Varianten zur Verfügung, wobei der Ablauf überall prinzipiell gleich ist. Das Beispiel und ein kurzer Infotext im Arbeitsblatt liefern einen entsprechenden Einstieg.

Ziel dieses Themas ist, den Lernenden das Verfahren als sehr sicher zu vermitteln und ihnen Beispiele für verschiedene 2FA-Verfahren aufzuzeigen. Sie sollen das Prinzip verstehen und das Verfahren nutzen können. Dazu sollen sie motiviert werden, darauf zu achten, wo sie überall bereits 2FA nutzen können und auch einrichten.

Der prinzipielle Ablauf der Anmeldung über zwei Faktoren ist im Arbeitsblatt dargestellt. Meist erfolgt beim ersten Faktor eine übliche Anmeldung über Nutzernamen und Passwort. Die Eingabe löst eine Anforderung für den zweiten Faktor aus. Dabei unterscheiden sich die Diensteanbieter mit ihren Systemen und stellen auch Faktoren zur Wahl. Beispielsweise wird ein Code per SMS verschickt oder in einer Authenticator-App angezeigt. Es gibt auch Lösungen mit Chipkarte, TAN-Generator oder Token. Eine grundsätzliche Anforderung ist, dass die Faktoren aus verschiedenen Bereichen stammen sollen: Ein Passwort ist beispielsweise „Wissen“, ein Fingerabdruck „Biometrie“, einen TAN-Generator oder das Handy für die SMS oder die Authentication muss ich in meinem „Besitz“ haben.

Nach der Einführung und dem Besprechen der Prinzipskizze erhalten die Lernenden über ein Video des BSI weitergehende Informationen zur Funktionsweise von 2FA. Für die Zielgruppe soll schließlich eine **Vertiefung** in ihre Lebenswelt und deshalb **für Spiele** erfolgen. Dazu können sie sich eine Broschüre vom BSI herunterladen, die Anleitungen zur Einrichtung der 2FA für Konsolen zusammenstellt.

Wie in allen Bereichen der Cybersicherheit müssen wir alle – und das gilt natürlich auch für Kinder und Jugendliche – stetig **am Ball bleiben**. Ermutigen Sie zum Abschluss der Unterrichtseinheit Ihre Schülerinnen und Schüler, neu eingerichtete Accounts immer von Anfang an richtig abzusichern und regelmäßig durchzuschauen, wo Passkeys neu angeboten werden (und sie auch einzurichten). Wo noch keine Passkeys möglich sind, sollte der Account zusätzlich mit der 2FA gesichert werden.

Weiterführende Links

1. Online-Account schützen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/accountschutz_node.html



2. Sichere Passwörter erstellen:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html



3. Passwörter verwalten mit einem Passwortmanager:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/Passwort-Manager/passwort-manager_node.html



4. Zwei-Faktor-Authentisierung:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/zwei-faktor-authentisierung_node.html



5. YouTube-Short zur 2FA:

https://www.youtube.com/shorts/Y_tB1YIz000



6. Podcast „Update verfügbar #40: Passkey statt Passwort – was steckt dahinter?“:

<https://www.youtube.com/watch?v=m0J40Xczj14&list=PLUEPo9QCkRA6TIFI0IUbF8oXvqmORoq4q&index=11&pp=gAQBiAQB>



7. YouTube-Short zu Passwortmanagern:

<https://www.youtube.com/shorts/sK8pTsuOhul>



8. YouTube-Short zu gehacktem Account:

<https://www.youtube.com/shorts/ZBemMqWsBFI>



9. Schritt für Schritt: Zwei-Faktor-Authentisierung für Gaming-Accounts und Konsolen:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweise_r_Checklisten_Flyer/SfS-Anleitung_2FA_Gamingsaccounts_Konsolen.html



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 Quellennachweis 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