

FÜR DEN UNTERRICHT

SMARTPHONE- UND APP-SICHERHEIT



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI



AB 1: CYBERSICHERHEIT UND WAS SIE UNS ANGEHT

Einführungsbeispiel

Hannah freut sich auf ein neues Smartphone. Sie ist interessiert an technischen Themen und sehr gut darin, eigene Videos und Fotos zu gestalten und auf TikTok und YouTube hochzuladen. Natürlich nutzt sie ihr Smartphone aber auch zum Telefonieren, Nachrichten schreiben und Surfen im Internet. Hannah weiß, dass man ein Smartphone und die genutzten Apps vor Missbrauch durch andere und vor Schadsoftware schützen muss. Doch warum genau und wie?

Warum wir uns alle schützen sollten, wollen wir gleich gemeinsam erarbeiten. Immerhin ist unser Smartphone ein sehr privater Gegenstand mit vielen persönlichen Daten und sensiblen Informationen. Es kann speichern, welche Webseiten wir besucht und welche Messages wir an wen verschickt und von wem bekommen haben. Apps wie WhatsApp und TikTok kennen unsere Freundeskreise. Auf dem internen Speicher oder in Clouds verwahren wir Audios, Bilder, Spiele und Videos. Niemand möchte, dass davon etwas in fremde Hände gerät. Das wäre oft nicht nur unangenehm, sondern kann echten Schaden anrichten. Deshalb wollen wir uns mit dem Thema „Cybersicherheit“ beschäftigen.

UNTERSTÜTZUNG BEI DER CYBERSICHERHEIT

Mit dem Thema Cybersicherheit befasst sich in Deutschland auch das „Bundesamt für Sicherheit in der Informationstechnik (BSI)“. Dort gibt es Expertinnen und Experten, die aufklären und sehr verständlich über konkrete Schutzmaßnahmen informieren. Das ist auch nötig, denn Cybersicherheit betrifft jeden.

www.bsi.bund.de



Einführungsaufgabe



Lest die folgende erfundene Geschichte zu Hannahs Bruder Olli. Sie ist zwar nicht wirklich passiert, kommt aber so oder ähnlich oft auch in der Realität vor

Gehackter Account: Der Fremde im eigenen Social Media-Profil

„Olli, was schreibst du da für einen Mist im Internet?!“ Die Nachricht seiner jüngeren Schwester Hannah lässt Olli stutzen. Internet? Auf welcher Plattform? Er hat schon seit etwa einem halben Jahr nichts mehr gepostet. Olli öffnet die App zu seinem Social Media-Profil, um sich das anzusehen. Dort entdeckt er dutzende Nachrichten und Kommentare. Scheinbar hat er vor zwei Stunden ein Video hochgeladen, das schlimmste Tierquälerei zeigt. Irgendjemand muss sich illegal und von ihm unbemerkt Zugang zu seinem Social Media-Account verschafft und dieses Video mit seinem Profil veröffentlicht haben! Olli ist irritiert. Eigentlich hat er sein Smartphone und seine Accounts doch gut gesichert und gerade keine Ahnung, wie da ein Fremder draufgekommen sein soll. Was will derjenige wohl erreichen und wie kann er in seinen Account gekommen sein? Diesen beiden Fragen wollen wir nachgehen.



Was will der Hacker von Ollis Online-Profil erreichen? Bearbeitet diese Frage in drei Gruppen. Jede Gruppe wählt einen der folgenden drei Schwerpunkte und macht sich dazu Notizen.

1. Thema „Privatsphäre“: Der Hacker dringt in die Privatsphäre von Olli ein. Erarbeitet eine kurze Beschreibung, was die Privatsphäre ist und warum sie für Fremde tabu sein muss.
2. Thema „Sich für jemand anderen ausgeben“: Der Hacker hat in Ollis Namen gepostet und das Video hochgeladen. Was meint ihr: Warum hat der Täter das gemacht? Was könnten seine Ziele/Absichten sein?
3. Thema „Kriminelles Handeln auf Plattformen“: Nachdem Hannah Olli informiert hat, hat er sofort überlegt, ob er weitere Accounts mit der gleichen E-Mail-Adresse und gleichem Passwort besitzt. Angenommen, der Hacker ist ein „richtiger Krimineller“ und hat es auch auf andere Accounts von Olli abgesehen: Was könnten seine Ziele sein bzw. worauf könnte er es abgesehen haben?

Zusammenfassung, Auswertung und Erfahrungsaustausch



Stellt eure drei Gruppenergebnisse in der Klasse vor. Erzählt dabei auch gerne von euren eigenen Erfahrungen. Hat jemand schon mal etwas Ähnliches wie Olli erlebt? Wie habt ihr auf diese Situation reagiert?

Nutzt bei eurer Ergebnispräsentation Sätze wie: „Wir müssen uns und unser Smartphone schützen, damit ... nicht ...“ oder: „Wir müssen uns und unser Smartphone schützen, um für ... zu sorgen.“ Eine Schülerin / ein Schüler notiert die Sätze auf einem großen Blatt, sodass ein Plakat entsteht. Es kann zum Beispiel als Überschrift haben: „Cybersicherheit ist wichtig.“

Olli möchte – wie sicher die meisten von euch – aber auch zukünftig nicht auf die Nutzung sozialer Medien verzichten. Dennoch ist ihm jetzt noch mal mehr bewusst geworden, dass soziale Medien auch einige Risiken mit sich bringen.

SOCIAL MEDIA – RISIKEN IM ÜBERBLICK

Soziale Medien bieten tolle Möglichkeiten zum Austausch mit anderen, bringen aber auch einige Risiken mit, die du kennen solltest. Einige Beispiele:

- Du gibst deine E-Mail-Adresse, Telefonnummer, Hobbies und Vorlieben an. Das könnten Firmen nutzen, um dir Werbung zu schicken.
- Deine Aktivitäten sind nicht nur für deine Freunde, sondern im ganzen Netzwerk für alle sichtbar – vielleicht sogar in Suchmaschinen, wenn sie aus den Voreinstellungen übernommen und nicht geändert werden.
- Videos, Texte und vor allem Bilder können durch Fremde auf weiteren Seiten im Internet veröffentlicht oder für andere Zwecke missbraucht werden.
- Online-Verbrecher versuchen, bestehende Nutzer-Accounts zu hacken, um die fremde Identität für ihre Betrügereien zu nutzen.



AB 2: DIE TECHNISCHE SEITE – INTERNET UND APPS

Hannah hat Olli den Tipp gegeben, sich nach dem Vorfall zunächst die Daten und Uhrzeiten der Messages des Hackers anzusehen, bevor er diese löscht. Diese zeigen eindeutig, dass der Hacker nicht mit Ollis Smartphone tätig gewesen sein konnte, weil Olli das zu dieser Zeit immer bei sich hatte. Er muss also irgendwie „von außerhalb“ auf den Account gekommen sein.

Wir wollen nun also besser verstehen, warum und wie Smartphones aus der Ferne gehackt werden können. Dazu brauchen wir einen kleinen Ausflug ins Internet und wir müssen noch besser verstehen, was Apps sind.

Smartphones sind über das Internet miteinander verbunden

Wenn wir mit unserem Smartphone Server (Knotenpunkte in einem Netzwerk), Computer oder andere Smartphones erreichen möchten, läuft die Verbindung vielfach über das Internet. Möchten wir zum Beispiel eine Text- oder Sprachnachricht verschicken, müssen wir in jedem Fall in einem „Netz“ sein. Je nachdem, was wir aktiviert haben, kann das ein **WLAN-Netzwerk** sein, das die Nachricht über einen Router ins Internet leitet oder ein **Mobilfunknetz**. Letzteres überträgt die Nachricht per Funk an einen Mobilfunkmast, der sie ins Internet einspeist. Der weitere Weg zum Empfänger führt durch ein großes, weltweites Leitungsnetz, das teils aus Funkverbindungen und teils aus Kabelverbindungen besteht. An Kreuzungen, sie heißen Knoten, werden die Nachrichten in die richtige Richtung navigiert. Oft gibt es verschiedene Wege vom Empfänger zum Ziel. Welcher gewählt wird, hat technische Gründe. Wir haben darauf keinen Einfluss. Die Dienstprogramme des Netzanbieters regeln das automatisch.

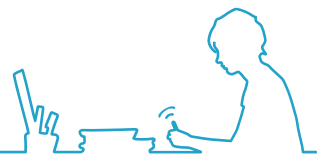


Geht zu zweit zusammen und stellt euch vor, eine Person in Hamburg kommentiert ein TikTok-Video. Welche Stationen durchläuft der Kommentar? Sortiert die Stationen in der richtigen Reihenfolge. Wenn ihr möchtet, könnt ihr die Reise des Kommentars als Comic oder Skizze darstellen.

- Der Kommentar kommt beim TikTok-Server an.
- Die Nachricht erreicht den nächsten Router oder Mobilfunkmast.
- Der Kommentar wird in der App eingegeben und abgeschickt.
- Andere Nutzerinnen und Nutzer sehen den Kommentar unter dem Video.
- Der Kommentar wird durch mehrere Knotenpunkte im Internet geleitet.
- Das Smartphone sendet den Kommentar über das WLAN oder Mobilfunknetz.

Dem Hacker keine Chance geben, auf Apps zuzugreifen

Hat es ein Hacker auf konkrete Anwendungen abgesehen, muss es ihm gelingen, in die jeweiligen Apps einzudringen und ggf. sogar einen Account zu übernehmen. Apps sind die **Programme**, die auf Smartphones **Anwendungen** ausführen. Einige Beispiele: WhatsApp (Nachrichten-App), YouTube



(Video-App), TikTok (Social Media-App), Google Maps (Navigations-App), Kamera (Foto- und Video-App), Clash of Clans (Spiel-App), Paypal (Bezahldienst), Banking-Apps usw.

Viele Apps sind ständig „in Bewegung“, zum Beispiel, indem sie dauerhaft mit dem Internet verbunden sind oder im Hintergrund laufen, obwohl ihr selbst gar nicht aktiv seid (z. B. Nachrichten empfangen, während ihr im Unterricht sitzt). Sie arbeiten über „Datenautobahnen“, die auch Cyberkriminelle nutzen können: So wie wir mit dem Smartphone auf das Internet zugreifen, versuchen Cyberkriminelle mitunter auch, auf unsere Geräte und Daten zuzugreifen. Deshalb ist es sehr wichtig, sowohl das Betriebssystem als auch Apps auf dem neuesten Stand zu halten.

SOFTWAREUPDATES ZEITNAH DURCHFÜHREN – EIN GRUNDPFEILER DER IT- BZW. CYBERSICHERHEIT

Mit Updates beseitigen Hersteller Fehler und Schwachstellen in ihrer Software. Sie schließen Sicherheitslücken oder fügen Funktionen hinzu. Updates später installieren? Auf keinen Fall! Sie sollten zeitnah durchgeführt werden, sobald sie bereitgestellt sind.

Das BSI hält praktische Tipps bereit, wie wir Updates im Blick behalten können und wie sie praktisch durchgeführt werden. Und aufpassen: Nicht auf gefälschte Pop-ups hereinfallen, die auf Webseiten für ein falsches, betrügerisches Update werben (Zusammengestellt aus [BSI - Softwareupdates schnellstmöglich installieren](#)).



Geht zu zweit zusammen und tauscht euch darüber aus, ob euch oder jemandem in eurem Bekanntenkreis schon einmal Sicherheitsvorfälle passiert sind. Diskutiert im Anschluss Szenarien, die Olli (dem Jungen aus dem Beispiel) passiert sein könnten und notiert diese.

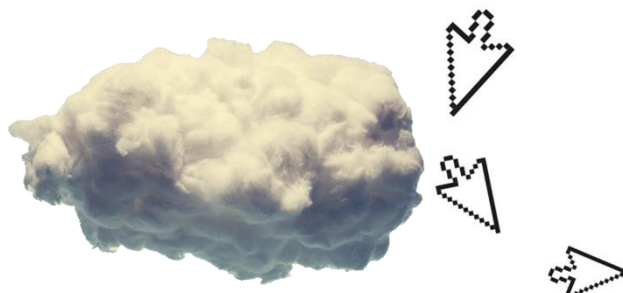


Hinweis: Falls euch keine Szenarien einfallen, könnt ihr dazu auch im Internet recherchieren. Eine mögliche Recherchehilfe kann der [Cybersicherheitsmonitor des BSI](#) sein.



Schaut euch zum Thema „Apps“ auch dieses Video vom BSI an. Notiert erste Ideen, wie ihr euch vor Sicherheitsrisiken schützen könnt und besprecht diese im Anschluss in der Klasse.

<https://www.youtube.com/watch?v=CzNI0zyEzf0>



AB 3: WESENTLICHER BASISSCHUTZ FÜR SMARTPHONES

Überblick über Schutzmöglichkeiten

Schutzmaßnahmen, um Hacker und Schadsoftware auszusperrern, setzen an verschiedenen Punkten an. Fünf Basismaßnahmen helfen euch schon richtig gut und sorgen für viel mehr Sicherheit.



Basismaßnahmen – sie haben keine feste Reihenfolge, ihre Anordnung symbolisiert einen Schutzring.

Die einzelnen Schutzmaßnahmen als Checkliste

Erinnert euch an Hannah und Olli aus dem

Einführungsbeispiel (AB 1). Hannah hat ihr neues Smartphone bekommen und möchte es so einrichten, dass sie gut vor Sicherheitsrisiken geschützt ist. Nach dem Vorfall mit Olli hat sie sich noch einmal besonders intensiv mit dem Thema beschäftigt und führt die Einrichtung jetzt mit ihm zusammen durch, um auch sein Smartphone noch besser zu schützen. Olli hatte seinen Social Media-Account lange nicht benutzt, aber nicht deinstalliert und dann die App-Updates verpasst. Das will er in Zukunft besser beachten. Beide führen nacheinander die folgenden Schritte aus, die auch ihr euch als Tipps merken solltet:

TIPP 1: NUTZE DIE ANGEBOTENEN UPDATES – FÜHRE SIE REGELMÄSSIG DURCH.

Von den Herstellern angebotene Updates schließen Sicherheitslücken. Oft werden Apps auch sinnvoll erweitert. So sorgen die Updates für Sicherheit und bringen die Software auf den jeweils aktuellen Stand. Du kannst auf deinem Smartphone auch einstellen, dass die Updates automatisch durchgeführt werden.

TIPP 2: RICHTE EINE BILDSCHIRMSPERRE EIN.

Denn sie tut, was ihr Name sagt: Sie sperrt den Bildschirm, also den Touchscreen. Er kann erst bedient werden, wenn er wieder freigeschaltet wird. Es gibt verschiedene Sperren: Muster, PIN, Passwort oder biometrische Verfahren wie einen Fingerabdruckscan oder die Gesichtserkennung.



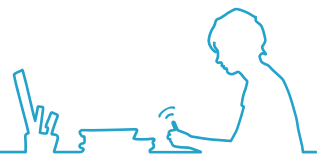
Schaut euch zum Thema Bildschirmsperren das folgende Video an.

<https://youtu.be/Uxut1MCp2W4?feature=shared>



Notiert das Wichtigste zu Bildschirmsperren und deren Vor- und Nachteilen aus dem Video.

Checkt dann in Partnerarbeit eure Smartphones und tauscht euch dazu aus: Habt ihr eine Bildschirmsperre? Warum oder warum nicht und welche nutzt ihr? Falls ihr keine eingerichtet habt, ihr es aber möchtet: Richtet euch eine Bildschirmsperre auf euren eigenen Smartphones ein.

**TIPP 3: ÜBERPRÜFE, OB DEINE ACCOUNTS DURCH SICHERE PASSWÖRTER GUT GESCHÜTZT SIND.**

Accounts sind Benutzerkonten, die du brauchst, um auf Dienste und Apps zuzugreifen. Das Google-Konto oder die Apple-ID, E-Mail-Konten, Social Media-Profil oder Messenger sind Beispiele. Nur du – niemand sonst – soll darauf zugreifen können. Eine Mindestsicherung besteht darin, dass du zum Anmelden einen Benutzernamen und ein Passwort eingeben musst. Ein erster wichtiger Schritt sind sichere Passwörter. Ganz wichtig ist, dass jeder Account ein eigenes Passwort bekommt.



Es gibt zwei Strategien für ein sicheres Passwort: Entweder du nutzt ein langes und weniger komplexes Passwort oder ein kürzeres und dafür komplexeres Passwort. Ein langes Passwort muss mindestens aus 25 Zeichen und zwei verschiedenen Zeichenarten bestehen. Ein kürzeres Passwort muss mindestens aus acht Zeichen und vier verschiedenen Zeichenarten bestehen.

TIPP 4: ACHE AUF SICHERE VERBINDUNGEN BEI SOGENANTEN „DRAHTLOSSCHNITTSTELLEN“ WIE Z. B. OFFENEM WLAN ODER BLUETOOTH. ÜBERTRAGE DAMIT KEINESFALLS SENSIBLE INHALTE.

- Schalte die WLAN-Funktion immer nur ein, wenn du sie benötigst. Das gilt vor allem für öffentliches WLAN (Hotspots im öffentlichen Raum) und für Bluetooth-Anwendungen.
- Rufe keine vertraulichen Daten über ein ungesichertes WLAN ab und versende auch keine darüber. Dazu gehören Zugangs-, Finanz- oder persönliche Daten wie Passwörter, Kreditkarteninformationen, Ausweisdaten oder private Fotos.



Olli hat nicht klären können, auf welchem Weg der Angriff bei ihm erfolgte. Gab es eine unsichere Verbindung? Verbindungen über das Mobilfunknetz sind verschlüsselt und sicher. Möglicherweise hat er mal bei einem WLAN nicht „aufgepasst“. Da kann die Strecke vom Smartphone zum Router (AB 2), der die Daten ins Festnetz leitet, unsicher sein. Bei fremden WLANs und Hotspots ist also Vorsicht angebracht. Auch die drahtlose Ankopplung von Geräten über Bluetooth kann ungesichert sein.

TIPP 5: SCHÜTZE DICH VOR VERLUST DEINER WICHTIGEN INHALTE UND RICHT DAZU EIN BACKUP EIN.

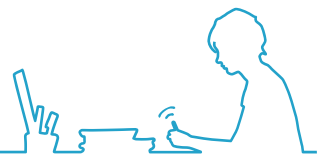
Wird dein Smartphone geklaut, durch einen Hacker geschädigt oder geht es kaputt, verlierst du alles, was darauf gespeichert ist. Ein Backup ist eine Datenkopie zur Sicherung an einem anderen Ort. Das kann eine Cloud, aber auch ein PC oder eine externe Festplatte sein. Backups müssen regelmäßig aktualisiert werden.



Geht in Vierergruppen zusammen und diskutiert gemeinsam, warum es sinnvoll ist, Backups zu machen. Tauscht euch im Anschluss darüber aus, ob ihr schon einmal auf ein Backup zurückgreifen musstet. Erstellt eine Checkliste zur Datensicherung anhand der [Quelle vom BSI](#).



Formuliert die fünf Tipps von oben als Sätze, die mit „Wir“ beginnen („Wir machen zeitnah Updates.“, „Wir richten eine Bildschirmsperre ein.“ usw.) und schreibt sie jeweils mit einer Begründung auf ein Plakat. Zusammen mit dem Plakat über Cybersicherheit habt ihr so alles Wesentliche immer gut im Blick.



AB 4: APPS SICHER NUTZEN

Habt ihr euch aus Arbeitsblatt 2 gemerkt, was Apps sind? Richtig: Es sind Anwenderprogramme auf dem Smartphone.

Allgemeine Tipps zum Schutz von Apps

Nicht jede App fordert eine Registrierung. Zum Beispiel könnt ihr Apps von Verkehrsbetrieben oft einfach herunterladen, öffnen und sofort den Fahrplan checken. Das ist ziemlich praktisch. Erst wenn ihr ein Ticket kaufen wollt, müsst ihr einen Account mit Anmeldedaten einrichten.



Maßnahmen für sichere Apps - sie sind gleichberechtigt wichtig (Bildquelle: Autor).

TIPP 6: NUTZE GRUNDSÄTZLICH NUR GUT GESCHÜTZTE ACCOUNTS. DAS GILT AUCH FÜR APPS.

Je nach App und Anbieter kann deine Anmeldung für den Account anders überprüft werden, zum Beispiel in nur einem Schritt (z. B. Passwort) oder in mehreren Schritten (z. B. zusätzlicher Einmalcode). Wähle in jedem Fall immer ein starkes Passwort und vergib für jeden Account ein eigenes.

Dieser Tipp schützt deine Apps vor Zugriff von außen. Doch woher weiß man, ob die App an sich auch sicher/seriös ist? Hannah ist zum Beispiel immer kritisch, wenn sie nach neuen Bild- und Videobearbeitungs-Apps sucht. Sie weiß, dass gute App-Bewertungen einzelner Nutzer im Netz oft von den Anbietern „gekauft“ werden und liest deshalb immer möglichst viele Bewertungen auf unterschiedlichen Portalen.

TIPP 7: WAS DU BEI DER AUSWAHL VON APPS NOCH BEACHTEN SOLLTEST

- Installiere Apps nur aus seriösen Quellen wie beispielsweise den großen App-Stores (z. B. Apple App Store, Google Play).
- Lade nur Anwendungen herunter, die du tatsächlich benötigst.
- Meide Quellen, bei denen du Zweifel an der Seriosität hast. Installiere beispielsweise keine App, die dir unverlangt als E-Mail-Anhang zugesandt oder als Download-Link angeboten wird.
- Auch Apps, die angeblich mehr können oder günstiger sind als das „Original“, sind verdächtig.
- Wenn du Zweifel an der Vertrauenswürdigkeit einer App beziehungsweise eines App-Entwicklers hast, reicht oft eine Suche im Internet aus, um sich über den Anbieter zu informieren. Achte dabei etwa auf Erfahrungsberichte, Bewertungen und Tests von etablierten Online-Portalen.
- Installiere Updates immer zeitnah bzw. stelle ein, dass sie automatisch ausgeführt werden. Prüfe danach noch einmal die Berechtigungen.
- Prüfe, wann die letzte Version veröffentlicht wurde und ob die App stetig weiterentwickelt wird.
- Deinstalliere Apps, die du nicht mehr nutzt.



Geht zu zweit zusammen und wählt jeweils zwei unterschiedliche Apps von eurem Smartphone aus. Überprüft diese Apps anhand der obenstehenden Tipps auf Seriosität und besprecht euch in Paarbeit.

Woher stammen die Apps? Könnt ihr Informationen über die Apps recherchieren? Findet ihr Anhaltspunkte, dass sie seriös sind? Gibt es möglicherweise negative Bewertungen und Berichte über Sicherheitsprobleme im Internet? Wer zweifelt, deinstalliert diese App besser. Beratet euch im Zweifel, ob ihr die App wirklich benötigt. Wenn ihr sie behalten wollt, prüft, ob ihr die neueste Version der App habt oder ob sie ein Update braucht.

Berechtigungen gezielt zuweisen

Euer Smartphone verfügt über zahlreiche grundlegende Funktionen, die eine Art Bibliothek bilden: zum Beispiel Kamera, Mikro, Speicherzugriff, Kontakte, Kalender und Standort. Darauf können verschiedene Apps zugreifen. Die Berechtigung einer App für erlaubte Zugriffe wird in den Einstellungen aktiviert.

Manche Berechtigungen sind für die Funktionalität zwingend notwendig. Eine Video-App kann nicht ohne Kamera und Mikrofon arbeiten, eine Navigationsapp nicht ohne Standort. Vielfach sind Berechtigungen deshalb voreingestellt. Aber oft genug kommt es vor, dass Berechtigungen für Apps aktiviert sind, die sie nicht zwingend brauchen. Das kann zu Missbrauch führen und macht das Smartphone unsicher. Beispielsweise braucht ein Streamingdienst kein Mikro und sollte dafür keine Berechtigung bekommen. Der Dienst ist dauerhaft mit dem Internet verbunden, weil er Filme in kleinen Datenpaketen sendet. Das kann eine angreifbare Verbindung sein, die das Smartphone bei eingeschaltetem Mikro zum „Spion“ im Wohnzimmer machen könnte.

TIPP 8: VERGIB BERECHTIGUNGEN GEZIELT UND ÜBERPRÜFE DIE EINSTELLUNGEN IMMER WIEDER!

Bei den Einstellungen im Betriebssystem eines Smartphones (z. B. Android, iOS) kannst du festlegen und auch ändern, welche Berechtigungen eine App haben soll. Das Berechtigungsverzeichnis findet man in Android meistens unter „Einstellungen – Datenschutz – Berechtigungsmanager“ und bei Apple unter „Einstellungen – Datenschutz & Sicherheit – Berechtigungen“. Überlege für jede App gründlich, welche Berechtigungen du zulassen willst. Erteile sie nur dann, wenn sie zwingend nötig sind oder du das Risiko überschaust. Braucht eine App eine Berechtigung, die für die Funktionalität erforderlich ist, fragt sie die Erteilung an. Du kannst dann immer noch gezielt zustimmen.



Interaktive Übung: Bewertung der Methoden zur Bildschirmsperre auf Smartphones

Ihr findet in der Übung Beispiele für Bildschirmsperren. Weist jeder Bildschirmsperre einer Bewertung zu.



Interaktive Übung: Abschlussquiz für die Lerneinheit

Beantwortet jeweils allein die sieben Fragen zum Thema Smartphone-Sicherheit. Die richtigen Antworten setzen eine Zusammenfassung des Wichtigsten zusammen. Schreibt auch diese sieben Merksätze auf ein Plakat für den Klassenraum.

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