Digital Citizenship

# Datenschutz und Sicherheit

## Kurs

Lektüre | Übungen | Fallstudien | Quiz

Erasmus+
ATHENS LIFELONG LEARNING INSTITUTE
TEAM 4 excellence
SEAL CYPRUS

# Strategische Partnerschaft zur Entwicklung offener Bildungsressourcen für den Unterricht zur digitalen Bürgerschaft

2019-3-RO01-KA205-078053

# DIGCIT

D15 - Digitale Bürgerschaft "Datenschutz und Sicherheit" Kurs

Revision: v.1.1

| | |
|---|---|
| **Intellektuelle Leistung** | IO2 - Bildungsmaterialien für digitale Bürgerschaft |
| **Tätigkeit** | Entwicklung von Lehrplänen |
| **Leitung des Projekts** | Arbeitskreis Ostviertel e. V. , Deutschland |
| **Fälligkeitsdatum** | 15. März 2021 |
| **Autoren** | Jan LEYE |
| **Abstrakt** | Der Kurs "Datenschutz und Sicherheit" befasst sich mit den Risiken und Vorteilen für die persönlichen Informationen und Daten der digitalen Bürger. Während die gesellschaftlichen Vorteile, die sich aus der Wahrnehmung von Rechten und Pflichten, Hobbys und sozialen Interaktionen im Internet ergeben, immens sind, tauchen immer mehr Bedrohungen für die Privatsphäre aller Bürger auf.<br>In diesem Kurs werden die wichtigsten Aspekte des sicheren Handelns und die Bedeutung des Schutzes der Privatsphäre vermittelt. |
| **Schlüsselwörter** | Modellkurs; digitale Bürgerschaft; Kursplan; Datenschutz; Sicherheit; digitale Umgebungen; soziale Netzwerke; Internet-Sicherheitsrisiken; Hardware; Software; Bildung; Reflexion; reflektierendes Denken |

**Danksagung**

Dieser Beitrag wurde von der Europäischen Kommission im Rahmen des Grant Agreement-2019-3-RO01-KA205-078053, ERASMUS+ Strategic Partnership project "Strategic partnership to develop open educational resources for teaching digital citizenship" gefördert.

**Haftungsausschluss**

"Die Unterstützung der Europäischen Kommission für die Erstellung dieser Veröffentlichung stellt keine Billigung des Inhalts dar, der ausschließlich die Meinung der Autoren widerspiegelt, und die Kommission kann nicht für die Verwendung der darin enthaltenen Informationen verantwortlich gemacht werden."

**Copyright-Hinweis**



# Inhalt

# Einführung

Datenschutz und Sicherheit sind alte Begriffe, die aber erst in den letzten Jahren an Bedeutung gewonnen haben. Das Modul "Privatsphäre und Sicherheit" erklärt die moderne Interpretation der Privatsphäre als Menschenrecht in einer digitalisierten Ära.

Das Digital Citizenship Educational Handbook des Europarats definiert Privatsphäre als ein Recht, das *"hauptsächlich den persönlichen Schutz der eigenen und der Online-Informationen anderer betrifft, während sich Sicherheit eher auf das eigene Bewusstsein für Online-Aktionen und -Verhalten bezieht".*

Privatsphäre und Sicherheit sind voneinander abhängig, vor allem in einem digitalen Umfeld. Angesichts der Bedrohungen, die von der Hardware, der Software und dem Nutzer selbst ausgehen, ist der Schutz der eigenen Privatsphäre eine ständige Herausforderung und Verantwortung für jeden digitalen Bürger.

Dieses Modul zielt darauf ab, das Bewusstsein für die Bedeutung der Privatsphäre in Bezug auf ein erfülltes Leben und die notwendigen Schritte zum Schutz dieser Privatsphäre zu schärfen. Es wird Wissen und praktische Ratschläge zu den Grundlagen der modernen Sicherheit angesichts moderner Risiken vermitteln. Die Module werden unter anderem folgende Themen abdecken

- Was ist Privatsphäre?
- Was ist Sicherheit?
- Was sind digitale Umgebungen?
- Wie wirkt sich die Privatsphäre auf unser Leben aus?
- Wie funktioniert ein digitales Gerät?
- Wie verhält man sich sicher und verantwortungsbewusst?

# 1. Modul 1 - Einführung in den Datenschutz

Quelle: Unsplash

## Überblick über den Kurs

**Zusammenfassung**: Dieses Modul behandelt die Grundlagen des Datenschutzes, seine Definition und seine Rolle in der heutigen digitalen Umgebung. Außerdem wird die Bedeutung der Privatsphäre als Menschenrecht aufgezeigt.

**Struktur:**

- Überblick über den Kurs
- Die Definition der Privatsphäre
- Digitale Privatsphäre
- Die Bedeutung der Privatsphäre
- Fallstudie
- Ergänzende Lektüre
- Übung
- Rückmeldung
- E-Quiz

**Lernziele:**

- Verstehen der Definition von Privatsphäre
- Erkennen Sie die Bedeutung der Privatsphäre
- Erklären Sie die Bedeutung der Privatsphäre

## Die Definition der Privatsphäre

Es gibt keine weltweit anerkannte Definition des Begriffs "Privatsphäre", da er je nach Kultur, Geschichte oder persönlicher Erfahrung unterschiedliche Bedeutungen haben kann. In diesem Kurs werden wir eine Definition verwenden, die für die meisten westlichen Demokratien ausreichend sein sollte:

Privatsphäre ist die Fähigkeit einer Person, sich in einem Zustand der Abwesenheit von Gesellschaft und Beobachtung zu befinden, oder kurz gesagt: das Recht, in Ruhe gelassen zu werden. Privatheit bedeutet, persönliche Informationen und Angelegenheiten geheim zu halten und persönliche Informationen und Angelegenheiten nur nach eigenem Willen mitzuteilen. Der Schutz der Privatsphäre bedeutet also die Freiheit von unbefugtem Eindringen in den persönlichen Raum, in persönliche Informationen und Angelegenheiten.

Die Verwirrung rührt oft daher, dass die Begriffe "Privatsphäre" und "Datenschutz" als Synonyme verwendet werden. Sie sind beide miteinander verbunden, aber während sich die Privatsphäre direkt auf den persönlichen Raum oder die Sphäre einer Person bezieht, bezieht sich der Datenschutz speziell auf den Schutz "aller Informationen über eine bestimmte oder bestimmbare natürliche (lebende) Person".[1] Die Privatsphäre umfasst alle Aspekte der persönlichen Sphäre, wie den physischen Schutz Ihres Hauses. Wenn Sie zum Beispiel Opfer eines unerwünschten körperlichen Kontakts werden, wurde Ihr Recht auf Privatsphäre verletzt, nicht aber Ihr Recht auf Datenschutz.

Das Recht auf Privatsphäre ist ein Menschenrecht, das in Artikel 12 der Allgemeinen Erklärung der Menschenrechte von 1948 verankert ist:

> *"Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung oder seinen Schriftverkehr sowie Angriffen auf seine Ehre und seinen Ruf ausgesetzt werden. Jeder hat Anspruch auf den Schutz des Gesetzes gegen solche Eingriffe oder Angriffe".*[2]


THE UNIVERSAL DECLARATION OF Human Rights

UNITED NATIONS

Quelle: Öffentlicher Bereich

[1] https://edps.europa.eu/data-protection_en

[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

Der Schutz der Privatsphäre wurde vom Europarat ausdrücklich anerkannt, als die Europäische Menschenrechtskonvention (EMRK) im Jahr 1950 unterzeichnet wurde und im September 1953 in Kraft trat. Artikel 8 der EMRK trägt den Titel "Recht auf Achtung des Privat- und Familienlebens" und besagt:

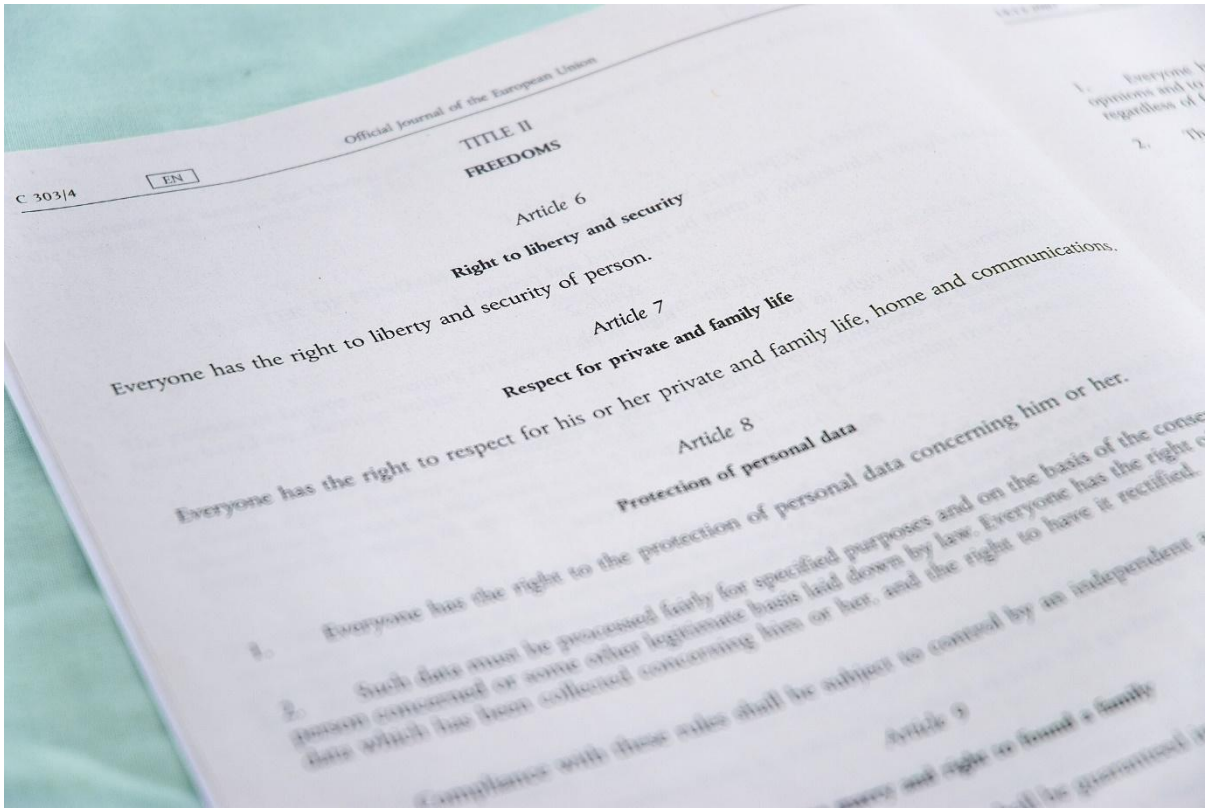
> *"(1) Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.*
>
> *2. (2) Eine Behörde darf in die Ausübung dieses Rechts nur eingreifen, soweit dies gesetzlich vorgesehen und in einer demokratischen Gesellschaft im Interesse der nationalen oder öffentlichen Sicherheit oder des wirtschaftlichen Wohls des Landes, zur Aufrechterhaltung der Ordnung oder zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist."*[3]

Darüber hinaus erkennt die Europäische Union das Recht auf Privatsphäre in den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union (GRR) an, die im Jahr 2000 ausgearbeitet wurde und im Dezember 2009 in Kraft trat:

> *"Artikel 7*
>
> *Achtung des Privat- und Familienlebens*
>
> *Jeder hat das Recht auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seiner Kommunikation.*
>
> *Artikel 8*
>
> *Schutz von personenbezogenen Daten*
>
> 1. *Jede Person hat das Recht auf den Schutz der sie betreffenden personenbezogenen Daten.*
> 2. *Diese Daten müssen nach Treu und Glauben für festgelegte Zwecke und auf der Grundlage der Einwilligung der betroffenen Person oder einer anderen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht auf Auskunft über die zu ihrer Person erhobenen Daten und das Recht, diese zu berichtigen.*
> 3. *Die Einhaltung dieser Vorschriften unterliegt der Kontrolle einer unabhängigen Behörde".*[4]

[3] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=DE




Quelle: Wikimedia

## Digitale Privatsphäre

Das digitale Zeitalter hat sowohl neue Möglichkeiten als auch neue Herausforderungen mit sich gebracht. Wenn wir über den Schutz der Privatsphäre in einem digitalen Umfeld sprechen, verwenden wir gewöhnlich den Begriff "digitale Privatsphäre". Die digitale Privatsphäre umfasst das Recht auf Privatsphäre und all seine Definitionen aus der analogen Welt sowie den Datenschutz.

Der Begriff "digitale Privatsphäre" kann verwirrend sein, da die Privatsphäre als Rechtsbegriff bereits alle Anwendungsbereiche abdeckt: Es spielt keine Rolle, ob die Privatsphäre in der realen Welt oder in einer digitalen Umgebung gefährdet ist, denn ihr Schutz gilt unabhängig von Technologie, Ort oder Zeit. Wenn wir von "digitaler" oder "elektronischer" Privatsphäre sprechen, wollen wir vor allem die spezifischen Risiken und Gefahren für die Privatsphäre hervorheben, die von neuen Technologien wie dem Internet, sozialen Netzwerken oder neuen Geräten ausgehen.

Die Europäische Union hat zwei wichtige Regelwerke geschaffen, die speziell die Rechte auf Privatsphäre und Datenschutz in digitalen oder elektronischen Umgebungen schützen: die Datenschutzrichtlinie für elektronische Kommunikation[5] (vollständiger Titel: Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation) und die Allgemeine Datenschutzverordnung[6] (GDPR). Beide versuchen, internetbezogene Belange des Schutzes der Privatsphäre und des Datenschutzes zu regeln, indem sie beispielsweise mehr Transparenz im Zusammenhang mit Marketing oder der Verfolgung personenbezogener Daten fordern.

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

## Die Bedeutung der Privatsphäre

Das Recht auf Privatsphäre ist eine Voraussetzung für die freie Entfaltung der Persönlichkeit, wie es in Artikel 22 der AEMR heißt:

> *"Jeder Mensch hat als Mitglied der Gesellschaft das Recht auf soziale Sicherheit und auf die Verwirklichung der wirtschaftlichen, sozialen und kulturellen Rechte, die für seine Würde und die freie Entfaltung seiner Persönlichkeit unerläßlich sind, durch innerstaatliche Anstrengungen und internationale Zusammenarbeit nach Maßgabe der Organisation und der Mittel des jeweiligen Staates."*[7]

Einige Mitgliedstaaten der Europäischen Union wie Deutschland oder die Niederlande erkennen in ihren jeweiligen Verfassungen ausdrücklich ein Persönlichkeitsrecht an, zum Beispiel in Artikel 2 des deutschen Grundgesetzes, in dem es heißt:

> *"(1) Jeder Mensch hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt oder gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt."*[8]

Andere Staaten wie Frankreich haben in ihrer Rechtsprechung andere Mittel gewählt, um die Entwicklung der Persönlichkeit zu schützen.

Allen gemeinsam ist jedoch die allgemeine Vorstellung von der Bedeutung der Persönlichkeit, ihrem Schutz und ihrer untrennbaren Verbindung zur Privatsphäre. Ohne den Schutz der Privatsphäre kann sich ein Mensch nicht frei entwickeln und leben.

## Fallstudie - Datenschutz durch Technik

**Datenschutz durch Design: Sozialverträgliche Datenerfassung ohne Nebenwirkungen für die Privatsphäre**

In diesem Video von der Privacy Week 2017 in Wien erklärt Konark Modi die gefährlichen "Nebenwirkungen" des aktuellen Industriestandards der Tech-Giganten, die so viele Daten wie möglich sammeln.

[7] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[8] https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0023

https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

Modi zeigt, dass die Privatsphäre bei der Gestaltung von Online-Diensten respektiert werden kann und stellt eine alternative, die Privatsphäre respektierende Version von "Google Analytics" vor.

Frage zur Selbstreflexion: Was ist ein Nebeneffekt im Zusammenhang mit der Datenerhebung?

## Übung 1: Privates Treffen im World Café

**Zielsetzungen:**

- Ihre Gewohnheiten bei der Veröffentlichung persönlicher Daten kennenlernen
- Erkennen von potenziellen Risiken und Gefahren für Ihre Privatsphäre

**Dauer:** 30 Minuten

**Werkzeuge:** Stift und Papier

**Methoden:** Plenum, Gruppenarbeit

**Beschreibung der Übung:** Die Schüler werden in vier Gruppen aufgeteilt. Jede Gruppe wird einem Tisch mit Permanentmarkern/Papier oder einer Sitzung mit einem virtuellen Whiteboard zugewiesen. Jedem Tisch/Raum wird eines der folgenden Datenschutzthemen zugewiesen: (1) Identitätsdiebstahl. (2) Recht auf Vergessenwerden. (3) Persönlichkeitsrechte. (4) Spionageprogramme. Jede Gruppe erhält 5 Minuten Zeit, um über diese Themen nachzudenken (Was bedeuten sie? Welchen Zusammenhang haben sie mit der Privatsphäre? Kennen wir Beispiele? Sind sie gefährlich oder nützlich für mich?) und ihre Ideen auf dem Papier/der virtuellen Tafel zu notieren. Nach 5 Minuten beginnen die Gruppen zu rotieren. Das Café wird geschlossen, sobald jede Gruppe jedes Thema diskutiert hat. Jede Gruppe bestimmt einen Sprecher, der die jeweiligen Ergebnisse für seine Gruppe präsentiert.

**Aufgaben:**

- Teilen Sie sich in Gruppen auf.
- Diskutieren Sie jedes Thema fünf Minuten lang.
- Teilen Sie Ihre Ergebnisse der Klasse mit (bitte denken Sie daran, dass Sie keine Informationen weitergeben müssen, die Ihnen Unbehagen bereiten könnten).

**Nachbesprechung:** Der Trainer sollte die universelle Bedeutung der Privatsphäre hervorheben und darauf hinweisen, dass sie viele Bereiche unseres Lebens und unseres Wohlbefindens betrifft.

**Lektionen gelernt:** Der Datenschutz ist ein komplexes Thema und erfordert aktives Nachdenken.

## Ergänzende Lektüre

- **Der Tag des Datenschutzes (jedes Jahr am 28. Januar$^{th}$ )**: "Dieses Jahr ist der 28. Januar ein ganz besonderer Tag, nicht nur für den Europarat, sondern für die gesamte weltweite Datenschutzgemeinschaft und vor allem für jeden Einzelnen, der durch dieses grundlegende Recht geschützt wird." https://www.coe.int/en/web/data-protection/data-protection-day

## E-Quiz

| **Online-Quiz** | | | |
|---|---|---|---|
| **Titel des Kurses:** | Datenschutz und Sicherheit | | |
| **Titel des Moduls:** | Einführung in den Datenschutz | | |
| **Richtig oder Falsch** | Geben Sie an, ob die folgenden Aussagen wahr (T) oder falsch (F) sind | | |
| **Erklärungen** | | T | F |
| 1 | Nach Ansicht der Vereinten Nationen ist die Privatsphäre ein Menschenrecht | | |
| 2 | Privatsphäre ist das Recht, alle Informationen über sich selbst geheim zu halten, auch gegenüber der Regierung | | |
| 3 | Die Europäische Union erkennt die Privatsphäre nicht ausdrücklich als ein Recht an. | | |
| 4 | "Privatsphäre" und "Datenschutz" sind mehr oder weniger Synonyme | | |
| 5 | GDPR steht für "Allgemeine Richtlinie zum Schutz der Privatsphäre". | | |
| 6 | Einige Gerichtsbarkeiten erkennen die Privatsphäre als Voraussetzung für die freie Entfaltung der Persönlichkeit an | | |
| 7 | Die Einhaltung von Datenschutzgesetzen und das Design moderner Software schließen sich gegenseitig aus | | |
| 8 | Datenschutz bezieht sich auf den Schutz aller Informationen, die sich auf eine identifizierte oder identifizierbare natürliche (lebende) Person beziehen | | |

# 2. Modul 2 - Einführung in die Sicherheit


Quelle: Pixabay

## Überblick über den Kurs

**Zusammenfassung**: Dieses Modul behandelt die Grundlagen der Sicherheit. Es erklärt die grundlegende Definition, die Beziehung zum Datenschutz und zeigt die Bedeutung der Sicherheit in digitalen Umgebungen auf.

**Struktur:**

- Überblick über den Kurs
- Die Definition von Sicherheit
- Die Bedeutung der Sicherheit
- Fallstudie
- Ergänzende Lektüre
- Übung
- Rückmeldung
- E-Quiz

**Lernziele:**

- Verstehen der Definition von Sicherheit
- Erkennen Sie die Bedeutung der Sicherheit
- die Bedeutung der Sicherheit im Zusammenhang mit dem Schutz der Privatsphäre zu erklären

## Die Definition von Sicherheit

Sicherheit bedeutet Freiheit von Gefahren, die durch äußere Bedrohungen verursacht werden, oder von Furcht oder Angst vor Schaden oder Gefahr. Die Menschenrechte beruhen zum Teil auf dem Grundsatz, dass sich der Mensch nach einem Zustand der Sicherheit sehnt.

Im Zusammenhang mit der digitalen Bürgerschaft bedeutet Sicherheit die Freiheit von Gefahren, die durch die eigenen Handlungen, Unterlassungen und das eigene Verhalten in einer digitalen oder Online-Umgebung verursacht werden können. Sie ist eng mit dem Schutz der Privatsphäre verbunden, denn ohne die Anwendung geeigneter Sicherheitsmaßnahmen ist Ihre Privatsphäre gefährdet. Der Europarat erklärt auf seiner Website:

> *"Um ein digitaler Bürger zu werden, muss man einen kritischen und ethischen Ansatz entwickeln, um sich in der digitalen Umgebung mit Vertrauen und Klarheit zurechtzufinden und entsprechend zu handeln."*[9]

Um sicher zu sein, muss sich der digitale Bürger daher potenzieller Risiken und Bedrohungen bewusst sein, die nicht nur ihm selbst, sondern auch anderen Menschen schaden können. Um den potenziellen Schaden, der durch mangelnde Sicherheit entsteht, besser zu verstehen, können wir uns eine Beispielliste mit persönlichen Daten ansehen:

- Vorname und Nachname
- Wohnanschrift
- Rufnummer
- E-Mail Adresse
- Geolokalisierungsdaten
- IP-Adressen
- Cookie-IDs

Die Weitergabe dieser Daten kann zu leichten und/oder schweren Schäden führen.

## Die Bedeutung der Sicherheit

Die digitale Umgebung birgt neue und oft genug unsichtbare Gefahren für den Einzelnen. Um die Bedeutung der digitalen Sicherheit zu verdeutlichen, können wir einen Blick auf die Corona-Pandemie werfen: Je mehr Menschen mit dem Virus infiziert sind, desto höher ist die Wahrscheinlichkeit, dass auch andere Menschen infiziert werden. Stellen Sie sich vor, Ihr Gerät ist von Malware befallen. Je nach Art der Malware könnte sie nicht nur Ihre Privatsphäre, sondern auch die anderer Menschen gefährden und sich negativ auf deren Leben auswirken.

Sicherheit sollte nicht als ein Privileg, eine Option oder ein freiwilliges Angebot betrachtet werden. Im Gegensatz dazu muss ein verantwortungsbewusster digitaler Bürger Sicherheit als eine bürgerliche Verantwortung für sich selbst und andere Bürger verstehen. Die Beachtung der Grundprinzipien der digitalen Sicherheit (siehe Modul 4) ist ein aktiver Beitrag zu einem gerechteren und positiveren digitalen Umfeld.

Bei der Sicherheit geht es nie nur darum, sich selbst zu schützen. Es geht um den Schutz von uns allen, einschließlich Ihrer Freunde und Familien.

[9] https://www.coe.int/en/web/digital-citizenship-education/privacy-and-security

## Fallstudie - STOP.THINK.CONNECT

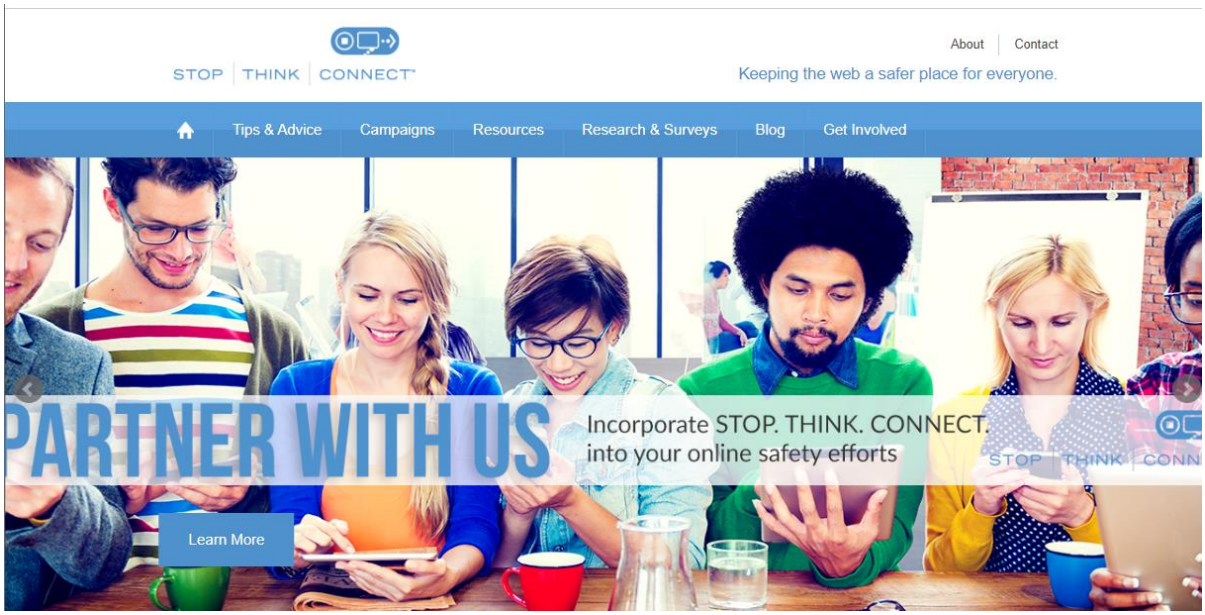
STOP.THINK.CONNECT. ist die erste weltweite Kampagne zur Sensibilisierung der Öffentlichkeit, die allen Internetnutzern helfen soll, ihre persönlichen Daten, ihre Kommunikation und ihre Transaktionen online sicherer zu machen.

Die in den USA ansässige Organisation "National Cybersecurity Alliance" und die "APWG Public Education Initiative" organisierten diese globale Kampagne zur Sensibilisierung für Online-Sicherheit mit dem Titel "STOP. THINK. CONNECT.". Sie empfehlen drei grundlegende Prinzipien im Zusammenhang mit der digitalen Sicherheit:

**"STOPP:** Bevor Sie das Internet nutzen, nehmen Sie sich Zeit, um die Risiken zu verstehen und zu lernen, wie man mögliche Probleme erkennt.

**DENKEN:** Nehmen Sie sich einen Moment Zeit, um sich zu vergewissern, dass der Weg vor Ihnen klar ist. Achten Sie auf Warnzeichen und überlegen Sie, wie sich Ihr Online-Handeln auf Ihre Sicherheit oder die Ihrer Familie auswirken könnte.

**VERBINDEN:** Genießen Sie das Internet mit größerer Zuversicht, weil Sie wissen, dass Sie die richtigen Schritte unternommen haben, um sich und Ihren Computer (und andere Geräte) zu schützen."




https://www.stopthinkconnect.org/

Mehr als 800 Wirtschaftsunternehmen, Bildungseinrichtungen, Regierungsbehörden und NRO haben das STOP. THINK. CONNECT. ™ Kampagne angenommen. Dreizehn nationale Ministerien und landesweit tätige NROs haben nationale Kampagnen durchgeführt.

Lesen Sie das Merkblatt https://education.apwg.org/safety-messaging-convention/ und überlegen Sie, wie sich Organisationen an der Kampagne beteiligen können.

## Übung 2: Zeichnen der Linie

**Zielsetzungen:**

- Den Unterschied zwischen personenbezogenen Daten und öffentlichen Daten verstehen

- Erkennen Sie Ihre eigenen Bedürfnisse in Bezug auf den Datenschutz
- Rechtfertigen Sie die Verwendung Ihrer persönlichen Daten

**Dauer:** 20 Minuten

**Werkzeuge:** Stift und Papier

**Methoden:** Plenum, kreative Bewerbung, Schreiben

Beschreibung der Übung: Denken Sie an die folgenden Beispiele für persönliche Daten: Ihr Name, Ihr Alter, Ihre Schuhgröße, Ihr Gewicht, Ihre Hobbys, Ihr Gehalt, die Marke Ihres Shampoos, der Name Ihres ersten Haustiers, die Farbe Ihrer Unterwäsche, die Note Ihrer letzten Prüfung, Ihr Gehalt, die Uhrzeit, zu der Sie Ihr Haus verlassen. Ordnen Sie jede dieser Daten einer der folgenden vier Kategorien zu: (1) Diese Daten sind privat; ich werde sie nicht weitergeben. (2) Diese Daten dürfen nur mit meinen Freunden geteilt werden. (3) Diese Daten können öffentlich gemacht werden. (4) Ich weiß nicht, wo ich diese Daten zuordnen soll.

**Aufgaben:**

- Erstellen Sie eine Tabelle auf Ihrem Papier, wobei jede Zeile eine der vier Kategorien darstellt
- Ordnen Sie alle Beispiele innerhalb von 5 Minuten einer der vier Kategorien zu
- Teilen Sie Ihre Ergebnisse der Klasse mit (bitte denken Sie daran, dass Sie keine Informationen weitergeben müssen, die Ihnen Unbehagen bereiten könnten)

**Nachbesprechung:** Der Trainer sollte die Gründe hervorheben, warum bestimmte Beispiele persönlicher Daten von den meisten Teilnehmern vorzugsweise nicht mit der Öffentlichkeit geteilt werden. Das Plenum sollte Schlussfolgerungen und Gemeinsamkeiten zum Thema personenbezogene Daten und Privatsphäre ziehen.

**Lektionen gelernt:** Persönliche Daten müssen geschützt werden. Ich sollte mir Zeit nehmen und nachdenken, bevor ich persönliche Daten weitergebe.

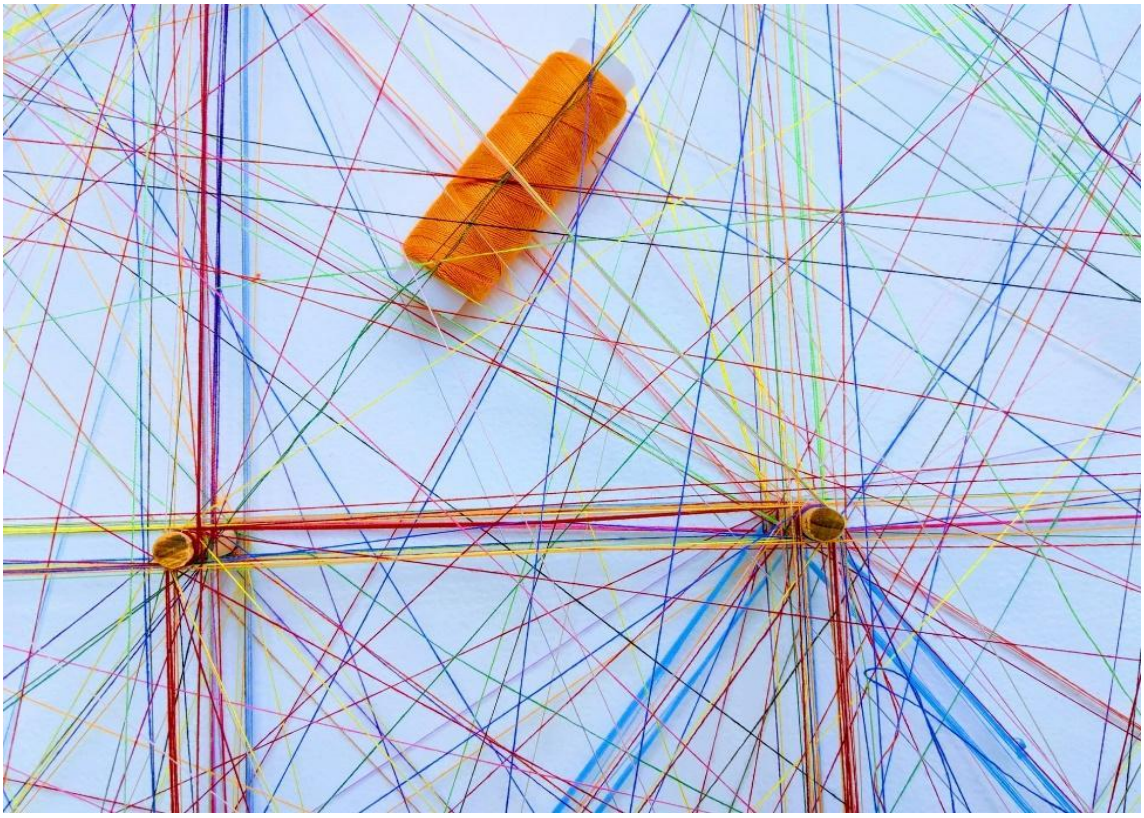
### Ergänzende Lektüre

- **Facebook-Datenleck**: Ein Twitter-Thread, in dem die Folgen und die mangelnde Berichterstattung über das Datenleck bei Facebook diskutiert werden, von dem rund 533 Millionen Facebook-Nutzer aus der ganzen Welt betroffen sind. https://twitter.com/UnderTheBreach/status/1349671294808285184

## E-Quiz

| **Online-Quiz** | | | |
|---|---|---|---|
| **Titel des Kurses:** | Datenschutz und Sicherheit | | |
| **Titel des Moduls:** | Einführung der Sicherheit | | |
| **Richtig oder Falsch** | Geben Sie an, ob die folgenden Aussagen wahr (T) oder falsch (F) sind | | |
| **Erklärungen** | | T | F |
| 1 | Ein Mangel an Sicherheit kann Ihre Privatsphäre gefährden | | |
| 2 | Die IP-Adresse Ihres Smartphones ist Teil Ihrer persönlichen Daten | | |
| 3 | Sicherheit bezieht sich auf Ihre Freiheit, Zugang zur Privatsphäre anderer zu erhalten | | |
| 4 | Wenn Sie ein angemessenes Sicherheitsbewusstsein haben, schützen Sie auch andere Menschen. | | |
| 5 | Sicherheit ist eine staatsbürgerliche Verantwortung für digitale Bürger | | |
| 6 | Ein kritisches und ethisches Verhalten in einem digitalen Umfeld ist Teil der Sicherheit | | |

# 3. Modul 3 - Datenschutz in einer digitalen Umgebung



Quelle: Unsplash

## Überblick über den Kurs

**Zusammenfassung**: In diesem Modul wird das Konzept der digitalen Umgebungen erläutert. Es konzentriert sich auf soziale und kommunikative Umgebungen und ihre jeweiligen Risiken für die Privatsphäre der Nutzer. In Bezug auf die Privatsphäre wird kritisch über die Bedeutung und die Probleme der größten sozialen Netzwerke reflektiert.

**Struktur:**

- Überblick über den Kurs
- Die Prämisse der digitalen Umgebungen
- Risiken sozialer Netzwerke und Messenger in einem digitalen Umfeld
- Fallstudie
- Ergänzende Lektüre
- Übung
- Rückmeldung
- E-Quiz

**Lernziele:**

- Die Definition von digitalen Umgebungen verstehen
- Erkennen des Einflusses von sozialen Netzwerken
- die vielschichtigen Bedrohungen der Privatsphäre in digitalen Umgebungen zu erkennen

## Die Prämisse der digitalen Umgebungen

Heutzutage bezieht sich die technische Definition eines digitalen Umfelds in der Regel auf digitale und elektronische Systeme, die integriert, verbunden und über das World Wide Web oder andere Online-Zugänge zugänglich sind. Für digitale Bürgerinnen und Bürger werden digitale Umgebungen jedoch oft durch den Kontext definiert und als vernetzte Online-Räume erlebt, die durch Technologie und digitale Geräte ermöglicht werden.[10]

Digitale Umgebungen können genutzt werden, um das Bewusstsein für Menschenrechte oder Themen der Zivilgesellschaft zu schärfen, indem man sich miteinander vernetzt und seine Meinung kundtut. Digitale Bürgerinnen und Bürger greifen mit Hilfe von digitalen Geräten wie Smartphones oder Laptops auf digitale Umgebungen zu. Sie erhalten Zugang zu verschiedenen Elementen digitaler Umgebungen, die unterschiedlichen Funktionen dienen.

Die sichere Teilhabe aller digitalen Bürgerinnen und Bürger an sozialen und kommunikativen Umfeldern ist jedoch mit einem notwendigen Maß an Medienkompetenz verbunden.

Um digitale Bürgerschaft zu erleben, sind Kommunikations- und soziale Dienste in digitalen Umgebungen am wichtigsten, zum Beispiel Websites, soziale Netzwerkplattformen oder Messenger. Die Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur stellt in ihrem Bericht über "Kultur im digitalen Umfeld" fest:

> *"Dazu gehört die Fähigkeit, die Vielfalt der Informationen, denen wir ausgesetzt sind (d.h. audiovisuelle Inhalte), kritisch zu analysieren, sich eine eigenständige Meinung zu bilden, sich aktiv an gesellschaftlichen Fragen zu beteiligen und neue Formen der sozialen Interaktion zu beherrschen."*[11]

Da digitale Umgebungen dazu neigen, ihre Schnittstellen, Zugänge, Funktionen und Verhaltensweisen schnell zu verändern, ist es wichtig, sie aktiv in formale und nicht formale Bildungsprozesse für Menschen aller Altersgruppen einzubeziehen.

## Risiken sozialer Netzwerke und Messenger in einem digitalen Umfeld

Das digitale Umfeld birgt Risiken für digitale Bürger aller Altersgruppen, und mit dem Aufkommen sozialer Netzwerke und Instant Messenger treten Probleme mit dem Schutz der Privatsphäre scheinbar häufiger denn je auf.

> *"Im Jahr 2020 nutzten über 3,6 Milliarden Menschen weltweit soziale Medien, eine Zahl, die bis 2025 auf fast 4,41 Milliarden ansteigen soll."*[12]

Wenn diese Dienste rücksichtslos genutzt werden, kann dies für den Nutzer soziale, finanzielle, emotionale, berufliche oder rechtliche Folgen haben. Die folgende Liste enthält die wichtigsten Datenschutzbedenken im Zusammenhang mit Websites sozialer Netzwerke:

- **Verlust der Datensouveränität**: Der Verlust Ihrer Fähigkeit, die Verarbeitung Ihrer personenbezogenen Daten zu kontrollieren

[10] "Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings", S. 79, 2017, Yannis Kotsanis (Doukas School, Griechenland), ISBN13: 9781522530534
[11] https://en.unesco.org/creativity/sites/creativity/files/dce-policyresearch-book2-en-web.pdf
[12] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

- **Mangel an Transparenz**: Die fehlende Möglichkeit für Sie, sich über den Umgang mit Ihren personenbezogenen Daten zu informieren
- **Falsche Wahrnehmung der Vorteile**: Eine Situation, in der der wahrgenommene Nutzen der Preisgabe von Teilen Ihrer persönlichen Daten größer zu sein scheint als das wahrgenommene Risiko der Weitergabe von Informationen auf einer Online-Plattform
- **Entspanntes Verhalten**: Die Unterschätzung der Folgen, die die Weitergabe persönlicher Daten haben könnte
- **Dauerhaftigkeit der Informationen:** Die Tatsache, dass Ihre persönlichen Daten wahrscheinlich dauerhaft online verfügbar sind (im Zusammenhang mit dem "Recht auf Vergessenwerden" in der Europäischen Union)
- **Profiling**: Die Gefahr, dass ein Profil über Sie erstellt wird, indem verfügbare persönliche Informationen und/oder Metadaten verwendet werden, z. B. im Rahmen von gezielter Werbung

Eine der größten Bedrohungen ist heutzutage das lockere Verhalten auf sozialen Netzwerkseiten wie Facebook, Twitter, Instagram oder TikTok. Jede dieser Seiten bietet ein unterschiedliches Maß an Privatsphäre. Seiten wie Facebook zwingen ihre Nutzer oft dazu, ihren echten Namen zu verwenden, da ihre Konten sonst geschlossen werden könnten, während andere soziale Netzwerkseiten die Verwendung von Pseudonymen fördern. Jede Website eines sozialen Netzwerks kann jedoch genügend persönliche Informationen bereitstellen, um Sie oder andere zu identifizieren, z. B. durch die Verwendung der gleichen Profilbilder in verschiedenen Netzwerken, durch das Posten von Bildern mit erkennbaren Umgebungen oder durch die Weitergabe von Standortinformationen mit Ihrem Profil.

Im Jahr 2020 befragte der US-amerikanische Satelliten-Internetanbieter "Viasat Savings" 1000 erwachsene US-amerikanische Bürger, wie viele Personen auf sozialen Netzwerkseiten ihre Profile privat halten:

> *"Wie sich herausstellte, ist es gleichmäßig aufgeteilt: Fast 50 % der von uns befragten Personen halten ihre Konten im privaten Modus, während die andere Hälfte sich dafür entscheidet, öffentlich zu sein. Laut Kyrsten Holland, Internetexpertin bei Viasatsavings.com, "haben Jung und Alt eines gemeinsam: Menschen zwischen 18 und 24 und 54+ sind die Altersgruppen, die ihre Social-Media-Konten am ehesten öffentlich machen."*[13]

Aber selbst wenn Sie Ihr Profil privat halten, sind die wichtigsten sozialen Netzwerke im Besitz privater Unternehmen mit der Absicht, Gewinne zu erzielen. Daher behalten sie sich in der Regel das Recht vor, Ihre persönlichen Daten - die Sie freiwillig zur Verfügung gestellt haben - zu nutzen, zu kombinieren (besonders wertvoll, wenn sie mehrere Dienste besitzen, z. B. Facebook, Instagram und WhatsApp) und/oder an andere Unternehmen zu verkaufen, die dann ihre Werbung (einschließlich politischer Kampagnen) auf Ihre Interessen ausrichten können.

Gleichzeitig lehrt uns die Erfahrung, dass man sich auf kein Unternehmen verlassen kann, wenn es darum geht, Ihre privaten Daten immer sicher zu verwahren. Alle großen sozialen Netzwerke sind in der Vergangenheit Opfer von Datenlecks geworden:

- **Instagram, TikTok, YouTube**: "Das Sicherheitsforschungsteam von Comparitech hat heute aufgedeckt, wie eine ungesicherte Datenbank fast 235 Millionen Instagram-, TikTok- und

[13] https://www.viasatsavings.com/news/blog/are-more-people-public-or-private-on-social-media/

YouTube-Nutzerprofile online offengelegt hat, was nur als massives Datenleck bezeichnet werden kann."[14]

- **Facebook:** "Das UpGuard Cyber Risk Team kann nun berichten, dass zwei weitere von Drittanbietern entwickelte Facebook-App-Datensätze gefunden wurden, die im Internet öffentlich zugänglich sind. Der eine, der von dem in Mexiko ansässigen Medienunternehmen Cultura Colectiva stammt, wiegt 146 Gigabyte und enthält über 540 Millionen Datensätze mit Details zu Kommentaren, Likes, Reaktionen, Kontonamen, FB-IDs und mehr."[15]
- **Twitter**: "Die Konten von einer Viertelmillion Twitter-Nutzern wurden gehackt. Dies ist der jüngste Fall in einer Reihe von aufsehenerregenden Sicherheitsverletzungen bei Internetfirmen. Anonyme Hacker haben sich möglicherweise Zugang zu rund 250.000 Konten des sozialen Netzwerks verschafft, darunter Benutzernamen, E-Mail-Adressen und Passwörter."[16]

Die folgenden Ratschläge sollten befolgt werden, wenn es um Fragen des Datenschutzes in einem digitalen sozialen oder Kommunikationsumfeld geht:

- Befolgen Sie stets die Grundsätze der Datenvermeidung und Datenminimierung: Geben Sie niemals persönliche Daten an und wenn Sie müssen, geben Sie so wenig wie möglich an (damit verbunden: aktivieren Sie immer so viele Datenschutzeinstellungen wie möglich)
- Laden Sie niemals Inhalte (z. B. Fotos oder Videos) hoch, für die Sie nicht die Rechte besitzen
- Geben Sie niemals persönliche Informationen oder Daten anderer Personen (z. B. private Fotos, Videos oder Nachrichten) ohne deren ausdrückliche Zustimmung weiter.
- Überprüfen Sie Anfragen von Freunden oder Familienmitgliedern immer offline.
- Melden Sie immer verdächtige Benutzer, die versuchen, Sie zur Weitergabe Ihrer persönlichen Daten zu überreden - andere sind vielleicht nicht so schlau!

Eine deutsche Studie aus dem Jahr 2012 zur digitalen Privatsphäre[17] zeigt, dass vor allem junge Nutzer einen sehr individuellen Ansatz für ihre digitale Privatsphäre wählen. Sie beteiligen sich an digitalen sozialen und kommunikativen Umgebungen oft in einem Tauziehen zwischen ihrem Bedürfnis nach sozialer Teilhabe und ihrer Angst um ihre Privatsphäre. Die Studie identifiziert drei Nutzertypen mit unterschiedlichen Privatsphärenstrategien:

- **Die aufschlussreichen Personen**: Dies ist die kleinste Gruppe unter den Studienteilnehmern. Sie zeichnen sich dadurch aus, dass sie offene Privatsphäre-Einstellungen in ihren Online-Konten haben und gleichzeitig viele persönliche Informationen weitergeben. Unter den jüngeren Menschen und Personen mit einem niedrigeren formalen Bildungsniveau gibt es relativ viele freizügige Personen. Die Studie deutet darauf hin, dass diese Gruppe ihre Daten entweder freiwillig weitergibt oder dass ihnen die Kompetenz und das Bewusstsein für sichere Datenschutzeinstellungen fehlen.
- **Die vorsichtigen Personen**: Diese Personengruppe hat vergleichsweise restriktive Datenschutzeinstellungen und scheut sich davor, persönliche Informationen zu teilen. Sie sind der Gegenpol zu den freizügigen Personen. Obwohl sie ihr bevorzugtes soziales Netzwerk

[14] https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=e35b1371111e

[15] https://www.upguard.com/breaches/facebook-user-data-leak

[16] https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security

[17] https://www.medienanstalt-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-71.pdf

häufig besuchen, möchten sie wahrscheinlich keine wichtigen sozialen Informationen verpassen.

- **Die Datenschutzbeauftragten:** Diese Personengruppe ist ständig aktiv, wenn es darum geht, Status-Updates und Kommentare in sozialen Netzwerken zu posten. Sie verfügen über ein umfangreiches Netzwerk von Kontakten und kennen viele von ihnen auch im wirklichen Leben. Sie scheinen Experten für den Schutz der Privatsphäre in einem digitalen Umfeld zu sein und können ihre Mitteilungsgewohnheiten gegen den Schutz ihrer Privatsphäre abwägen.

Die Studie kommt zu dem Schluss, dass potenzielle Bedrohungen der Privatsphäre das Verhalten der Nutzer kaum beeinflussen. Interessanterweise werden die Grundsätze der digitalen Bürgerschaft selbst nicht aktiv angestrebt.

## Fallstudie - Soziale Medien und Identitätsdiebstahl

Ein Artikel, der die moderne Anwendung des Identitätsdiebstahls durch die Nutzung von Websites sozialer Netzwerke erörtert. Er stellt vier Fälle von Identitätsdiebstahl vor und gibt Tipps, wie man sich vor dieser Art von Betrug schützen kann.

Jessica Velasco für socialnomics.net, 13/01/2016: https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

> *"Fallstudie: Die vielen Sarah Palins*
>
> *Die ehemalige Gouverneurin von Alaska, Sarah Palin, ist keine Unbekannte, was Kontroversen und gefälschte Twitter-Konten angeht. Im Jahr 2011 ging Palins offizielles Twitter-Konto, AKGovSarahPalin (jetzt@SarahPalinUSA), in einem Meer von gefälschten Konten zunehmend unter.*
>
> *Ein besonders bemerkenswerter Vorfall ereignete sich, als ein Palin-Imitator eine offene Einladung zu einem Grillfest im Haus von Sarah Palins Familie twitterte. Daraufhin musste Palins Sicherheitspersonal zu ihrem Wohnsitz in Alaska entsandt werden, um potenzielle Partygäste abzuschrecken.*
>
> *Dieses Phänomen ist nicht nur auf Sarah Palin beschränkt. Viele Persönlichkeiten des öffentlichen Lebens und Politiker, insbesondere umstrittene wie der Präsidentschaftskandidat 2016 Donald Trump, haben eine Vielzahl von Fake-Accounts, die ihre Identität annehmen. "*

Frage zur Selbstreflexion: Setzen Sie sich durch übermäßiges Teilen dem Risiko eines Identitätsdiebstahls aus?

## Übung 3: Gemeinschaft

**Zielsetzung:**

- Verständnis und Anwendung von Methoden zum Schutz der Privatsphäre in Online-Communities

**Dauer:** 25 Minuten

**Werkzeuge:** digitale Geräte mit aktiver Internetverbindung, Stift und Papier

**Methoden:** Plenum, Forschung, Gruppenarbeit

**Beschreibung der Übung:** Die SchülerInnen arbeiten in kleinen Gruppen (maximal 4 Personen) zusammen. Die Gruppe wählt eine soziale Netzwerkseite mit einem hohen Kommunikationsaufkommen (z. B. Facebook, Twitter, Instagram, Twitch, TikTok). Im Idealfall sind alle SchülerInnen bereits auf der gewählten Seite aktiv. Anschließend versuchen sie, eine Lösung für jede der folgenden Aufgaben zu finden: (1) Wie kann ich die restriktivsten Privatsphäre-Einstellungen in meinem Profil aktivieren? (2) Wie kann ich ein peinliches Bild von mir entfernen, das andere Personen auf der Plattform geteilt haben? (3) Wie kann ich andere Nutzer melden oder blockieren? (4) Wo finde ich die Nutzungsbedingungen und was sagen sie über meine Privatsphäre aus? (5) Wie kann ich mein Profil löschen und ist es wirklich weg?

**Aufgaben:**

- Wählen Sie innerhalb von 3 Minuten eine Website eines sozialen Netzwerks
- Besuchen Sie die Websites eine Viertelstunde lang und beantworten Sie die 5 Fragen mit Hilfe der Website oder der Recherche
- Teilen Sie Ihre Ergebnisse der Klasse mit (bitte denken Sie daran, dass Sie keine Informationen weitergeben müssen, die Ihnen Unbehagen bereiten könnten).

**Nachbesprechung:** Der Trainer sollte sich auf die Hindernisse konzentrieren, die soziale Netzwerke schaffen, um den Zugang zu den persönlichen Daten ihrer Nutzer zu erhalten. Der Trainer sollte auch Erfahrungen aus dem wirklichen Leben einbeziehen, die einige der SchülerInnen vielleicht schon in Bezug auf einige der Herausforderungen gemacht haben.

**Lektionen gelernt:** Wenn Informationen erst einmal öffentlich sind, ist es schwer, sie wieder zurückzubekommen. Seien Sie vorsichtig, wenn Sie Teil großer sozialer Netzwerke sind, sie sind nicht Ihr Freund.

## Ergänzende Lektüre

- **Warum wir süchtig nach sozialen Medien sind: Die Psychologie der Likes**: "Likes in sozialen Medien machen süchtig, weil sie das Gehirn beeinflussen, ähnlich wie die Einnahme chemischer Substanzen. Likes symbolisieren einen Reputationsgewinn, was dazu führt, dass man sich ständig mit Gleichaltrigen vergleicht." https://steverosephd.com/why-we-are-addicted-to-likes/

## E-Quiz

| **Online-Quiz** | | | |
|---|---|---|---|
| **Titel des Kurses:** | Datenschutz und Sicherheit | | |
| **Titel des Moduls:** | Datenschutz in einer digitalen Umgebung | | |
| **Richtig oder Falsch** | Geben Sie an, ob die folgenden Aussagen wahr (T) oder falsch (F) sind | | |
| **Erklärungen** | | T | F |
| 1 | Es gibt keinen gesellschaftlichen Nutzen für digitale Umgebungen | | |
| 2 | Mehr als 3 Milliarden Menschen nutzen inzwischen soziale Netzwerke | | |
| 3 | Facebook löscht meine persönlichen Daten automatisch nach einer bestimmten Zeit | | |
| 4 | Großen Technologieunternehmen kann man im Allgemeinen vertrauen, dass sie sorgfältig mit meinen persönlichen Daten umgehen | | |
| 5 | Datenvermeidung ist der sicherste Weg, um meine persönlichen Daten zu schützen | | |
| 6 | Facebook kann meine Daten verwenden, um mein Erlebnis gemäß den Nutzungsbedingungen zu personalisieren. | | |
| 7 | Profiling ist eine Gefahr für meine Privatsphäre | | |
| 8 | Identitätsdiebstahl ist eine große Gefahr für unerfahrene Nutzer sozialer Medien | | |

# 4. Modul 4 - Sicherheitsrisiken in einem digitalen Umfeld


Quelle: Unsplash

## Überblick über den Kurs

**Zusammenfassung**: Dieses Modul führt in die Grundlagen und die verschiedenen Bedrohungen für Hardware und Software ein. Es konzentriert sich auf die Risiken des täglichen Lebens und die Rolle des Benutzers als kritischer Teil typischer Sicherheitsschwachstellen.

**Struktur:**

- Überblick über den Kurs
- Einführung in die Hardware
- Einführung in die Software
- Bedrohungen für Hardware und Software
- Fallstudie
- Ergänzende Lektüre
- Übung
- Rückmeldung
- E-Quiz

**Lernziele:**

- die Rolle von Hardware und Software in digitalen Umgebungen zu verstehen
- Identifizierung der individuellen Risiken beim Einsatz von Hardware und Software
- Erkennen von benutzerbezogenen Risiken bei der Nutzung von Hard- und Software

## Einführung in die Hardware

Wir haben jeden Tag mit verschiedenen Geräten zu tun, die an einer digitalen Umgebung teilnehmen, z. B. Smartphones, Desktop-PCs oder Geldautomaten. Mit dem Begriff Hardware werden die physischen Komponenten dieser Geräte bezeichnet. Während die Hardware selbst eine kritische Schwachstelle sein kann, wurden Sicherheitsmaßnahmen in erster Linie für Software- und Benutzerfragen getroffen (s. nächstes Thema).

Die Kombination mehrerer Hardwarekomponenten macht unsere Geräte funktionsfähig:

- Die CPU (Central Processing Unit) ist für die Ausführung der verschiedenen Befehle und Berechnungen zuständig, die für die ordnungsgemäße Funktion unserer Geräte erforderlich sind. Sie finden eine CPU zum Beispiel in Ihrem Smartphone, Ihrem Laptop, Desktop-PC oder Tablet.
- Die GPU (Graphics Processing Unit) ist für alle grafisch anspruchsvollen Prozesse wie Videostreaming oder Videospiele zuständig. Hochbelastete GPUs benötigen eine hohe Leistung und können selbst komplexe und langwierige Berechnungen in kurzer Zeit durchführen.
- Das HDD (Hard Disk Drive) und das SSD (Solid State Drive) sind Speichergeräte. Sie werden verwendet, um Daten oder Software zu speichern. Ihr Unterschied liegt in ihrer Architektur: HDDs verwenden eine magnetische Speichertechnologie, während SSDs und alle mobilen Geräte eine Flash-Speichertechnologie verwenden.
- Die Hauptplatine oder das Mainboard ist das Herzstück eines jeden Computers oder mobilen Geräts. Es verbindet alle elektronischen Komponenten des Geräts miteinander.
- Die RAM-Karte (Random Access Memory) ist eine Form des Computerspeichers. Das Gerät speichert die aktuell ausgeführten Programme, Programmteile und Daten im RAM. Die Zugriffsgeschwindigkeit des RAMs und die Größe seiner Speicherkapazitäten können die Geschwindigkeit eines Geräts drastisch erhöhen.

## Einführung in die Software

Software bezieht sich auf alle Arten von Programmen oder Apps, die wir auf unseren Geräten installieren können, z. B. LibreOffice Writer, den VLC-Player oder Ihre persönliche Banking-App. Während die Hardware für die Ausführung der Arbeit verantwortlich ist, können wir mithilfe von Software die Aufgabe bestimmen, die unsere Geräte erledigen sollen.

Es gibt verschiedene Arten von Software für unterschiedliche Zwecke:

- Systemsoftware bezieht sich auf alle Programme und Daten, die zur Steuerung der Prozesse verwendet werden, die einen Computer zum Laufen bringen. Systemsoftware ist eng mit der Hardware des jeweiligen Geräts verbunden und steuert die Nutzung von Ressourcen; sie stellt also die Infrastruktur im Computer bereit. Beispiele für Systemsoftware sind:
    - Betriebssysteme, wie Linux, Windows, Android oder iOS
    - Gerätetreiber für externe Hardware wie Drucker oder Lautsprecher.
- Anwendungssoftware bezieht sich auf alle Programme, die bestimmte Aufgaben für die Benutzer ausführen und nicht mit System- oder Dienstprogrammen zusammenhängen. Alle modernen Geräte können eine Reihe unterschiedlicher Anwendungssoftware ausführen:
    - Medienplayer, zum Beispiel der VLC-Player
    - Textverarbeitungsprogramme, zum Beispiel LibreOffice Writer
    - Schnittsoftware, zum Beispiel Adobe Premiere Pro

- E-Mail-Programme, zum Beispiel Mozilla Thunderbird
- Webbrowser, zum Beispiel Mozilla Firefox.

Anwendungssoftware kann entweder vom Nutzer selbst installiert werden, was in den meisten Fällen durch Herunterladen der Programmdaten von einer Online-Quelle geschieht, oder sie ist auf bestimmten Geräten wie Smartphones vorinstalliert und im Lieferumfang enthalten.

- Als Hilfssoftware bezeichnet man Software, die die Infrastruktur, Betriebssysteme oder Anwendungssoftware mit zusätzlichen Funktionen unterstützt. Hilfssoftware ist oft in Betriebssysteme integriert, wobei einige von ihnen im Hintergrund arbeiten, weshalb die Unterscheidung zwischen Systemsoftware und Hilfssoftware nicht immer eindeutig ist. Typische Beispiele für bekannte Hilfssoftware sind:
  - Anti-Viren-Programme
  - Programme zur Datenwiederherstellung
  - Datei-Manager

## Bedrohungen für Hardware und Software

Wie wir in den vorherigen Modulen festgestellt haben, müssen wir besonders auf unsere persönlichen Daten und Informationen achten. Die Vorteile und Erleichterungen, die sich aus der Online-Erledigung vieler Aufgaben oder Alltagsroutinen ergeben, können zum Beispiel unsere Privatsphäre bedrohen:

- Sie sind vielleicht krank und möchten einen Arzt aufsuchen. Sie suchen mit Google auf Ihrem Smartphone nach einem spezialisierten Arzt. Dann rufen Sie den Arzt mit Ihrem Smartphone an und vereinbaren einen Termin, den Sie in der Kalender-App Ihres Smartphones speichern. Am Tag des Termins kaufen Sie mit Ihrem Smartphone ein Straßenbahnticket und nutzen Google Maps, um Ihr Ziel zu erreichen. Nach dem Termin gehen Sie in die nächstgelegene Apotheke und kaufen die verschriebenen Medikamente über Google Pay mit Ihrem Smartphone.
- Sie suchen auf der Dating-App Tinder nach interessanten Menschen. Nachdem Sie eine Weile mit einer interessanten Person gechattet haben, tauschen Sie über Ihr Smartphone Ihre E-Mail-Adressen aus. Sie verwenden eine E-Mail-Client-App auf Ihrem Smartphone, und nach einer Weile tauschen Sie Ihre Telefonnummern aus. Sie nutzen WhatsApp und rufen einander von Zeit zu Zeit an. Schließlich treffen Sie sich zu Ihrer ersten Verabredung im wirklichen Leben. Die Kalender-App auf Ihrem Smartphone erinnert Sie an Ihre Verabredung und Sie verwenden PayPal auf Ihrem Smartphone, um die Kinokarten zu bezahlen. Später am Abend nutzen Sie Ihre Smartphone-Zahlungsoptionen, um die Getränke in der Bar zu bezahlen, bevor Sie sich voneinander verabschieden und einen Uber rufen, um nach Hause zu fahren.

Wie die Beispiele zeigen, verwenden wir oft genug ein und dasselbe Gerät für verschiedene Zwecke und teilen und speichern dabei sensible, persönliche Informationen. Wenn sich jemand Zugang zu diesem Gerät verschafft, kann er leicht die intimsten Details Ihres Privatlebens erfahren oder zumindest rekonstruieren.

1. **Hardware-Risiken**

   Im Zuge des technologischen Fortschritts wird die Entwicklung von Hardwarekomponenten immer komplexer. Ein aktuelles Beispiel aus dem Jahr 2018 zeigt zwei Beispiele für kritische Hardware-Schwachstellen: "Meltdown" und "Spectre" nutzen Schwachstellen in modernen CPU-Chips aus und können für den Zugriff auf Daten in Programmen und Betriebssystemen

genutzt werden. Die Schwachstellen können in Smartphones, Desktop-PCs und im Grunde in jedem Gerät, das einen dieser CPU-Chips verwendet, ausgenutzt werden. Es gibt noch weitere Beispiele für Angriffe auf Hardwarekomponenten, z. B. "RAMbleed", die jedoch in der Regel schwierig auszuführen sind und bestimmte Voraussetzungen erfordern.

Es gibt zwar Möglichkeiten, sich vor solchen Schwachstellen zu schützen (siehe nächster Abschnitt), aber die größte Bedrohung für Ihre Hardware ist der direkte Zugriff. Es ist zwar unwahrscheinlich, dass ein Angreifer auf Ihren Desktop-PC zu Hause zugreift, aber ein USB-Stick oder Ihr Smartphone kann leicht verloren gehen (was nicht immer von der Nachlässigkeit des Nutzers abhängt - teure Smartphones ziehen zum Beispiel Diebe an).

2. **Software- und Netzwerkrisiken**

   Software- und Netzwerkrisiken können eine Bedrohung für die Sicherheit Ihres gesamten Geräts darstellen. Sie resultieren häufig entweder aus Softwarefehlern (z. B. weil den Programmierern bei der Erstellung der Software ein Fehler unterlaufen ist), aus Online-Angriffen und/oder aus verschiedenen Arten von Malware (Software, die absichtlich gegen die Interessen des Benutzers handelt, indem sie den Computer schädigt), einschließlich Viren, Würmern, Trojanern, Spyware oder Adware.

3. **Benutzerbezogene Risiken**

   Die größte Bedrohung geht von den Nutzern aus, die sich bei der Verwendung ihrer Geräte unvorsichtig, naiv oder uninformiert verhalten, häufig im Zusammenhang mit der falschen Verwaltung von Passwörtern oder der Verwendung persönlicher Finanzdaten. Zu den nutzerbezogenen Risiken gehören auch Konzepte der Cyberkriminalität wie digitales Social Engineering, z. B. über Phishing. In diesem Fall gibt sich der Angreifer als vertrauenswürdiger Kommunikationspartner aus, um sich Zugang zu persönlichen Daten zu verschaffen oder sein Opfer zu manipulieren, damit es eine bösartige Handlung ausführt.

## Fallstudie - Der Lieblingsbetrüger meiner Großmutter

Eine 88-jährige chinesische Großmutter wird von einem Betrüger davon überzeugt, dass eine Elitetruppe der Regierung ihre Hilfe benötigt, um einen internationalen Verbrecherring aufzudecken. Mit Hilfe von Telefonanrufen, einem "geheimen Treffen" in einem abgelegenen Hotel und einer ausgeklügelten Geschichte, die auf die Bedürfnisse von "Laolao" eingeht, gelingt es dem Betrüger, ihre Bankkonten zu leeren und ihre Ersparnisse abzuheben.

Ein Meinungsbeitrag von Frankie Huang in der New York Times, 12.07.2019:
https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

Frage zur Selbstreflexion: Wer sind die häufigsten Opfer von Finanzbetrügern?

## Übung 4: Die Invasion

**Zielsetzungen**

- Verstehen, warum Sicherheit wichtig ist
- Erkennen der Folgen von Sicherheitsmängeln
- Analyse der Sicherheitsfragen

**Dauer:** 20 Minuten

**Werkzeuge:** Smartphones oder Computer mit aktiver Internetverbindung, Stift und Papier

**Methoden:** Rollenspiel, Plenum, kreative Anwendung, praktische Anwendung

**Beschreibung der Übung:** Melden Sie sich bei Ihrem Gerät an und stellen Sie sich vor, dass jemand anderes vollständigen Zugriff darauf hat. Arbeiten Sie sich durch Ihre Apps, Mediendateien und Messenger-Inhalte und beantworten Sie dabei die folgenden drei Fragen: (1) Welche privaten, beruflichen oder finanziellen Informationen könnte der Angreifer über Sie erfahren? (2) Welche privaten, beruflichen oder finanziellen Informationen könnte der Angreifer über Ihre Familie und Freunde in Erfahrung bringen? (3) Welche Informationen wären am peinlichsten, wenn Sie sie mit einem Fremden teilen würden?

**Aufgaben:**

- Beantworten Sie alle drei Fragen so weit wie möglich innerhalb von fünfzehn Minuten.
    - Schreiben Sie die Antworten in Aufzählungspunkten auf.
    - Teilen Sie Ihre Ergebnisse der Klasse mit (bitte denken Sie daran, dass Sie keine Informationen weitergeben müssen, die Ihnen Unbehagen bereiten könnten).

**Nachbesprechung:** Der Schulungsleiter sollte ein Gleichgewicht zwischen dem neu erworbenen Wissen und dem affektiven Charakter der Aufgabe finden. Der Schulungsleiter sollte konkrete Schlussfolgerungen ziehen, um die Sicherheit der Geräte aller Teilnehmer zu verbessern.

**Lektionen gelernt:** Gerätesicherheit ist auf mehreren Ebenen wichtig und schützt uns vor Schaden.

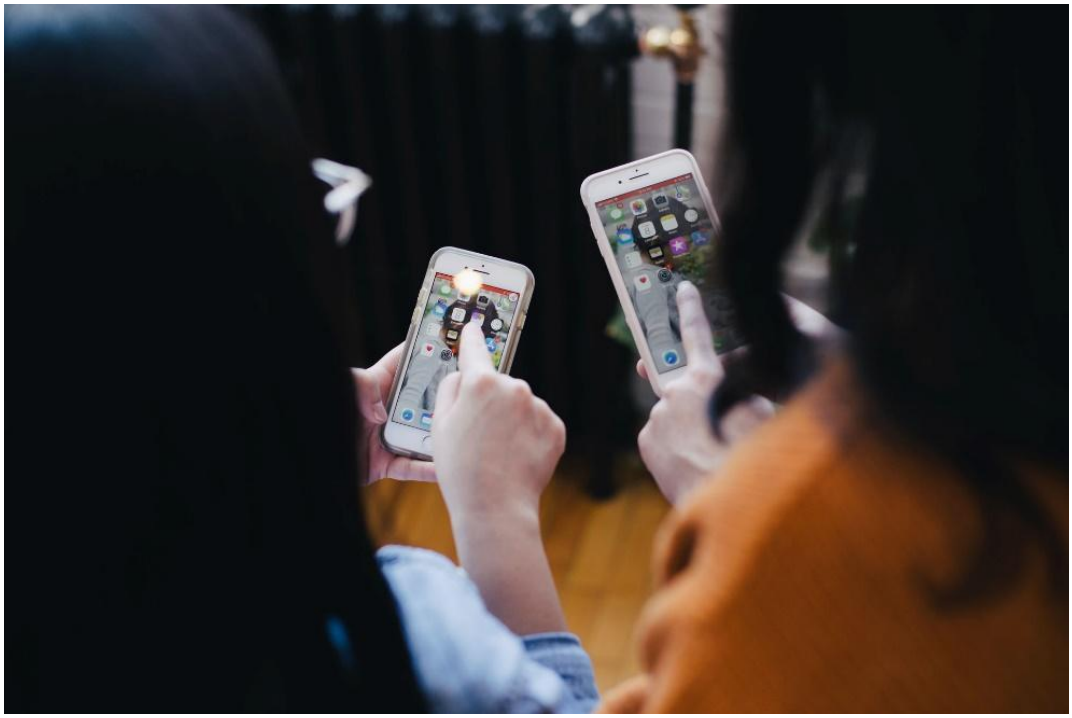
## Ergänzende Lektüre

- **Project Zero**: "Project Zero wurde 2014 gegründet und ist ein Team von Sicherheitsforschern bei Google, die Zero-Day-Schwachstellen in Hardware- und Softwaresystemen untersuchen, auf die sich Nutzer weltweit verlassen." https://googleprojectzero.blogspot.com/
- **Firefox Monitor**: Die Mozilla-Stiftung sammelt Datenlecks. Durch Eingabe einer E-Mail-Adresse prüft der Firefox Monitor, ob diese Adresse in vergangenen Datenlecks enthalten war. Diese Informationen können Ihnen helfen, sich selbst oder andere besser zu schützen, z. B. vor Social-Engineering-Angriffen. https://monitor.firefox.com/

E-Quiz

| **Online-Quiz** | | | |
|---|---|---|---|
| **Titel des Kurses:** | Datenschutz und Sicherheit | | |
| **Titel des Moduls:** | Sicherheitsrisiken in einem digitalen Umfeld | | |
| **Richtig oder Falsch** | Geben Sie an, ob die folgenden Aussagen wahr (T) oder falsch (F) sind | | |
| **Erklärungen** | | T | F |
| 1 | Mein Betriebssystem ist eine Anwendungssoftware | | |
| 2 | Sicherheitslücken auf meinem digitalen Gerät sind immer softwarebedingt | | |
| 3 | Ich kann eine Rechnung, die mir mein Internetanbieter in einer .zip-Datei geschickt hat, bedenkenlos öffnen | | |
| 4 | Die Weitergabe meiner Geolokalisierungsdaten gefährdet meine Privatsphäre | | |
| 5 | Die Benutzer sind oft selbst für Sicherheitslücken verantwortlich | | |
| 6 | Adware schützt mein Gerät vor unerwünschter Werbung | | |

# 5. Modul 5 - Sicherheitstipps für das digitale Umfeld



Quelle: Unsplash

## Überblick über den Kurs

**Zusammenfassung**: Dieses Modul bietet zugängliche Tipps zu Hardware-, Software- und benutzerbezogenen Sicherheitsfragen, wobei der Schwerpunkt auf praktischen Ratschlägen als wichtigem Bestandteil des Datenschutzes liegt.

**Struktur:**

- Überblick über den Kurs
- Tipps zur Sicherheit von Hardware
- Tipps zur Software-Sicherheit
- Tipps zur benutzerbezogenen Sicherheit
- Fallstudie
- Ergänzende Lektüre
- Übung
- Rückmeldung
- E-Quiz

**Lernziele:**

- Erinnern Sie sich an die grundlegenden Mittel der Sicherheit in digitalen Umgebungen
- Entwicklung einer grundlegenden Sicherheitsstrategie zum Schutz der eigenen Privatsphäre und der anderer Personen
- Entwickeln Sie eine Haltung, die ein bewusstes und verantwortungsvolles Online-Verhalten und -Interaktionen fördert.
- Anwendung von Sicherheitsmaßnahmen für die eigenen Geräte, Konten und digitalen Interaktionen

Der Schutz Ihrer persönlichen Informationen und Daten ist keine leichte Aufgabe, aber die Mühe lohnt sich, um sich und andere vor verschiedenen Arten von Schäden zu schützen, die sich negativ auf Ihr Berufs- und/oder Privatleben auswirken. Diese Liste enthält allgemeine Regeln, die Sie immer befolgen sollten:

## Tipps zur Sicherheit von Hardware

- **Kaufen Sie Hardware von vertrauenswürdigen Herstellern**: Für den Durchschnittsnutzer ist es nahezu unmöglich, sich über Sicherheitslücken in Verbrauchergeräten wie Smartphones, Laptops oder Routern zu informieren. Ein guter Ausgangspunkt ist der Standort und die jeweilige Rechtsprechung des Hardwareherstellers, die ihn zur Einhaltung von Gesetzen zum Datenschutz und zur Sicherheit verpflichten könnte.
- **Lassen Sie Geräte nicht unbeaufsichtigt**: Tragen Sie sensible Informationen nicht auf mobilen Geräten wie Smartphones oder USB-Laufwerken mit sich herum. Wenn Sie es doch tun müssen, vergewissern Sie sich, dass Ihre Geräte zumindest durch ein Passwort oder eine PIN geschützt sind, oder noch besser, dass sie mit einer Verschlüsselungssoftware verschlüsselt sind, z. B. mit VeraCrypt. Wenn Sie einen Desktop-Computer verwenden, sperren Sie immer Ihren Bildschirm oder schalten Sie ihn aus, wenn er nicht benutzt wird.
- **Deaktivieren Sie die Geolokalisierungs- und Bluetooth-Einstellungen**: Solange Sie sie nicht benötigen, gibt es keinen Grund, sie aktiviert zu lassen, da sie möglicherweise viele Metadaten über Sie liefern.
- **Stecken Sie keine Geräte unbekannter Herkunft ein**: Diese Regel ist besonders wichtig in einer professionellen Arbeitsumgebung. Stecken Sie niemals USB-Laufwerke oder andere mobile Speichermedien in Ihren Desktop-Computer, wenn diese nicht vorher auf mögliche Sicherheitsrisiken geprüft wurden.
- **Kaufen Sie Sicherungsgeräte**: Der Verlust wichtiger Daten kann Ihrem Berufs- oder Privatleben großen Schaden zufügen (z. B. durch den Verlust Ihrer Dissertation). Nehmen Sie sich immer die Zeit, wichtige Daten regelmäßig zu sichern, und suchen Sie sich einen sicheren Ort, an dem Sie diese Sicherungskopie aufbewahren können.

## Tipps zur Software-Sicherheit

- **Halten Sie Ihre Software auf dem neuesten Stand**: Dazu gehören System-, Dienstprogramm- und Anwendungssoftware. Aktivieren Sie automatische Updates für Ihre Programme, Anwendungen und Ihr Betriebssystem, unabhängig von dem Gerät, das Sie verwenden.
- **Verwenden Sie Software aus vertrauenswürdigen Quellen**: Große Open-Source-Projekte sind in der Regel eine gute Quelle für leistungsfähige und sichere Software, zum Beispiel Firefox als Webbrowser oder LibreOffice für Büroanwendungen. Seien Sie besonders vorsichtig, wenn Sie Apps auf Ihr Mobilgerät herunterladen, die nicht vom PlayStore oder AppStore geprüft wurden.
- **Schützen Sie Ihren Browser**: Da für den Zugriff auf das WWW in der Regel ein Browser verwendet wird, ist es äußerst wichtig, diesen immer so sicher wie möglich zu halten. Die meisten Browser unterstützen die Installation von Erweiterungen wie Werbeblockern (z. B. uBlock Origin), Tracking-Blockern (z. B. Facebook Container), Firewalls (z. B. uMatrix) oder automatischen Umleitungen auf https-Seiten (z. B. HTTPS everywhere).
- **Installieren Sie Anti-Malware-Software (optional)**: Der Nutzen von Anti-Malware-Software ist umstritten, da die Programme selbst potenzielle und reale Sicherheitsrisiken darstellen.

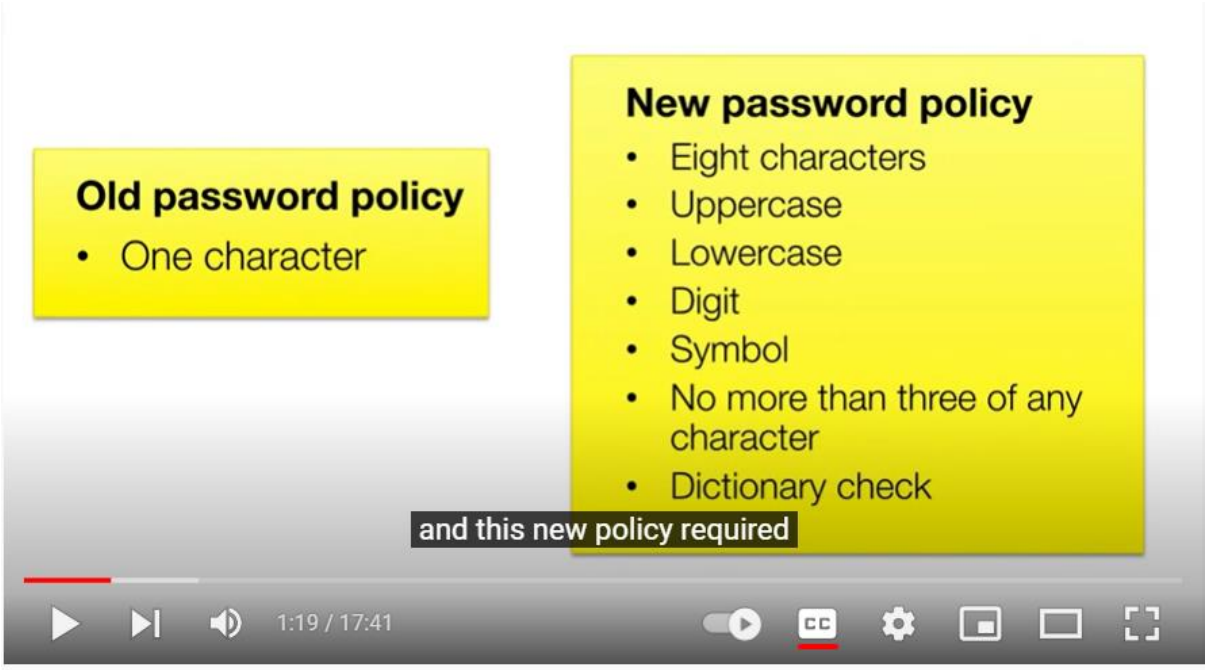
Um Ihr System zu schützen, erfordert Antiviren-Software in der Regel einen tiefen Zugriff auf Ihr System - wenn aber die Antiviren-Software selbst kompromittiert wird, ist Ihr System plötzlich offen für Angriffe, die es ohne die Antiviren-Software gar nicht erst gegeben hätte. Wenn Sie ein verantwortungsbewusster Benutzer sind, sollten Sie ohnehin nie mit Malware-Software in Kontakt kommen. Für unerfahrene Benutzer, die anfälliger für Malware-Fallen wie E-Mail-Anhänge sind, kann Antiviren-Software dennoch von Nutzen sein.

## Tipps zur benutzerbezogenen Sicherheit

- **Seien Sie vorsichtig bei unbekannten Quellen:** Klicken Sie niemals auf Links oder Anhänge von unaufgeforderten E-Mails oder anderen Nachrichten auf irgendeinem Gerät.
- **Verwenden Sie eine gute Passwortverwaltung:** Verwenden Sie einen Passwortmanager (z. B. KeyPass), um sichere Passwörter zu erstellen und diese sicher zu speichern. Verwenden Sie niemals das gleiche Passwort zweimal.
- **Reduzieren Sie die Verwendung persönlicher Informationen auf ein Minimum:** Sie sollten sich immer überlegen, ob die unaufgeforderte Weitergabe von persönlichen Informationen und Daten in einer digitalen Umgebung notwendig ist, z. B. in sozialen Netzwerken. Dies hat in der Regel keinen Nutzen, kann Ihnen aber später schaden, z. B. wenn Sie Opfer von Social Engineering-Versuchen werden.
- **Vermeiden Sie Betrügereien:** Lernen Sie, Fremden im Internet oder bei einem Telefonanruf nicht zu vertrauen. Social Engineering in einem digitalen Umfeld ist besonders für ältere Menschen gefährlich, zum Beispiel der berüchtigte Großeltern-Betrug. Informieren Sie sich und andere und stellen Sie sicher, dass Sie **niemals** persönliche Daten und Informationen über unsichere digitale Kanäle wie unverschlüsselte E-Mails, Messenger-Chats oder Telefonanrufe weitergeben.

## Fallstudie - Lorrie Faith Cranor: Was ist los mit deinem Pa$$w0rd?

"Lorrie Faith Cranor hat Tausende von echten Passwörtern untersucht, um die überraschenden, sehr häufigen Fehler herauszufinden, die Benutzer - und gesicherte Websites - machen, um die Sicherheit zu gefährden. Und wie, werden Sie sich fragen, hat sie Tausende von echten Passwörtern untersucht, ohne die Sicherheit der Benutzer zu gefährden? Das ist eine Geschichte für sich. Es sind geheime Daten, die man kennen sollte, vor allem, wenn Ihr Passwort 123456 lautet ..."




Freigegeben von der TED-Organisation am 24/06/2014: https://www.youtube.com/watch?v=0SkdP36wiAU

Frage zur Selbstreflexion: Wie sicher sind Ihre Passwörter?

## Übung 5: Gemeinsam sicher

**Zielsetzungen:**

- Verstehen, warum Sicherheit wichtig ist
- Darstellung der wichtigsten Sicherheitsmaßnahmen

**Dauer:** 20 Minuten

**Werkzeuge:** Stift und Papier

**Methoden:** Plenum, kreative Anwendung, Präsentation

**Beschreibung der Übung**: Jeder Schüler stellt sich ein altes Familienmitglied vor, das seinen ersten Laptop gekauft hat, um endlich die Vorteile der modernen Technologie zu nutzen. Dieses Familienmitglied weiß, wie man den neuen Laptop startet und bittet die SchülerInnen um Hilfe bei (1) der Einrichtung einer E-Mail-Adresse, (2) der Einrichtung von Online-Banking, (3) der Einrichtung eines Profils auf Facebook, (4) der Installation der WhatsApp-Desktop-App, (5) der morgendlichen Arbeit in einem Café und der Möglichkeit, dort online zu gehen. Jeder Schüler bereitet eine kleine Präsentation vor und konzentriert sich auf die wichtigsten Sicherheitsaspekte, die er seinem Familienmitglied zeigen möchte.

**Aufgaben:**

- Schreiben Sie in 15 Minuten mindestens drei Stichpunkte zu den wichtigsten Sicherheitsaspekten für jedes der 5 Szenarien auf.

- Teilen Sie Ihre Ergebnisse der Klasse mit (bitte denken Sie daran, dass Sie keine Informationen weitergeben müssen, die Ihnen Unbehagen bereiten könnten).

**Nachbesprechung:** Der Trainer sollte betonen, welche Schlussfolgerungen die Teilnehmer aus der Übung für ihre eigenen Sicherheitsgewohnheiten ziehen können. Sie sollten auch an das Gemeinschaftsgefühl appellieren, sich gegenseitig zu helfen, um sicher zu bleiben.

**Lektionen gelernt:** Sicherheit ist wichtig, um uns vor Schaden zu schützen, und wir sollten uns gegenseitig unterstützen, um sicher zu bleiben.

## Ergänzende Lektüre

- **Will Styler**: "Erinnern Sie sich an die Dissertation, an der ich gearbeitet habe? [...] Nun, ein großer Teil der Arbeit, die ich gemacht habe, ist verschwunden, weil ich einige schlechte Entscheidungen getroffen und viel Pech gehabt habe. Ich möchte Ihnen mitteilen, was ich falsch gemacht habe und wie Sie nicht so werden wie ich." https://wstyler.ucsd.edu/posts/lost_dissertation_files.html

## E-Quiz

| **Online-Quiz** | | | |
|---|---|---|---|
| **Titel des Kurses:** | Datenschutz und Sicherheit | | |
| **Titel des Moduls:** | Sicherheitstipps für das digitale Umfeld | | |
| **Richtig oder Falsch** | Geben Sie an, ob die folgenden Aussagen wahr (T) oder falsch (F) sind | | |
| **Erklärungen** | | T | F |
| 1 | Es ist sicher genug, überall dasselbe Passwort zu verwenden, wenn Sie es nie weitergeben. | | |
| 2 | Automatische Sicherheitsupdates können mein Betriebssystem schützen | | |
| 3 | Anti-Malware-Programme machen mein Gerät immer sicherer | | |
| 4 | Sicherheitslücken auf meinem digitalen Gerät sind immer softwarebedingt | | |
| 5 | Mein Smartphone ist sicher, wenn es PIN-geschützt ist | | |
| 6 | Ich kann eine APK-Datei, die ich von einer Website heruntergeladen habe, sicher auf meinem Smartphone ausführen | | |

# 6. Bewertung von Quizfragen

## Modul 1

1) Welcher der folgenden Sätze passt eher zu einer Beschreibung von Sicherheit online und nicht von Privatsphäre online?
   a) Der persönliche Schutz der eigenen Person
   b) Der Schutz der Online-Informationen anderer
   c) Eigenes Bewusstsein für Online-Aktionen und -Verhalten

2) Welcher der folgenden Regelsätze schützt die Privatsphäre in digitalen oder elektronischen Umgebungen?
   a) Die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy)
   b) Die eSecurity-Richtlinie
   c) Die Datenschutz- und Sicherheitsrichtlinie

3) Wie lautet der vollständige Titel des Regelwerks der Datenschutzrichtlinie für elektronische Kommunikation?
   a) Richtlinie über den Schutz der Privatsphäre und Online-Verhaltensweisen
   b) Richtlinie über Datenschutz und Sicherheit im Internet
   c) Richtlinie über den Schutz der Privatsphäre und elektronische Kommunikation

4) Was bedeutet GDPR?
   a) Allgemeine Datenschutzverordnung
   b) Allgemeine Datenschutzverordnung
   c) Allgemeine Datenschutzbestimmungen

## Modul 2

1) Wann ist der Datenschutztag?
   a) 28. Januar
   b) 28. Juni
   c) 28. Dezember

2) Wie heißt die weltweite Kampagne zur Sensibilisierung für Online-Sicherheit, die von der National Cybersecurity Alliance und der APWG Public Education Initiative organisiert wird?
   a) STOP. DENKEN. VERBINDEN

b) STOP. UMDENKEN. KONTAKT

c) ANFANGEN. DENKEN. KOMMENTAR

3) Welche Inhalte dürfen Sie online veröffentlichen?

a) Alle Fotos, die von Google stammen

b) Von meinen Freunden aufgenommene Fotos

c) Meine eigenen Fotos

4) Welcher der folgenden Nutzertypen kümmert sich am wenigsten um seine Datenschutzeinstellungen?

a) Die vorsichtigen Personen

b) Die aufschlussreichen Personen

c) Die Datenschutzbeauftragten

## Modul 3

1) Welche der folgenden Personen ist für die Ausführung der verschiedenen Befehle und Berechnungen zuständig, die für das ordnungsgemäße Funktionieren der Geräte erforderlich sind?

a) CPU (Central Processing Unit)

b) GPU (Graphics Processing Unit)

c) HDD (Festplattenlaufwerk)

2) Was bedeutet RAM?

a) Entfernter zusätzlicher Speicher

b) Speicher mit wahlfreiem Zugriff

c) Bereich Betrag Maßnahmen

3) Welche der folgenden Begriffe beziehen sich auf Dienstprogramme?

a) Linux

b) VLC-Spieler

c) Anti-Viren-Programm

4) Was ist ein "Meltdown"?

a) Eine Hardware-Schwachstelle

b) Eine Anwendungssoftware

c) Eine Systemsoftware

## Modul 4

1) Welche Art von Risiken sind mit Malware, Spyware und Adware verbunden?
   a) Hardware-Risiken
   b) Software- und Netzwerkrisiken
   c) Benutzerbezogene Risiken

2) Die Verwendung eines Passwortmanagers hat mit welcher Art von Sicherheit zu tun?
   a) Sicherheit der Hardware
   b) Software-Sicherheit
   c) Benutzerbezogene Sicherheit

3) Was macht Adware?
   a) Erzeugt automatisch Online-Anzeigen
   b) Automatische Werbung blockieren
   c) Hilft bei der Formatierung Ihrer Hardware

4) Welche der folgenden Begriffe beziehen sich auf Anwendungssoftware?
   a) Web-Browser
   b) Betriebssysteme
   c) Programme zur Datenwiederherstellung

## Modul 5

1) Welche der folgenden Geräte werden NICHT als Speichergeräte verwendet?
   a) HDD (Festplattenlaufwerk)
   b) SSD (Solid State Drive)
   c) GPU (Graphics Processing Unit)

2) Welcher der folgenden Sätze ist richtig?
   a) Die Einstellungen für soziale Medien bieten mir vollen Schutz meiner Daten
   b) Ich muss die Datenschutzeinstellungen in sozialen Medien anpassen, um meine Daten zu schützen

c) Meine Daten in den sozialen Medien sind vollständig geschützt, sobald ich nur meine eigenen Fotos poste

3) Mit welchen Risiken ist Cyberkriminalität verbunden?

a) Benutzerbezogene Risiken

b) Software-Risiken

c) Hardware-Risiken

4) Wo kann Betrug vorkommen?

a) Nur offline

b) Nur online

c) Offline und online

# 7. Referenzen

Europarat (2014). Leitfaden zu den Menschenrechten für Internetnutzer

Netter, M., Herbst, S., Pernul, G. (2013). Interdisziplinäre Wirkungsanalyse der Privatsphäre in sozialen Netzwerken

Ladan, M. I. (2015). Soziale Netzwerke: Fragen des Datenschutzes und Vorsichtsmaßnahmen

Schenk, M., Niemann, J., Reinmann, G., Roßnagel, A. (2012). Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen

Gross, R., Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case)

Cranor, L.F. (2014). Was ist los mit deinem Pa$$w0rd? https://www.youtube.com/watch?v=0SkdP36wiAU

Velasco, J. (2016). für socialnomics.net, 4 Case Studies in Fraud: Soziale Medien und Identitätsdiebstahl, https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

The New York Times (2019). My Grandmother's Favorite Scammer. https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

APWG (2010). STOP. THINK. CONNECT.™ Kampagne zur Öffentlichkeitsarbeit. https://education.apwg.org/safety-messaging-convention/

Media.ccc.de (2017). Privacy by Design: Sozialverträgliche Datenerhebung ohne datenschutzrechtliche Nebeneffekte. https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

# Anhang

## Bewertungsbögen für Quiz

### Bewertungsquiz Modul 1 - Checkblatt - richtige Antworten

1c

2a

3c

4b

### Auswertungsquiz Modul 2 Checkblatt - richtige Antworten

1a

2a

3c

4b

### Evaluierungsquiz Modul 3 Checkblatt - richtige Antworten

1a

2b

3c

4a

### Bewertungsquiz Modul 4 - Checkblatt - richtige Antworten

1b

2c

3a

4a

### Bewertungsquiz Modul 5 - Checkblatt - richtige Antworten

1c

2b

3a

4c

## Checkliste zur Überprüfung der Unterrichtsgestaltung für Jugendbetreuer

| Nein | Kriterien | Ja | Nein |
|---|---|---|---|
| **1. Ziele** | | | |
| 1.1 | Sind die Ziele für die Lernenden klar formuliert? | | |
| 1.2 | Sind die Kursanforderungen mit den Zielen vereinbar? | | |
| 1.3 | Decken die Kapitel/Themen die Ziele des Kurses gründlich ab? | | |
| 1.4 | Stimmen die Lernziele mit den Lernergebnissen überein? | | |
| 1.5 | Entspricht der Gesamtinhalt und -aufbau des Kurses den Lehrzielen? | | |
| **2. Aufbau** | | | |
| 2.1 | Verfügt der Kurs über eine knappe und umfassende Übersicht oder einen Lehrplan? | | |
| 2.2 | Enthält der Kurs Beispiele, Analogien, Fallstudien, Simulationen, grafische Darstellungen und interaktive Fragen? | | |
| 2.3 | Setzt die Kursstruktur geeignete Methoden und Verfahren ein, um den Lernerfolg zu messen? | | |
| **3. Inhalt** | | | |
| 3.1 | Fließt der Inhalt nahtlos, ohne grammatikalische, syntaktische und taktische Fehler? | | |
| 3.2 | Ist der Inhalt aktuell? | | |
| 3.3 | Ist der Inhalt auf den Lehrplan abgestimmt? | | |
| 3.4 | Sind die erwünschten Ergebnisse in den Inhalt integriert? | | |
| 3.5 | Ist der Inhalt mit dem Urheberrecht vereinbar und wird das gesamte zitierte Material korrekt zitiert? | | |
| 3.6 | Regt der Kurs die Studierenden zu kritischem und abstraktem Denken an? | | |
| 3.7 | Gibt es für den Kurs Voraussetzungen oder ist ein technischer Hintergrund erforderlich? | | |
| **4. Bewertung** | | | |
| 4.1 | Sind die Aufgaben relevant, effizient und beziehen die Schüler in eine Vielzahl von Leistungsarten und Aktivitäten ein? | | |
| 4.2 | Sind die Übungs- und Bewertungsfragen interaktiv? | | |
| 4.3 | Konzentrieren sich die Übungs- und Bewertungsaufgaben auf die Ziele des Kurses? | | |
| **5. Technik - Gestaltung** | | | |
| 5.1 | Ist das Design klar und konsistent, mit entsprechenden Hinweisen? | | |
| 5.2 | Sind die Bilder und Grafiken von hoher Qualität und für den Kurs geeignet? | | |
| 5.3 | Ist der Kurs einfach zu navigieren und bietet er Unterstützung bei der technischen und der Kursverwaltung? | | |
| 5.4 | Ist die Struktur der Kursnavigation konsistent und zuverlässig? | | |
| 5.5 | Sind die Hardware und Software des Kurses definiert? | | |
| 5.6 | Sind der Ton und der Text auf dem Bildschirm synchronisiert? | | |
| 5.7 | Erlaubt es die Architektur des Kurses den Lehrkräften, Inhalte, Aktivitäten und zusätzliche Bewertungen hinzuzufügen? | | |

## Feedback zum Thema für Studenten

| **Bewertung des Moduls** | | | | | | |
|---|---|---|---|---|---|---|
| **Titel des Kurses:** | | | | | | |
| **Titel des Moduls:** | | | | | | |
| **Teil A:** | Geben Sie auf einer Skala von 1 bis 5, wobei 1 die niedrigste und 5 die höchste Zustimmung bedeutet, an, wie Sie die folgenden Punkte beurteilen | | | | | |
| Beobachtungen | | 1 | 2 | 3 | 4 | 5 |
| 1 | Das Thema war interessant | | | | | |
| 2 | Ich glaube, die behandelten Themen waren wichtig | | | | | |
| 3 | Ich möchte mehr über das Gebiet erfahren | | | | | |
| 4 | Ich habe neue Dinge gelernt, die ich in Zukunft wahrscheinlich anwenden werde | | | | | |
| 5 | Ich möchte meine Fähigkeiten in diesem Bereich verbessern | | | | | |
| 6 | Ich werde diesen Kurs wahrscheinlich weiterempfehlen | | | | | |
| **Teil B:** | In dem dafür vorgesehenen Feld können Sie Ihre Kommentare und Empfehlungen abgeben | | | | | |
| **Teil C:** | Bitte geben Sie in dem dafür vorgesehenen Feld Ihre E-Mail-Adresse an, wenn Sie über dieses Projekt auf dem Laufenden gehalten werden möchten. | | | | | |