WHAT ABOUT ME

UNTERRICHTSMODUL SICHERHEIT IM INTERNET

SICHERHEIT IM INTERNET

ARBEITSBLATT UND LEHRERINFORMATION

Fachinhalte:

- Persönlichkeits- und Urheberrecht
- Datenschutz und -sicherheit
- Schadprogramme wie Viren, Trojaner, Malware
- Zugriffs- und Zugangskontrolle
- Passwörter, Verschlüsselung, PIN
- Persönlichkeits- und Bewegungsprofile im Internet
- Sicherheits-Apps, Backup, Updates

Herausgeber: Arbeitgeberverband Gesamtmetall

SICHERHEIT IM INTERNET

VORAUSSETZUNGEN

Die Schülerinnen und Schüler sollten ein eigenes Smartphone besitzen und breite Praxiserfahrungen im Umgang damit sowie mit der Installation und Nutzung verschiedener Apps haben. Sie verfügen über ein Grundwissen zu mobilen Diensten und Daten und den Systemeinstellungen des Smartphones. Die Schülerinnen und Schüler sind mit der mobilen Internet-Recherche vertraut.

GESAMTZEIT: 90 MINUTEN

HINWEISE ZUM STUNDENABLAUF

PHASE	INHALT	ZEIT
1. Einstieg und Motivation	Starten Sie die Unterrichtseinheit mit einem Impuls: Jemand hat heimlich eine Spionage-App auf dem Handy der Jugendlichen installiert. Nun können Gespräche mitgehört, der WhatsApp-Chat mitgelesen oder die Fotogalerie durchsucht werden. Fragen Sie die Schülerinnen und Schüler, was ihnen ganz spontan dazu als persönliches Schreckensszenario einfällt. Vielleicht haben sie auch schon eigene negative Erfahrungen gemacht, z. B. beim Surfen im Internet oder bei der Vernetzung in sozialen Medien. Lassen Sie die Schülerinnen und Schüler Vermutungen anstellen, ob sie sich möglicherweise selbst schon wissentlich oder unwissentlich in einer fragwürdigen rechtlichen Grauzone befunden haben.	10 Min.
2. Datenschutz, Datensicherheit und Urheberrecht	Mit einer Zuordnungsaufgabe erarbeiten sich die Schülerinnen und Schüler in Einzelarbeit die Rechtsbegriffe und Maßnahmen zu den Themen Datenschutz, Datensicherheit, Urheber- und Persönlichkeitsrecht. In einer Grafik werden die Fachbegriffe gegeneinander abgegrenzt und Überlappungen veranschaulicht. Die Schülerinnen und Schüler ergänzen die grafischen Symbole mit den zugehörigen Fachbegriffen, um ihr Gesamtverständnis zu sichern.	30 Min.
3. Sich im Internet bewegen: rechtliche Sicht und Datensicherheit	Teilen Sie die Klasse in zwei Gruppen ein, die „Upload“- und die „Download“-Gruppe. Diese bleiben für den Rest der Unterrichtseinheit bestehen. Die Gruppen diskutieren zunächst die typischen Aktivitäten beim Datenaustausch zwischen Netz und Handy und vollziehen die Handlungen gedanklich oder durch Ausprobieren mit dem Smartphone nach. Unterstützt werden die Überlegungen durch die Darstellungen in der Tabelle. Zur Ergebnissicherung ordnen die Gruppen den Anwendungen die notwendigen Arten von Daten im Up- oder Download zu, hierzu gehören auch mögliche Schaddaten. Im Anschluss teilen die Teams alle ausgetauschten Datenströme in einer weiteren Grafik in verschiedene Kategorien ein. Diese bilden die juristischen Schutzrechte ab und stellen auch die Bedrohungen dar.	30 Min.
4. Schutzmaßnahmen für Smartphone und Nutzer	Im ersten Teil der dritten Aufgabe machen sich die Gruppen mit den Bedrohungen und Rechtsverletzungen vertraut. Im zweiten Teil erarbeiten sie sich genaue Kenntnisse zu den Zugangswegen. In einer Zuordnungsaufgabe diskutieren sie alle denkbaren Schutzmaßnahmen und korrekte Handlungsanweisungen zur Vermeidung von Rechtsverletzungen und ordnen die geeigneten Maßnahmen den Bedrohungen und Rechtsverletzungen zu. Zur Ergebnissicherung stellen die Gruppen ihre Ausarbeitungen im Plenum vor.	20 Min.

BINNENDIFFERENZIERUNG

- ▶ Die Basisaufgabe ist von allen Schülerinnen und Schülern zu lösen.
- ▶▶ Die Bonusaufgabe ist optional, sie dient als Reserve oder Ergänzung für leistungsstärkere Lernende.

HAUSAUFGABE:

Erkunde den aktuellen Sicherheitsstatus deines Smartphones. Prüfe dazu die zehn wesentlichen Sicherheitsmerkmale in der Tabelle und trage den aktuellen Status deines Handys ein. Beurteile abschließend, wie gut dein Smartphone geschützt ist. Wenn du mehr als vier Aussagen mit „Ja“ beantworten konntest, ist dein Handy gut geschützt.

Mein Smartphone ...	Ja/Name/Funktion/Wann?	Nein
... ist immer unter Aufsicht und bei mir.		
... hat eine Bildschirmsperre.		
... hat die SIM-Karte per PIN-Abfrage geschützt.		
... verwendet sichere Passwörter.		
... hat gerade ein Sicherheits-Software-Update aktualisiert.		
... hat eine Antivirus-App installiert.		
... hat nur Apps aus dem offiziellen Play-/App-Store installiert.		
... hat alle Apps auf dem aktuellen Stand.		
... hat Bluetooth, WLAN und GPS-Ortung nur, wenn ich es aktiviere.		
... hat wichtige Daten per Backup auf einem externen Datenträger gesichert.		

SICHERHEIT IM INTERNET

Bewusster für Sicherheit im Internet zu sorgen, ist die Antwort auf Cyberkriminalität. So nennt man Straftaten mit modernen Informationstechniken, die uns heute immer häufiger begegnen. Immer wieder berichten die Medien, dass große Server mit Millionen von Nutzerdaten gehackt oder Schadprogramme per E-Mail verschickt werden. Damit werden Rechner mit Viren infiziert oder Passwörter durch Trojaner ausgespäht. Gefühlt betrifft das vor allem Nutzer von Computern. Dies ist ein Irrtum: Gerade das Smartphone stellt als Mini-Computer mit mehrfacher Funkanbindung eine breite Angriffsfläche für Bedrohungen aus dem Internet dar. Jedoch ist es bislang wenig geschützt. Als ständiger Begleiter in allen Lebenslagen wird das Smartphone zum spontanen, oft wenig überlegten Datenaustausch vor allem mobil genutzt. Beispiele sind die sozialen Medien, das Herunterladen von Apps, die mobile Nutzung von Online-Diensten an öffentlichen Hotspots, die externe Lautsprecherverbindung per Bluetooth-Funk oder schlicht unbekümmertes Surfen im Internet. Medienverfügbarkeit im Internet und die Vernetzung mit anderen führen auch dazu, selbst ungewollt zum Täter zu werden und fremdes geistiges Eigentum zu teilen und damit das Urheberrecht zu verletzen. Dieses Arbeitsblatt klärt auf und gibt Hilfestellung für mehr Sicherheit im Internet mit dem Smartphone.

AUFGABEN

▶ Basisaufgabe ▶▶ Bonusaufgabe

1. DATENSCHUTZ, DATENSICHERHEIT UND URHEBERRECHT

Die Textbausteine in Abbildung 1 beschreiben verschiedene juristische Rechtspositionen und Maßnahmen, die im Zusammenhang mit Sicherheit im Internet von Bedeutung sind.

▶ Lies die Beschreibungen aufmerksam durch und ordne den Texten anschließend die richtige Überschrift zu. Trage dazu jeweils die Großbuchstaben bei der passenden Überschrift ein.

MATERIAL | **JURISTISCHE RECHTSPOSITIONEN UND MASSNAHMEN**

Das Persönlichkeitsrecht ist ein umfassendes Grundrecht und in mehrere Einzelschutzrechte unterteilt. Die verschiedenen Einzelrechte schützen die Persönlichkeit, also das Ansehen, die Ehre und die persönlichen Daten sowohl in der analogen Welt als auch in der digitalen Datenverarbeitung. Es umfasst besonders das **Recht auf Selbstbestimmung** und das **Grundrecht Datenschutz**. Dieses wird auch als das **Recht auf informationelle Selbstbestimmung** bezeichnet.

Recht auf Selbstdarstellung	Grundrecht auf Datenschutz	Urheberrecht	Datensicherheit
C	A	B	D
Dieses Recht schützt das geistige Eigentum einer Person an ihren Werken, das sind z. B. Texte, Musik, Bilder oder Fotos. Dazu gehören auch Werke in digitaler Form. Das Recht verhindert, dass andere die Werke des Urhebers ohne dessen Erlaubnis nutzen.	Dieses Recht stellt sicher, dass die Person selbst darüber bestimmt, wie sie sich in der Öffentlichkeit darstellt. Sie entscheidet selbst, wie und ob ihr Name, ihr Bild oder das eigene Wort veröffentlicht wird. Außerdem ist die Ehre geschützt, d. h. niemand darf die Person öffentlich beleidigen oder ihr falsche Aussagen unterschieben.	Dieses Recht stellt sicher, dass eine Person selbst darüber bestimmt, ob und wem sie ihre eigenen, personenbezogenen Daten anvertraut und wie die Daten dann verwendet werden dürfen. Dieses Recht schließt auch die Speicherung und Verarbeitung der Daten in Computersystemen ein.	Dies ist ein Überbegriff für technische und organisatorische Maßnahmen zur Sicherung von Daten. Damit sind alle Daten gemeint, also allgemeine und personenbezogene Daten, analoge Daten (z. B. Akten) aber auch digitale Daten. Die Maßnahmen umfassen Technik und Organisation, um die Daten gegen Bedrohungen zu sichern. Solche Bedrohungen können z. B. Verfälschungen, unerlaubte Einsicht in Daten und die Zerstörung oder der Verlust von Daten sein.

Abbildung 1

MATERIAL GELTUNGSBEREICHE DER RECHTE UND MASSNAHMEN

In Abbildung 2 sind die Geltungsbereiche und Überlappungen der verschiedenen Rechte und Maßnahmen als Ovale dargestellt. Die Daten sind durch die zylindrischen Datenspeicher symbolisiert. Die Bedrohungen von außen bilden explosive, schwarze Pfeile.

▶ Vergleiche die Darstellung in Abbildung 2 mit den Rechten und Begriffen aus Abbildung 1 und mache dir die Bedeutung der eingezeichneten Symbole, die Überschneidungen der Geltungsbereiche und die Bedrohungen von außen bewusst. Ordne dann den Symbolen in der Grafik die zugehörigen Fachbegriffe zu. Trage die zutreffende Überschrift auf der Linie und den Buchstaben in den weißen Kreis ein.

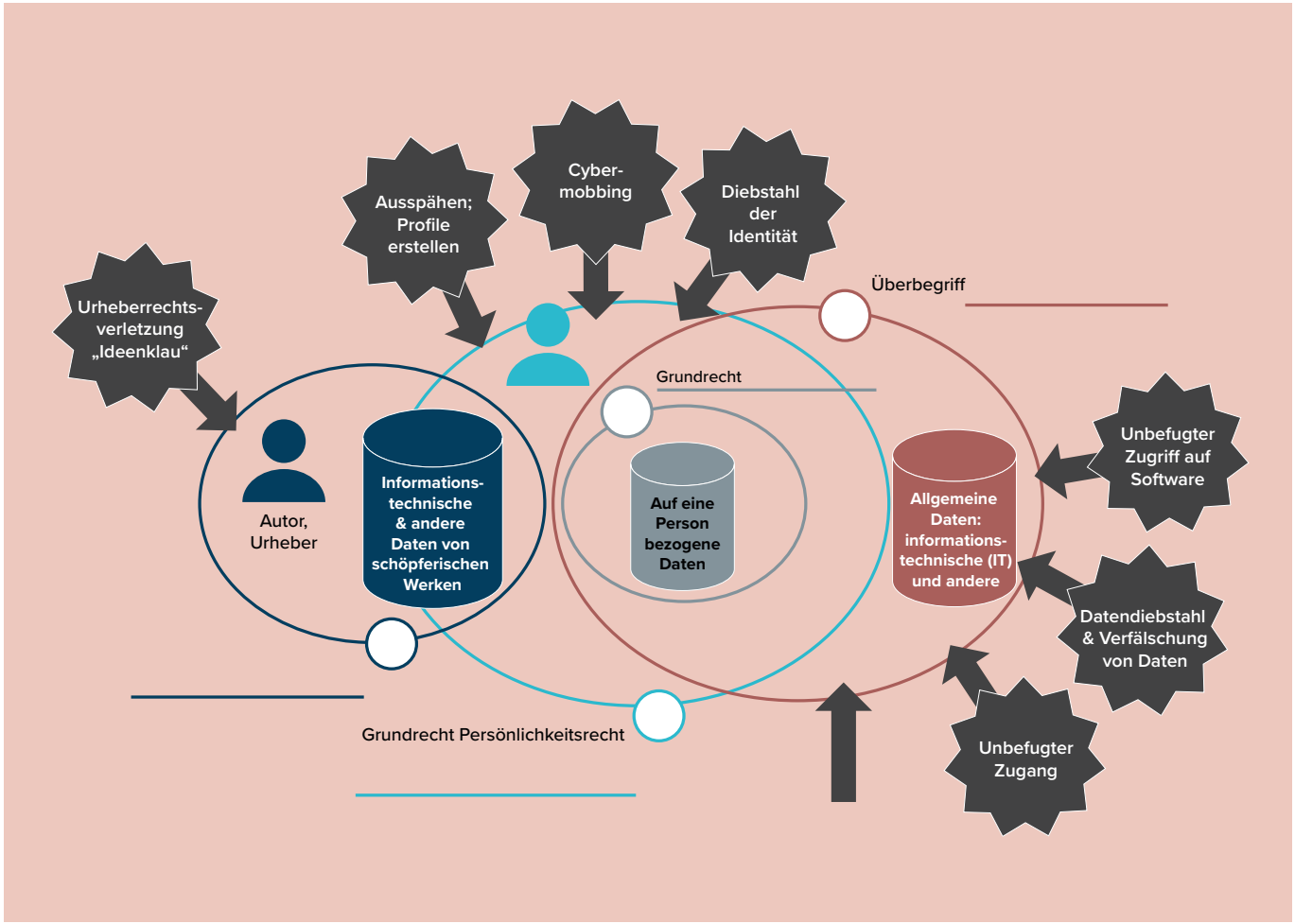


Abbildung 2

2. SICH IM INTERNET BEWEGEN: RECHTLICHE SICHT UND DATENSICHERHEIT

Abbildung 3 zeigt zunächst eine Übersicht typischer Aktivitäten, wenn ihr euch mit dem Smartphone im Internet bewegt. Dabei kann das Handy wahlweise sowohl auf Mobilfunkverbindungen als auch auf private und öffentliche WLANs oder Bluetooth-Verbindungen zugreifen. Passend zu den Aktivitäten sind in der Übersicht darunter verschiedene Datenkategorien aufgeführt. Diese werden beim Senden (Upload) und Empfangen (Download) zwischen Handy und Internet ausgetauscht.

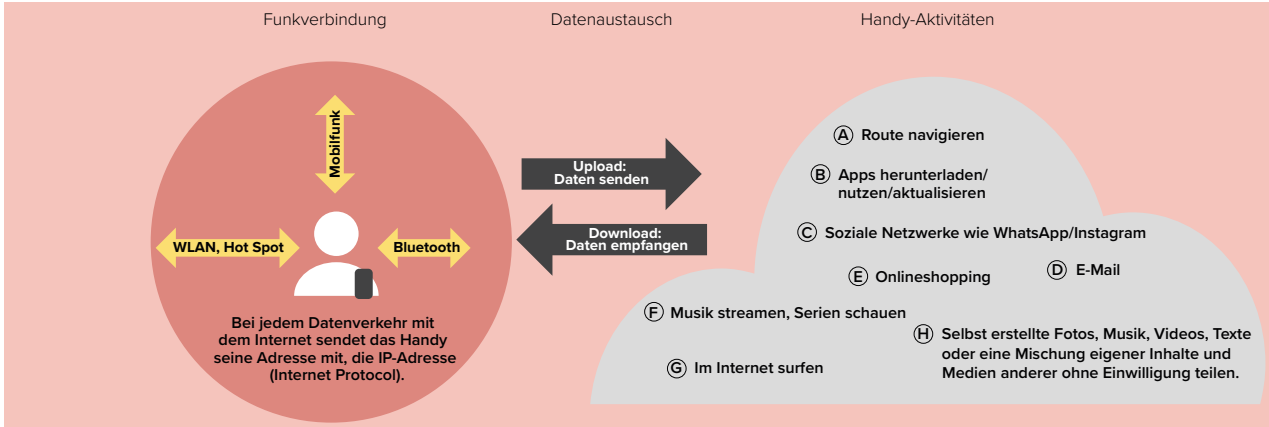
- Macht euch mit den Handy-Aktivitäten vertraut und diskutiert oder probiert sie gedanklich aus. Welche wesentlichen Eingaben sind nötig? Welche Daten-Kategorien werden jeweils empfangen oder gesendet? Macht euch Notizen dazu.

- Schaut euch die Daten-Kategorien in der Tabelle genau an und ordnet sie den Handy-Aktivitäten zu. Tragt dazu die Zahlen der Datenkategorien in den Kreis um den Großbuchstaben ein:

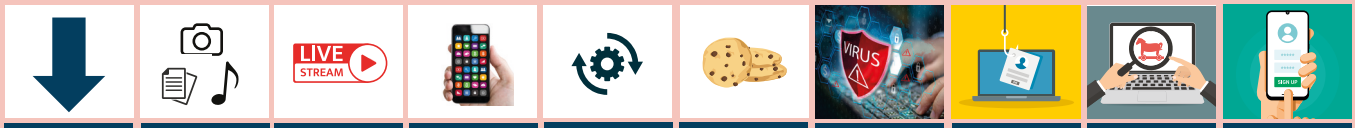
Die Upload-Gruppe trägt zu jeder Aktivität die gesendeten Daten-Typen mit einem Kreis umrandet ein. Daten, die nur manchmal oder ungewollt übertragen werden, bekommen einen gestrichelten Kreis. Die Download-Gruppe trägt zu jeder Aktivität die empfangenen Daten-Typen mit einem Viereck umrandet ein. Daten, die nur manchmal oder ungewollt übertragen werden, bekommen ein gestricheltes Viereck. *Achtung: In der Tabelle sind die Handy-Aktivitäten vereinfacht durch Großbuchstaben dargestellt.*

MATERIAL

AKTIVITÄTEN UND DATENKATEGORIEN BEI UP- UND DOWNLOADS



Datenkategorien



Download per Mobilfunk, WLAN, Hot Spot, Bluetooth	**Inhalte** wie Text, Bilder, Fotos, Musik, Videos	**Streamen** von Musik, Videos	Software, **Apps**	**Updates**, Sicherheits-aktualisierung	**Cookies:** kleine Textdatei vom Webserver mit Speicherung beim Nutzer	Schadpro-gramme wie **Viren, Malware**	**Phishing:** Email mit Abfrage von Kontaktdaten; Anforderung von Ausweis-kopie	**Trojaner, verstecktes Programm** zum Aus-spähen von Eingabedaten, unerwünschte **Huckepack Apps** zu-sammen mit Nutzsoftware	**Freigabe Online-Account, Quitting**
1	2	3	4	5	6	7	8	9	

A B C D E F G H

Upload per Mobilfunk, WLAN, Hot Spot oder Bluetooth	**Eigene Inhalte** wie Text, Bilder, Fotos, Musik, Videos, Chat	**PIN, TAN:** Per-sönlicher Iden-tifikations-Code oder eindeutige, einmalige **Transaktions-nummer**	**IP (Internet Protocol)-Adresse, Email-Adresse** als Nutzerken-nung	**Persönliche Daten:** Alter, Geschlecht, Name, Vorna-me, Adresse	**Benutzerna-me, Passwort:** Persönliche Zugangsbe-rechtigung zu einem Compu-ter-Konto	**GPS- Standort:** Aktueller Auf-enthaltsort	**Eingaben** wie Bestätigung, OK, Ablehnen, Abbrechen	**Bankverbin-dungsdaten:** Kontonum-mer, IBAN, Name
1	2	3	4	5	6	7	8	

Abbildung 3

MATERIAL
JURISTISCHE SCHUTZRECHTE UND SICHERHEITSBEDINGUNGEN

Abbildung 4 teilt das Datenaufkommen im Up- und Download aus den Handy-Aktivitäten in verschiedene Kategorien juristischer Schutzrechte oder Sicherheitsbedingungen ein. Die Farben kennzeichnen dabei die unterschiedlichen Kategorien. Wenn mehrere Eigenschaften gleichzeitig zutreffen, überlappen sich die Bereiche. Manche Daten gehören auch zur Kategorie der Bedrohungen.

▶ Diskutiert in eurer Gruppe die euch zugeteilten Daten-Kategorien im Up- oder Download (siehe Abbildung 3) und ordnet sie jeweils den unterschiedlichen Bereichen zu. Tragt hierzu die Nummer mit dem Kreis (Upload) oder Viereck (Download) in die Grafik ein. Mehrfachnennungen sind möglich. Stellt anschließend euer Gruppenergebnis im Plenum vor.

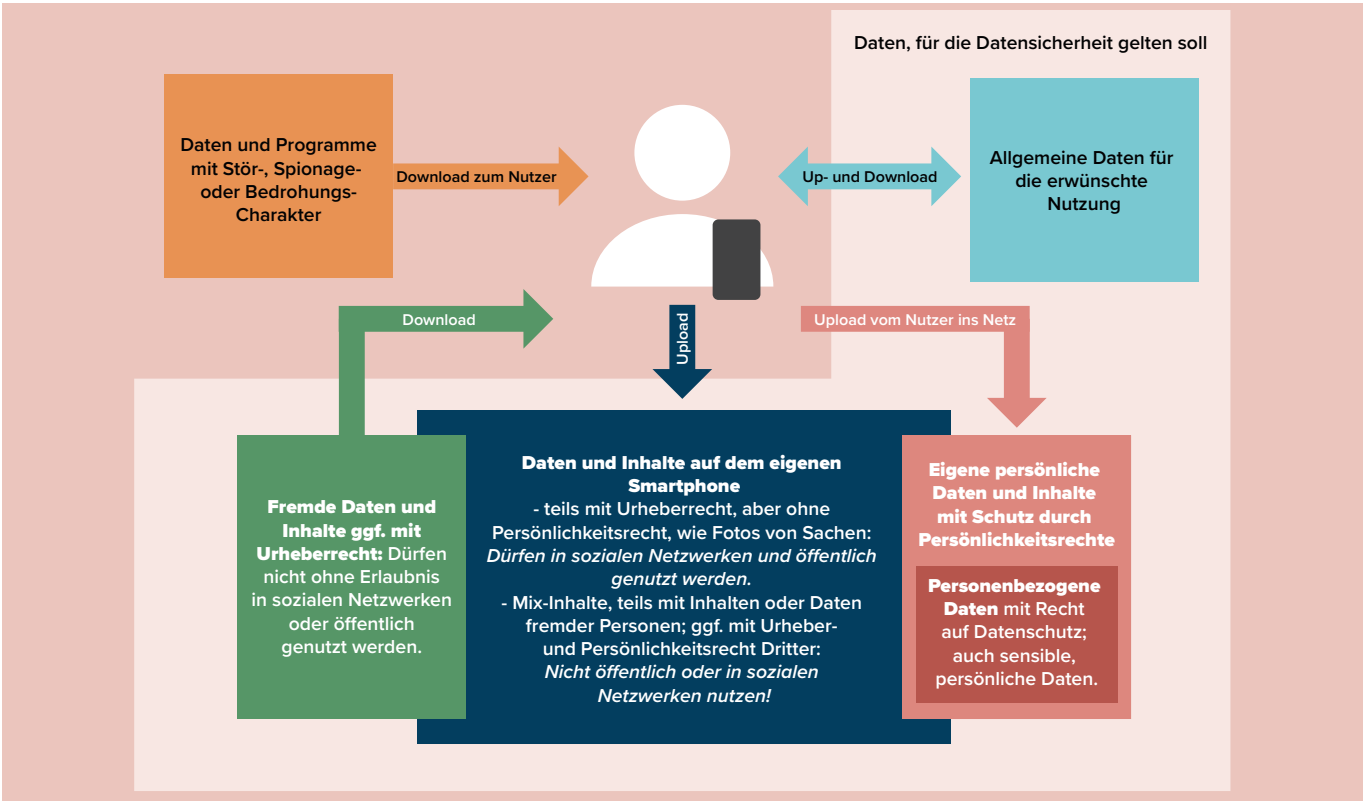


Abbildung 4

▸▸ PASSWORT KNACKEN

Ein gutes Passwort ist ein sicherer Schutz vor unbefugtem Zugriff auf ein Computer- oder Online-Konto. Dabei spielen die Länge und die Zusammensetzung der Zeichen des Passworts eine entscheidende Rolle. Untersucht hier die Sicherheit eines Passworts mit 3 Ziffern „***“. Jede Stelle hat Ziffern aus dem Bereich 0 bis 9.

- Findet aus der Übersicht der Schutzmaßnahmen die geeigneten Maßnahmen für die euch zugeordneten Bedrohungen heraus und tragt die passenden Großbuchstaben in den Kasten unter der Bedrohung ein. Stellt eure Ergebnisse abschließend im Plenum vor.
- Mit welcher einfachen Methode kann man das Passwort sicherer machen?
- Um wie viele Kombinationsmöglichkeiten wird die Sicherheit des Passworts verbessert, wenn man Groß- und Kleinbuchstaben zulässt: a-z und A-Z mit je 26 Zeichen?

3. SCHUTZMASSNAHMEN FÜR SMARTPHONE UND NUTZER

In Abbildung 5a und 5b sind nochmals die Bedrohungen für das Smartphone aus Aufgabe 1 sowie mögliche Rechtsverletzungen aufgeführt.

- Lest die eurer Gruppe zugeteilten Textbausteine aufmerksam durch und verbindet die zusammengehörigen Satzstücke. Diskutiert und begründet eure Zuordnung.

MATERIAL | **BEDROHUNGEN UND RECHTSVERLETZUNGEN**

GRUPPE „UPLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Unbefugter Zugang - Diebstahl - Unbemerkte Fremdnutzung **ist, wenn ...**	... sich ein Krimineller z. B. in sozialen Netzwerken oder per E-Mail mit falscher Identität ausgibt. Das erlaubt ihm, im falschen Namen einzukaufen, Online-Banking zu machen, den Ruf zu schädigen oder falsche Anrufe zu tätigen.
Datendiebstahl - aus internem oder externem Speicher oder - Verfälschung von Daten **wird möglich, wenn ...**	... unerwünscht eindringende Schadprogramme auf das Software-System zugreifen und es beschädigen. Die Schadprogramme können ferngesteuert werden und geheime Zugangsdaten ausspähen, unbemerkt Sicherheitslücken erzeugen, Daten zerstören und Systemfunktionen beschädigen.
Mit Schadsoftware wie - Virus - Malware - Schadprogrammen **infiziert sich das Smartphone dadurch, dass ...**	... das Opfer durch Messenger-Dienste wie Chats oder Anrufe beleidigt, bedroht oder bloßgestellt wird. Es werden Unwahrheiten und gefälschte Medien verbreitet.
Identitätsdiebstahl bedeutet, dass ...	... das Handy nicht verschlüsselt ist oder externe Speicher wie Datenbanken geknackt, Daten entwendet oder verändert werden. Das sind z. B. Daten wie E-Mail-Adressen oder Daten aus einem Online-Speicher.
Cybermobbing bedeutet, dass ...	... jemand unerlaubt und unbemerkt das Smartphone mit allen Daten nutzt, entwendet oder ausliest. Sensible Daten auf Smartphone und SD-Karte wie Fotos, E-Mails oder Passwörter können unerlaubt kopiert, verarbeitet und verfälscht werden und unbefugten Zugang zu den eigenen Konten ermöglichen.

Abbildung 5a

GRUPPE „DOWNLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Ausspähen, d. h. - ausgespäht werden durch Spionage-Apps (Spyware) **liegt vor, wenn ...**	... „Tracker“-Apps auf Webservern sich merken, welche Seiten besucht werden, wie auf der Seite agiert wird und entsprechende personalisierte Werbebanner und Interessenprofile erstellen. Örtliche Bewegungsprofile entstehen durch Sammeln der personenbezogenen Daten aus Online-Aktionen an verschiedenen Orten.
Profile wie - Persönlichkeitsprofil - Bewegungsprofil **werden dadurch erstellt, dass ...**	... Fotos und Mediendaten mit und ohne Abbildung anderer ohne Erlaubnis veröffentlicht und geteilt werden.
Unter der **Urheberrechtsverletzung**, also „Ideenklau“, versteht man, dass ...	... eine Spyware-App das Nutzerverhalten überwacht. Sie hat Zugriff auf Nachrichten, Browserverläufe, Anruflisten und Chats in sozialen Medien.
Datenverlust bedeutet, dass ...	... Daten beabsichtigt oder unbeabsichtigt gelöscht werden, unauffindbar oder zerstört sind.
Eine **Verletzung des Persönlichkeitsrechts anderer** ist, dass ...	... von anderen Personen erstellte Fotos oder Mediendaten ohne Erlaubnis heruntergeladen, gespeichert und getauscht werden. Das gilt auch für Videos und Musik aus illegalen Quellen und für eigene Mix-Produktionen und Collagen aus Vorlagen anderer.

Abbildung 5b

MATERIAL

„INFEKTIONS-“ UND ZUGANGSWEGE / SCHUTZMASSNAHMEN

Ihr habt nun die Bedrohungen für ein Smartphone kennengelernt. Abbildung 6a zeigt die wesentlichen „Infektions-“ und Zugangswege solcher Bedrohungen und Abbildung 6b nennt geeignete Schutzmaßnahmen.

- Diskutiert in eurer Gruppe die euch zugeteilten Bedrohungen und macht euch mit den jeweiligen Zugangswegen und Gegenmaßnahmen vertraut.
- Findet aus der Übersicht der Schutzmaßnahmen die geeigneten Maßnahmen für die euch zugeordneten Bedrohungen heraus und tragt die passenden Großbuchstaben in den Kasten unter der Bedrohung ein. Stellt eure Ergebnisse abschließend im Plenum vor.

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „UPLOAD“

1. Unbefugter Zugang	2. Datendiebstahl	3. Schadprogramme und unbefugter Zugriff auf Software	4. Identitäts-Diebstahl	5. Cybermobbing
• Das Smartphone liegt ohne Aufsicht sichtbar und zugänglich herum. • Es ist keine Bildschirmsperre aktiviert. • Die Daten sind im internen Speicher und auf der SD-Karte unverschlüsselt.	• Daten im internen Handyspeicher und auf der SD-Karte sind nicht verschlüsselt. • WLAN- und Bluetooth-Verbindung als Zugang zum Handy.	• Merkwürdige E-Mail oder Social-Media-Nachricht mit Link oder Anhang • Versteckt in Apps von unseriösen Anbietern • Infizierte Website	• Das Abfangen von Zugangsdaten zu Online-Accounts, z. B. mit gefälschten E-Mails oder Websites. • Häufig reicht das Wissen von Name, Adresse und Geburtsdatum des Opfers für die falsche Identität aus.	• Fremde legen falsche Identität in sozialen Netzwerken an. • Fremde Personen kennen private Daten von Dritten.

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „DOWNLOAD“

6. Ausspähen	7. Profile erstellen	8. Urheberrechtsverletzung	9. Datenverlust	10. Verletzung des Persönlichkeitsrechts
• Die Installation der Spionage-App durch Sicherheitslücken beim Besuch krimineller Websites. • Durch die manuelle Installation durch Fremde.	• Durch umfangreiche Berechtigungen bei Apps oder in den sozialen Netzwerken. • Cookie-Erlaubnis im Browser • Browser-Erweiterung und Tracking-Apps auf der Website erfassen Surf-Aktivität und Vorlieben. • Die Standorterfassung durch Bluetooth, WLAN und GPS.	• Von Dritten gemachte Fotos oder Musik werden ohne Erlaubnis weiterverbreitet oder veröffentlicht. • Das kostenlose Herunterladen und Speichern von aktuellen Mediendaten wie Songs oder Filmen von unseriösen, illegalen Websites. • Das Veröffentlichen von eigenen Produktionen mit Versatzstücken aus fremden Medien-Dateien.	• Datenverlust nach „Hard-Reset“. Das Handy wird nach fehlerhaftem Betrieb zurückgesetzt. • Daten werden versehentlich gelöscht. • Das Smartphone geht kaputt.	• Das Veröffentlichen oder Teilen von Fotos und Mediendaten mit und ohne Abbildung anderer ohne deren Erlaubnis in den sozialen Netzwerken oder im Internet.

Abbildung 6a

ÜBERSICHT DER SCHUTZMASSNAHMEN

A) Nur notwendige Berechtigungen für installierte Apps zulassen.
B) Diebstahl-App installieren, die das gestohlene Gerät ortet, Daten aus der Ferne sperrt oder löscht.
C) Kostenlose Musik-Download-Apps oder Probe-Abo bei Streaming-Diensten nutzen.
D) Einwilligung der abgebildeten Person
E) Musik und Medien-Daten Dritter nur mit 1–2 engsten Freunden teilen.
F) - Bluetooth und WLAN in der Öffentlichkeit abschalten.
- Nicht mit unbekannten Geräten zusammenschalten.
- Bluetooth-Verbindungen auf „unsichtbar“ schalten.
- GPS-Ortung nur gewollt einschalten.
G) Daten auf dem Handy im Menü „Einstellungen/Gerätesicherheit“ verschlüsseln. Davor Backup machen.
H) Anti-Viren-App installieren
I) Niemals Bankdaten, Kreditkarteninfos oder Passwörter per E-Mail versenden.
J) Bildschirmsperre mit PIN, Tastatur-Muster oder Passwort
K) Fremden nicht zu viel Persönliches preisgeben wie Adresse, E-Mail oder Geburtsdatum.
L) Für jedes Online-Konto ein eigenes, sicheres Passwort verwenden und sich nach der Online-Sitzung abmelden.
M) Keine Browser-Erweiterungen (Add-Ons) installieren.
N) Regelmäßiges Backup wichtiger Daten
O) Apps nur aus den offiziellen Playstores herunterladen.
P) Erlaubnis einholen zur Nutzung von Mediendaten anderer Personen.
Q) Adressleiste im Browser auf Seriosität überprüfen.
R) Nur technisch notwendige Cookies erlauben.
S) Handyhülle individuell wählen, um Verwechslungen zu vermeiden.
T) Bei Registrierung im Online-Dienst nur notwendige Angaben machen.
U) Keine Anhänge unklarer Herkunft öffnen oder verdächtige Links anklicken.
V) Smartphone nie unbeaufsichtigt offen liegen lassen.
W) Installation einer mobilen Sicherheits-App, die das Handy nach Spyware durchsucht.
X) Geräte-Software immer auf dem neuestem Stand halten und Aktualisierungen durchführen.

Abbildung 6b

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

HAUSAUFGABE

Lösungsvorschlag:

Mein Smartphone ...	Ja/Name/Funktion/Wann?	Nein
... ist immer unter Aufsicht und bei mir.	Ja	
... hat eine Bildschirmsperre.	Ja, PIN / Fingerabdruck, Muster-PIN	
... hat die SIM-Karte per PIN-Abfrage geschützt.	Ja, die PIN-Abfrage ist aktiviert.	
... verwendet sichere Passwörter.	Ja, niemals persönliche Daten wie Geburtstag oder 0000, 1111, 1234.	
... hat gerade ein Sicherheits-Software-Update aktualisiert.	Ja, in dieser Woche.	
... hat eine Antivirus-App installiert.	Ja, kostenlose App, z. B. McAfee oder Avast.	
... hat nur Apps aus dem offiziellen Play-/App- Store installiert.	Ja, ich habe in „Einstellungen“ die Installation von Apps unbekannter Herkunft blockiert.	
... hat alle Apps auf dem aktuellen Stand.	Ja, ich mache regelmäßig anstehende Updates.	
... hat Bluetooth, WLAN und GPS-Ortung nur, wenn ich es aktiviere.	Ja, ich aktiviere diese Funktionen bewusst unter „Einstellungen“, wenn ich sie nutzen möchte.	

EINSTIEG UND MOTIVATION

Lösungsvorschlag:

Impuls-Szenario:
Der Besuch einer unseriösen Website oder ein kurzer, unbeaufsichtigter Moment am Handy reicht aus, damit eine Spionage-App, wie z. B. FlexiSpy, illegal installiert werden kann. Nach der Installation verbirgt die App ihre Dateien, sodass die Spionage-App nach außen kaum erkennbar ist. Nur an einem erhöhten Datenvolumen, verkürzter Akku-Laufzeit oder verlangsamten Prozessen könnte man erkennen, dass eine solche App auf dem Smartphone installiert wurde. Zudem sperrt die App ihre Dateien, sodass eine Deinstallation verhindert wird. Die Spionage-App kann alle Aktivitäten wie Chat-Verläufe, Standort-Daten, Anrufprotokolle, Kalendereinträge, Textnachrichten oder die Kamera auslesen und per Internet auf einen Server schicken. Dort können die Inhalte mitgelesen werden.

Mögliche Erfahrungen der Schülerinnen und Schüler:
- Tracking-Apps verfolgen meine Surf-Aktivitäten und Vorlieben im Internet und blenden personalisierte Werbung ein.
- Privater Chat-Verlauf wird als Screenshot weiterverbreitet.
- Private Fotos werden von Dritten ohne Erlaubnis in sozialen Netzwerken veröffentlicht.
- Man erhält Fotos, Videos mit unangenehmen Inhalten (Gewalt, Sex, politischer Extremismus).
- Identitätsdiebstahl und Anmeldung bei Kontaktbörsen unter falschem Namen.
- Durch Klicken eines Links ein Schadprogramm herunterladen.
- Der Aufenthaltsort kann verfolgt werden.
- Hohe Kosten durch Drittanbieter aus Schadprogrammen.
- Falsche Warenbestellungen
- Hohe Mobilfunkrechnung durch Nutzung mobiler Datendienste im Ausland ohne Internet-Flat.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

1. DATENSCHUTZ, DATENSICHERHEIT UND URHEBERRECHT

JURISTISCHE RECHTSPOSITIONEN UND MASSNAHMEN

Lösungsvorschlag:

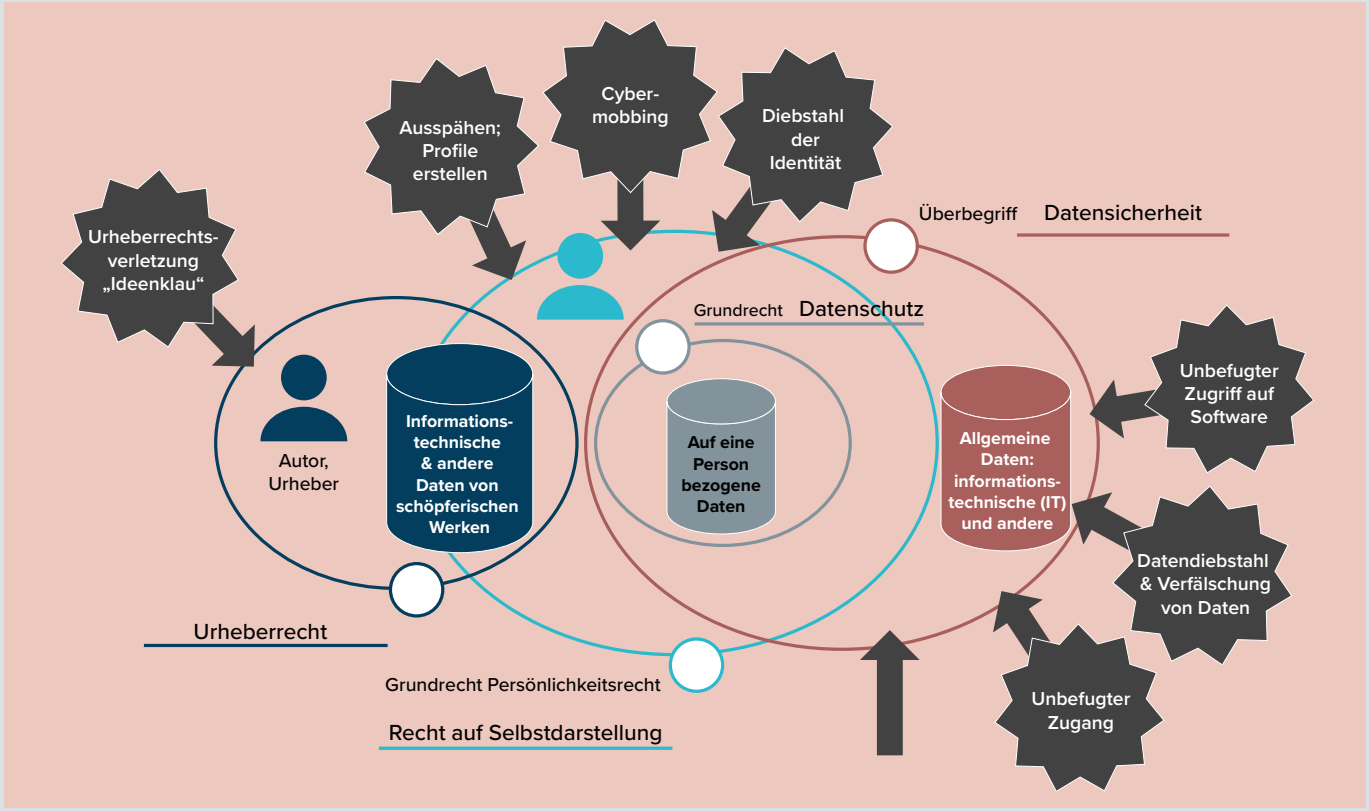
Das Persönlichkeitsrecht ist ein umfassendes Grundrecht und in mehrere Einzelschutzrechte unterteilt. Die verschiedenen Einzelrechte schützen die Persönlichkeit, also das Ansehen, die Ehre und die persönlichen Daten sowohl in der analogen Welt als auch in der digitalen Datenverarbeitung. Es umfasst besonders das **Recht auf Selbstbestimmung** und das **Grundrecht Datenschutz**. Dieses wird auch als das **Recht auf informationelle Selbstbestimmung** bezeichnet.

A	B	C	D
Recht auf Selbstdarstellung	Grundrecht auf Datenschutz	Urheberrecht	Datensicherheit
C	**A**	**B**	**D**
Dieses Recht schützt das geistige Eigentum einer Person an ihren Werken, das sind z. B. Texte, Musik, Bilder oder Fotos. Dazu gehören auch Werke in digitaler Form. Das Recht verhindert, dass andere die Werke des Urhebers ohne dessen Erlaubnis nutzen.	Dieses Recht stellt sicher, dass die Person selbst darüber bestimmt, wie sie sich in der Öffentlichkeit darstellt. Sie entscheidet selbst, wie und ob ihr Name, ihr Bild oder das eigene Wort veröffentlicht wird. Außerdem ist die Ehre geschützt, d. h. niemand darf die Person öffentlich beleidigen oder ihr falsche Aussagen unterschieben.	Dieses Recht stellt sicher, dass eine Person selbst darüber bestimmt, ob und wem sie ihre eigenen, personenbezogenen Daten anvertraut und wie die Daten dann verwendet werden dürfen. Dieses Recht schließt auch die Speicherung und Verarbeitung der Daten in Computersystemen ein.	Dies ist ein Überbegriff für technische und organisatorische Maßnahmen zur Sicherung von Daten. Damit sind alle Daten gemeint, also allgemeine und personenbezogene Daten, analoge Daten (z. B. Akten) aber auch digitale Daten. Die Maßnahmen umfassen Technik und Organisation, um die Daten gegen Bedrohungen zu sichern. Solche Bedrohungen können z. B. Verfälschungen, unerlaubte Einsicht in Daten und die Zerstörung oder der Verlust von Daten sein.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

GELTUNGSBEREICHE DER RECHTE UND MASSNAHMEN

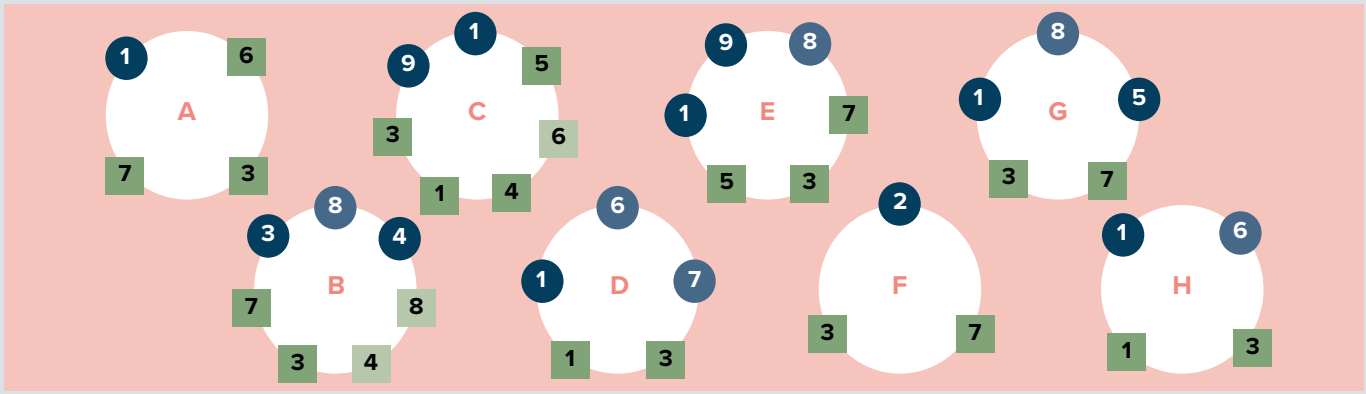
Lösungsvorschlag:



2. SICH IM INTERNET BEWEGEN: RECHTLICHE SICHT UND DATENSICHERHEIT

AKTIVITÄTEN UND DATENKATEGORIEN BEI UP- UND DOWNLOADS

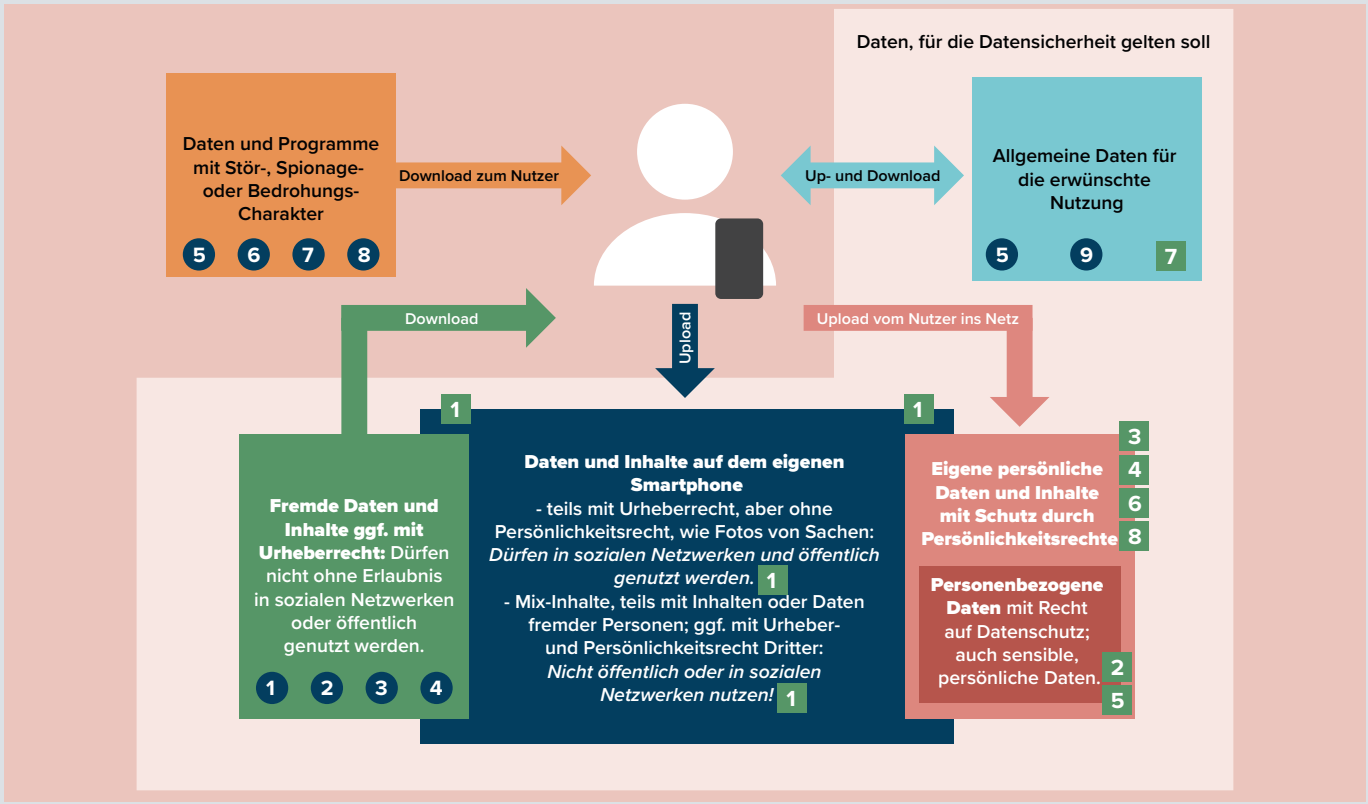
Lösungsvorschlag:



HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

JURISTISCHE SCHUTZRECHTE UND SICHERHEITSBEDINGUNGEN

Lösungsvorschlag:



BONUSAUFGABE: PASSWORT KNACKEN

- Die Entwicklung der Formel: Anzahl der Zeichen N von 0–9 ist N=10 Für jedes Zeichen N_1 an der ersten Stelle kann die zweite Stelle N_2 je 10 Zeichen und die dritte Stelle N_3 auch 10 Zeichen annehmen. Die Stellen multiplizieren sich. Die Anzahl der Kombinationen = N_1*N_2*N_3 = 10*10*10 = 1.000 Möglichkeiten.
- Die Methode zur Verbesserung der Passwort-Sicherheit: Wenn die Zahl der Versuche auf 3 begrenzt wird, ist die Treffer-Wahrscheinlichkeit sehr klein.
- Die Kombinationsmöglichkeiten für größeren Zeichenvorrat: Anzahl der Zeichen N_1 ist a–z = 26, zusätzlich A–Z = 26, zusätzlich 0–9 = 10. An der Stelle N_1 können also insgesamt 62 verschiedene Zeichen auftreten. Dasselbe gilt für N_2 und N_3. Also N_1 = N_2 = N_3 = 62. Die Kombimöglichkeiten jeder Stelle multiplizieren sich, also ergibt sich wie oben: Kombinationsmöglichkeiten: N_1*N_2*N_3 = $(N_1)^3$ = 238.328. Das sind 237.328 Möglichkeiten mehr als im ersten Beispiel, also rund das 238-fache.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

3. SCHUTZMASSNAHMEN FÜRSMARTPHONE UND NUTZER

BEDROHUNGEN UND RECHTSVERLETZUNGEN

Lösungsvorschlag:

GRUPPE „UPLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Unbefugter Zugang - Diebstahl - Unbemerkte Fremdnutzung **ist, wenn ...**	... sich ein Krimineller z. B. in sozialen Netzwerken oder per E-Mail mit falscher Identität ausgibt. Das erlaubt ihm, im falschen Namen einzukaufen, Online-Banking zu machen, den Ruf zu schädigen oder falsche Anrufe zu tätigen.
Datendiebstahl - aus internem oder externem Speicher oder - Verfälschung von Daten **wird möglich, wenn ...**	... unerwünscht eindringende Schadprogramme auf das Software-System zugreifen und es beschädigen. Die Schadprogramme können ferngesteuert werden und geheime Zugangsdaten ausspähen, unbemerkt Sicherheitslücken erzeugen, Daten zerstören und Systemfunktionen beschädigen.
Mit Schadsoftware wie - Virus - Malware - Schadprogrammen **infiziert sich das Smartphone dadurch, dass ...**	... das Opfer durch Messenger-Dienste wie Chats oder Anrufe beleidigt, bedroht oder bloßgestellt wird. Es werden Unwahrheiten und gefälschte Medien verbreitet.
Identitätsdiebstahl bedeutet, dass ...	... das Handy nicht verschlüsselt ist oder externe Speicher wie Datenbanken geknackt, Daten entwendet oder verändert werden. Das sind z. B. Daten wie E-Mail-Adressen oder Daten aus einem Online-Speicher.
Cybermobbing bedeutet, dass ...	... jemand unerlaubt und unbemerkt das Smartphone mit allen Daten nutzt, entwendet oder ausliest. Sensible Daten auf Smartphone und SD-Karte wie Fotos, E-Mails oder Passwörter können unerlaubt kopiert, verarbeitet und verfälscht werden und unbefugten Zugang zu den eigenen Konten ermöglichen.

GRUPPE „DOWNLOAD“

BEDROHUNG	MÖGLICHE RECHTSVERLETZUNG
Ausspähen, d. h. - ausgespäht werden durch Spionage-Apps (Spyware) **liegt vor, wenn ...**	... „Tracker“-Apps auf Webservern sich merken, welche Seiten besucht werden, wie auf der Seite agiert wird und entsprechende personalisierte Werbebanner und Interessenprofile erstellen. Örtliche Bewegungsprofile entstehen durch Sammeln der personenbezogenen Daten aus Online-Aktionen an verschiedenen Orten.
Profile wie - Persönlichkeitsprofil - Bewegungsprofil **werden dadurch erstellt, dass ...**	... Fotos und Mediendaten mit und ohne Abbildung anderer ohne Erlaubnis veröffentlicht und geteilt werden.
Unter der **Urheberrechtsverletzung**, also „Ideenklau“, versteht man, dass ...	... eine Spyware-App das Nutzerverhalten überwacht. Sie hat Zugriff auf Nachrichten, Browserverläufe, Anruflisten und Chats in sozialen Medien.
Datenverlust bedeutet, dass ...	... Daten beabsichtigt oder unbeabsichtigt gelöscht werden, unauffindbar oder zerstört sind.
Eine **Verletzung des Persönlichkeitsrechts anderer** ist, dass ...	... von anderen Personen erstellte Fotos oder Mediendaten ohne Erlaubnis heruntergeladen, gespeichert und getauscht werden. Das gilt auch für Videos und Musik aus illegalen Quellen und für eigene Mix-Produktionen und Collagen aus Vorlagen anderer.

HINWEISE UND LÖSUNGEN ZU DEN AUFGABEN

„INFEKTIONS-“ UND ZUGANGSWEGE / SCHUTZMASSNAHMEN

Lösungsvorschlag:

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „UPLOAD“

1. Unbefugter Zugang	2. Datendiebstahl	3. Schadprogramme und unbefugter Zugriff auf Software	4. Identitäts-Diebstahl	5. Cybermobbing
• Das Smartphone liegt ohne Aufsicht sichtbar und zugänglich herum. • Es ist keine Bildschirmsperre aktiviert. • Die Daten sind im internen Speicher und auf der SD-Karte unverschlüsselt.	• Daten im internen Handy-speicher und auf der SD-Karte sind nicht ver-schlüsselt. • WLAN- und Bluetooth-Verbindung als Zugang zum Handy.	• Merkwürdige E-Mail oder Social-Media-Nachricht mit Link oder Anhang • Versteckt in Apps von unseriösen Anbietern • Infizierte Website	• Das Abfangen von Zu-gangsdaten zu Online-Accounts, z. B. mit gefälschten E-Mails oder Websites. • Häufig reicht das Wissen von Name, Adresse und Geburtsdatum des Opfers für die falsche Identität aus.	• Fremde legen falsche Identität in sozialen Netz-werken an. • Fremde Personen kennen private Daten von Dritten.
V J B S	G F	O H X U	Q I K L	K T

„INFEKTIONS-“ UND ZUGANGSWEGE
GRUPPE „DOWNLOAD“

6. Ausspähen	7. Profile erstellen	8. Urheberrechtsverletzung	9. Datenverlust	10. Verletzung des Persönlichkeitsrechts
• Die Installation der Spio-nage-App durch Sicher-heitslücken beim Besuch krimineller Websites. • Durch die manuelle Installa-tion durch Fremde.	• Durch umfangreiche Berechtigungen bei Apps oder in den sozialen Netzwerken. • Cookie-Erlaubnis im Browser • Browser-Erweiterung und Tracking-Apps auf der Web-site erfassen Surf-Aktivität und Vorlieben. • Die Standorterfassung durch Bluetooth, WLAN und GPS.	• Von Dritten gemachte Fotos oder Musik werden ohne Erlaubnis weiterver-breitet oder veröffentlicht. • Das kostenloses Herunterladen und Speichern von aktuellen Mediendaten wie Songs oder Filmen von unseriösen, illegalen Websites. • Das Veröffentlichen von eigenen Produktionen mit Versatzstücken aus fremden Medien-Dateien.	• Datenverlust nach „Hard-Reset“. Das Handy wird nach fehlerhaftem Betrieb zurückgesetzt. • Daten werden versehentlich gelöscht. • Das Smartphone geht kaputt.	• Das Veröffentlichen oder Teilen von Fotos und Mediendaten mit und ohne Abbildung anderer ohne deren Erlaubnis in den sozialen Netzwerken oder im Internet.
W A	R M T F	P E C	N	D