

FÜR PÄDAGOGINNEN UND PÄDAGOGEN

SMARTPHONE- UND APP-SICHERHEIT



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

Ablauf der Unterrichtseinheit

Phase	Inhalt	Sozial- / Aktionsform
Arbeitsblatt 1 Cybersicherheit und was sie uns angeht (ca. 2 U-Std.)	Die Einführung erfolgt durch kurze Fallbeispiele mit der Schülerin Hannah und ihrem Bruder Olli als Protagonisten, die unterschiedliche Anknüpfungspunkte zur Identifikation bieten: Hannah wird später ein neues Smartphone einrichten. Ollis Social-Media-Account wurde gehackt. Ollis Fall dient als Grundlage für eine Gruppenarbeit, in der die grundlegende Bedeutung von Cybersicherheit erarbeitet wird. Die Ergebnisse werden auf einem Plakat festgehalten. Um Schülerinnen und Schüler in ihrer Medien-Erfahrungswelt zu erreichen, steht Social Media im Vordergrund. Das Hacken des Accounts bietet aber auch Anknüpfungspunkte für das Erörtern weiterer Gefahrenquellen.	Lesen des Arbeitsblatts in Einzelarbeit, Gruppenarbeit, Ergebnispräsentation, Diskussion im Plenum, Plakaterstellung
Arbeitsblatt 2 Technische Seite – Internet und Apps (ca. 2 U-Std.)	Das Arbeitsblatt • erklärt in Grundzügen die Funktionsweise des Internets und darüber auch mögliche missbräuchliche Zugriffe auf Endgeräte aus der „Ferne“ • erläutert, dass sowohl die Schnittstellen zum Smartphone als auch die darauf installierten Apps geschützt werden müssen. Für den Schutz sind sowohl Hersteller und Anbieter verantwortlich (durch sichere Dienste, die die Endgeräte durch Updates auf dem aktuellen sicheren Stand halten) als auch die User selbst, die die Updates installieren müssen. Weitere konkrete Maßnahmen schließen sich auf dem nächsten Arbeitsblatt an.	Lesen des Arbeitsblatts in Einzelarbeit, Paararbeit, Erklärvideo schauen und im Plenum besprechen
Arbeitsblatt 3 Wesentlicher Basisschutz für Smartphones (2 U-Std.)	Das Arbeitsblatt erläutert Basisschutzmaßnahmen in Form von handlungsauffordernden Tipps. Diese werden an kurzen Beispielen erläutert: • Updates – regelmäßig nutzen • Bildschirmsperre – sich für eine Variante entscheiden und diese aktivieren	Lesen des Arbeitsblatts in Einzelarbeit, Erklärvideo schauen, in Partnerarbeit Einstellungen des eigenen Smartphones prüfen, von Mitschülerinnen und -schülern lernen („Peer-to-Peer“-Vermittlung), Plakaterstellung

	• Accounts auf Schutzmaßnahmen prüfen – Mindestsicherung mit Benutzername und Passwort • „Drahtlosschnittstellen“ – offenes WLAN und Bluetooth mit Vorsicht nutzen und nur bei Bedarf aktivieren • Backups gegen Datenverluste durchführen	
Arbeitsblatt 4 Apps sicher nutzen (3 U-Std.)	Neben den Basisschutzmaßnahmen auch Apps sicher nutzen • nur seriöse Apps herunterladen – nach einem Kriterienkatalog (aus BSI-Unterlagen) • Berechtigungen für Apps gezielt zuweisen • Accounts absichern Das Arbeitsblatt schließt mit einer interaktiven Übung, die eine Gesamtzusammenfassung generiert. Für dieses Arbeitsblatt sind 3 U-Std. veranschlagt, um sich ausführlich mit dem Kriterienkatalog für sichere Apps auseinandersetzen zu können.	Lesen des Informationstextes in Einzelarbeit, Partnerarbeit, Unterrichtsgespräch, interaktive Übungen „Berechtigungen zuweisen“ und „Abschlussquiz mit Zusammenfassung“ in Einzelarbeit, ggf. Plakaterstellung

Hintergrundinformationen zum Thema der Einheit und Lösungshinweise zu den Aufgaben

Einordnung der Unterrichtseinheit

Die Unterrichtseinheit verfolgt **fächerübergreifend** das Ziel, Schülerinnen und Schüler zum sicheren Umgang mit dem Smartphone anzuleiten. Damit die Jugendlichen weder Opfer von Datenmissbrauch werden noch sich als Täter betätigen, bedarf es Aufklärung von zwei Seiten: medienpädagogische Aufklärung und Vermittlung von Schutzmaßnahmen. Die Unterrichtseinheit fokussiert sich auf Schwerpunkt 2, also die Vermittlung von Cybersicherheit. Sie umfasst im Kern Schutzmaßnahmen technischer Natur.

Bei den meisten Jugendlichen ist das Smartphone sehr positiv besetzt und ein unentbehrlicher Teil ihres Alltagslebens. Zugleich sind sie sich häufig möglicher Risiken wie Datenmissbrauch oder dem unberechtigten Teilen von Texten, Bildern und Videos nicht bewusst. Damit sie entsprechende Schutzmaßnahmen akzeptieren und nicht als einschränkend empfinden, müssen diese für sie sinnstiftend sein und ihre Funktionen verstanden werden. Weder ein verordneter Maßnahmenkatalog noch bloße Appelle wären sonderlich hilfreich.

Darauf ist das **methodische Vorgehen** ausgerichtet. Es erfolgt ein situativer Zugang zu den Themen über Beispiele. Maßnahmen werden abgeleitet, erklärt und dann handlungsorientiert formuliert.

Zu den einzelnen Arbeitsblättern

Arbeitsblatt 1: Cybersicherheit und was sie uns angeht

Arbeitsblatt 1 setzt beim Risikobewusstsein der Schülerinnen und Schüler an, das individuell unterschiedlich ausgeprägt sein wird. Kern ist eine Gruppenarbeit, bei der herausgearbeitet wird, wieso der Schutz des Smartphones wichtig ist und wie er gelingen kann. Dabei ist kein fester Katalog von Risiken und Gefahren angestrebt, weil dieser in jeder Klasse etwas anders ausfallen wird. Indem die Schülerinnen und Schüler zusammentragen, was ihnen selbst wichtig ist, werden sie motiviert, sich um geeignete Schutzmaßnahmen zu kümmern.

Der Einstieg erfolgt über **2 miteinander verwobene Fallbeispiele**, die im Verlauf der Unterrichtseinheit wiederholt aufgegriffen werden. Die beiden Protagonisten Hannah und Olli bieten unterschiedliche Identifikationspersonen: Hannah ist eine Smartphone-Nutzerin, die technikaffin und insgesamt bereits gut informiert ist. Sie hat im Hinblick auf ihre Smartphone-Nutzung differenzierte Interessen. Sie wartet auf ihr neues Smartphone, das sie so einrichten möchte, dass es gut geschützt ist. Ihr Interesse an präventiven Schutzmaßnahmen wird in Arbeitsblatt 3 aufgegriffen. Vorab wird jedoch erst einmal die Brücke zu ihrem Bruder Olli geschlagen, der eine negative Erfahrung im Netz macht (Quelle: [BSI - Identitätsdiebstahl in Social Media Kanal](#)). Diese Vorgehensweise liefert die nötige Verständnisgrundlage, um darauf aufbauend Handlungsempfehlungen zu erarbeiten.



Hannah hat wahrgenommen, dass ihr Bruder Olli Merkwürdiges im Netz verbreitet und spricht ihn an. Schnell stellt sich heraus, dass Ollis Social Media-Account gehackt worden sein muss. An diesen Fall wird die erste Gruppenarbeit angeknüpft. Die Schülerinnen und Schüler sind aufgefordert, das möglicherweise entstandene Schadenszenario herauszuarbeiten und zusammenzufassen. Das kann bis hin zu Aspekten von Cyberkriminalität ausgeführt werden. Olli hat natürlich ein Interesse an Aufklärung, wie das passiert sein kann und was er zukünftig gegen einen solchen Angriff tun kann.

Zur Ergebnissicherung der daran anschließenden Gruppenaufgabe und des Erfahrungsaustauschs wird die gemeinsame Gestaltung eines **Klassen-Plakats** vorgeschlagen. In weiteren Arbeitsphasen können ebenfalls Plakate entstehen, sodass das Gesamtergebnis der Unterrichtseinheit als kleine Wandzeitung dokumentiert wird. Alternativ ist eine digitale Form der Dokumentation denkbar, wie zum Beispiel die Gestaltung eines E-Books oder einer Projekt-Webseite.

Als Arbeitshilfe sind Satzstrukturen in zwei Formulierungsvarianten angeführt. **Anregungen zu Aspekten**, die in die Diskussion eingebracht werden können, wenn sich das Brainstorming festfährt oder zu einseitig wird, sind etwa:

„Wir wollen unser Smartphone vor Schadsoftware schützen, damit Hacker ...

- nicht die nur für unsere Freunde bestimmten Messages lesen und weiterverbreiten.“
- sich nicht für uns ausgeben.“
- keine Anschriften/Kontakte stehlen.“
- nicht unsere Daten kopieren.“
- nicht unser Standortprofil abzapfen.“
- nicht unsere Identität für Betrugereien verwenden.“
- nicht in unserem Namen im Internet shoppen/einkaufen.“
- nicht unsere Passwörter auslesen.“

- nicht unsere App-Berechtigungen manipulieren.“
- nicht unsere Alarm-Funktionen ausschalten.“
- unsere Termine nicht faken.“

Oder: „Wir wollen unser Smartphone schützen, um ...

- unsere Privatsphäre für uns zu behalten.“
- keine Belästigungen zu erfahren.“
- nicht gemobbt zu werden.“
- finanzielle Schädigung, zum Beispiel beim Online-Shopping, zu vermeiden.“

Meist handelt es sich nicht um gezielte Angriffe auf einzelne Menschen. Stattdessen gehen Kriminelle nach dem Gießkannenprinzip vor, sodass es immer ein paar Treffer gibt.

Da Ollis Geschichte Bezug zur Nutzung Sozialer Netzwerke nimmt, gibt es am Ende des Arbeitsblatts noch eine kurze Zusammenstellung potenzieller Risiken, über die man hinsichtlich der Nutzung von Social Media Bescheid wissen sollte. Mehr lässt sich in einem Informationsblatt des BSI nachlesen, auf das im Arbeitsblatt verwiesen wird ([BSI - Soziale Netzwerke – vor der Anmeldung](#)).



Arbeitsblatt 2: Die Technische Seite – Internet und Apps

Das Arbeitsblatt knüpft in Bezugnahme auf Ollis Fall daran an, dass Schutzmaßnahmen nötig sind, weil abgegriffene persönliche Daten für kriminelles Vorgehen im Netz unterschiedlich missbraucht werden können. Anschließend geht es darum, wie Cyberkriminelle grundsätzlich vorgehen. Der Fokus liegt auf **zwei zentralen Fragen**:

- Wie kann jemand Zugriff auf ein fremdes Smartphone bekommen?
- Wie kann er darauf die Anwendungen für sich nutzen und Accounts übernehmen?

Der **Zugang zum fremden Smartphone** erfolgt – zu einem kleinen Teil – in der Umgebung der Opfer, wenn ihr ungesichertes Smartphone in die Hände von Tätern fällt. Der überwiegende Teil der Fälle vollzieht sich jedoch durch den Zugang über das Internet bzw. ungesicherte Schnittstellen, wie WLAN oder Bluetooth. Die Schülerinnen und Schüler sollen diesen Weg verstehen. Dazu wird die Funktionsweise des Internets vereinfacht erklärt. In einer Aufgabe überlegen die Lernenden, welchen Weg ein Kommentar in einem sozialen Netzwerk vom Verfassen bis zum Erscheinen durchläuft. Damit andere Zuschauer oder auch man selbst beispielsweise einen Kommentar unter einem Video auf TikTok sehen kann, werden folgende Stationen durchlaufen (schemenhaft): Der Kommentar verlässt das Smartphone des Absenders und gelangt in ein lokales Netzwerk (Funkmast/WLAN-Router), dann zum Internet-Service-Provider und in die globale Internet-Infrastruktur. Der Kommentar geht auf den TikTok-Server, dann wieder in die globale Internet-Infrastruktur, zum Internet-Service-Provider des Zuschauers, ins lokale Netzwerk und schließlich auf das Smartphone des Zuschauers. Die gesamte Übertragung, Verarbeitung und Anzeige des Kommentars erfolgt in der Regel in weniger als einer Sekunde.

Als **Kernerkenntnis** sollte formuliert werden, dass der Weg angreifbar ist. Das genaue „Wie“ lässt sich im gegebenen Rahmen nicht vermitteln. Die Jugendlichen werden aber verstehen, dass für Sicherheit **erstens die Diensteanbieter** sorgen und **zweitens wir User** aktiv sein müssen. Diensteanbieter erkennen immer wieder Sicherheitslücken in ihrer Software, beseitigen diese und bieten Updates an. Außerdem ist im Internet vieles nicht privat, auch wenn es sich so anfühlt! Kommentare sind oft

öffentlich sichtbar, je nachdem, wie das Profil eingestellt ist. Manche Plattformen speichern alles – auch dann, wenn es gelöscht wird. Und: Apps verdienen oft Geld mit Daten.

Diese Aufgabe lässt sich auch sehr gut mit einem Einstiegsgespräch zum Thema „Privatsphäre“ verbinden. Ergänzend können reale Beispiele von TikTok/YouTube-Kommentaren anonymisiert gezeigt und diskutiert werden. Ziel ist, ein Bewusstsein dafür zu schaffen, dass digitale Kommunikation nicht „unsichtbar“ bleibt – und dass es klug ist, sich vor dem Posten zu überlegen, wer was sehen darf.

Für User ist das zeitnahe Durchführen von Updates die erste Maßnahme der Zugangssicherung. Eine weitere besteht in der Vorsicht bezüglich offener Netze. Hat jemand Fremdes trotz Schutzmaßnahmen Zugriff auf das Smartphone erlangt, ist für den Cyberkriminellen die **erste Hürde** geschafft.

Hat er es auf dem Smartphone auf konkrete Anwendungen abgesehen, muss es ihm in der **zweiten Etappe** gelingen, in betreffende Apps einzudringen. Deshalb schließen sich auf diesem Arbeitsblatt noch grundlegende Erläuterungen zu Apps und die Frage an, wie es bei diesen zu Sicherheitsrisiken kommen kann. Auf Basis eines [Videos des BSI](#) und einer daran anschließenden Gruppendiskussion werden die Lernenden auf die Darstellung konkreter Schutzmaßnahmen vorbereitet, die auf Arbeitsblatt 3 in Form von fünf handlungsanleitenden Tipps erarbeitet werden.



Arbeitsblatt 3: Wesentlicher Basisschutz für Smartphones

Noch einmal Bezug nehmend auf die Geschichte von Hannah und Olli werden nun konkrete Tipps für die sichere Einrichtung von Smartphones erarbeitet.

Die Maßnahmen des Basisschutzes sind gleichberechtigt. Es macht aber Sinn, ein erstes Augenmerk auf **Updates** zu legen (**Tipps 1**). Denn wenn Hersteller Sicherheitslücken erkannt haben, ist die Phase zwischen Erkennen des Mangels und der Beseitigung kritisch. In dieser Zeitspanne können Cyberkriminelle, die darauf aufmerksam werden, die Lücke ausnutzen. Der Tipp lautet deshalb nicht nur, angebotene Updates überhaupt zu nutzen, sondern sie regelmäßig und vor allem zeitnah zu installieren.

Näher befassen sollten sich die Schülerinnen und Schüler mit **Bildschirmsperren (Tipps 2)**, die den unmittelbaren Zugang zum Smartphone für Unbefugte verhindern. Die hauptsächlich **genutzten fünf Methoden für Bildschirmsperren** sind im AB aufgeführt und werden im Video erläutert. User eines Smartphones müssen sich für eine Variante unter den Gesichtspunkten der Sicherheit und Praktikabilität entscheiden. Die verschiedenen Möglichkeiten lassen sich nicht in eine klare Favoritenreihe bringen: Die einfache PIN gilt zum Beispiel als unsicher, dafür ein Passwort als sicher, aber umständlich. Für biometrische Verfahren galt die Technik lange als nicht ausgereift, aber mittlerweile wird zu Fingerabdruck oder Gesichtserkennung geraten, da die Methode sehr sicher ist – Muster sind abgeschlagen, weil zwar einfach, aber auch unsicher.

Der **Accountschutz (Tipps 3)** ist ein Muss. Der im Beispiel gehackte Account von Olli zeigt anschaulich dessen Wichtigkeit. Wurde ein Account gehackt, kennt der Hackende in der Regel dessen Zugangsdaten. Werden diese auf dem Smartphone noch für andere Apps verwendet, hat er auch darauf Zugriff. Das ist – bildlich gesagt – wie bei einem Schlüssel, der für mehrere Zimmer in einem Haus passt. Der Accountschutz wird dennoch nur kurz behandelt und es wird erklärt, wann Passwörter „stark“ sind. Das Thema wird aufgrund seines Umfangs und seiner Bedeutung als späteres eigenständiges Thema in einem weiteren Medienpaket behandelt.

Bezüglich der gebotenen Vorsicht bei der Nutzung von **Drahtlosschnittstellen** wie offenem WLAN oder Bluetooth (**Tipp 4**) kommt nochmals Olli zum Zug. Sein Account ist gehackt worden und er hat eine Vermutung, wo die Schwachstelle lag. Die offenen Verbindungen sind typische Angriffspunkte. Aus Bequemlichkeit werden diese oft dauerhaft aktiviert, was jedoch Gefahren birgt.

Backups (Tipp 5) sind keine Maßnahme gegen Datenmissbrauch, sondern dienen zum Sichern der eigenen Daten, wenn man z. B. keinen Zugriff mehr auf das Smartphone hat. Backups werden oft als lästig empfunden und vernachlässigt, sind aber extrem wichtig. Der Sinn von Backups wird in einer Aufgabe aufgegriffen und Fälle, wo diese schon einmal genutzt werden mussten, werden diskutiert. Nicht jeder möchte aus Sicherheitsbedenken seine Daten automatisch in einer Cloud sichern. Der angeregte Peer-to-Peer-Austausch kann zum Betrachten des Für und Wider hilfreich sein und Tipps zum „Wie“ liefern.

Arbeitsblatt 4: Sicher mit Apps arbeiten

Erstens sorgt es für Sicherheit, wenn für **Apps benötigte Accounts sicher eingerichtet** und abgesichert werden (**Tipp 6**). **Zweitens** dürfen **Apps** nicht selbst ein Sicherheitsrisiko darstellen. Um das zu gewährleisten, dürfen wir – ganz verkürzt gesagt – nur seriöse Apps herunterladen. Ein **Kriterienkatalog für die Auswahl von Apps (Tipp 7)** gliedert das näher auf.

Drittens sollte Apps nur der **Zugriff auf Funktionen des Smartphones** gewährt werden, die für die Funktionalität dringend benötigt werden. Die Zuteilung oder der Entzug von Berechtigungen erfolgt über die Einstellungen (**Tipp 8**). Das Berechtigungsmanagement verschiedener Smartphone-Fabrikate und Betriebssysteme variiert. Die interaktive Übung arbeitet exemplarisch mit zehn Berechtigungen, wie sie praktisch überall vorhanden sind: Kamera-Zugriff, Mikrofon-Zugriff, Standort-Zugriff, Kontakte-Zugriff, Speicherzugriff (Speicher lesen/schreiben), Kalender-Zugriff, Benachrichtigungen, Bluetooth-Zugriff, Geräte- und App-Verlauf).

Ziel der Beschäftigung mit den Berechtigungen ist es, dass die Schülerinnen und Schüler verstehen, dass – plakativ gesagt – die Berechtigungssteuerung der Hebel ist, mit dem sie festlegen, was eine App von sich aus darf und was nicht und woraufhin sie die Berechtigungen dann auch einstellen.

Weiterführende Links

1. *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



2. *Wegweiser für den digitalen Alltag: Smartphone, Tablet & Co sicher nutzen:*

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Wegweise_r_Checklisten_Flyer/Brosch_A6_Mobilkommunikation.html



3. *Schritt für Schritt automatische Updates einrichten:*

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



4. *Schritt für Schritt zur Datensicherung:*

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