DE

SMART 04

Mobile Sicherheit

In diesem Modul lernen Sie, auf was Sie bei der Nutzung mobile Technologien achten müssen.

Kurs starten >

Co-funded by the Erasmus+ Programme of the European Union

SMART MODUL 4

Mobile Sicherheit

In den letzten Jahrzehnten haben sich mobile Geräte weiterentwickelt. Dies hat den mobilen Zugang zu Bankgeschäften, Apps und dem Internet ermöglicht. Mit diesen neuen Funktionen wächst auch die Sorge um die Datensicherheit. In diesem Modul werden wir über Datenschutz, das Erstellen und Ändern von Passwörtern, sicheres Surfen im WLAN und den Schutz vor Cybermobbing und sogenannten Internet-Trollen sprechen.

Zielgruppe

Dieses Modul richtet sich an alle, die etwas über Datenschutz, sicherer Internetnutzung, Cookies sowie die rechtlichen Rahmenbedingungen (GDPR) lernen wollen.

Das Lernmaterial ist recht anspruchsvoll und es empfiehlt sich, es mit einer weiteren Person durchzuarbeiten.

Schulungsleiter:innen können Sich mit Hilfe des Materials weitebilden und Schulungen über Sicherheit im digitalen Zeitalter anbieten.

Was Sie in diesem Modul lernen werden

1. EU/ US Datenschutzrichtlinie GDPR.
2. Erstellen und Ändern von Passwörten.
3. Wie Sie verhindern, gehackt zu warden.
4. Wie Sie sich vor Cybermobbing schützen können.

Kapitel innerhalb des Moduls

1. Einführung: Mobile Sicherheit und Datenschutz.
2. Authentifizierung: Erstellen und Ändern von Passwörtern.
3. Wie schütze ich mein mobiles Gerät?
4. Umgang mit Cybermobbing.

SMART | MODUL 4 | KAPITEL 1

Einführung: Mobile Sicherheit und Datenschutz.

Persönliche Informationen sind eines der wertvollsten Güter, die wir besitzen. In der heutigen Zeit wird diese wichtige Ressource von vielen Verbraucher:innen völlig unterschätzt, nicht aber von den Unternehmen! Einige der größten Unternehmen der Welt sind durch die geschickte Nutzung Ihrer Daten erfolgreich geworden. In diesem Kapitel wird das Dateneigentum im Zeitalter mobiler Technik und der "Cloud" erläutert.

Was Sie lernen werden

1. Die Datenschutz-Grundverordnung der Europäischen Union (GDPR).
2. Schutz persönlicher Daten durch die GDPR.
3. Was sind Cookies?
4. Arten persönlicher Daten.
5. Wo werden Ihre Daten gespeichert?
6. Wie erstelle ich ein Backup meines mobilen Geräts?

Datenanalyse – ein rasant wachsendes Geschäft

Das Sammeln und Auswerten von Daten ist für Unternehmen wichtig, um die Bedürfnisse der Kund:innen zu verstehen. Die Analyse von Daten soll Unternehmen helfen, ihre Dienstleistungen zu verbessern.

Websites und Apps ermöglichen so z. B. dem/der Nutzer:in einer Smartwatch, die Anzahl der an einem Tag zurückgelegten Schritte zu sehen. Die Datenanalyse wird häufig auf (Ihre) persönlichen Daten angewandt.

Personenbezogene Daten

Personenbezogene Daten sind Informationen, die sich auf eine identifizierbare Person beziehen.

Unternehmen müssen personenbezogene Daten von Bürgern gemäß der **Allgemeinen Datenschutzverordnung (GDPR)** schützen, indem sie sensible Informationen, die gespeichert oder über öffentliche Netze gesendet werden, verschlüsseln.

Auf die GDPR wird später in diesem Kapitel eingegangen.

Warum Datenschutz auf mobilen Geräten so wichtig ist

Wenn eine Person oder eine Organisation ohne Zustimmung oder Erlaubnis Zugang zu persönlichen Daten (Adresse, Alter und Geschlecht, Gesundheitsfragen, finanzieller Status, Interessen usw.) erhält, kann dies zu Problemen für die Person führen, deren Daten gesammelt werden. Personenbezogene Daten sind Daten, die sich auf eine identifizierbare Person beziehen. Solche Informationen helfen dabei, einen Dienst für Sie zu personalisieren. Unternehmen müssen Ihre personenbezogenen Daten gemäß der **GDPR** schützen, indem Sie sensible Daten wie die oben genannten Beispiele für personenbezogene Daten, die über öffentliche Netze an Dritte gesendet werden, verschlüsseln: https://gdpr-info.eu/.

Die GDPR

Um zu verhindern, dass Unternehmen personenbezogene Daten von Bürger:innen ohne deren Zustimmung erhalten, hat die Europäische Kommission die Allgemeine Datenschutzverordnung (**GDPR**) eingeführt.

Die GDPR schützt die personenbezogenen Daten von Bürger:innen, die in der Europäischen Union leben und arbeiten.

GDPR – welche Rechte garantiert die EU?

Die GDPR gibt in Bezug auf Daten den EU-Bürger:innen:

- das Recht auf Information
- das Recht auf Auskunft
- das Recht auf Berichtigung und Löschung
- das Recht auf Einschränkung der Verarbeitung
- das Recht auf Datenübertragbarkeit
- das Recht auf Widerspruch
- das Recht auf automatisierte Profilerstellung

Welche Daten sind personenbezogen?

Um die Bedeutung der Datenschutzrechte in der EU zu verstehen, müssen wir die Arten von personenbezogenen Daten kennen, die von der GDRP abgedeckt sind.

Wir betrachten nun einige typische Beispiele für Daten, die als personenbezogene Daten betrachtet werden können und daher schützenswert sind.

Beispiele für personenbezogene Daten

1

2

3

Demografische Daten sind personenbezogen

Wenn eine Person ein Formular ausfüllt, um z. B. einen Zuschuss zu beantragen, vertraut sie der Organisation, die das Formular erstellt, dass sie sensible Informationen vertraulich behandelt. Dies ist eine Art von personenbezogenen Daten.

Beispiele für personenbezogene Daten

1

2

3

Krankenakten

Ein Arztbesuch gilt als vertraulich. Die Daten, die über eine/n einzelne/n Patient:in aufgezeichnet werden, sind ebenfalls höchst vertraulich und können daher als personenbezogene Daten betrachtet werden.

Beispiele für personenbezogene Daten

1

2

3

Aufzeichnung täglicher Aktivitäten

Eine Aufzeichnung der getätigten Einkäufe, besuchten Orte und unternommenen Reisen sind ebenfalls personenbezogene Daten.

Alltagsroutinen

Mobile Geräte zeichnen außergewöhnlich viele Details über die täglichen Aktivitäten einer Person auf. Viele dieser persönlichen Daten landen in den Cloud-Datenbanken von mobilen Apps. Anhand dieser Daten können Technologieunternehmen Ihnen detaillierte Informationen über Ihre Aktivitäten zur Verfügung stellen.

Beispiele für personenbezogene Daten

4

5

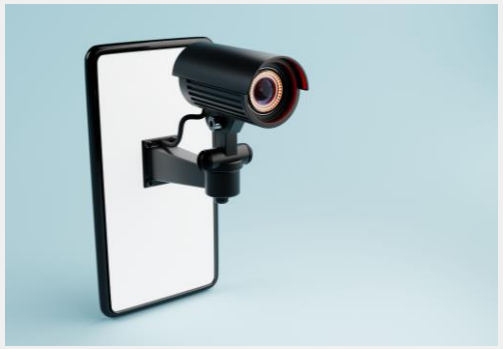
Individuelle finanzielle Informationen

Kontoauszüge, Kreditwürdigkeit und Bankguthaben sind eine weitere Kategorie personenbezogener Daten. Sie können dazu verwendet werden, Sie als ausgabefreudige oder zurückhaltende Person einzustufen.

Beispiele für personenbezogene Daten

4

5



Bilder und Aufnahmen von Personen

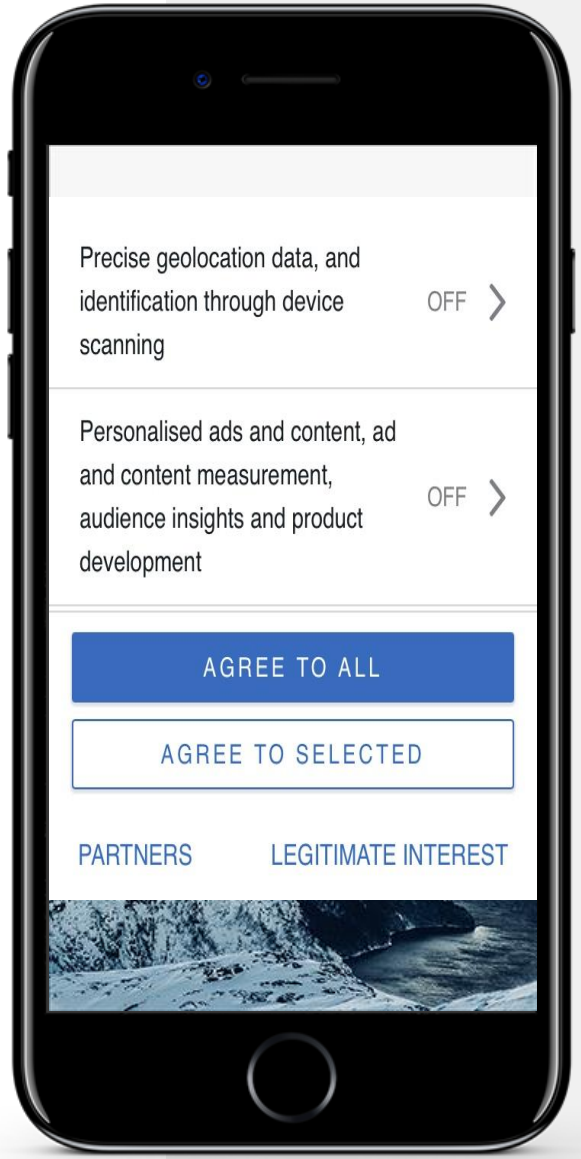
Besitzer:innen von Sicherheitskameras müssen bei der Speicherung von Videomaterial vorsichtig sein, da es personenbezogene Daten enthalten kann. Selbiges gilt für Tonaufnahmen. Beide sollten nur mit dem Einverständnis der betroffenen Personen aufbewahrt werden.

Cookies: Erlaubnis der Weitergabe personenbezogener Daten

Cookies sind kleine Dateien, die Websites an Ihr Gerät senden, um bestimmte Informationen über Sie zu speichern (z. B. Ihre Anmeldedaten).

Nach den Bestimmungen der GDPR muss eine Website die Zustimmung der Nutzer:innen zur Installation von Cookies auf seinem Gerät einholen.

Wenn Sie das nicht möchten, können Sie entweder die Optionen "Alle ablehnen" oder "Ausgewählten zustimmen" wählen (wie in der Abbildung hier gezeigt). Die Deaktivierung von Cookies bedeutet, dass die Website nicht personalisiert ist und sich nicht an Details wie ein Passwort oder Einkäufe erinnern kann.

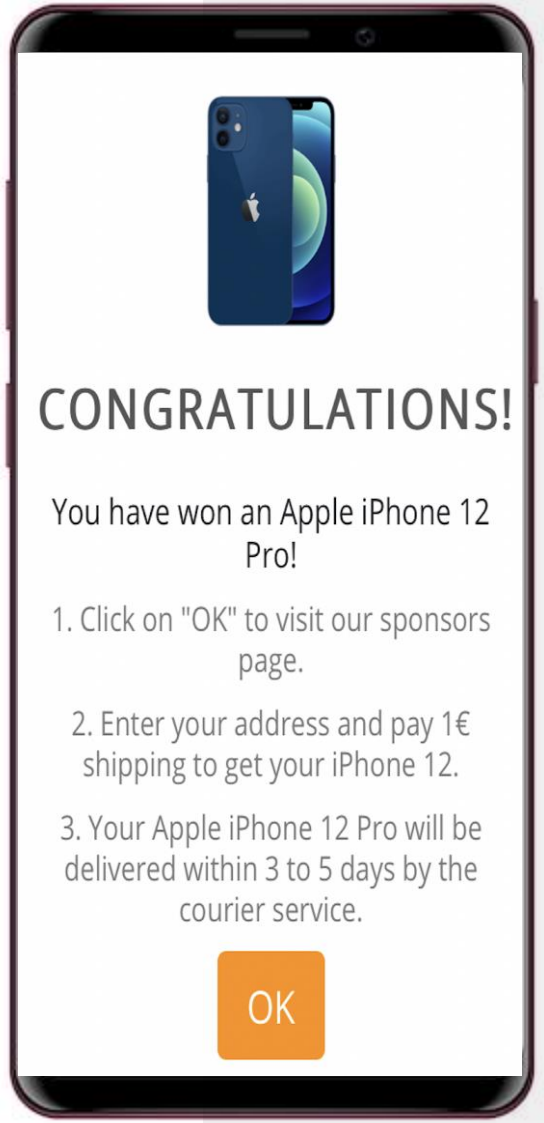


Aufpassen bei bestimmten Benachrichtigungen!

Manchmal erscheinen interessante Nachrichten auf Ihrem Mobilgerät. Wenn Sie eine Nachricht für einen Preis sehen, der zu schön ist, um wahr zu sein, handelt es sich in der Regel um einen Trick, Ihnen Geld zu stehlen.

Wenn Sie eine solche Nachricht erhalten, ist es wichtig, kein Formular auszufüllen, niemals auf einen Link zu klicken und keine persönlichen Daten weiterzugeben, es sei denn, Sie wissen, dass die Nachricht von einer vertrauenswürdigen Quelle stammt.

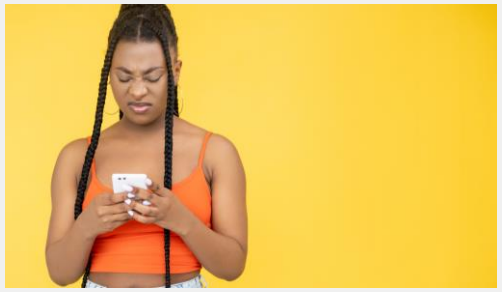
Auch bei Nachrichten, die Sie auf Ihrem Handy lesen, kann es sich um "Fakes" handeln - also um Nachrichten, die falsch oder erfunden sind.



Was ist die Cloud?

Die so genannte Cloud ist ein weltweites Netz von leistungsstarken Computern und der Software, die auf diesen Computern läuft. Ihre persönlichen Daten können von Ihnen erfasst und in einem Cloud-Computer irgendwo auf der Welt gespeichert werden. Von Ihnen erstellte Daten können ebenfalls in der Cloud gespeichert werden und Sie können von mehreren Geräten aus auf diese Daten zugreifen. Die Speicherung und Analyse erfolgt auf Cloud-Computern in einem Datenzentrum und nicht lokal auf dem Gerät der Nutzer:innen. https://www.cloudflare.com/en-gb/learning/cloud/what-is-the-cloud

Vorteile der Cloud-Nutzung



Problem: Der Gerätespeicher ist begrenzt

Die meisten mobilen Geräte haben nur eine begrenzte Speicher- und Rechenleistung. Irgendwann ist der Speicherplatz erschöpft und das Gerät ist weniger leistungsfähig.

Lösung: Daten in die Cloud auslagern

Dateien, Fotos und Videos können in die Cloud kopiert werden. Cloud-Computer sind sehr leistungsfähig und können viele Daten speichern. Es ist jedoch wichtig, zu berücksichtigen, dass sie auch in der Cloud Ihre Daten schützen müssen.

Datenschutz

Wie sicher sind Daten, auf einem Cloud-Computer gespeichert sind?

Abgesehen davon, dass Unternehmen die Daten der Nutzer:innen nutzen, können persönliche Daten in der Cloud gehackt und für kriminelle Zwecke verwendet werden. Die Sicherheit der Cloud ist wichtig für persönliche Daten und mobile Geräte. Stellen Sie sicher, dass Ihr Dienstanbieter und Ihre Daten in der EU ansässig sind.

Vor- und Nachteile der Cloud-Nutzung

Vorteile

- Personalisierung und besserer Service
- Mehr Speicherplatz
- Mehr Daten bedeuten "intelligentere" Entscheidungen
- Alle Daten sind "an einem Ort„

Nachteile

- Möglicher Verlust des Datenschutzes
- Möglichkeit von Diebstahl und Betrug
- Schwierig, hochgeladene Daten zu löschen

Quiz

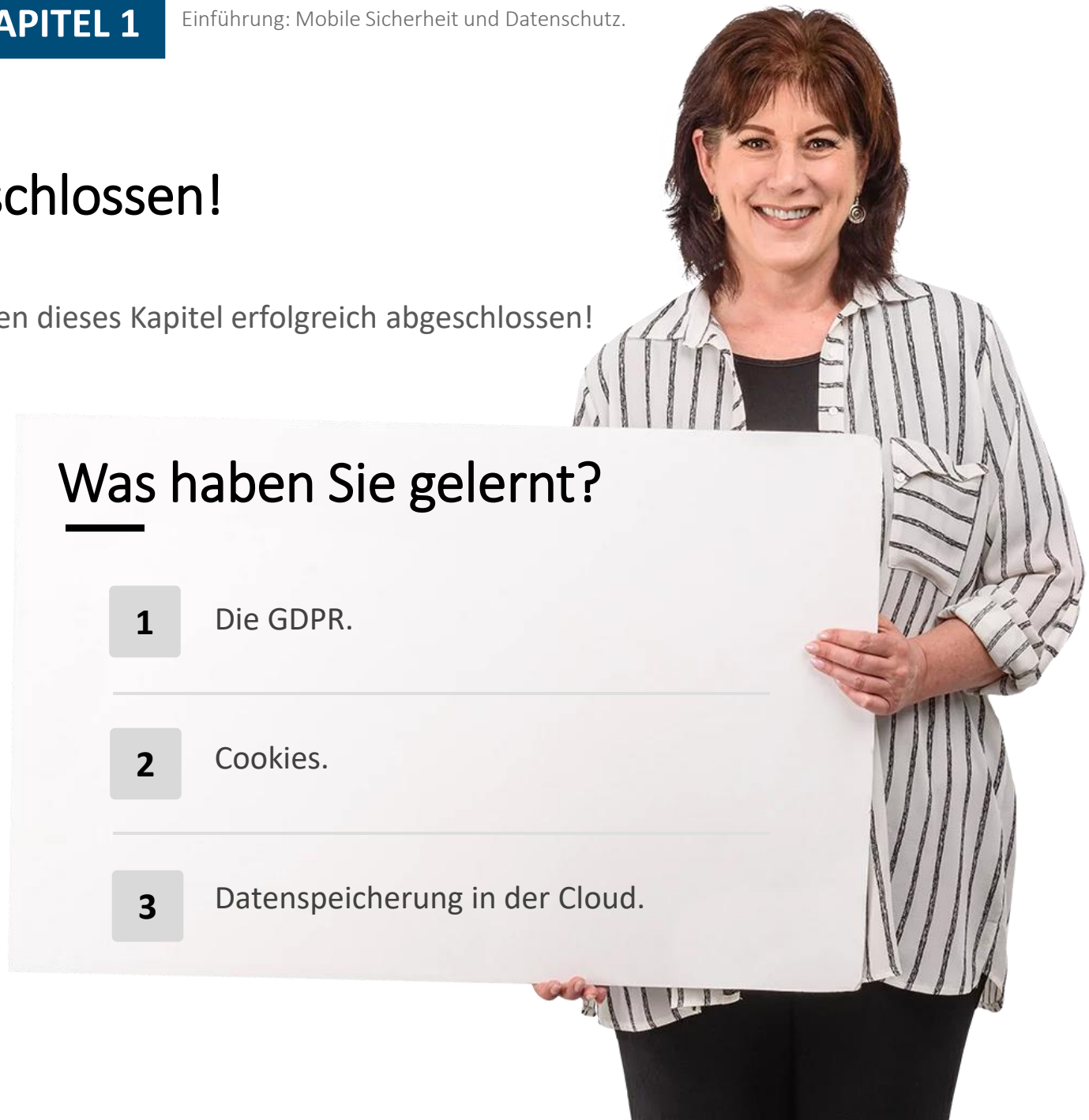
Click the **Quiz** button to edit this object

Zusammenfassung von Kapitel 1

1. Datenschutz
2. Datenschutz durch GDPR
3. Cookies
4. Cloud-Nutzung
5. Datenspeicherung in der Cloud
6. Verständnis für den Datenschutz bei mobilen Daten

Kapitel abgeschlossen!

Glückwunsch! Sie haben dieses Kapitel erfolgreich abgeschlossen!



Was kommt als Nächstes?

Nun können Sie entweder dieses Kapitel wiederholen oder unserer Lernempfehlung folgen, indem Sie auf eine der unten stehenden Schaltflächen klicken:

Wiederholen

Weiter

SMART | MODUL 4 | KAPITEL 2

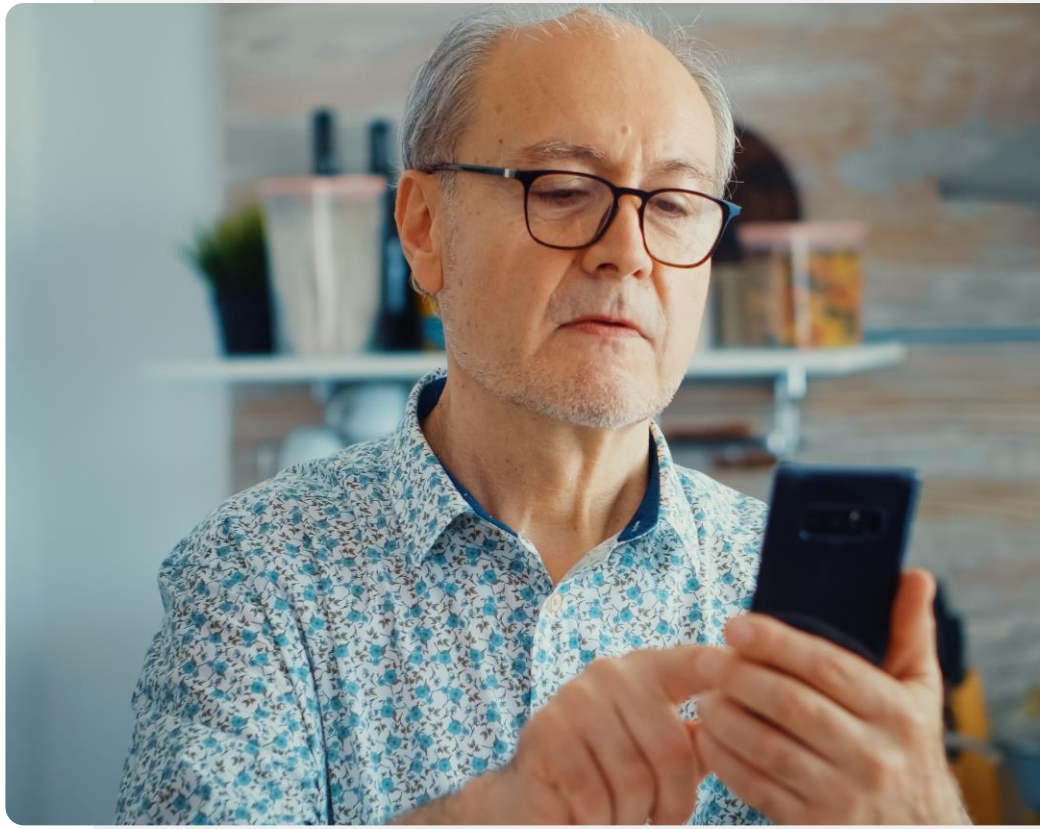
Authentifizierung: Erstellen und Ändern von Passwörtern

In diesem Kapitel erfahren Sie mehr über die Authentifizierung, d. h. die Erkennung der Identität, um den Zugriff auf Dienste zu ermöglichen. Die Authentifizierungstechnologie unterstützt die Sicherheit und den Schutz von persönlichen Daten. Hier lernen Sie Arten der Authentifizierung und biometrische Ansätze kennen und erfahren, wie Sie sichere Passwörter erstellen.

Authentifizierung – wie Geräte ihre Nutzer:innen erkennen

Unter **Authentifizierung** versteht man das Verfahren zur Erkennung der Identität eines Nutzers. Dies geschieht häufig beim Öffnen einer App und dient der Überprüfung, um sicherzustellen, dass nicht eine andere Person ihre Daten einsehen kann.

Verschiedene Systeme verlangen unterschiedliche Informationen, die so genannten **Credentials**, um eine Identität zu bestätigen. Dieser Berechtigungsnachweis ist oft ein Passwort, kann aber auch andere Formen der Authentifizierung umfassen. (https://www.veriff.com/blog/what-is-authentication)



Was Sie lernen werden

1. Wann benötigen Sie Authentifizierung?
2. Arten der Authentifizierung.
3. Erstellen eines sicheren Passworts.
4. Biometrische Authentifizierungsmethoden.

Arten der Authentifizierung

Die Möglichkeiten zur Authentifizierung von Mobilgerätebenutzer:innen haben in den letzten Jahrzehnten stark zugenommen.

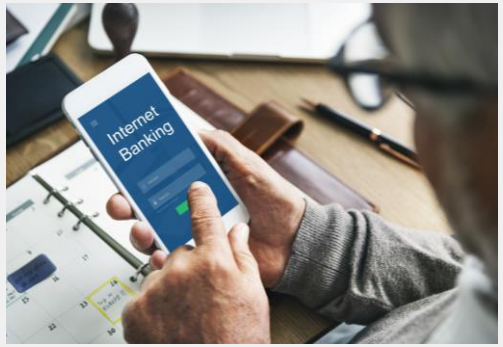
Im Folgenden werden einige der wichtigsten Authentifizierungsarten, die auf einem mobilen Gerät verfügbar sind, vorgestellt.

Arten der Authentifizierung

1

2

3



Passwörter

Passwörter sind wahrscheinlich die häufigste Form der Authentifizierung. Sichere Passwörter enthalten in der Regel Buchstaben, Zahlen und andere Zeichen. Dieses Thema wird später in diesem Kapitel behandelt.

Arten der Authentifizierung

1

2

3

Zertifikate

Ein digitales Zertifikat ist ein elektronisches Dokument, das auf dem Konzept eines Führerscheins oder eines Reisepasses basiert. Ein Beispiel ist das digitale Zertifikat, das die vollständigen Impfdaten für die COVID-19-Impfung enthält.

Arten der Authentifizierung

1

2

3

Biometrische Authentifizierung

Die biometrische Authentifizierung ist ein Sicherheitsverfahren, das auf einzigartige Merkmale der Gerätebesitzer:innen wie Gesicht, Stimme oder Fingerabdrücken beruht. Mobile Geräte unterstützen verschiedene biometrische Authentifizierungsansätze.

Arten der Authentifizierung

4

5

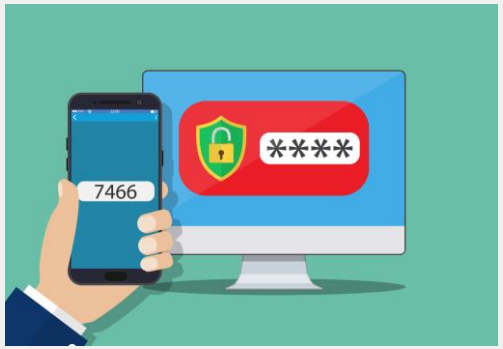
Token

Bei diesem Ansatz müssen die Nutzer:innen ihre Anmeldedaten nur einmal eingeben und erhalten einen geheimen digitalen Schlüssel - einen sogenannten Token. Das kann beispielsweise eine elektronische Fahrkarte sein.

Arten der Authentifizierung

4

5



Zwei-Faktor Authentifizierung

Bei der Anmeldung (z. B. auf bestimmten Webseiten), wird ein Code an das hinterlegte Mobilgerät gesendet, der in eine App oder auf einer Website eingegeben werden muss. Dies nennt sich Zwei-Faktor-Authentifizierung.

Passwörter

Die wahrscheinlich beliebteste Art der Authentifizierung, die seit vielen Jahren auf mobilen Geräten verwendet wird, ist das Passwort.

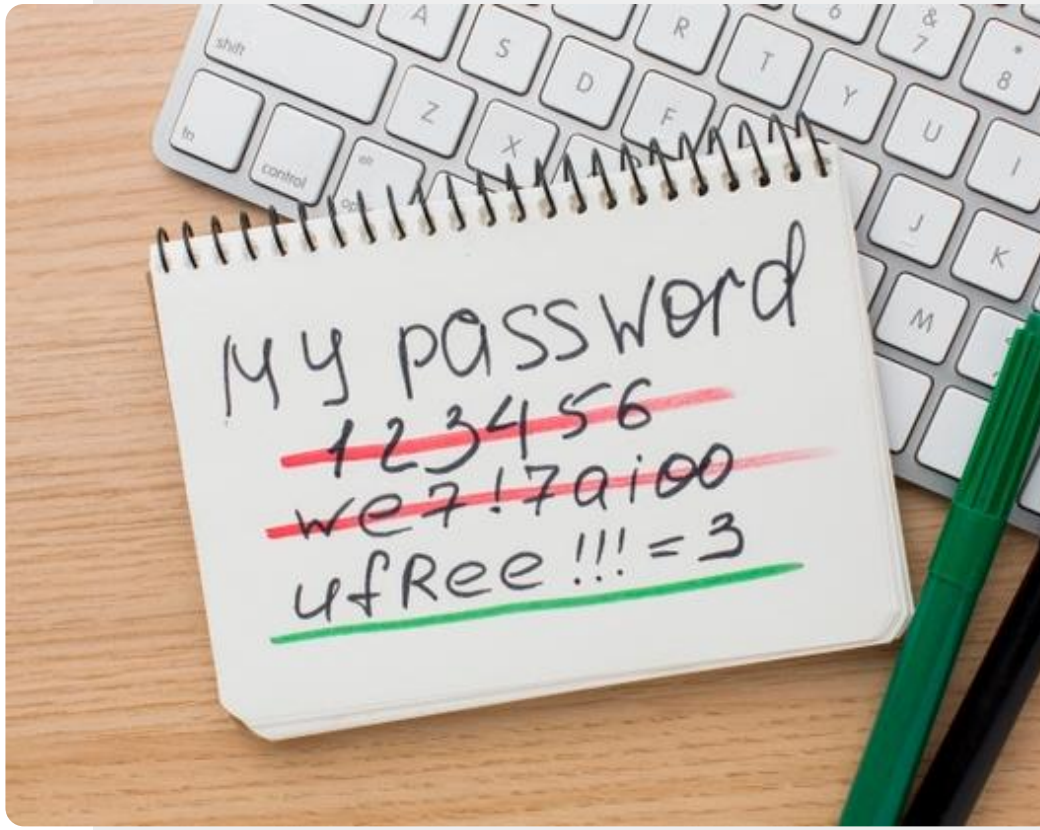
Das Passwort auf dem Bild ist leicht zu erraten und daher nicht sehr sicher. Überlegen Sie sich ein stärkeres Passwort!

Starke Passwörter

Viele Webseiten verlangen, dass Sie ein Passwort wählen, das einige der folgenden Eigenschaften aufweist:

- Mindestens 8 Zeichen lang
- Enthält Groß- und Kleinbuchstaben
- Enthält eine Zahl
- Enthält ein Interpunktionszeichen

Schauen wir uns nun an, wie ein leicht zu merkendes Passwort mit diesen Elementen erstellt werden kann.



Ein starkes Passwort erstellen

1

2

3

Nehmen Sie ein bekanntes Wort

Schreiben Sie ein langes Wort oder Wörter auf, die für Sie eine große Bedeutung haben, aber für andere nicht offensichtlich sind.

Ein starkes Passwort erstellen

1

2

3

Ersetzen Sie einzelne Buchstaben

Nutzen Sie diese Zeichen für einzelne Buchstaben:

1 = ! e = 3 a = @ 8 = % E =£ I =| S = $ S = 5

C =(T = + G = 6 O = 0 I = 1 Z = 2 B = 8

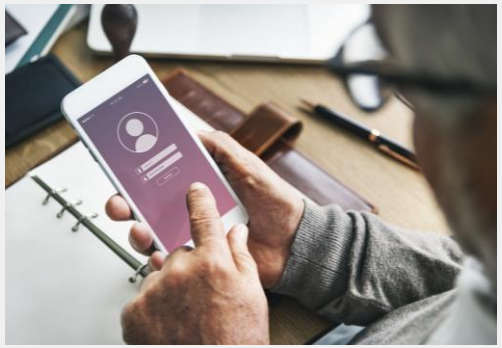
Ein Beispiel: **Caroline** könnte **(@rol1nE** heißen

Ein starkes Passwort erstellen

1

2

3



Benutzen Sie das Passwort

Falls Sie das Passwort auf einem Papier notiert haben, dann bewahren Sie es an einem sehr sicheren Ort auf, z. B. in einem Safe.

Sie können nun das neue sichere Passwort auf einem Gerät oder einer Website eingeben.

Schützen Sie ihr Passwort

Sobald Sie Ihr Passwort erstellt haben, müssen Sie es schützen.
Am besten ist es, wenn Sie es sich einfach merken, aber wenn Sie sich dazu entscheiden, es aufzuschreiben, sollten Sie es an einem wirklich sicheren Ort aufbewahren.
Sie sollten ein Kennwort NIEMALS irgendwo mit oder in der Nähe Ihres Gerätes aufbewahren.

Können Sie António helfen?

Antonio möchte ein starkes und sicheres Passwort erstellen.

✓Lernen Sie António kennen: hier

✓ António wählt **grenzenlos** als Ausgangswort für sein Passwort.

✓Wie können Sie **grenzenlos** zu einem starken Passwort machen? Schauen Sie sich die Arbeitsschritte auf den vorherigen Folien an.

Smartphones und SIM-Karten

Mobilgeräte können mit **Passwörtern** geschützt werden. SIM-Karten auf einem Gerät sind mit einem **PIN**-Code versehen, den Sie eingeben müssen, um auf das Netz zuzugreifen. Sie ermöglichen den Zugang zu den Kontakten auf Ihrer SIM-Karte und wenn das Gerät gestohlen wird, kann die SIM-Karte auch in ein anderes Gerät eingesetzt werden, um Ihr Guthaben zu nutzen. Wenn der **PIN**-Code dreimal falsch eingegeben wird, ist ein zweiter Code, der so genannte **PUK**-Code, erforderlich. Aus diesem Grund ist es wichtig, den **PIN**-Code und den **PUK**-Code an einem sicheren Ort aufzubewahren, sobald Sie sie mit Ihrem Gerät oder Ihrer SIM-Karte erhalten haben.

Biometrische Authentifizierung

Wir haben bereits erwähnt, dass ein biometrisches Authentifizierungssystem einzigartige Merkmale benutzt, um Ihnen den Zugriff auf das Gerät oder System zu ermöglichen.

Lassen Sie uns nun einige dieser Ansätze betrachten.

Biometrische Authentifizierung bei mobilen Geräten

1

2

3

Fingerabdrücke

Fingerabdrücke sind einzigartig. Viele moderne Mobilgeräte sind mit Fingerabdruckscannern ausgestattet und das Telefon kann entsperrt werden, indem der Finger auf den Fingerabdruckscanner gelegt wird, um das Telefon zu entsperren.

Biometrische Authentifizierung bei mobilen Geräten

1

2

3

Retina-Scan

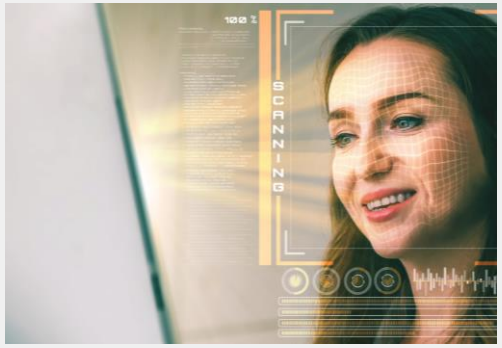
Genau wie Fingerabdrücke sind auch die Muster im Auge jeder Person einzigartig. Die Kamera in einigen Mobilgeräten kann das Netzhautmuster erkennen und es zum Entsperren des Geräts verwenden.

Biometrische Authentifizierung bei mobilen Geräten

1

2

3



Gesichtserkennung

Ein weiteres ähnliches Verfahren zur Authentifizierung ist der Gesichtsscan. Auch hier wird eine Kamera verwendet, um die einzigartigen Gesichtsmerkmale zu erkennen und das Gerät zu entsperren.

Können Sie Tom helfen?

Tom möchte ein Authentifizierungsverfahren an seinem Smartphone einrichten.

✓Lernen Sie Tom kennen: hier

✓ Tom hat früher in einem IT-Unternehmen gearbeitet und kennt sich mit Technik aus, aber er ist mit modernen Authentifizierungsverfahren nicht vertraut. Er möchte sein Smartphone sichern, damit andere nicht auf seine Daten zugreifen können.

✓Beraten Sie Tom anhand der Informationen, die Sie auf den vorherigen Folien erhalten haben. Welcher Authentifizierungsansatz passt am besten zu ihm?

Autorisierung

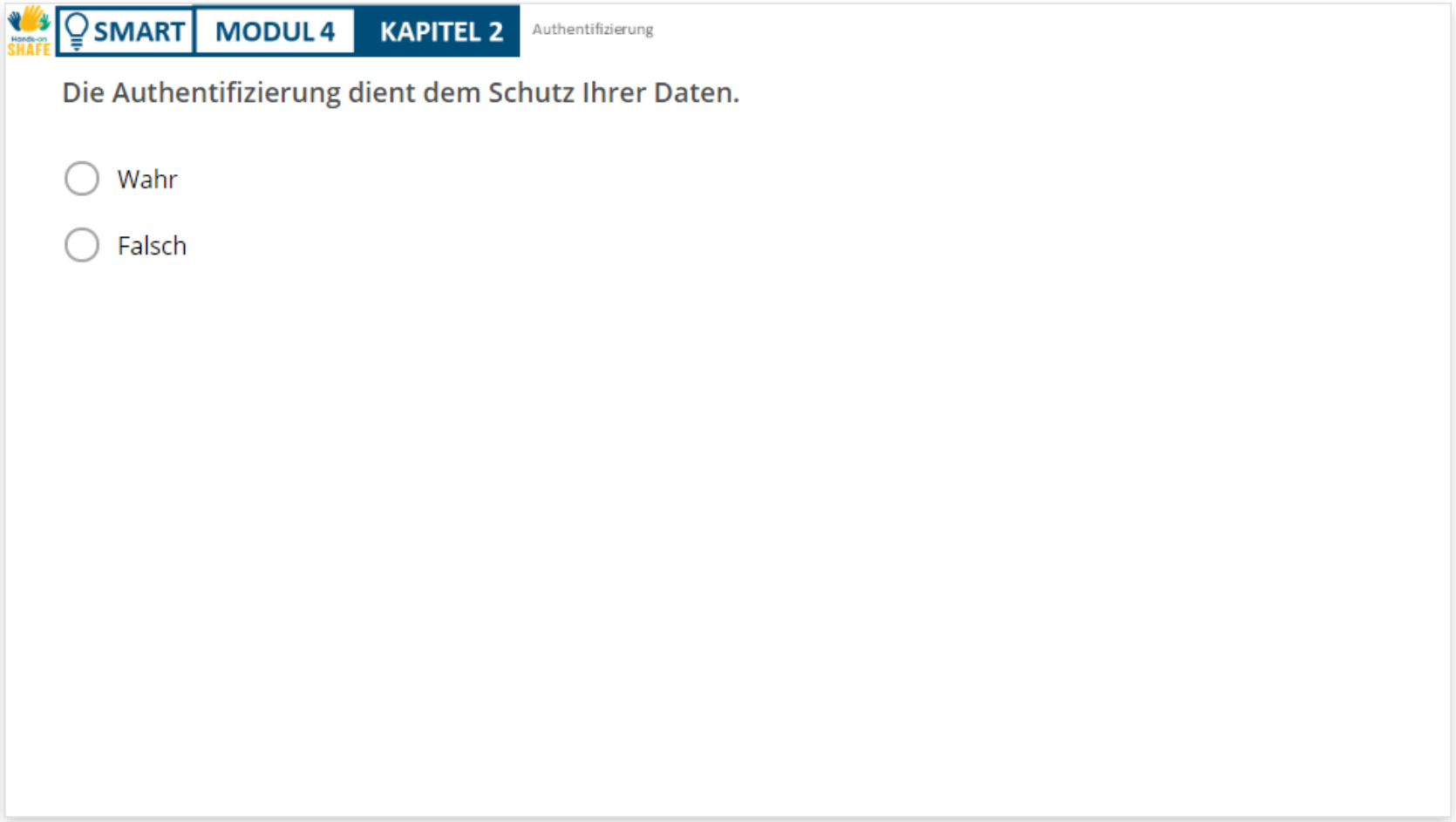
Sobald das Gerät Sie authentifiziert hat, haben Sie die Berechtigung, auf das Gerät oder System zuzugreifen.

Sie können die Berechtigung haben, alle Gerätefunktionen oder nur einige davon zu nutzen.

Es ist leicht, die Authentifizierung, die der Identifikation dient und die **Autorisierung**, die danach erfolgt, zu verwechseln.

Quiz

Click the **Quiz** button to edit this object

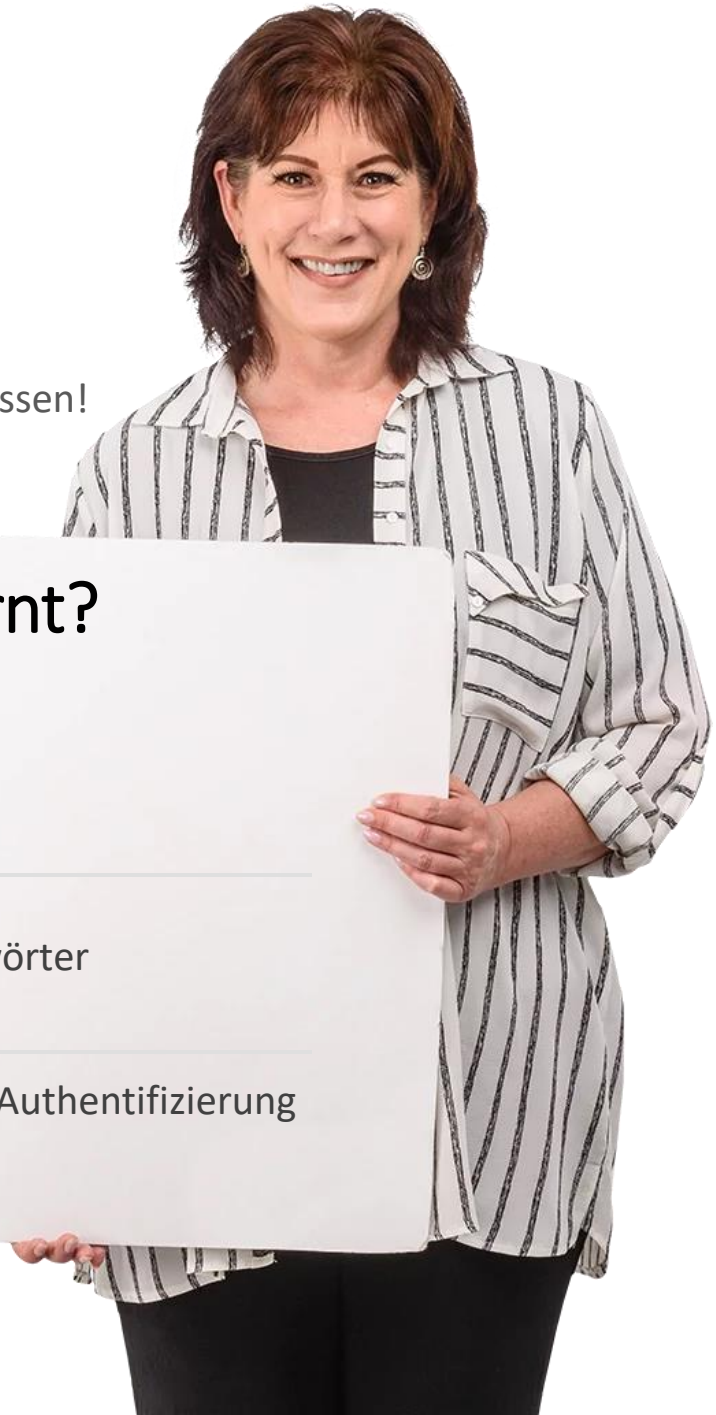


Zusammenfassung von Kapitel 2

1. Datenschutz und Authentifizierung
2. Arten der Authentifizierung
3. Erstellen von Passwörtern
4. Anwenden der Sicherheitsmaßnahmen

Kapitel abgeschlossen!

Glückwunsch! Sie haben dieses Kapitel erfolgreich abgeschlossen!



Was haben Sie gelernt?

1. Authentifizierung
2. Erstellen starker Passwörter
3. Unterschied zwischen Authentifizierung und Autorisierung

Was kommt als Nächstes?

Nun können Sie entweder dieses Kapitel wiederholen oder unserer Lernempfehlung folgen, indem Sie auf eine der unten stehenden Schaltflächen klicken:

Wiederholen **Weiter**

SMART MODUL 4 KAPITEL 3

Wie schütze ich mein mobiles Gerät?

Auch in der digitalen Welt müssen sie ihr Mobilgerät schützen. Es ist anfällig für Hacker:innen und Viren. In diesem Kapitel geht es darum, wie Sie Ihr Smartphone, Ihre Privatsphäre und Ihre Daten vor Cyberangriffen, z. B. Viren, schützen können.

Was Sie lernen werden

1. Schutz des Geräts vor unerlaubtem Zugriff.
2. Virenschutz.
3. Schadprogramme, Ransomware und DDoS.
4. Sichere Nutzung von HotSpots.

Schutz des Gerätes vor unerlaubtem Zugriff

1

2

3

Verschlüsseln Sie ihr Gerät

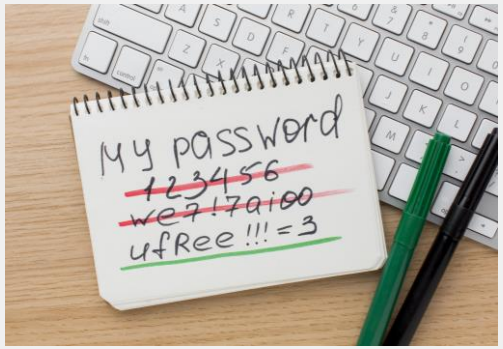
Sperren Sie Ihr Mobilgerät mit Passwörtern oder im Idealfall mit eingeschalteter biometrischer Authentifizierung. Sperren Sie Ihre SIM-Karte mit einem PIN-Code und bewahren Sie Ihre PIN- und PUK-Codes an einem sicheren Ort auf.

Schutz des Gerätes vor unerlaubtem Zugriff

1

2

3



Starke Passwörter benutzen

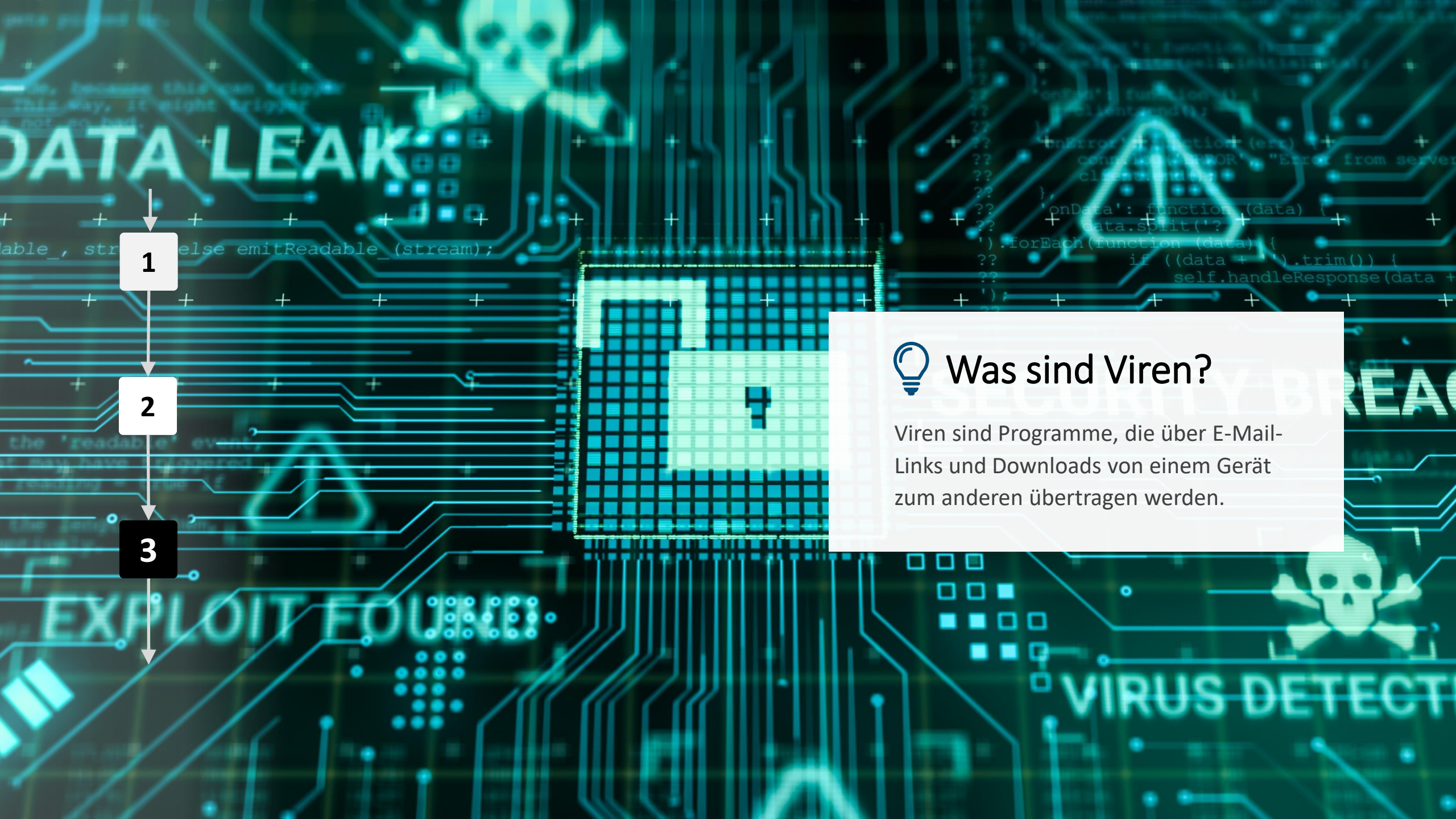
Im letzten Kapitel haben Sie gelernt, sichere Passwörter zu erstellen und zu verwenden, die Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Damit schützen Sie ihr Gerät vor unbefugten Zugriffen.

Schutz des Gerätes vor unerlaubtem Zugriff

1
2
3

Vorsicht bei Downloads

Laden Sie Dateien wie Dokumente, Videos, Musik oder Bilder nur von Webseiten herunter, denen Sie vertrauen (z. B. von Geräteherstellern oder großen Softwarefirmen). Dateien, die von nicht vertrauenswürdigen Webseiten heruntergeladen werden, können Viren enthalten und Ihre Hardware beschädigen. Webseiten mit Adressen, die mit https beginnen, schützen Sie davor.



Was sind Viren?

Viren sind Programme, die über E-Mail-Links und Downloads von einem Gerät zum anderen übertragen werden.

Schutz des Gerätes vor unerlaubtem Zugriff

4

5

6

Laden Sie aktuelle Software-Updates herunter

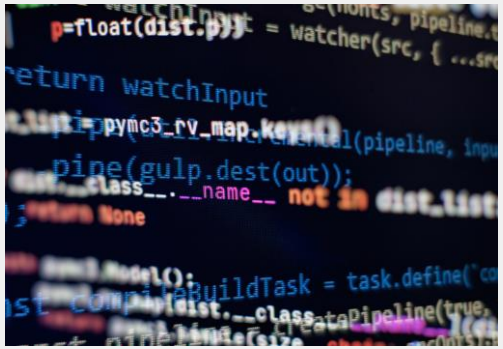
Der Hersteller des Mobilgeräts sendet Benachrichtigungen über neue Software-Updates. Updates helfen, ein Gerät vor Sicherheitslücken zu schützen, die es jemandem ermöglichen könnten, Daten von Ihrem Gerät abzugreifen. Laden Sie diese auf das Gerät herunter und aktualisieren Sie es.

Schutz des Gerätes vor unerlaubtem Zugriff

4

5

6



Daten verschlüsseln

Die meisten mobilen Geräte verfügen über eine Option zur Verschlüsselung Ihrer Daten. Durch die Verschlüsselung wird es für Unbefugte schwieriger, die auf dem Gerät gespeicherten Daten einzusehen. Autorisierte Benutzer:innen können das Gerät wie gewohnt verwenden.

Verschlüsselung

Verschlüsselung ist die Methode, mit der Informationen in unlesbare Codes umgewandelt werden, die die wahre Bedeutung der Informationen verbergen, außer für den/die Nutzer:in, der/die den Schlüssel hat.
Die Social-Media-App WhatsApp verfügt über eine Ende-zu-Ende-Verschlüsselung, so dass die Kommunikation zwischen zwei Nutzer:innen nicht von einer anderen Person "abgehört" werden kann.

Schutz des Gerätes vor unerlaubtem Zugriff

4

5

6

Öffentliches WLAN

WLAN in öffentlichen Räumen wie Flughäfen und Cafés kann riskant sein. Manchmal ist das, was Sie für das WLAN des Cafés halten, in Wirklichkeit der Laptop eines/r Hacker:in, der/die die Verbindung zu Ihrem Telefon für unlautere Zwecke nutzen kann. Seien Sie vorsichtig!

Öffentliches WLAN

Kriminelle spionieren manchmal öffentliche WLAN-Netzwerke aus und sammeln Daten, die online übertragen werden.

Auf diese Weise können sie an Bankdaten, Passwörter und andere sensible Informationen gelangen.

Vor-und Nachteile von öffentlichem WLAN

Vorteile

- Kostenlos
- Mobiles Datenvolumen wird nicht verbraucht
- Einfach zu verbinden
- Einfach verfügbar

Nachteile

- Nicht sicher
- Das WLAN des "Hotspots" könnte gefälscht sein
- Geringere Geschwindigkeit als Ihr eigener Mobilfunkempfang

Hackerangriffe

Ziel eines Hackerangriffs ist es, sich Zugang zu verschaffen, um Daten zu stehlen oder die Daten einer Organisation zu zerstören.

Schadprogramme, Ransomware, DDoS

*„Als **Schadprogramm** bezeichnet man Computerprogramme, die entwickelt wurden, um, aus Sicht des Opfers, unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Die bisher bekannte Malware kann man grundsätzlich in drei verschiedene Klassen einteilen: Die Computerviren, die Computerwürmer und die Trojanischen Pferde.“ (Quelle:* https://de.wikipedia.org/wiki/Schadprogramm)

*“**Ransomware** sind Schadprogramme, mit deren Hilfe ein Eindringling den Zugriff des Computerinhabers auf Daten, deren Nutzung oder auf das ganze Computersystem verhindern kann. Dabei werden private Daten auf dem fremden Computer verschlüsselt oder der Zugriff auf sie verhindert, um für die Entschlüsselung oder Freigabe ein Lösegeld zu fordern.“ (Quelle:* https://de.wikipedia.org/wiki/Ransomware)

“Denial of Service (DOS) bezeichnet die Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Häufigster Grund ist die Überlastung des Datennetzes.

*Im Fall einer durch eine Vielzahl von gezielten Anfragen verursachten, mutwilligen Dienstblockade spricht man von einer **Denial-of-Service-Attacke (DDoS)**”. (Quelle:* https://de.wikipedia.org/wiki/Denial_of_Service#Distributed-Reflected-Denial-of-Service-Angriff)

Können Sie Tom helfen?

Tom schützt sein Samrtphone mittels Authentifizierung. Gibt es noch weiter sinnvolle Maßnahmen?

✓Lernen Sie Tom kennen: hier

✓ Tom hat früher in einem IT-Unternehmen gearbeitet und kennt sich mit Technik aus. Er möchte sein Smartphone sichern, damit andere nicht auf seine Daten zugreifen können.

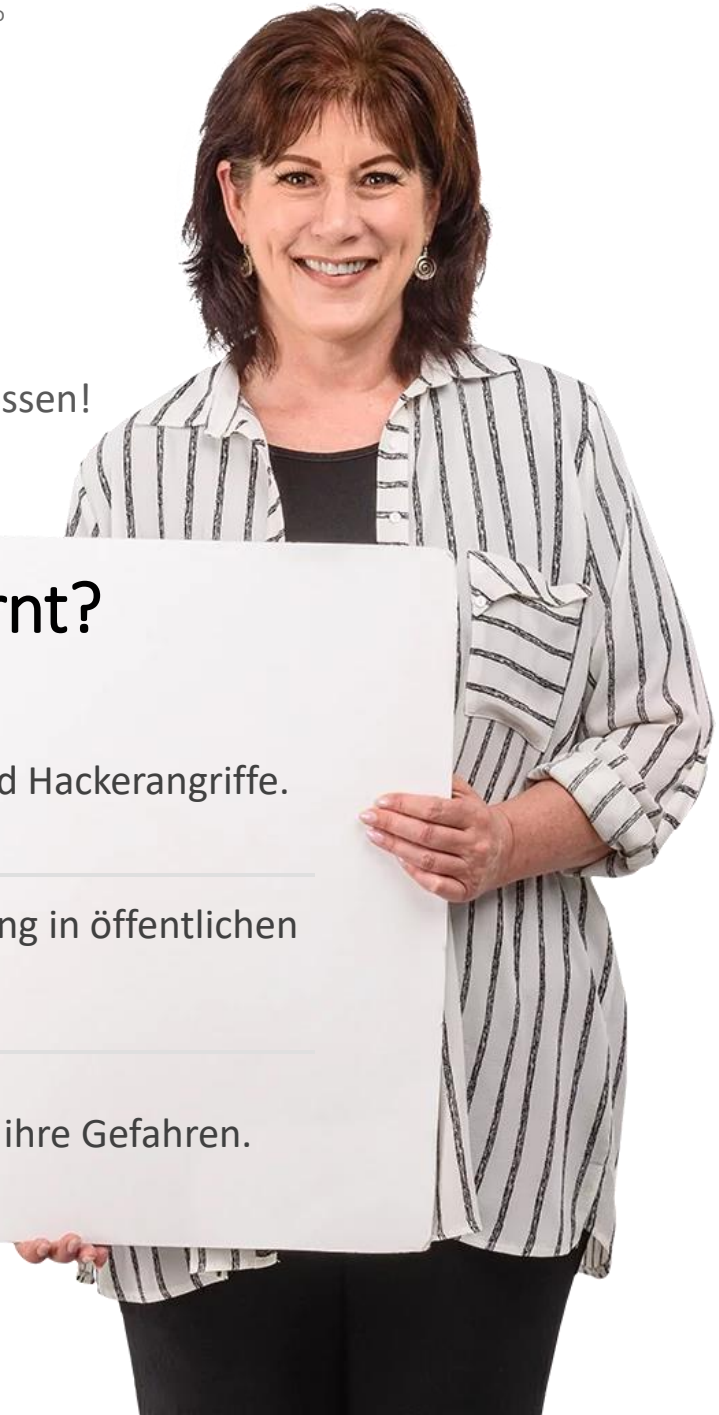
✓Beraten Sie Tom anhand der Informationen, die Sie auf den vorherigen Folien erhalten haben. Wie kann er sein Smartphone und seine Daten weiterhin gut schützen?

Zusammenfassung von Kapitel 3

1. Schutz mobiler Geräte.
2. Viren und Hackerangriffe.
3. Schadprogramme, Ransomware und DDoS.
4. Gefahren von öffentlichem WLAN.

Kapitel abgeschlossen!

Glückwunsch! Sie haben dieses Kapitel erfolgreich abgeschlossen!



Was haben Sie gelernt?

1. Schutz gegen Viren und Hackerangriffe.
2. Vorsicht bei der Nutzung in öffentlichen Netzwerken.
3. Schadprogramme und ihre Gefahren.

Was kommt als Nächstes?

Nun können Sie entweder dieses Kapitel wiederholen oder unserer Lernempfehlung folgen, indem Sie auf eine der unten stehenden Schaltflächen klicken:

Wiederholen **Weiter**

SMART | MODUL 4 | KAPITEL 4

Umgang mit Cybbermobbing

Was sollten Sie tun, wenn Sie Ziel von Cybermobbing werden? Wenn man die Person nicht sieht, ist es leichter, den Schaden zu übersehen, der durch Cybermobbing angerichtet wird. In diesem Kapitel befassen wir uns mit den menschlichen Aspekten der digitalen Kommunikation und damit, was online geteilt werden sollte und was nicht.

Was Sie lernen werden

1. Cybermobbing erkennen.
2. Umgang mit anstößigen Inhalten.
3. Was gehört ins Netz? Und was nicht?
4. Online-Freundschaften: Sicherheitsaspekte.

Was ist Cybermobbing?

Cybermobbing wird definiert als *eine* ***"aggressive, vorsätzliche Handlung, die von einer Gruppe oder Einzelperson unter Verwendung elektronischer Kontaktformen wiederholt und über einen längeren Zeitraum hinweg gegen ein Opfer verübt wird, das sich nicht ohne weiteres verteidigen kann."*** **- Smith 2018**

Cybermobbing umfasst in der Regel drei Elemente:

- die Absicht zu schaden
- Ungleichgewicht der Macht
- Wiederholungstaten

Arten von Cybermobbing

Cybermobbing kann über Textnachrichten, Telefonanrufe, E-Mails, Instant Messenger, Social-Media-Plattformen oder in Chatrooms erfolgen.

Oft handelt es sich um verletzende Worte, abfällige Kommentare, dem Posten von gefälschten Informationen in öffentlichen Foren oder Blogs oder dem Hacken von Konten für persönliche Drohungen gewalttätiger oder sexueller Natur.

– Rao 2018

Umgang mit Cybermobbing

Nach Ansicht von Expert:innen gibt es folgende Möglichkeiten, wie man mit Cyber-Mobbing umgehen kann.

Ignorieren: Wenn möglich, ignorieren und blockieren Sie den/die Täter*in.

Aufzeichnen: Notieren Sie sich Zeit, Datum und Inhalt aller Mobbing-Inhalte, damit Sie sie bei Bedarf melden können.

Unterstützung durch Freunde: Teilen Sie Ihre Erfahrungen mit Freunden und Verwandten, damit Sie sich nicht isoliert fühlen.

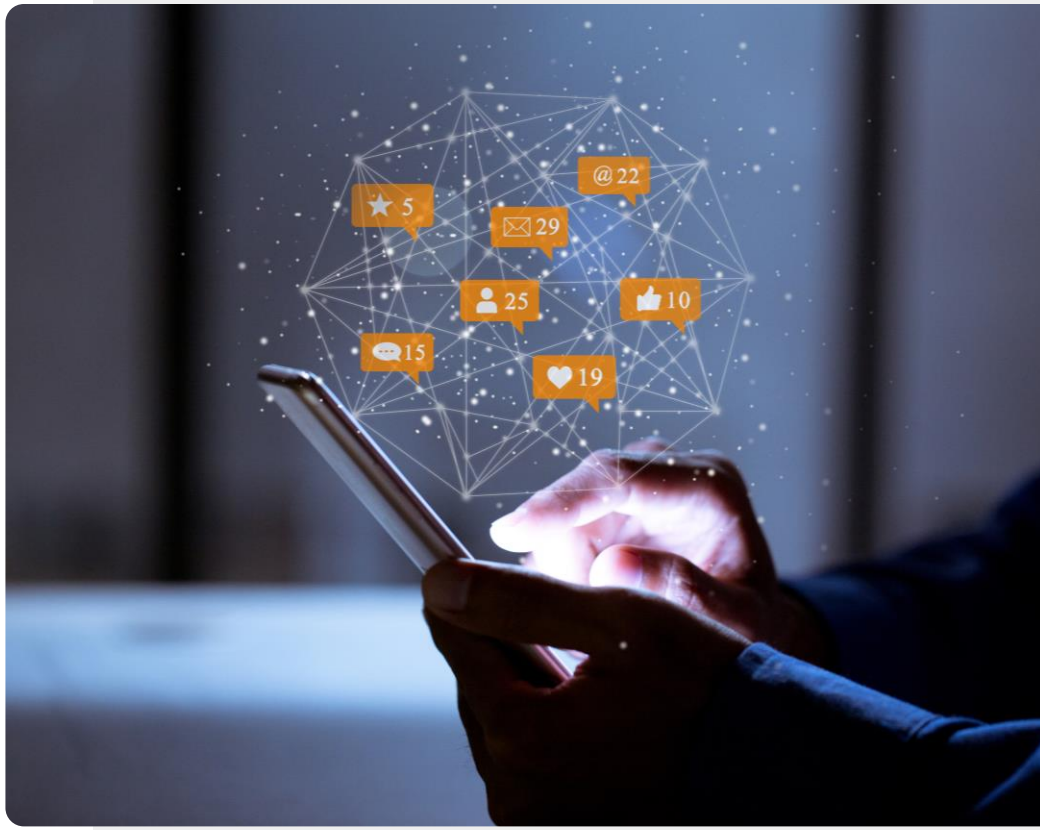
Melden: Wenden Sie sich an Moderator*innen der Seite oder des Forums.

Persönliche Informationen in sozialen Netzwerken teilen

Wenn Sie Informationen in sozialen Medien teilen, sollten Sie davon ausgehen, dass sie dort für eine lange Zeit zu finden sind. Machen Sie sich nicht angreifbar!

*"Auch wenn es den Anschein hat, dass die Informationen nur mit Ihren Freund*innen und Ihrer Familie geteilt werden, können sie auch an Hacker oder Täter*innen gelangen. "Wenn Ihre Daten einmal in der freien Wildbahn sind, bleiben sie dort und können von einer Vielzahl skrupelloser Personen genutzt werden."*

Joseph Turow – Penn State



Cybermobbing melden

Ihr Dienstanbieter oder das entsprechende soziale Netzwerk kann Ihnen helfen, unerwünschte Nachrichten und Anrufe zu blockieren.

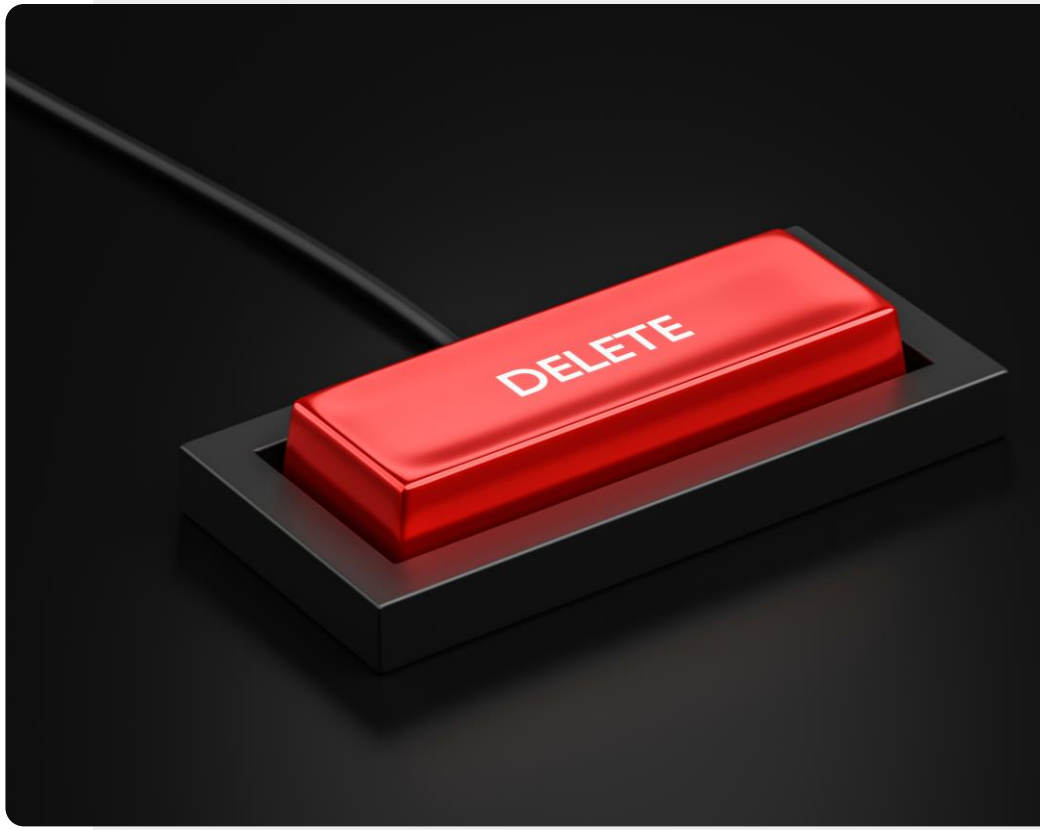
Wenn die Situation ernster ist, können Sie sich an die Polizei melden.

Anonym im Internet

In sozialen Medien können Sie Ihr Profil oft so einstellen, dass es für die Öffentlichkeit nicht sichtbar ist.

Es ist vielleicht nicht immer möglich, Ihre Beiträge in sozialen Medien oder Internetforen zu löschen, aber Sie können Ihre Identität löschen, so dass diese Beiträge anonym werden.

In einigen Fällen können Sie eine Anfrage an eine Suchmaschine wie Google senden, damit Ihre Daten nicht in den Suchergebnissen erscheinen.



Wurde ich gehackt?

Wenn sich jemand Zugang zu Ihrem E-Mail- oder anderen Konten verschafft, kann er damit gefälschte E-Mails an Ihre Kontakte schicken und sich als Sie ausgeben. Dies wird als **"Pwning"** (sprich: pawning) bezeichnet.

Wenn Sie dasselbe Passwort für verschiedene Konten verwenden, z. B. für E-Mails, könnte Ihr Konto gehackt werden.

Hier können Sie nachschauen, ob eines Ihrer Konten betroffen ist und gegebenenfalls handeln:

https://haveibeenpwned.com/

Vorsicht bei Online-Freundschaften

Überprüfen Sie die Angaben, die Sie von "neuen" Freund:innen erhalten haben.

Geben Sie keine persönlichen Informationen weiter, sondern führen Sie neutrale Gespräche.

Leihen Sie einem/r "neuen" Freund:in kein Geld.

Echte Freund:innen werden sich für Ihre Interessen interessieren und Sie nicht dazu benutzen, ihre Probleme zu lösen.

Vor- und Nachteile von Online-Freundschaften

Vorteile

- Sie können sich weltweit vernetzen.
- Sie können viele Personen finden, die Ihre Interessen teilen.
- Online chatten ist oft unkomplizierter als ein persönliches Gespräch.
- Sie können ihr Konto jederzeit löschen.

Nachteile

- Persönliche Gespräche lassen sich dennoch nicht ganz ersetzen.
- Beim Teilen persönlicher Information müssen Sie vorsichtig sein.
- Die emotionale Distanz macht es einfacher, beleidigender zu werden.

Anstößige Inhalte

Zu unangemessenen Inhalten gehören Aufnahmen von *"Terroranschlägen, Enthauptungen und Bombenanschlägen; Grausamkeiten gegenüber Menschen und Tieren; Selbstverletzung; Inhalte, die Anorexie und Essstörungen fördern; Inhalte, die Selbstmord befürworten; sexueller Missbrauch und Vergewaltigung; Gewalt und verstörende Inhalte; Online-Pornos".* https://www.nspcc.org.uk/keeping-children-safe/online-safety/inappropriate-explicit-content/

Im Internet wird eine Person, die unangemessene Inhalte mit der Absicht veröffentlicht, andere Leser*innen zu provozieren oder zu beleidigen, als „**Troll“** bezeichnet.

Umgang mit anstößigen Inhalten

Die meisten Suchanbieter verfügen über Funktionen, die anstößige Inhalte filtern. Die **"SafeSearch“-Funktion** von Google befindet sich beispielsweise hier: https://www.google.com/preferences.

Ganz oben auf der Seite können Sie auf das Symbol "SafeSearch aktivieren" klicken.

Sie können **SafeSearch** auch dauerhaft einstellen. Google blockiert dann sowohl Texte auf Webseiten für Erwachsene als auch Bilder, die mit diesen Seiten verbunden sind.

Können Sie Teresa helfen?

Teresa ist mit Cybermobbing in Berührung gekommen. Was kann sie tun?

✓Lernen Sie Teresa kennen: hier

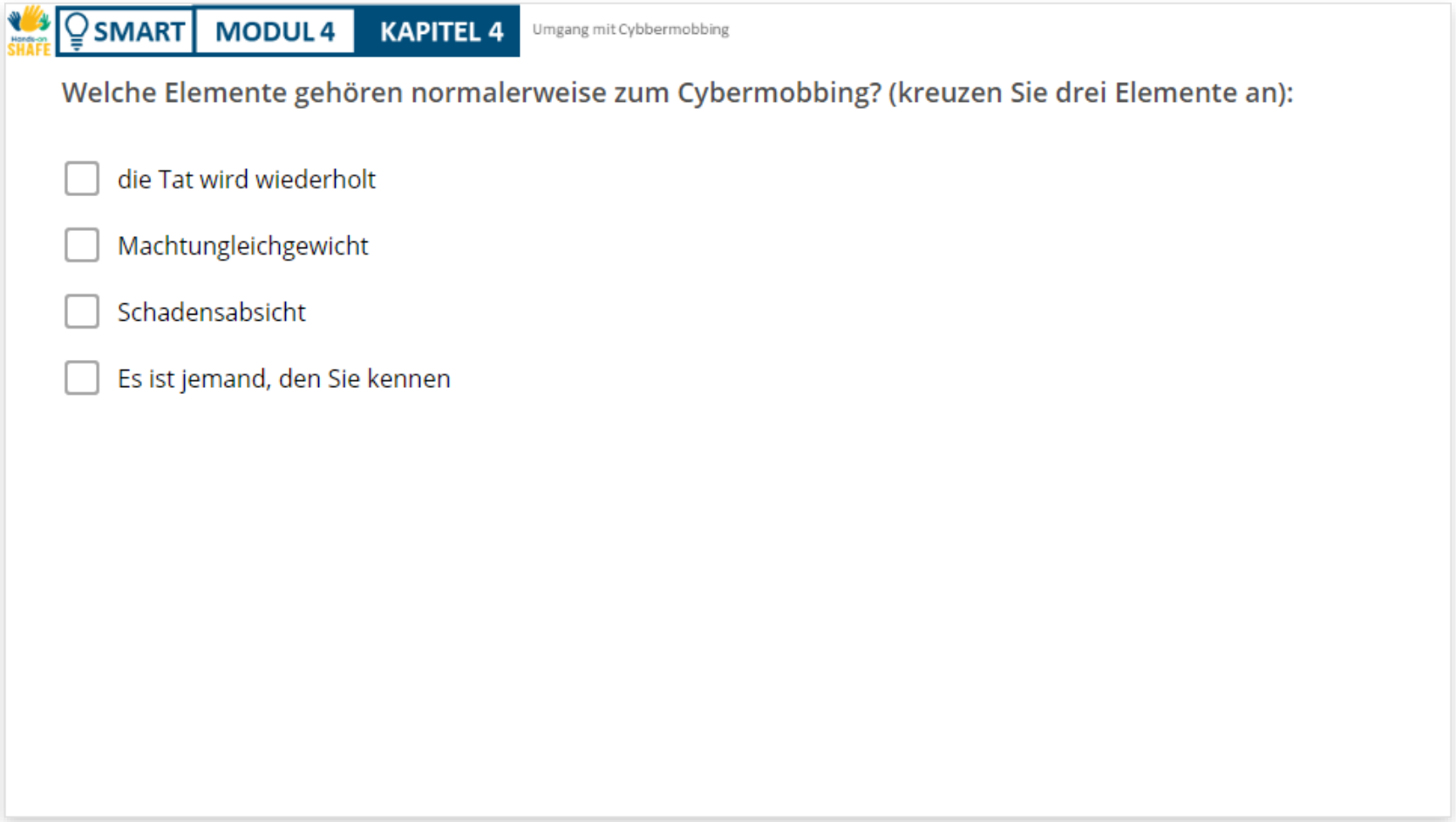
✓Teresa nutzt digitale Technologie, um mit ihren Freund:innen in Kontakt zu bleiben, aber kürzlich war sie von Cybermobbing betroffen. Bisher ist es kein ernster Fall, aber sie würde trotzdem gerne wissen, wie sie damit umgehen soll - vor allem, wenn es weitergehen sollte.

✓Gehen Sie die bisherigen Folien noch einmal durch und überlegen Sie, wie Sie Teresa helfen können.

✓An wen sollte sich Teresa wenden, wenn das Cybermobbing schlimmer wird?

Quiz

Click the **Quiz** button to edit this object

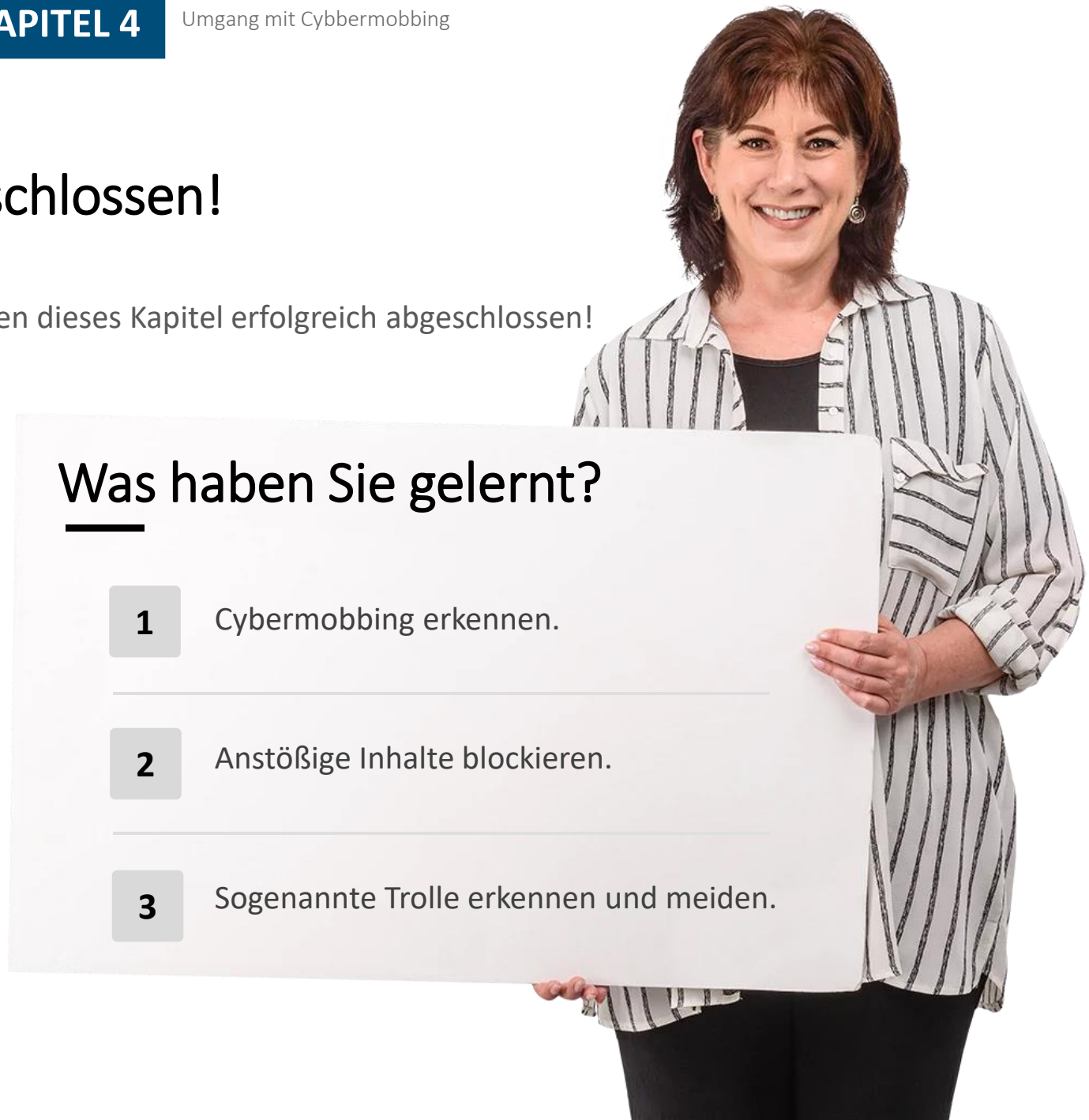


Zusammenfassung von Kapitel 4

1. Cybermobbing erkennen und melden.
2. Anstößige Inhalte erkennen und blockieren.
3. Vorsicht bei Online-Freundschaften.
4. Vorsichtiger Umgang mit persönlichen Informationen.
5. Blockieren von unerwünschten Inhalten und Schutz des Kontos.

Kapitel abgeschlossen!

Glückwunsch! Sie haben dieses Kapitel erfolgreich abgeschlossen!



Was kommt als Nächstes?

Nun können Sie entweder dieses Kapitel wiederholen oder unserer Lernempfehlung folgen, indem Sie auf eine der unten stehenden Schaltflächen klicken:

Wiederholen

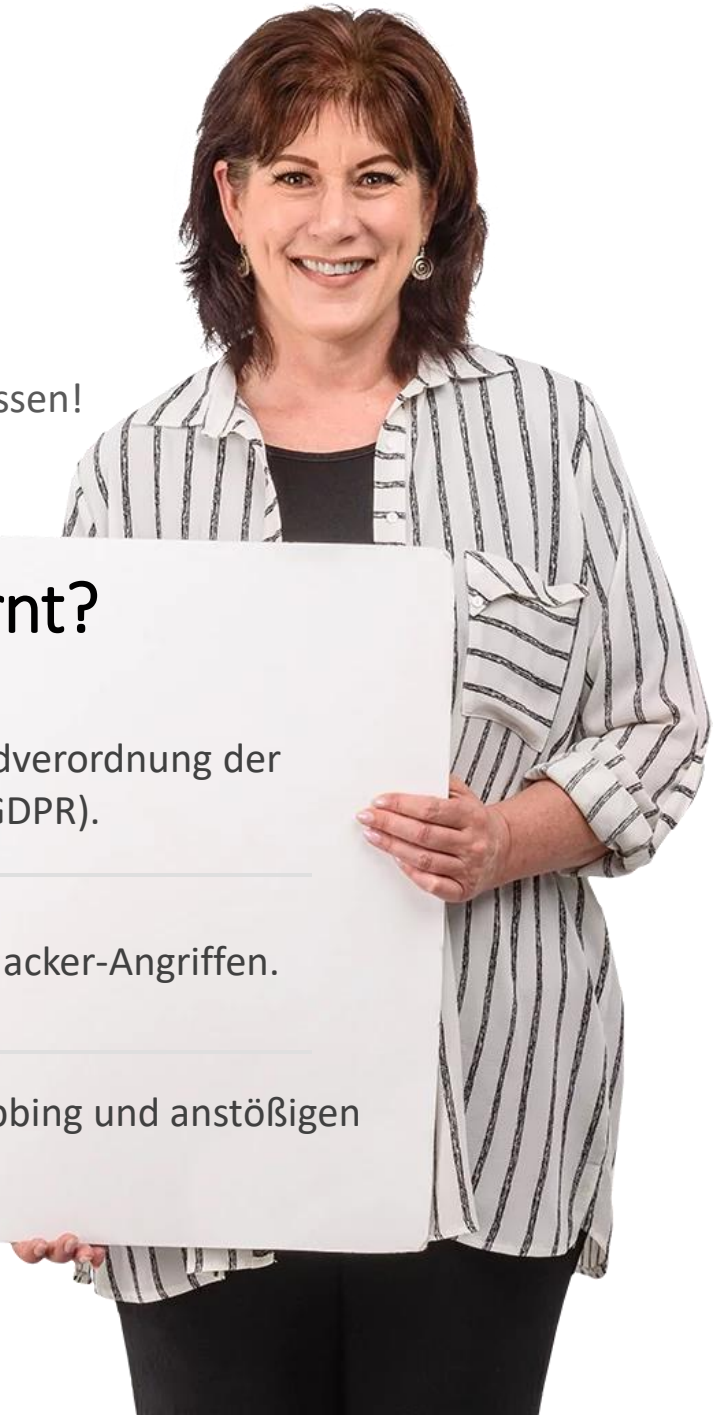
Weiter

Zusammenfassung von Modul 4

1. Sicherheit bei Smartphones.
2. Die Datenschutz-Grundverordnung der Europäischen Union (GDPR).
3. Authentifizierungsmethoden.
4. Erstellen starker Passwörter.
5. Schadprogramme, Ransomware und DDoS.
6. Umgang mit Cybermobbing.
7. „SafeSearch“-Funktion bei Google.

Modul abgeschlossen!

Glückwunsch! Sie haben dieses Modul erfolgreich abgeschlossen!



Was haben Sie gelernt?

1. Die Datenschutz-Grundverordnung der Europäischen Union (GDPR).
2. Schutz vor Viren und Hacker-Angriffen.
3. Umgang mit Cybermobbing und anstößigen Inhalten.

Was kommt als Nächstes?

Nun können Sie entweder dieses Modul wiederholen oder unserer Lernempfehlung folgen, indem Sie auf eine der unten stehenden Schaltflächen klicken:

Wiederholen

Weiter