

BEGLEITMATERIAL FÜR PÄDAGOGINNEN UND PÄDAGOGEN

CYBERSICHERHEIT FÜR 10- BIS 14-JÄHRIGE



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

Inhalt

Thema 1: Schutzmaßnahmen Smartphone- und App-Sicherheit.....	3
Thema 2: Phishing und Schadsoftware	8
Thema 3: Accountschutz.....	12
Nutzungsbedingungen	17
Impressum	18

Thema 1: Schutzmaßnahmen Smartphone- und App-Sicherheit

Kurzinformation zur Unterrichtseinheit

Fach/Fächer	Fächerübergreifend, Informatik, Wirtschaft
Schulform	Alle Schulformen
Bundesland	deutschlandweit
Jahrgangsstufe(n)	5. bis 8. Klasse
Anzahl Unterrichtsstunden	9

Teaser

Ein Großteil der über 12-jährigen Schülerinnen und Schüler besitzt ein eigenes Smartphone und ist damit im Internet unterwegs. Smartphones machen uns das Leben leichter und oft auch einfach nur Spaß. Damit verbunden sind aber auch viele Herausforderungen: Diebstahl von sensiblen Daten, Phishingversuche oder Schadsoftware sind nur einige wenige. Diese Unterrichtseinheit sensibilisiert früh für grundlegende Schutzmaßnahmen gegen potenzielle Bedrohungen und motiviert Schülerinnen und Schüler, sich tiefergehend mit dem Thema Cybersicherheit zu befassen.

Beschreibung

Die Unterrichtseinheit ist der **erste Themenblock eines Medienpakets zur Cybersicherheit** und legt Grundlagen, auf die in nachfolgenden Einheiten aufgebaut werden kann.

Bei der starken Durchdringung aller Lebensbereiche mit digitalen Anwendungen wird guter Schutz vor Gefahren und Schäden stetig wichtiger. Das gilt für Erwachsene wie für Kinder und Jugendliche, die sich möglicher Gefahren oft nicht bewusst sind. Auch wenn junge Menschen meist von der Technik und ihren Möglichkeiten fasziniert sind und über eine erstaunliche Bedienkompetenz verfügen, bedeutet das nicht, dass sie sich bereits ausreichend mit Schutzmaßnahmen im Internet beschäftigen konnten oder wollten.

Viele bestehende Bildungsmaßnahmen und -initiativen, die sich an Kinder und Jugendliche richten, haben meist eine medienpädagogisch orientierte Ausrichtung, also greifen z. B. Themen wie Cybermobbing, Sexting und Grooming auf. Konkrete Materialien zu Cybersicherheitsthemen richten sich dagegen bisher bzgl. Ansprache und Lebensweltbezüge eher an Erwachsene.

Beide Bereiche – Medienpädagogik und Cybersicherheit – sind eng miteinander verbunden. Die Autorin Silke Müller macht in einem Podcast des BSI eine Bestandsaufnahme, wie sehr Kinder und Jugendliche auf verschiedene Weisen im Netz gefährdet sind und geschützt werden müssen. Gefahren sind zum Beispiel nicht jugendfreie Inhalte im Netz, Fakes von Social-Media-Profilen und Konversationen und Inhalte in WhatsApp-Gruppen. Der Zusammenhang von Social Media und Mobbing ist unabweisbar. Gewaltdarstellungen nehmen zu. All das braucht eine medienpädagogische Antwort und vor allem eine Begleitung der Kinder in der digitalen Welt. Dazu gehört, dass die Kinder und Jugendlichen zum Thema Cybersicherheit qualifiziert werden und die Maßnahmen kennenlernen, mit denen sie sich im digitalen Alltag besser schützen können.

In ihrem auf die Bestsellerliste des Spiegels gelangten Buches „Wer schützt unsere Kinder?“ schlägt die Autorin dazu ein Schulfach „Digitalkunde“ vor. Der Link zum Podcast: [Podcast](#).



Das Medienpaket des BSI zur Cybersicherheit lässt sich als Baustein zur Lösung der umrissenen Probleme verorten. Diese erste Unterrichtseinheit zu „Schutzmaßnahmen“ möchte gezielt die Zielgruppe der Kinder und Jugendlichen für das Thema Cybersicherheit sensibilisieren. Anknüpfungspunkte hierzu findet man in den **Lehrplänen** der Bundesländer für die verschiedenen Schulformen – meist mit Schwerpunkt auf Datensicherheit und Datenschutz. Die Einheit kann aber auch im Rahmen von Projekttagen und -wochen umgesetzt werden.

Didaktisch-methodischer Kommentar

Basierend auf inhaltlich relevanten Materialien zur Cybersicherheit, wie sie das [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](#) herausgibt, arbeitet die Unterrichtseinheit ausgewählte Inhalte in zweierlei Hinsicht auf:



1. Die Inhalte werden **didaktisch** auf wesentliche Kernthemen priorisiert, die der Lebenswelt von Kindern und Jugendlichen entsprechen und mit den Zielen der Lehrpläne korrespondieren. Zugleich werden Inhalte, die teils komplex und schwer greifbar sind, möglichst verständlich dargestellt und ihr Bezug zur Lebenswelt der Altersgruppe wird konkret hergestellt.
2. **Methodisch** sind die Inhalte so weit wie möglich situativ angebunden. Das macht abgeleitete Handlungsempfehlungen und -aufforderungen verständlich und praxisnah. Für eine hohe Wirksamkeit sollen Inhalte weitgehend selbst erarbeitet werden. Die Unterrichtseinheit gibt den Schülerinnen und Schülern grundlegende Informationen, die in unterschiedlichen Aufgabenformaten und -methoden weiterbearbeitet werden. Ziel ist es, den Lernenden handlungsorientiert und alltagsnah zu mehr Kompetenz im Bereich der Cybersicherheit zu verhelfen. Dem Grundlagencharakter der Unterrichtseinheit entsprechend wird dabei im Wesentlichen die Kompetenz erworben, das eigene Smartphone grundständig sicher einzurichten.

Ausgangspunkt der Unterrichtseinheit sind **Situationen aus der Lebenswelt** der Schülerinnen und Schüler. Um Kinder und Jugendliche in ihrer Lebenswelt abzuholen, legt das Medienpaket den Fokus insbesondere auf das in der Altersgruppe meistgenutzte Endgerät „Smartphone“ bzw. damit verbundene mobile Anwendungen.

Die Unterrichtseinheit startet mit zwei Beispielen, die später mehrfach aufgegriffen werden. Ihre anfängliche Auswertung mündet zum einen darin, zu reflektieren, welche **Ziele Cyberkriminelle** verfolgen könnten. Zum anderen führen sie zur Frage, **wie es technisch möglich ist**, Zugriff auf fremde Geräte und Accounts zu erhalten. Über einen kurzen Umriss der Funktionsweise des Internets wird deutlich, dass zum einen das Gerät vor Fremdzugriff und Schadsoftware geschützt werden muss. Zum anderen gilt es, die auf dem Gerät laufenden Anwendungen (= Apps) sicher zu nutzen.

So vorbereitet werden die **konkreten Schutzmaßnahmen** plausibel, die in der Unterrichtseinheit nun folgen: regelmäßige Updates, Bildschirmsperre, Accountsicherung, Vorsicht bei offenen WLAN-Netzwerken und Bluetooth sowie Backups zur Datensicherung. Die Unterrichtseinheit schließt mit dem sicheren Umgang mit Apps, also z. B. dem Schutz von Accounts, Installieren von Updates und dem gezielten Einstellen entsprechender Berechtigungen.

Beschreibung zu den Arbeitsblättern

Arbeitsblatt 1: Über ein Beispiel wird anschaulich zu den Fragen hingeführt, was Cyberkriminelle zu erreichen versuchen und wie sie auf fremde Geräte und in Anwendungen gelangen könnten. Exemplarisch werden Risiken der Nutzung von Social-Media-Plattformen aufgezeigt, in denen sich Schülerinnen und Schüler schon früh bewegen.

Arbeitsblatt 2: In groben Zügen wird die Funktionsweise des Internets soweit erklärt, dass ersichtlich wird, warum Netze wesentlicher Einfallstor für Cyberkriminelle sind. Das Zusammenspiel von Internet und Apps sowie die Bedeutung von Updates wird verdeutlicht.

Arbeitsblatt 3: Es werden fünf Basismaßnahmen zum Geräte- und Datenschutz handlungsorientiert eingeführt – Updates, Bildschirmsperre, Accountschutz, sicherer Umgang mit WLAN und Bluetooth, Datenbackups.

Arbeitsblatt 4: Es werden drei Maßnahmen zum sicheren Umgang mit Apps behandelt – Accountschutz für Apps, die kompetente Auswahl von Apps und die gezielte Zuweisung von Berechtigungen für Apps.

Kompetenzen

Fachkompetenz

Die Schülerinnen und Schüler

- verstehen das Konzept des Internets als ein Netz, das alle Teilnehmenden technisch verbindet.
- wissen, dass an allen Zugangs- und Schnittstellen dieses Netzes potenzielle Möglichkeiten für ein unberechtigtes Eindringen bestehen.
- verstehen, dass neben unberechtigtem Eindringen in Geräte und in Anwendungen auch von den auf das Smartphone heruntergeladenen Apps Gefahren ausgehen bzw. diese als Einfallstor dienen können.

Medienkompetenz

Die Schülerinnen und Schüler

- kennen die Basisschutzmaßnahmen für Smartphones, Accounts und Apps.
- erweitern ihre Recherchefähigkeit hinsichtlich Cybersicherheitsthemen.
- verstehen, was Berechtigungen sind und was sie bewirken, und wissen, dass sie bei den jeweiligen Apps gezielt erteilt bzw. entzogen werden können.

Sozialkompetenz

Die Schülerinnen und Schüler

- stärken ihre Sensibilität hinsichtlich unangemessener Kommunikation und Fehlverhalten im Netz.
- bauen ihre Fähigkeit aus, auch voneinander zu lernen sowie sich eigenständig Inhalte zu erschließen.

Weiterführende Links

1. Videoreihe und Sicherheitshinweise des BSI zum Schutz von Smartphones und Tablets:
<https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basischutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/Smartphone-Sicherheit/smartphone-sicherheit.html>
2. Smartphone und Tablet effektiv schützen:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Basischutz-fuer-Computer-Mobilgeraete/Schutz-fuer-Mobilgeraete/schutz-fuer-mobilgeraete_node.html
3. Wegweiser für den digitalen Alltag – Smartphone, Tablet & Co sicher nutzen:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Brosch_A6_Mobilkommunikation.html
4. Schritt für Schritt automatische Updates einrichten:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/SfS-Anleitung_automatische_Updates.html
5. Schritt für Schritt zur Datensicherung:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/SfS-Anleitung_Datensicherung.html
6. YouTube-Short zum Thema Backups:
<https://www.youtube.com/shorts/xTOVsPgXQVU>
7. YouTube-Short zum Thema Updates:
<https://www.youtube.com/shorts/Dhs8xhtB8jE>

8. YouTube-Short zum Thema Smartphone absichern 1:

<https://www.youtube.com/shorts/cPfzL0KWB94>



9. YouTube-Short zum Thema Smartphone absichern 2:

<https://www.youtube.com/shorts/XEN05M5bZVo>



10. YouTube-Short zum Thema Smartphone-Schutz:

<https://www.youtube.com/shorts/9-rXpQxixOQ>



11. YouTube-Short zum Thema Jugendschutz Smartphone:

https://www.youtube.com/shorts/a3Y_zqy_S1M



Thema 2: Phishing und Schadsoftware

Kurzinformation zur Unterrichtseinheit

Fach/Fächer	Fächerübergreifend, Informatik, Wirtschaft
Schulform	Alle Schulformen
Bundesland	deutschlandweit
Jahrgangsstufe(n)	5. bis 8. Klasse
Anzahl Unterrichtsstunden	8

Teaser

Grundlegende Schutzmaßnahmen und Accountschutz sind unerlässlich, halten aber kriminelle Akteure im Internet nicht uneingeschränkt fern. Beim Phishing versuchen Angreifer, ihre Zielperson zur Preisgabe von sensiblen Daten zu verleiten oder Schadsoftware zu verbreiten und damit Geräte zu infizieren. In dieser Unterrichtseinheit geht es darum, solche Gefahren und deren Merkmale zu erkennen, sich zu schützen und zu wissen, was im Schadensfall zu tun ist.

Beschreibung

Die Unterrichtseinheit ist der **zweite Themenblock des Medienpakets zur Cybersicherheit**. Sie bearbeitet Schutzmaßnahmen, die neben dem Basisschutz gleichwertig wichtig, aber anders angelegt sind. Während die Basisschutzmaßnahmen Barrieren gegen Angreifer bieten oder für technische Sicherheit sorgen, können **Phishing-Versuche** und die Infektion mit **Schadprogrammen** nicht gänzlich von vornherein vereitelt werden. Stattdessen muss man aufmerksam sein und sie – bildlich gesagt – ins Leere laufen lassen. Der erste Schritt für den Schutz ist, der möglicherweise eigenen Betroffenheit wachsam gegenüberzustehen und sich der Gefahren bewusst zu sein.

Deshalb beginnt die Unterrichtseinheit mit einem fiktiven Beispiel einer verdächtigen E-Mail aus der Lebenswelt der Jugendlichen – aus dem Bereich Online-Spiele. Daran anknüpfend sprechen die Schülerinnen und Schüler über eigene Erfahrungen mit Phishing.

Im Kern vermittelt die Unterrichtseinheit, wie man verdächtige Nachrichten erkennt und welche Absichten Angreifer damit verfolgen. Da es mehrere Unterarten von Phishing und viele Formen von Schadsoftware gibt, können diese nur kurz angesprochen werden. Danach fokussiert sich die Unterrichtseinheit darauf, dass in den meisten Fällen ähnliche Prinzip zu erläutern und konzentriert sich auf grundlegende und vor allem auch praktikable Handlungsempfehlungen zum Schutz.

Im Mittelpunkt steht der Appell, keinesfalls auf die in den Nachrichten enthaltenen Anforderungen einzugehen und zum Beispiel keine Call-to-Action-Buttons oder Links anzuklicken und keine Downloads auszuführen. Dazu gibt es konkrete Tipps auf jedem Arbeitsblatt.

Zum Schluss wird das Thema **Identitätsdiebstahl** vertieft. Dies erfolgt anhand eines Beispiels mit einem ziemlich überraschenden Schadensszenario zum Online-Shopping. Der Hacker schädigt einen

Dritten finanziell über die gehackten Mail- und Social-Media-Konten eines Jugendlichen und eine nicht erkannte Fake-Nachricht. Das führt vor Augen, wie auch Jugendliche von Finanzbetrügerei betroffen sein können.

Zusätzlich zu dieser Unterrichtseinheit können die Schülerinnen und Schüler in der interaktiven Übung „Stationen WhatsApp-Nachricht“ den „unsichtbaren Weg“ digitaler Kommunikation anhand der durchlaufenden Stationen einer WhatsApp-Nachricht entdecken. Dazu begleiten die Schülerinnen und Schüler den Weg einer Nachricht aus Deutschland bis nach Australien anhand einer Bildsequenz, die in die korrekte Reihenfolge gebracht werden muss. Die interaktive Übung kombiniert dabei kurze Erklärungen und Visualisierungen, um technische Abläufe verständlich und greifbar zu machen.

Didaktisch-methodischer Kommentar

Der Inhalt dieser Unterrichtseinheit rückt vor allem das eigene Verhalten in den Vordergrund – nämlich den Angriff zu erkennen und den Forderungen des Angreifers nicht nachzukommen. Das gilt auch für Schadsoftware, wenn sie getarnt als Anhang oder Link in Nachrichten auf das Gerät des Opfers geschickt wird und der User die Schadsoftware beim Download oder Anklicken unbemerkt installiert.

Die **didaktische Reihung des Lernstoffs** ergibt sich bei dem Thema wie folgt: Die Schülerinnen und Schüler werden für die Gefahren sensibilisiert und gewinnen die Einsicht, dass auch sie betroffen sein können. Sie sollen lernen, dass sie aufmerksam sein müssen, um verdächtige Nachrichten zu identifizieren und Schutzmaßnahmen kennen und nutzen sollten. Zudem sollen sie lernen, was im Ernstfall zu tun ist. Dieses Wissen wird zunächst für **Phishing** erarbeitet, wo es darum geht, nicht auf Betrugsversuche und Forderungen eines Absenders einzugehen, der an Daten gelangen will. Dann folgt die Bearbeitung des Themas **Schadsoftware**. Hier muss die Interaktion mit verdächtigen Inhalten und das Herunterladen von getarnten schädlichen Dateien vermieden werden. Schadsoftware kann über Dateianhänge oder infizierte Webseiten (Link in der Nachricht) verbreitet werden und auf das eigene Geräte gelangen. Beide Themen bilden die Grundlagen, die abschließend durch das Thema **Identitätsdiebstahl** noch vertieft werden.

Schadsoftware kann natürlich auch über andere Wege auf Smartphones oder Computer gelangen, wie es in der ersten Unterrichtseinheit thematisiert wird.

Methodisch ist auch diese Unterrichtseinheit so angelegt, die Inhalte weitgehend selbstständig erarbeiten zu lassen. Auf jedem Arbeitsblatt erschließen sich die Schülerinnen und Schüler nach einer knappen Einführung oder einem Beispiel die Inhalte aus Videos und Arbeitstexten des BSI. Daran knüpfen jeweils Fragestellungen und Aufgaben an. Zum einen erstellen sich die Lernenden darüber schon selbst Handlungstipps, zum anderen gibt es am Ende des Arbeitsblatts kurze, zusammenfassende Praxistipps.

Diese Arbeitsweise begründet sich dreifach. Sie sorgt lernpsychologisch für hohe Wirksamkeit. Den Schülerinnen und Schülern werden authentische Fachinformationen des BSI auf aktuellem Stand zugänglich gemacht. Nicht zuletzt wird eingeübt, was alle User digitaler Anwendungen zunehmend benötigen: sich in der schnell weiterentwickelnden digitalen Welt kontinuierlich relevante Informationen selbst zu erschließen.

Beschreibung zu den Arbeitsblättern

Arbeitsblatt 1: Jana und ihre Freundin Hannah analysieren eine verdächtige Gewinnspiel-Mail in einem Dialog, der erste Impulse liefert, bevor die Schülerinnen und Schüler eigene Erfahrungen im Plenum einbringen und diskutieren.

Arbeitsblatt 2: Das Prinzip und die Ziele von Phishing-Versuchen werden erläutert, Varianten wie Smishing, Quishing und Vishing kurz vorgestellt und anschließend Erkennungsmerkmale sowie Schutzmöglichkeiten erarbeitet.

Arbeitsblatt 3: Die verschiedenen Arten von Schadprogrammen werden unterschieden, beispielhaft Möglichkeiten benannt, wie sie auf Geräte gelangen und mögliche Schäden erläutert.

Arbeitsblatt 4: Ein Online-Shopping-Beispiel zeigt, wie Identitätsdiebstahl zum Geldbetrug führt. Abschließende Tipps fassen die Einheit zusammen.

Kompetenzen

Fachkompetenz

Die Schülerinnen und Schüler

- wissen, dass über E-Mail, SMS und weitere Kommunikationskanäle Nachrichten mit betrügerischen Absichten breit gestreut und oft willkürlich versendet werden und auch sie die Empfänger solcher Nachrichten sein können.
- verstehen, dass sie sich über den Basisschutz ihres Geräts und den Accountschutz hinaus auch gezielt gegen Phishing-Nachrichten absichern müssen.
- wissen, dass Phishing, Smishing, Quishing und Vishing zu Betrugszwecken genutzt wird und können wesentliche Formen von Schadsoftware unterscheiden.

Medienkompetenz

Die Schülerinnen und Schüler

- verstehen, dass Phishing (und vergleichbare Nachrichten) sie über gängige Kommunikationswege erreichen kann und sie zu einer Handlung veranlassen zu versuchen, über die der Absender z. B. an sensible Daten kommt. Diese können in der Folge für unterschiedliche betrügerische Zwecke genutzt werden.
- kennen wesentliche Kriterien, mit denen sich Phishing und andere Formen erkennen lassen.
- wissen, anhand welcher Merkmale sie betrügerische Nachrichten erkennen und mit welchen Maßnahmen sie sich schützen können.

Sozialkompetenz

Die Schülerinnen und Schüler

- verstehen, welche persönlichen Folgen es haben kann, wenn sich jemand durch Identitätsdiebstahl als ein anderer im Netz ausgibt und zum Beispiel Unwahrheiten über den Geschädigten verbreitet oder ihn finanziell schädigt.
- wissen, dass persönliche Daten zur Privatsphäre gehören, in die kein Fremder und auch sonst niemand unerlaubt Einblick haben soll und darf.

Weiterführende Links

1. Phishing - how much is the phish!?
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html
2. Wie schützt man sich gegen Phishing?
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Schutz-gegen-Phishing/schutz-gegen-phishing_node.html
3. Wie erkenne ich Phishing-E-Mails und -Webseiten?
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Wie-erkenne-ich-Phishing-in-E-Mails-und-auf-Webseiten/wie-erkenne-ich-phishing-in-e-mails-und-auf-webseiten_node.html
4. Phishing – Checkliste für den Ernstfall:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweiser_Checklisten_Flyer/Checkliste_BSI_ProPK_Phishing.pdf?__blob=publicationFile&v=4
5. Schadprogramme – Fragen & Antworten:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/schadprogramme_node.html
6. So schützen Sie sich vor digitalem Identitätsdiebstahl und gehackten Accounts:
https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html
7. „Update verfügbar/Ein Podcast des BSI #29: Phishing, Smishing, Quishing & Co. – Das BKA ermittelt“:
<https://www.youtube.com/watch?v=KJOTIofG4UI&list=PLUEPo9QCKRA6TIFI0IUbF8oXvqmORoq4q&index=23>
8. „Update verfügbar/Ein Podcast des BSUI #49: Alarmstufe Rot für private Daten – Schutz vor Identitätsdiebstahl“:
<https://www.youtube.com/watch?v=ALeJN96zEN8&t=2s>

Thema 3: Accountschutz

Kurzinformation zur Unterrichtseinheit

Fach/Fächer	Fächerübergreifend, Informatik, Wirtschaft
Schulform	Alle Schulformen
Bundesland	deutschlandweit
Jahrgangsstufe(n)	5. bis 8. Klasse
Anzahl Unterrichtsstunden	8

Teaser

Schülerinnen und Schüler nutzen auf ihren Smartphones eine Vielfalt von Anwendungen über das Internet. Sie haben gelernt, grundlegende Schutzmaßnahmen gegen potenzielle Bedrohungen in der digitalen Welt auf ihren Geräten einzurichten. Nun erfahren sie in dieser Unterrichtseinheit mehr dazu, wie sie gezielt und effektiv ihre Accounts schützen können. Mit dem Accountschutz wird die Barriere gegen einen fremden und nicht legitimierten Zugriff auf ihre sensiblen Daten aufgebaut. Das ist entscheidend, um den Missbrauch dieser Daten zu verhindern. Die Maßnahmen umfassen starke Passwörter und als weitere Sicherungsverfahren Passkey und eine Zwei-Faktor-Authentisierung bei der Anmeldung.

Beschreibung

Die Unterrichtseinheit ist der **dritte Themenblock des Medienpakets zur Cybersicherheit** und vertieft zuvor erworbene Grundlagen. Die Schülerinnen und Schüler bauen damit ihre Kenntnisse zur Accountsicherung weiter aus.

Vorherige grundlegende Themen haben sich damit befasst, das Smartphone als Gerät abzusichern, sich in sicheren Netzen zu bewegen und über Updates für aktuelle Software ohne bekannte Sicherheitslücken zu sorgen. Damit werden schon viele Versuche vereitelt, auf fremde Geräte einzudringen.

Hacker und Cyberkriminelle suchen jedoch noch andere Wege, um an fremde Daten zu gelangen. So versuchen sie häufig, Anmeldedaten von Accounts in Erfahrung zu bringen. Gelingt ihnen dies, haben sie Zugriff auf die sensiblen Daten in der jeweiligen Anwendung. Deshalb ist es unerlässlich, jeden Account bestmöglich zu schützen. Da nur Verfahren genutzt werden können, die der Diensteanbieter anbietet, vermittelt die Unterrichtseinheit betreffende Verfahren. Im einfachsten Fall ist das eine Anmeldung mit Benutzername und Passwort, wo der User nur die Möglichkeit hat, möglichst starke Passwörter zu verwenden. Auch muss für jeden Account ein anderes Passwort genutzt werden. Um die darüber anwachsende Zahl von Passwörtern zu beherrschen, helfen Passwortmanager. Sichere Verfahren sind hingegen Passkeys und 2FA. Sie werden erklärt, ihre Funktionsweise verständlich gemacht und die grundlegenden Schritte ihrer Verwendung werden vermittelt.

Didaktisch-methodischer Kommentar

Kinder und Jugendliche unterschätzen Gefahren leicht. Sie können sich vielfach nicht wirklich vorstellen, warum ausgerechnet sie von einem Cyberangriff betroffen sein sollten. Da die Diensteanbieter die Anmeldung mit Nutzernamen und Passwort aber verlangen, müssen sie ihre Accounts natürlich sichern und beschränken sich dann aber meist auf sehr einfache Passwörter (was Erwachsene übrigens oft auch so machen). Die Unterrichtseinheit setzt deshalb **didaktisch** an zwei Punkten an:

- Einleitend wird herausgearbeitet, welche Daten aus Accounts abgegriffen werden könnten und was die Kinder und Jugendlichen für sich schützenswert finden. So bleibt Schutzwürdigkeit nicht auf dem Niveau abstrakter Begriffe wie Betrug, Diebstahl, Erpressung, sondern wird auf konkretere, auf Beispiele bezogene Schutzwünsche der Schülerinnen und Schüler heruntergebrochen und anschaulich gemacht.
- Die anfangs vielleicht als zu komplex und umständlich empfundenen Schutzverfahren werden auf einfache Weise in ihrer Wirkung erklärt. Es wird dargelegt, welchen Grad an Sicherheit sie bieten. So werden sie als nützlich und „machbar“ wahrgenommen und die Motivation gesteigert, sie auch tatsächlich anzuwenden.

Methodisch ist die Einheit so angelegt, die Inhalte weitgehend selbstständig erarbeiten zu lassen. Auf jedem Arbeitsblatt erschließen sich die Schülerinnen und Schüler nach einem kurzen Beispiel und bewusst knapper thematischer Einführung den Wissensstoff aus Videos und Arbeitstexten des BSI. Daran knüpfen jeweils Fragestellungen und Aufgaben an. Für den Transfer in die Praxis gibt es am Ende jeden Arbeitsblatts kurze, nicht überfordernde Praxistipps.

Diese Arbeitsweise begründet sich dreifach. Sie sorgt lernpsychologisch für hohe Wirksamkeit. Den Schülerinnen und Schülern werden authentische Fachinformationen des BSI auf aktuellem Stand zugänglich gemacht. Nicht zuletzt wird so eingeübt, was alle User digitaler Anwendungen zunehmend benötigen: sich in der schnell weiterentwickelnden digitalen Welt kontinuierlich relevante Informationen selbst zu erschließen.

Der **fachliche Inhalt** umfasst Passwörter, Passwortverwaltung, Passkeys und Zwei-Faktor-Authentisierung (2FA). Der Funktionsweise und die grundlegende Handhabung werden jeweils erklärt. Je nach Gerät und System variiert die Einrichtung im Einzelnen. Hier kann ggf. noch Hilfestellung gegeben und die Schülerinnen und Schüler angeregt werden, sich für häufig genutzte Dienste zum Beispiel Passkeys einzurichten. Am Ende soll auch klar werden, dass sich die Schülerinnen und Schüler zwischen „nur Passwort“ plus 2FA oder Passkey als passwortlose Alternative entscheiden sollten. Das verbindet sich mit der Erkenntnis, dass vom Diensteanbieter jeweils angebotene höhere Verfahren auch genutzt werden sollten, um den Account bestmöglich zu schützen.

Beschreibung zu den Arbeitsblättern

Arbeitsblatt 1: Ein Einführungsbeispiel beschreibt ein realistisches Hacken eines Social-Media-Accounts. In einem Brainstorming sammeln die Schülerinnen und Schüler, was sie selbst für schützenswert erachten und werden darüber für die Wichtigkeit der Accountsicherung sensibilisiert.

Arbeitsblatt 2: Einfache und starke Passwörter werden unterschieden und die Regeln für starke Passwörter vermittelt. Lokale und cloudbasierte Passwortmanager werden als Helfer vorgestellt.

Arbeitsblatt 3: Die Funktionsweise von Passkeys wird erläutert und plausibel gemacht, warum sie sicherer und komfortabler sind. Die grundlegenden Schritte beim Einloggen mit Passkey werden gezeigt.

Arbeitsblatt 4: Der prinzipielle Ablauf einer Anmeldung mit 2FA wird gezeigt und die Sicherheit dieses Verfahrens verständlich gemacht, wenn dabei ein starkes Passwort als ein Faktor dient. Es wird außerdem auf Material verwiesen, welche Konsolen sich bereits mit 2FA sichern lassen.

Kompetenzen

Fachkompetenz

Die Schülerinnen und Schüler

- kennen die Regeln für starke Passwörter und können selbst welche bilden.
- verstehen die Funktionsweise von Passkeys und kennen die dafür überall grundlegend gleichen Anmeldeschritte.
- wissen, wie die beiden Faktoren von 2FA bei der Anmeldung ineinandergreifen.

Medienkompetenz

Die Schülerinnen und Schüler

- können reflektieren, welche Inhalte ihrer Accounts ihnen persönlich wichtig sind und haben das Bewusstsein ausgebildet, dass sie diese schützen müssen.
- wissen, dass sie viele und komplexe Passwörter mit einem Passwortmanager verwalten können, der über ein Master-Passwort oder Passkeys gesichert wird.
- wissen, dass nur Anmeldeverfahren möglich sind, die vom Diensteanbieter angeboten werden und dass sie sich immer für das Verfahren mit der höchsten Sicherheit entscheiden sollten.

Sozialkompetenz

Die Schülerinnen und Schüler

- bauen ihre Fähigkeit aus, auch voneinander zu lernen und sich eigenständig Inhalte zu erschließen.

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_tB1Ylzo0o



6. Podcast-Folge zu Passkeys:

<https://www.youtube.com/watch?v=m0J40Xczj14&list=PLUEPo9QCkRA6TIFi0IUbF8oXvqmORoq4q&index=12>



7. #39 - Wie schützen wir Kinder und Jugendliche im digitalen Alltag?

https://www.youtube.com/watch?v=S_IsNxODiXc&list=PLUEPo9QCkRA6TIFi0IUbF8oXvqmORoq4q&index=12



8. YouTube-Short zu Passwortmanagern:

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



9. YouTube-Short zu gehacktem Account:

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



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



Nutzungsbedingungen

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

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