Digitale Lebenswelten

INHALT

Cyberfibel –

How to / Kurzanleitung

Orientierung

Jedes Kapitel in den digitalen Lebenswelten und in den digitalen Kompetenzen ist durch ein Icon gekennzeichnet. Das Icon am rechten Seitenrand kennzeichnet, in welchem Kapitel Sie sich gerade befinden. Die Icons unterstützen zudem Ihre Orientierung bei Verweisen auf andere Kapitel der Cyberfibel. Die Legende im Umschlag der Cyberfibel führt alle Icons zu den zugehörigen Kapiteln auf.

Übungen

In den Lebenswelten der Cyberfibel können Sie mit den angebotenen Übungen das vermittelte Grundlagenwissen praktisch anwenden und erweitern. Sie befähigen dazu, Strategien und Verhaltensweisen für die sichere und souveräne Nutzung des Internets einerseits selbst zu erwerben, andererseits an andere weiterzugeben. Zur Verfügung stehen Aufgaben

- in Einzelarbeit, für das Zuhause oder das Lernen im Kurs und
- in Gruppenarbeit, die in Schulungen eingesetzt werden können.

Glossar

Am Ende der Digitalen Lebenswelten und der Digitalen Kompetenzen ist jeweils ein alphabetisches Glossar eingefügt, in dem Fachbegriffe definiert und erklärt werden. Alle im Glossar enthaltenen Begriffe sind im Text unterstrichen.

Linktipps

Die Cyberfibel bietet Ihnen anhand geprüfter Linktipps weiterführende Materialien, welche ausgewählte Artikel, Videos und Arbeitsmaterialien beinhalten. Zu den Linktipps wird stets der Herausgeber und eine Beschreibung mit angegeben. Wenn Sie den vierstelligen Webcode auf der Webseite (https://www.cyberfibel.de) eingeben, können Sie von dort aus auf die verlinkten Webseiten zugreifen, ohne dass Sie nach diesen suchen oder lange Links abtippen müssen.

Webcode: 1 1 1 1

Beispielhafter Webcode

Disclaimer: Unser Angebot enthält Links zu externen Websites Dritter, auf deren Inhalte wir keinen Einfluss haben. Deshalb können wir für diese fremden Inhalte auch keine Gewähr übernehmen. Auch können wir für mögliche Aufwände, Kosten oder sonstige nachteilige Folgen keine Haftung übernehmen, die durch die Nutzung von externen Webseiten oder aber auch im Rahmen von Übungen entstehen können. Für die Inhalte der verlinkten Seiten ist stets der jeweilige Anbieter oder Betreiber der Seiten verantwortlich und eine Benutzung der Seiten sowie die Übernahme oder Anwendung ihrer Inhalte erfolgt daher stets auf eigene Verantwortung. Bei Bekanntwerden von Rechtsverletzungen werden wir derartige Links umgehend entfernen.

Vorwort

Die Cyberfibel – Für Wissensvermittler/-innen in der digitalen Aufklärungsarbeit

Liebe Leser/-innen,

wir freuen uns, Ihnen heute die erste Auflage der Cyberfibel zu überreichen. Die Cyberfibel möchte Ihnen künftig dabei helfen, Fragen des sicheren und selbstbestimmten Umgangs im digitalisierten Alltag zu klären: So geht es um soziale Netzwerke, Ihr digitales Zuhause, Einkaufen und Bankgeschäfte im Internet sowie Fragen der vernetzten Mobilität. Die Cyberfibel gibt konkrete Anleitungen, wie Sie das Internet im Alltag sicherer nutzen können – und Ihr Wissen weitergeben: Sie kann damit als Handbuch und Wegbegleiter im Umgang mit Kindern und jungen Menschen ebenso genutzt werden, wie zur Vermittlung von digitalen Kompetenzen für Familien, Senioren sowie im schulischen und ehrenamtlichen Umfeld.

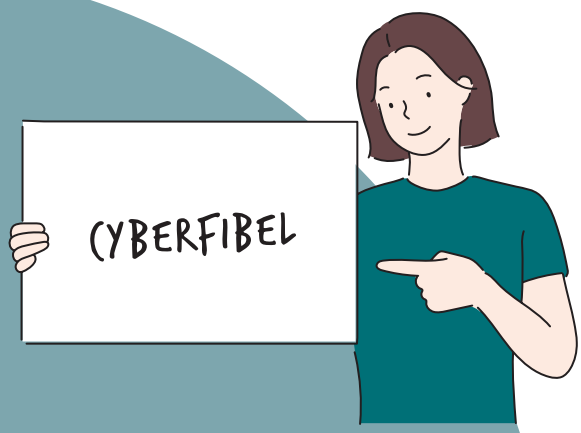
Für den einfachen Gebrauch unterscheidet die Cyberfibel nach Lebenswelten und digitalen Kompetenzfeldern. Sie bündelt die Expertise des Bundesamts für Sicherheit in der Informationstechnik (BSI) mit den praktischen Erfahrungen von Deutschland sicher im Netz e. V. (DsiN) und unserer Partner des Deutschland Dialogs für digitale Aufklärung, in welchem Vertreter aus Politik, Wirtschaft und Zivilgesellschaft gemeinsam Projekte zur digitalen Aufklärung in verschiedenen Themenfeldern entwickeln.

Als „lebendiges Handbuch“ werden wir die Cyberfibel stetig erweitern - um das Aufklärungsangebot stetig zu verbessern und Ihren Alltag noch sicherer zu machen, möchten wir auch Ihre Erfahrungen und Hinweise zum Umgang mit der Cyberfibel in künftigen Ausgaben berücksichtigen. Deshalb sind wir für Ihre aktive Nutzung sowie auch kritische Rückmeldungen dankbar, die unsere Redaktion gern unter info@cyberfibel.de entgegennimmt – für ein sicheres Internet für alle.

Viel Freude und ergebnisreiches Lernen und Lehren mit Ihrer Cyberfibel wünscht

Dr. Michael Littger
Geschäftsführer Deutschland sicher im Netz e.V.

Steffen Ganders
Fürsprecher Deutschland Dialog für digitale Aufklärung


CYBERFIBEL

Mit der Cyberfibel sicher ins Netz

Die Reise im Internet buchen, mit Freund/-innen und Familie chatten, mit Carsharing flexibel zur Arbeit fahren oder die Rechnung online begleichen: In immer mehr Lebensbereichen gibt es digitale Angebote, die uns das Leben erleichtern und unseren Alltag bereichern können. Daraus ergeben sich aber auch zahlreiche neue Herausforderungen und Fragen in Bezug auf die Nutzung von Onlineangeboten, die Sicherheit der Kommunikation und der Daten.

Welches Wissen und welche Fähigkeiten sind notwendig, um sicher und selbstbestimmt im Internet unterwegs zu sein? Und wie können Menschen mit verschiedenen Hintergründen diese Kompetenzen für ihren Alltag erlernen? Die Cyberfibel ist ein eigens für diese Fragen konzipiertes, leicht verständliches Handbuch für Wissensdurstige und Wissensvermittler/-innen, um Basiswissen und Digitalkompetenzen rund um das Thema Cybersicherheit weiterzugeben. Sie geht von alltäglichen Fragen und Bedürfnissen aus – und schafft Orientierung anhand von Hintergrundinformationen, Tipps für die Praxis und konkreten Anwendungsaufgaben.

Die Cyberfibel ist ein lebendiges Werk, welches sowohl als Handbuch in der gedruckten Variante als auch digital zur Verfügung steht (https://www.cyberfibel.de). Durch die Onlinefassung werden Entwicklungen und Erweiterungen des Themenspektrums permanent berücksichtigt, die in regelmäßigen Abständen auch durch Neuauflagen der gedruckten Cyberfibel nachvollzogen werden.

Aufklärungsarbeit zur Cybersicherheit

Die Cyberfibel richtet sich an alle Menschen, die beruflich oder ehrenamtlich in der Verbraucherberatung oder -aufklärung tätig sind und in Vereinen, Stiftungen, Bildungseinrichtungen oder Verbänden dazu beitragen, andere Personen im sicheren Umgang mit der digitalen Welt zu unterstützen. Die Cyberfibel ist die Grundlage für die Wissensvermittlung – und damit auch für die eigene Wissensaneignung im Sinne eines begleitenden Nachschlagewerks. Die Publikation hilft bei der Vorbereitung und Durchführung von Seminaren oder Beratungsgesprächen. Vorkenntnisse sind nicht erforderlich; vielmehr geht es darum, Sie und andere Menschen darin zu befähigen, sich selbstbestimmt und souverän im Netz zu bewegen und so eigene Lösungskompetenzen zu entwickeln.

Die Elemente der Cyberfibel

Die Cyberfibel umfasst zwei Bereiche: Im ersten Teil zeigen die digitalen Lebenswelten alltägliche Anwendungsbereiche digitaler Technologien im privaten und beruflichen Alltag. Dabei geht es unter anderem darum, Verhaltensweisen im Internet zu reflektieren und darauf aufbauend Strategien zu entwickeln, wie Internetangebote sicher und sinnvoll individuell genutzt werden können. Im zweiten Teil, den digitalen Kompetenzen, thematisiert die Fibel Risiken in der Onlinewelt und gibt praktische Empfehlungen, wie Sie sich und Ihre Geräte vor möglichen Bedrohungen aus dem Netz schützen können. Alle Lebenswelten und Kompetenzen können dabei sowohl nacheinander als auch unabhängig voneinander betrachtet werden, da sie nicht aufeinander aufbauen.

Die Übungen und Links der Cyberfibel

In den Lebenswelten der Cyberfibel können Sie mit den angebotenen Übungen das vermittelte Grundlagenwissen praktisch anwenden und erweitern. Sie befähigen dazu, Strategien und Verhaltensweisen für die sichere und souveräne Nutzung des Internets einerseits selbst zu erwerben, andererseits an andere weiterzugeben.

ZUR VERFÜGUNG STEHEN AUFGABEN

- in Einzelarbeit, für das Zuhause oder das Lernen im Kurs und
- in Gruppenarbeit, die in Schulungen eingesetzt werden können.

Alle Übungen sollten von einer fachkundigen Person, begleitet werden, z. B. von der Schulungsleitung. Bei der Durchführung der Übungen zuhause sollte ein fachkundiges Familienmitglied, eine Bekannte oder ein Bekannter dabei sein. Insbesondere ist darauf zu achten, dass keine Verträge abgeschlossen und keine Zahlungsverpflichtungen eingegangen werden.
Zusätzlich bietet Ihnen die Cyberfibel anhand geprüfter Linktipps weiterführende Materialien, welche ausgewählte Artikel, Videos und Arbeitsmaterialien beinhalten. Richten sich diese Inhalte an eine spezielle Zielgruppe wie Seniorinnen und Senioren oder Lehrkräfte, ist die Zielgruppe mit aufgeführt. Andernfalls richten sie sich allgemein an die Nutzerinnen und Nutzer.

Die Initiatoren der Cyberfibel

Das Handbuch ist ein Projekt des Bundesamts für Sicherheit in der Informationstechnik (BSI) und Deutschland sicher im Netz e. V. (DsiN).
Die redaktionelle und inhaltliche Verantwortung für den ersten Teil, die Lebenswelten, liegt bei DsiN, für den zweiten Teil, die Kompetenzen, liegt sie beim BSI.
Die Cyberfibel ist eine Initiative des Deutschland Dialogs für digitale Aufklärung, in welchem Vertreter aus Politik, Wirtschaft und Zivilgesellschaft gemeinsam Projekte zur digitalen Aufklärung in verschiedenen Themenfeldern entwickeln. Im Rahmen dessen wurden Feedback-Partner eingebunden, die auf Grundlage ihrer Erfahrungen und Expertise Anregungen und Ideen vorgebracht haben. Zu den Mitwirkenden zählten unter anderem das Bundesnetzwerk Bürgerschaftliches Engagement, der Bundesverband Die Verbraucher Initiative e. V. sowie weitere ausgewählte Mitglieder von DsiN wie eBay Kleinanzeigen und Samsung Electronics (Fürsprecher).

LEGENDE

LEBENSWELT 1
Online dabei sein und
ins Netz starten

LEBENSWELT 2
Online einkaufen und bezahlen

LEBENSWELT 3
Online vernetzen und austauschen

LEBENSWELT 4
Online Reise planen und
vernetzt mobil sein

LEBENSWELT 5
Online sein in Haus und Freizeit

Weitere Lebenswelten aus dem Alltag folgen!

Auch auf www.cyberfibel.de **sind künftig Updates der Lebenswelten in digitaler Form zu finden.**

GLOSSAR

DIGITALE LEBENSWELTEN

Die **digitalen Lebenswelten** zeigen Ihnen Möglichkeiten auf, wie digitale Technologien und Angebote im Alltag zum Einsatz kommen und sicher angewendet werden können. Über Verweise auf **digitale Kompetenzen** können vertiefende Informationen über die sichere Verwendung im zweiten Bereich der Cyberfibel nachgeschlagen werden. Ergänzt wird dies durch Linktipps zu weitergehenden Informationen sowie durch Übungen, in denen das Gelernte einzeln oder gemeinsam vertieft und diskutiert werden kann.

DIE LEBENSWELTEN IM ÜBERBLICK:

- **Lebenswelt 1** ▶ **Online dabei sein und ins Netz starten**
- **Lebenswelt 2** ▶ **Online einkaufen und bezahlen**
- **Lebenswelt 3** ▶ **Online vernetzen und austauschen**
- **Lebenswelt 4** ▶ **Online Reisen planen und vernetzt mobil sein**
- **Lebenswelt 5** ▶ **Online sein in Haus und Freizeit**

Linktipp

Verband Sichere Digitale Identität
Herausgeber: Verband Sichere Digitale Identität (VSDI)
Beschreibung: Webseite, die Antworten auf Fragen zum Themenkomplex Sichere digitale Identität anbietet.

Webcode: 1 1 1 1

LEBENSWELT 1
Online dabei sein und ins Netz starten

Ob Sie im Internet über den Browser surfen, E-Mails versenden oder in Suchmaschinen recherchieren, sicher ist: Sie benötigen einen Zugang ins Internet. Dieser Zugang erfolgt über ein Endgerät: Dies kann der stationäre Computer zu Hause oder am Arbeitsplatz sein, oder aber ein mobiles Gerät wie ein Smartphone oder Tablet – Ihnen steht hier eine große Vielfalt an Möglichkeiten zur Verfügung.

Doch wie funktioniert das Internet, wie ist es entstanden und wie findet man sich als Einsteiger/-in oder Gelegenheitsnutzer/-in mit den immer neuen Möglichkeiten zurecht? Welche Begriffe sind besonders wichtig, wenn man über das Internet spricht? Und vor allem: Wie kann man selbst die ersten Schritte online gehen? Die **digitale Lebenswelt** „Online dabei sein und ins Netz starten“ bietet Ihnen einen Einblick in die Geschichte des Internets, grundlegende Begriffe und erste Anwendungsmöglichkeiten.

IN DER LEBENSWELT „ONLINE DABEI SEIN UND INS NETZ STARTEN“ LERNEN SIE,

- was das Internet ist,
- wie das Web 2.0 zur Entwicklung des Internets beigetragen hat,
- wie das Internet in Ihrem Zuhause sowie unterwegs funktioniert,
- die Grundlagen des Surfens im Browser kennen,
- wie Sie online recherchieren.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.

STATION 1

Das weltweite Netz der Möglichkeiten entdecken

Hätten Sie das gedacht? Die Anfänge des Internets reichen über 50 Jahre zurück bis in die späten 1960er Jahre. Wir sprechen zu diesem Zeitpunkt von insgesamt vier Großrechnern, die untereinander Informationen austauschen können. Der Begriff Internet steht für „interconnected networks“ und bezeichnet einen Zusammenschluss aus vielen selbstständigen Computernetzwerken. Diese sind heute rund um den Globus miteinander verbunden und können weltweit Daten austauschen. Jeder Text, aber auch jedes Bild oder Video wird im Netz durch Daten repräsentiert. Daten beinhalten Informationen, welche von Computern verarbeitet werden können. Sie werden auf anderen Computern gespeichert, den Servern. Sie stellen die Daten zum Abruf bereit.

In den letzten 50 Jahren hat sich das Netz rasant weiterentwickelt. Unsere moderne Onlinewelt hat einmal mit sehr wenigen vernetzten Geräten für militärische und universitäre Zwecke begonnen. Heute gibt es eine Vielzahl von Geräten und Nutzungsmöglichkeiten. Neben den gängigen internetfähigen Geräten wie Desktop-PCs, Laptops, Tablets und Smartphones sind mittlerweile immer mehr digitale und internetfähige Geräte vernetzt: Armbanduhren, Fernseher, Spielekonsolen, Fahrzeuge, Rasenmäher, Beleuchtung, Heizungen, Waschmaschinen, Kühlschränke und Kinderspielzeug können inzwischen auch Daten empfangen und senden. Hierbei spricht man vom Internet der Dinge (englisch: Internet of Things, IoT). Durch das IoT sind Geräte leichter in der Lage, automatisiert Aufgaben zu erledigen.

Linktipps

Die Geschichte des Internets von den Anfängen bis in die Gegenwart
Herausgeber: Landesmedienzentrum Baden-Württemberg
Beschreibung: Übersichtliche Zeitleiste, die die Entstehung und Entwicklung des Internets darlegt

Informatik-Geschichte in Bildern
(Infografik: Von Caesar bis zum Web 2.0)
Herausgeber: Sonnentaler Projekt / Freie Universität Berlin
Beschreibung: Grafik, die wesentliche Meilensteine in der Entwicklung des Internets darstellt

Das Netz – Eine kurze Geschichte des Internets
Herausgeber: Deutsches Technikmuseum
Beschreibung: Video, welches anschaulich die Entstehung des Internets erläutert

Was ist das Internet? Eine Einführung
Herausgeber: Deutschland sicher im Netz e. V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Handreichung #1 des Digital-Kompasses, die über Entstehung, Funktionen sowie Chancen und Risiken des Internets informiert
Zielgruppe: Vor allem Senior/-innen

Webcode: 2 1 1 1

Lernziel **Bekommen Sie ein Gespür dafür, wie und an welchen Stellen Sie und andere online gehen.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Zählen Sie die Geräte auf, mit denen Sie zurzeit das Internet nutzen, und die Geräte, mit denen Sie in den letzten fünf oder zehn Jahren online gegangen sind.

2. Nennen Sie weitere internetfähige Geräte, die Sie besitzen, mit denen Sie aber bewusst nicht ins Internet gehen.

3. Fragen Sie in Ihrem Familien-, Freundes- oder Bekanntenkreis, mit wie vielen und welchen Geräten sie online gehen. Fällt Ihnen dabei etwas auf? Sind bestimmte Geräte in jedem Haushalt zu finden und andere nur bei Menschen eines bestimmten Alters?

REFLEXION

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Führen Sie ein Interview mit einem oder zwei weiteren Schulungsteilnehmer/-innen über deren persönliche Internetgeschichte. Mögliche Fragen sind:

a) Wie häufig sind Sie online?

b) Welche Vorteile sehen Sie im Onlinesein, welche Nachteile?

c) Wann und wie häufig entscheiden Sie bewusst, offline zu sein?

d) Hat sich die Anzahl der Geräte, mit denen Sie in den letzten Jahren online gegangen sind, verändert?

e) Befragen Sie Freunde, Familienmitglieder oder Bekannte: Wer hat die meisten Geräte, mit denen er online gehen kann? Wer die wenigsten?

REFLEXION

Das Mitmachnetz

Brauchte es für die Veröffentlichung von Inhalten im Internet jahrzehntelang Spezialwissen, gibt es besonders seit Mitte der 1990er Jahre neue Möglichkeiten für Nutzerinnen und Nutzer im Internet. Während zuvor von den meisten Menschen vorrangig Inhalte konsumiert wurden, entstanden zunehmend Onlineangebote, mit denen recht einfach Inhalte, zum Beispiel Texte und Bilder, auf Webseiten selbst erstellt, gestaltet oder bearbeitet werden konnten. Auch die Kommunikation im Netz veränderte sich: Immer mehr Menschen nutzen ganz selbstverständlich Angebote wie Foren oder Chats, um synchron (in Echtzeit) oder asynchron (zeitversetzt) im Internet zu kommunizieren.

Insbesondere Chats bringen einen Nachteil mit sich: Mimik und Gestik sind durch das Kommunizieren via Text nicht erkennbar. Um Missverständnisse zu vermeiden, werden Smileys und Emoticons genutzt. Dabei handelt es sich um kleine Bilder von Gesichtern mit verschiedenen emotionalen Ausdrücken, die Mimik und Gestik repräsentieren.

Das Internet entwickelte sich immer mehr zu einem echten „Mitmachnetz“ für viele. Unter anderem Tim O’Reilly prägte hierfür den Begriff „Web 2.0“.

Die Onlinedienste, die dafür benötigt werden, sind in vielen Fällen einfach bedienbar, sodass keine Programmierkenntnisse mehr benötigt werden. Für Verbraucher/-innen bedeutet das Mitmachnetz, dass sie zu aktiven Produzent/-innen werden.

Eine klassische Beteiligungsform ist der Internetblog. Das ist eine Internetseite, auf der eine oder mehrere Personen Beiträge veröffentlichen. In den meisten Fällen befassen sich Blogs mit gezielten Fragen zu einem Thema und haben einen aktuellen Anlass. Sie laden die Leserinnen und Leser auch oft dazu ein, die Texte zu kommentieren, sodass eine Kommunikation entsteht. Darüber hinaus gibt es auch noch weitere Möglichkeiten, sich im Mitmachnetz zu beteiligen: Insbesondere die sozialen

Netzwerke tragen dazu bei. Haben Sie zum Beispiel schon einmal bei einer Abendveranstaltung über Twitter live mitdiskutiert? Darüber hinaus können Sie Gruppen in den sozialen Netzwerken einrichten, um mit Gleichgesinnten regelmäßig über ein bestimmtes Thema zu diskutieren.

Auch Bewertungen von Restaurants und Dienstleistungen oder die Arbeit an gemeinschaftlich entstehenden Wissensportalen wie Wikipedia sind Möglichkeiten, sich aktiv im Netz zu beteiligen.

Viele Möglichkeiten des Mitmachnetzes basieren darauf, dass Sie etwas von sich selbst öffentlich im Internet preisgeben und somit private Inhalte mit Ihren Kontakten oder potenziell für alle Menschen auf der Welt sichtbar teilen. Bei Veröffentlichungen sollten Sie deswegen entscheiden, welche Angaben Sie machen. Über welche Themen berichten Sie in Ihrem Blog? Welche Fotos veröffentlichen Sie in Ihrem sozialen Netzwerk? Was erfahren die Zuschauerinnen und Zuschauer Ihres Video-Kanals über Sie?

Halten Sie sich immer vor Augen, dass das Publikum im Internet riesengroß ist. Was einmal online ist, lässt sich oft nicht mehr entfernen – einige Ihrer Datenspuren sind daher oft im Nachhinein nicht mehr veränderbar. Datensparsamkeit ist eine grundsätzliche Verhaltensregel im Internet. Das betrifft insbesondere den Umgang mit personenbezogenen Daten wie Telefonnummer, Anschrift, E-Mail-Adresse oder Fotos von Ihnen oder anderen **Kompetenzteil 4, Station 3 > Datensparsamkeit**.

Linktipp

Web 2.0
Herausgeber: Prof. Dr. Katja Artsiomenka und Prof. Dr. Horst Pöttker
Beschreibung: Erklärung des Begriffs „Web 2.0“ und aktueller Forschungsstand

Webcode: 2 1 1 2

Lernziel **Lernen Sie das Mitmachnetz kennen. Finden Sie Wege, sich einzubringen**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Schreiben Sie einen fiktiven Beitrag für einen Internetblog, in dem Sie die Chancen und Risiken des „Bloggens“, des Veröffentlichens von Internetbeiträgen, gegenüberstellen. Überlegen Sie sich vorher, wie Sie Ihren Beitrag strukturieren und wie lang dieser sein soll.

2 Stellen Sie sich vor, Sie würden einen Blog im Internet führen. Was wäre das Thema Ihres Blogs? Über welche Inhalte würden Sie informieren – und warum? Skizzieren Sie ein kurzes Design der Startseite.

PRAXIS + VERTIEFUNG

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

PRAXIS + VERTIEFUNG

1 Tauschen Sie sich in der Gruppe über Ihre Erfahrungen mit sozialen Netzwerken aus:

a) Zu welchen Themen haben Sie bereits Beiträge in sozialen Netzwerken veröffentlicht? Wenn Sie noch keine Beiträge veröffentlich haben: Zu welchen Themen möchten Sie gerne Beiträge veröffentlichen?

b) Wie reagieren Sie auf Beiträge in sozialen Netzwerken? Diskutieren Sie in der Gruppe, welche Reaktionen welche Auswirkungen haben können. Erstellen Sie eine Liste mit Formulierungen für ein faires Miteinander im Netz

2 Tauschen Sie sich aus: Beschreiben Sie in der Gruppe Ihr Sicherheitsgefühl, wenn Sie online gehen und tauschen Sie sich über persönliche Sicherheitstipps aus, die Ihnen helfen, Ängste und Unsicherheiten abzubauen.

3 In Foren unterhalten sich Internetnutzer/-innen in der Regel öffentlich für alle sichtbar, Antworten können zeitversetzt, also Stunden oder Tage später, erscheinen. In Chats verläuft das Gespräch dagegen privat in kleinen Räumen, Antworten werden in Echtzeit, kurz nach dem Absenden der Nachricht, erwartet. Erläutern Sie: Zu welchen Anlässen oder über welche Themen sollte man einen Beitrag in einem öffentlichen Forum veröffentlichen? Welche Informationen gehören dagegen eher in einen privaten Chat? Welche Daten gehören Ihrer Meinung nach überhaupt nicht ins Internet?

Mit der Vielfalt im Netz umgehen

In verschiedenen Bild- und Video-Kanälen, in Blogs oder sozialen Netzwerken kann heutzutage jeder seine Meinung veröffentlichen und auch Nachrichten eigenständig bekannt machen. Es ist eine Herausforderung für jeden und jede, Informationen auch bewerten zu können. Denn: Wo viele Menschen mit unterschiedlichen Motivationen Texte und Materialien online stellen, entstehen auch – gewollt oder ungewollt – Falschmeldungen. Diese werden auch als Fake News bezeichnet. Einige wurden möglicherweise versehentlich veröffentlicht, andere sollen bewusst manipulieren. Werden diese Nachrichten dann unreflektiert geteilt und kommentiert, erreichen sie schnell eine große Öffentlichkeit.

Gibt es eine Nachricht, die oft geteilt wird, erweckt das den Eindruck, dass viele Menschen sie für seriös halten.
Aus diesem Grund sollten Sie regelmäßig hinterfragen,
welche Nachrichten wahr und welche falsch sind.

ES IST HILFREICH, SICH FOLGENDE FRAGEN ZU STELLEN:

- Was ist die Quelle? Ist sie seriös?
- Werden Behauptungen belegt?
- Sind die Informationen und Argumente plausibel?
- Gehört das Bild zum Text?
- Ist die Nachricht aktuell?

Gerade Hasspropaganda und Hetze werden darüber hinaus noch verstärkt durch den Effekt der Filterblase: Weil einige Webseiten oder soziale Netzwerke versuchen, algorithmisch vorauszusagen, welche Informationen der Benutzer oder die Benutzerin auffinden möchte, werden vermehrt Inhalte gezeigt, die der eigenen Meinung entsprechen.

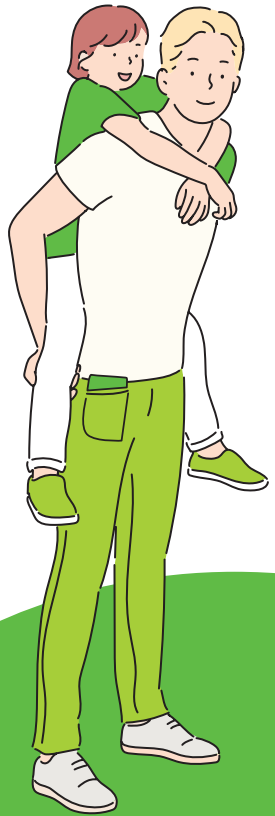
Linktipps

Was sind Fake News?
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Broschüre mit Informationen rund um das Thema Fake News und Aufgabenstellungen für Schulklassen
Zielgruppe: Vor allem Lehrkräfte

Was sind Social Bots?
Herausgeber: Bundeszentrale für politische Bildung
Beschreibung: Text, der die Technologie, verschiedene Arten und den Einfluss von Social Bots erläutert

Fake News – Es ist kompliziert
Herausgeber: First Draft
Beschreibung: Webseite eines gemeinnützigen Projekts, das sich mit den verschiedenen Arten, Gründen und Wegen der Verbreitung von Fake News beschäftigt

Webcode: 2 1 1 3



Lernziel **Vergleichen und prüfen Sie Nachrichtenquellen hinsichtlich ihrer Inhalte.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Welche Nachrichtenquellen nutzen Sie persönlich? Listen Sie diese auf. Sortieren Sie nach Art der Quelle, zum Beispiel in gedruckter Form und Online. Wie sind die Nachrichten aufgearbeitet? Gibt es ein Team von Journalist/-innen oder handelt es sich um einen privaten Blog? Sie finden Informationen dazu im Impressum.

2 Prüfen Sie, ob es zu den Ihnen bekannten analogen Nachrichtenquellen (zum Beispiel Zeitungen, Zeitschriften) auch eine Onlineversion, zum Beispiel eine Webseite, gibt. Gibt es Unterschiede in der Aufbereitung der Informationen?
Lebenswelt 1, Station 3 > Im Netz surfen

3 Entscheiden Sie sich für ein aktuelles Thema. Recherchieren Sie drei Artikel in unterschiedlichen Medien dazu und vergleichen Sie diese in Bezug auf die genannten Informationen und Quellen, auf Aktualität und Plausibilität. Schätzen Sie dann die Seriosität ein.

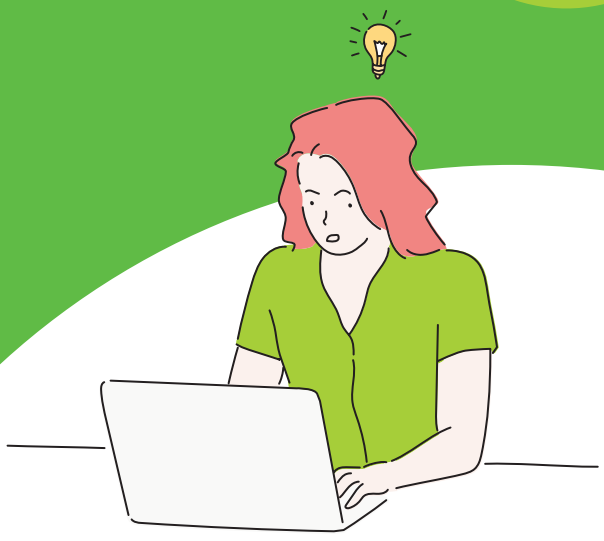
REFLEXION

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1. Sammeln Sie in der Gruppe verschiedene seriöse Nachrichtenquellen (zum Beispiel Zeitungen oder Nachrichtensendungen im TV).

2. Begründen Sie anhand der oben im Text aufgezählten Fragen vor den Teilnehmer/-innen, warum die jeweilige Nachrichtenquelle seriös oder eben nicht seriös erscheint.

REFLEXION



STATION 2

Wie das Internet funktioniert

Das Internet für zu Hause

Viele Menschen haben heute ganz verschiedene Geräte, um das Internet zu nutzen. Die mobile Nutzung über Tablets und Smartphones wird dabei zunehmend selbstverständlich, der heimische PC auf dem Schreibtisch spielt aber immer noch eine große Rolle. Um mit Ihren Geräten von zu Hause aus online zu gehen, benötigen Sie einen Internetdienstanbieter, den man Provider nennt. Dieser schließt beispielsweise Ihren PC ans Internet an und ist in diesem Fall Ihr Telefon- oder Kabelanschlussanbieter. Der zur Verfügung gestellte Anschluss wird mit einem Router verbunden. Der Router stellt die Schnittstelle zwischen Internet und PC dar und übermittelt die Daten.

Die Verbindung zwischen dem Router und dem PC kann mithilfe eines LAN-Kabels, eines speziellen Kabels für das Übertragen von Daten in Netzwerken, oder kabellos über WLAN (Wireless Local Area Network), also über Funksignale, hergestellt werden. So fungiert der Router als Herzstück der digitalen Vernetzung zu Hause und verbindet in den meisten Fällen nicht nur den PC, sondern auch weitere internetfähige Geräte sowohl untereinander als auch mit dem Internet.

Sie können die Einstellungen Ihres Routers ändern, zum Beispiel das Passwort des WLANs. Die Anleitung dazu finden Sie in der Gebrauchsanweisung Ihres Geräts.

Ein so zentrales Gerät wie Ihr Router braucht natürlich auch einen umfassenden Schutz **Kompetenzteil 1, Station 1 > Sichere Interneteinstellungen für zu Hause**.

Darüber hinaus zählen die Firewall und ein Virenschutzprogramm zum Basisschutz für Ihre Geräte zu Hause. Eine Firewall schützt den PC oder das Netzwerk vor Zugriffen von außen. Dabei überwacht sie den laufenden Datenverkehr und beschränkt beziehungsweise unterbindet unerlaubte Zugriffe. So können Sie zum Beispiel in einer Firewall einstellen, dass ein bestimmtes Programm auf Ihrem PC nicht mit dem Internet verbunden werden darf. Ein Virenschutzprogramm durchsucht Ihren PC nach Schadprogrammen. Diese können zum Beispiel vertrauliche Daten an Unbefugte übermitteln. Der Einsatz beider Schutzmaßnahmen ist absolut empfehlenswert. Achten Sie dabei immer darauf, das Virenschutzprogramm und die Firewall aktuell zu halten **Kompetenzteil 2, Station 3 > Schutzprogramme nutzen und Kompetenzteil 2, Station 1 > Software aktuell halten**).

Lernziel **Richten Sie sichere Grundeinstellungen für das Internet zu Hause ein.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Recherchieren Sie im Internet nach Virenschutzprogrammen und Testergebnissen zu diesen. Nutzen Sie dafür Suchmaschinen **Lebenswelt 1, Station 3 > Im Netz surfen**. Welches Virenschutzprogramm bietet nach Ihrer Recherche den besten Schutz?

2 Schauen Sie im Handbuch bzw. in der Gebrauchsanweisung Ihres Routers nach, wie das WLAN-Passwort geändert wird und wie ein WLAN-Zugang für Gäste eingerichtet werden kann. Fragen Sie die Schulleitung bzw. ein Familienmitglied oder einen Bekannten, ob man Ihnen zeigen kann, wie das funktioniert. Alternativ können Sie auch professionelle Dienstleister beauftragen, die Sie bei der Einrichtung Ihres Routers zu unterstützen. Ggf. bietet auch Ihr Internetanbieter einen solchen Service an.
Kompetenzteil 1, Station 1 > Sichere Interneteinstellungen für zu Hause.

3 Tipp: Lassen Sie sich von einem Familienmitglied oder Bekannten erläutern, welche weiteren Änderungen an einem Router vorgenommen werden können, z. B. wie der WLAN-Kanal geändert wird.

PRAXIS

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Finden Sie sich in einer Kleingruppe zusammen. Stellen Sie sich vor, Sie lebten in einer Wohngemeinschaft. Sie möchten, dass Ihr WG-PC durch ein Antivirenprogramm geschützt ist.

Welche Möglichkeiten haben Sie?

Was sind für Sie Entscheidungskriterien?

Welche Vor- und Nachteile könnten bestimmte Programme haben?

2 Vergleichen Sie die Ergebnisse der Kleingruppen in der großen Runde.

PRAXIS

Das Internet für unterwegs

Auch unterwegs können Sie mit Ihren Geräten online gehen. Viele der heute üblichen Geräte wie Smartphones und Tablets sind nahezu ununterbrochen im Internet. Haben Sie einen entsprechenden Vertrag mit Ihrem Internetanbieter, können Sie per Mobilfunk surfen. Dazu müssen Sie in den Einstellungen Ihres Smartphones oder Tablets den Menüpunkt „Mobile Daten“ aktivieren.

Wenn Sie das Internet unterwegs nutzen möchten, brauchen Sie keinen Router, sondern die Möglichkeit des Empfangs eines Funknetzes der Mobiltelefonie. Der Empfang von Daten kann vom Provider pro Monat hinsichtlich des Umfangs (gemessen in Gigabyte oder Megabyte) begrenzt werden. Informieren Sie sich diesbezüglich am besten bei Ihrem Mobilfunkanbieter.

Die Möglichkeit, die mobile Datenverbindung zu nutzen, haben Sie bei PCs und Notebooks oft nicht direkt. Viele Mobilfunkanbieter bieten jedoch einen Surfstick an. Dieser erinnert optisch an einen herkömmlichen USB-Stick und stellt eine mobile Datenverbindung her.

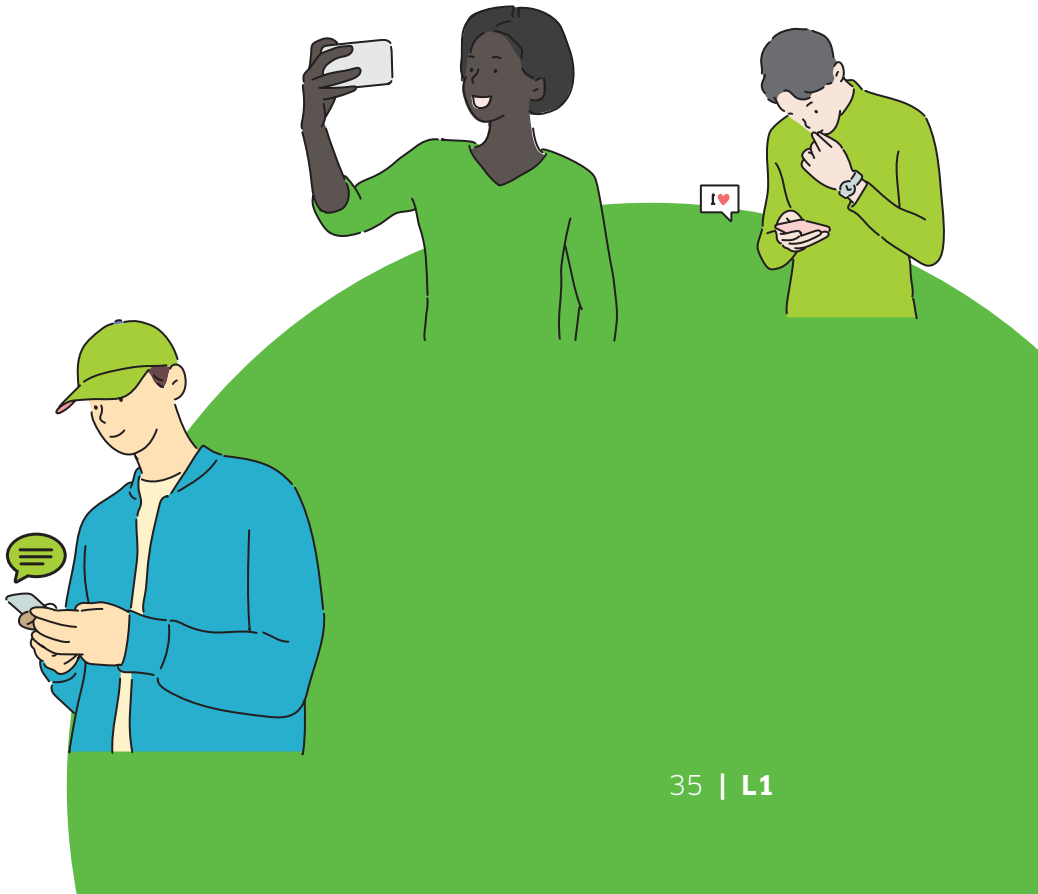
Stehen Ihnen die mobilen Datenverbindungen nicht zur Verfügung, können Sie auf öffentliche WLAN-Netze zugreifen. Dieses Angebot ist häufig in Cafés, Hotels, Einkaufszentren, aber auch im Nah- und Fernverkehr verfügbar. Die Verbindung können Sie ebenfalls über die Einstellungen Ihres Mobilgerätes herstellen. In den meisten Fällen brauchen Sie dafür ein Passwort. Da die Datenübertragung jedoch oft unverschlüsselt geschieht, besteht ein erhöhtes Risiko, dass Unbefugte auf Ihre Daten zugreifen können. Rufen Sie deswegen keine vertraulichen Daten über ein fremdes WLAN-Netz ab, ohne zusätzliche Sicherheitsmaßnahmen zu ergreifen.

Außerdem sollten Sie bedenken, dass eine Drahtlosschnittstelle wie das WLAN ein Einfallstor für Cyberkriminelle sein kann. Darum sollten Sie diese Schnittstellen am mobilen Gerät deaktivieren, wenn sie nicht benötigt werden. So können sich Laptop, Tablet, Smartphone und Co. nicht unbemerkt in ungeschützte Netzwerke einwählen ☞ **Kompetenzteil 1, Station 2 > Sichere Interneteinstellungen für unterwegs**.

Linktipp

Mein Tablet und ich
Herausgeber: Stiftung digitale Chancen
Beschreibung: Broschüre mit anschaulicher Einführung in den Umgang mit dem Tablet

Webcode: 2 1 1 4



Lernziel **Üben und reflektieren Sie den Umgang mit öffentlichem WLAN.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 In welchen Situationen nutzen Sie unterwegs das Internet? Wofür nutzen Sie Ihr mobiles Datenvolumen? Wenn Sie das Internet bisher nicht mobil nutzen: In welchen Situationen haben Sie unterwegs die Möglichkeit vermisst, das Internet zu nutzen?

2 Prüfen Sie gemeinsam mit einem Familienmitglied oder Bekannten an verschiedenen Standorten, wie viele und welche WLAN-Netze dort jeweils existieren. Gehen Sie dazu in die entsprechenden Einstellungen Ihres Geräts. Sind diese meist passwortgeschützt oder nicht? Beachten Sie: Wählen Sie sich nicht in ein ungeschütztes WLAN-Netz ein.

3 Was wissen Sie über die Schutzmaßnahmen der Betreiber, zum Beispiel von Hotels, Cafés oder Einkaufszentren? Recherchieren Sie im Internet dazu oder führen Sie direkt Interviews.

4 Recherchieren Sie den Artikel „22.000 Menschen willigen ein, Klos zu putzen“ („Süddeutsche Zeitung“, 17. Juli 2017). Dieser schildert, wie Festivalbesucher/-innen den fragwürdigen Bedingungen eines WLAN-Betreibers zustimmten. Wie ist Ihr eigener Umgang mit AGB und Datenschutzerklärungen?

Tipp: Einige Provider bieten an verschiedenen Standorten kostenpflichtige WLAN-Zugänge (Hotspots) an. Prüfen Sie, ob es einen solchen Zugang bei Ihnen in der Nähe gibt. Was können Sie über seine Sicherheit aussagen? Beachten Sie: Die Nutzung dieser Hotspots kann Kosten verursachen.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Stellen Sie die oben genannten Fragen in Ihrer Schulungsgruppe. Welche unterschiedlichen Einsatzzwecke für die Nutzung des Internets unterwegs lassen sich festhalten? Erstellen Sie gemeinsam eine Liste.

2 Machen Sie in Kleingruppen eine Exkursion in Ihrer Umgebung. Prüfen Sie mit denen Ihnen zur Verfügung stehenden Geräten (Smartphones oder Laptops) gemeinsam an verschiedenen Standorten (zum Beispiel Einkaufsstraßen oder -zentren, Restaurants, Hotels) die Möglichkeit, WLAN-Netze zu nutzen. Wie viele WLAN-Netze kommen dabei zusammen? Wie viele davon sind passwortgeschützt, wie viele nicht?

PRAXIS + REFLEXION

STATION 3

Im Netz surfen

Ins Internet mit dem Browser

Wenn Sie mit Ihrem PC, Tablet oder Smartphone im Internet surfen möchten, benötigen Sie dafür ein spezielles Programm: den Browser. Das englische Wort „to browse“ bedeutet so viel wie „blättern“ oder „schmökern“. Gängige Browser sind zum Beispiel Chrome, Safari oder Mozilla Firefox. In der Regel ist auf einem internetfähigen Gerät bereits ein Browser beim Kauf installiert. Andere können kostenfrei aus dem Internet heruntergeladen werden. Mithilfe des Browsers haben Sie Zugang zu unzähligen Webseiten. Sie benötigen lediglich die Adresse einer Internetseite, die Sie in das Adressfeld oben im Browser eingeben, und die Seite wird aufgerufen. Oder Sie finden die Seite über eine Suchmaschine.

Surfen Sie im Internet, speichert der Browser ab, welche Webseiten Sie besucht haben. Die Adressen der Seiten werden im Browserverlauf dokumentiert. Die Inhalte der Webseiten werden darüber hinaus im Cache, in einem Ordner auf Ihrem PC, gespeichert. Der Cache ist vergleichbar mit einem Zwischenlager: Er speichert beispielsweise Bilder einer aufgerufenen Webseite, wodurch sich deren Ladezeiten bei einem erneuten Aufruf verkürzen. Dies kann dazu führen, dass Sie nicht immer die aktuelle Version der Webseite sehen. Um diese anzuzeigen, nutzen Sie die Funktion „Aktualisieren“ Ihres Browsers. Sie können zudem sowohl den Browserverlauf als auch den Cache löschen. Das ist bei den meisten Browsern über die Einstellungen möglich.

Darüber hinaus werden während des Besuches von Internetseiten oft Cookies auf Ihrem PC gespeichert. Cookies sind kleine Textdateien. Sie

werden unter anderem zu Werbe- und Marketingzwecken eingesetzt und enthalten eine wiedererkennbare ID-Nummer, mit deren Hilfe Informationen gesammelt werden, welche Seite wann und wie oft aufgerufen wurde. Dadurch kann Ihnen entsprechende Werbung angezeigt werden. Wenn Sie das nicht wünschen, stellen Sie in Ihrem Browser ein, dass die Cookies beim Schließen regelmäßig gelöscht werden.

Außerdem bietet fast jeder Browser Möglichkeiten zur Personalisierung. Sie können somit das Programm nach Ihren persönlichen Vorstellungen anpassen, indem Sie beispielsweise eine individuelle Startseite einrichten. Sie können Lesezeichen anlegen, um Ihre Lieblingsseiten mit einem Klick aufrufen zu können. Mittels Software-Erweiterungen (Plug-ins und Add-ons) können Zusatzfunktionen dem Browser hinzugefügt werden, etwa das Ausblenden von Werbung mithilfe von Adblockern.

Linktipps

Browser & Co: Sicher unterwegs im Netz
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Informationen von Deutschland sicher im Netz e.V. zum sicheren Surfen

Surfen im Internet – Zu Hause und mobil
Herausgeber: Deutschland sicher im Netz e.V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e.V.
Beschreibung: Handreichung des Digital-Kompasses
Zielgruppe: Vor allem Senior/-innen

BSI-Sicherheitsquiz
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Testen Sie Ihr Wissen mit dem Sicherheitsquiz des BSI

Webcode: 2 1 1 5

Lernziel **Nutzen Sie die Sicherheitseinstellungen Ihres Browsers.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Besuchen Sie drei verschiedene Webseiten Ihrer Wahl (zum Beispiel Sportvereine, Behörden, Blogs oder Nachrichtenseiten). Beschreiben und vergleichen Sie die eingeblendeten Fenster, in denen Sie gegebenenfalls der Speicherung von verschiedenen Arten von Cookies zustimmen sollen. Was ist hervorgehoben?
Wo finden Sie Einstelloptionen?

2 Prüfen Sie in den Einstellungen Ihres Browsers, wann Sie Cookies löschen und den Cache leeren können und wählen Sie eine Option, die Ihrem Nutzungsverhalten und -empfinden entspricht.

3 Richten Sie eine Startseite für Ihren PC ein. Nutzen Sie dafür das Menü oder die Einstellungen Ihres Browsers.

Tipp: Besuchen Sie die von Ihnen aufgerufenen Seiten mit dem PC und die gleichen Seiten mit dem Smartphone. Welche Unterschiede stellen Sie fest?

VERTIEFUNG + PRAXIS

VERTIEFUNG + PRAXIS

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Teilen Sie sich in Kleingruppen auf, wählen Sie pro Gruppe einen Browser aus. Prüfen Sie jeweils in den Einstellungen des Browsers, wie und wo Sie den Browserverlauf, den Cache oder Cookies löschen können. Erklären Sie die Vorgehensweise den weiteren Gruppen.

2 Rufen Sie in einer Kleingruppe eine Nachrichtenseite mit verschieden großen Smartphones, mit dem Tablet und mit dem PC auf. Vergleichen Sie die unterschiedlichen Darstellungen der Seite.

Recherche mit Suchmaschinen

Wenn Sie im Internet surfen, haben Sie grundsätzlich zwei Möglichkeiten, um auf Webseiten mit gewünschten Informationen zu gelangen: den gezielten Besuch einer Seite oder eine offene Recherche. Möchten Sie beispielsweise eine Zugverbindung zum Wohnort Ihrer Familie abfragen, kennen Sie vielleicht bereits eine Internetadresse mit einer aktuellen Fahrplanauskunft. Diese Seite können Sie dann gezielt aufrufen, um die gewünschten Informationen zu erhalten. Falls Sie sich jedoch nach alternativen Reisemöglichkeiten umschauen wollen, werden Sie höchstwahrscheinlich recherchieren müssen. Im Internet existieren mehrere Milliarden Webseiten – stets die passende Seite zu kennen, die gerade benötigt wird, ist also so gut wie unmöglich. Suchmaschinen können hier Abhilfe schaffen.

Suchmaschinen sind Dienste im Internet, die einen Großteil der online verfügbaren Inhalte nach einem Begriff oder einer Begriffskombination durchsuchen. Auch Bilder, Videos oder Nachrichten sowie Shopping-Angebote können über Suchmaschinen gefunden werden. Eine bekannte Suchmaschine ist Google. Das Wort „googeln“ hat es bis in den Duden geschafft und sich als Begriff für die Internetrecherche allgemein etabliert. Zudem gibt es weitere Suchmaschinen wie Yahoo oder Bing, DuckDuckGo, Ecosia oder Startpage. Manche Suchmaschinen zeichnen sich dadurch aus, dass sie datenschutzfreundlich sind oder keine personalisierte Werbung einsetzen. Außerdem existieren spezielle Suchmaschinen für Kinder wie fragFINN oder Blinde Kuh, die einen geschützten, altersgerechten Raum zum Surfen bieten.

Viele Suchmaschinen besitzen die Möglichkeit, Rechercheergebnisse zu filtern, zum Beispiel um nur Webseiten in deutscher Sprache anzuzeigen oder nur Veröffentlichungen für einen bestimmten Zeitraum. Diese Option finden Sie im Menü auf der Webseite der Suchmaschine unter „Einstellungen“. Hier lassen sich je nach Anbieter auch weitere Anpassungen vornehmen.

Über die Einstellungen Ihres jeweiligen Browsers können Sie Ihre bevorzugte Suchmaschine als Startseite festlegen. Sie erscheint dann immer, sobald Sie den Browser öffnen. Das ist praktisch, wenn Sie viel recherchieren.

Suchmaschinen sind kostenfrei und finanzieren sich in der Regel über eingeblendete Werbung. Angezeigt werden daher nicht nur die gewünschten Suchergebnisse, sondern auch Reklame. Diese ist als solche gekennzeichnet. Außerdem gibt es Unternehmen, die spezialisierte Anbieter bezahlen, um möglichst weit oben in der Ergebnisliste zu bestimmten Suchbegriffen zu erscheinen. Die Rangfolge kann somit beeinflusst werden.

Linktipps

Checkliste: Informationen gezielt und sicher suchen und finden
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: DigiBitS-Checkliste zum Suchen und Finden von Informationen im Internet
Zielgruppe: Vor allem Lehrkräfte

Informationskompetenz: Richtig recherchieren und das Gefundene bewerten, einordnen und nutzen
Herausgeber: Landesmedienzentrum Baden-Württemberg
Beschreibung: Anregungen für die Praxis

Die Politik des Suchens
Herausgeber: Bundeszentrale für politische Bildung
Beschreibung: Dossier zu Suchmaschinen

Suchen und Finden im Internet
Herausgeber: Internet-ABC e. V. bei der Landesanstalt für Medien NRW
Beschreibung: Online-Lernmodul für Kinder
Zielgruppe: vor allem Lehrkräfte, Kinder

Onlinerecherche und Suchmaschinen
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Unterrichtsmaterialien für Jugendliche im Materialpool von DigiBitS – Digitale Bildung trifft Schule
Zielgruppe: Vor allem Lehrkräfte

Webcode: 2116

Lernziel Recherchieren Sie mit Suchmaschinen.

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Recherchieren Sie die Öffnungszeiten eines Stadtbads in Ihrer Nähe. Geben Sie dazu den Begriff „Öffnungszeiten“ sowie den Namen des Stadtbads und den Ort, unter Umständen auch den Stadtteil, ein. Prüfen Sie, welche unterschiedlichen Ergebnisse Sie erhalten, wenn Sie ein oder zwei der Begriffe nicht eingeben.

2 Suchen Sie nach einer Person im Internet, die Sie persönlich kennen. Was wird im Internet über die Person offenbart? Vergleichen Sie die digitalen Informationen über die Person mit dem, was Sie über die Person wissen.

Tipp: Wollen Sie sich vertieft damit beschäftigen, mit welchen Tricks Webseiten in der Ergebnisliste weiter oben erscheinen? Dann recherchieren Sie nach dem Begriff „Suchmaschinenoptimierung“ beziehungsweise „Search Engine Optimizing“.

REFLEXION + PRAXIS

1 Recherchieren Sie in Kleingruppen mit jeweils einer anderen Suchmaschine Antworten auf die folgenden Fragen:

a) Wann findet der nächste Eurovision Song Contest statt?

b) Wann beginnen und enden die Sommerferien dieses Jahr in Frankreich?

c) Wer ist der Erfinder des Computers?

d) Was bedeutet „Web 3.0“?

e) Welche Prämie erhielt die deutsche Fußball-Nationalmannschaft der Frauen für den Europameistertitel 1989 vom Deutschen Fußball-Bund (DFB)?

f) Warum ist Pluto kein Planet mehr?

2 Vergleichen Sie gemeinsam Ihre Suchbegriffe, Ergebnislisten und Antworten. Welche Unterschiede, vor allem in den verschiedenen Ergebnislisten, stellen Sie fest? Analysieren Sie, mit welchen Suchbegriffen man besonders schnell ist: Sollte man besser die ganze Frage eingeben oder einzelne Wörter?

Tipp: In ein oder zwei Gruppen können statt unterschiedlicher Suchmaschinen auch verschiedene Portale mit Suchfunktionen genutzt werden. So eignen sich beispielsweise für die Suche nach Orten auch Kartendienste. Für die Suche nach Begriffen können Online-Enzyklopädien genutzt werden. Auch hier ist ein Vergleich der Antworten auf die gestellten Fragen interessant.

STATION 4

Programme und Apps kennenlernen

Neben dem Aufrufen von Webseiten können Sie auf Ihren internetfähigen Geräten auch Programme und Apps nutzen. Damit Computer, aber auch Smartphones und andere mobile Endgeräte funktionieren, muss ein Betriebssystem installiert sein. Programme nutzen das Betriebssystem als Grundlage, auf deren Basis dann alle anderen Anwendungen und Apps funktionieren. Bekannte Betriebssysteme für Computer sind beispielsweise Windows, Mac OS oder Linux. Bei Smartphones sind es zum Beispiel Android oder iOS.

Darüber hinaus gibt es vielfältige Programme, die das Arbeiten am PC vereinfachen. Einige davon sind kostenlos, andere müssen Sie kaufen. Klassischerweise haben die meisten Geräte eine Software zur Text- oder Bildverarbeitung. Es gibt aber auch spezielle Anwendungen, wie zum Beispiel Programme für die Steuererklärung.

Programme werden von Softwareentwicklern in einer bestimmen Programmiersprache geschrieben. Einige Programmierer veröffentlichen ihren Quellcode. Entsprechende Programme gelten dann als „open source“ oder „quelloffen“. Diese Programme werden häufig als vertrauenswürdig eingestuft, weil offengelegt wurde, wie das Programm funktioniert, welche Hintergrundaktivitäten ablaufen und welche persönlichen Daten verwendet werden, während das Programm genutzt wird. Jedoch gilt auch hier: Es gibt keine absolute Sicherheit. Deswegen ist es wichtig, die Seriosität der Quelle zu prüfen. Auf Smartphone und Tablet heißen die Programme Apps, die Kurzform des englischen Begriffs „Application“,

also eine Anwendungssoftware. Diese kleinen, nützlichen Programme können Sie sich von App-Stores oder Play-Stores auf das Smartphone herunterladen. Die Palette an Apps reicht sehr weit: von Nachrichten- oder Wissens-Apps über Messenger (Apps zum Kommunizieren) bis hin zu Onlinespielen. Zudem sind oftmals einige Apps auf dem Gerät voreingestellt – wie zum Beispiel ein Kalender, eine Uhr oder ein Taschenrechner.

Alle Programme, Apps sowie das Betriebssystem sollten immer aktuell gehalten werden, damit Sie keine Sicherheitslücken bieten. Mehr dazu im

Kompetenzteil 2, Station 1 > Software aktuell halten.

Wie Sie Apps bei Ihrer Reiseplanung nutzen können, erfahren Sie in der

Lebenswelt 4 > Online Reisen planen und vernetzt mobil sein.

Linktipps

Sicherer Umgang mit mobilen Endgeräten und Apps
Herausgeber: Deutschland sicher im Netz e. V
Beschreibung: Checkliste von DigiBitS – Digitale Bildung trifft Schule
Zielgruppe: Lehrkräfte

Empfehlenswerte Kinder-Apps
Herausgeber: Jugendschutz.net
Beschreibung: Eine Übersicht über pädagogisch geprüfte Apps bietet das Angebot „Klick-Tipps“ von Jugendschutz.net

Webcode: 2117

Lernziel **Lernen Sie Programme und Apps kennen.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Öffnen Sie den App- oder Play-Store Ihres Smartphones. Suchen Sie drei verschiedene Apps zum Lernen von Fremdsprachen. Nutzen Sie dafür entweder Kategorien oder geben Sie einen Suchbegriff in das Suchfeld ein. Gehen Sie die Funktionen durch und recherchieren Sie, ob es Erfahrungsberichte zu dieser App gibt (zum Beispiel bei Bewertungen oder in Rezensionen). Begründen Sie dann, für welche App Sie sich entscheiden würden.

2 Wenn Sie einen PC mit Windows-Betriebssystem nutzen, klicken Sie auf das Fenster-Symbol am linken Bildschirmrand. Dort finden Sie die Programme, alphabetisch sortiert. In Ihrem Mac finden Sie die Programme im Finder. Welche Programme sind vorinstalliert, welche nutzen Sie davon?

PRAXIS

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Ändern Sie die Übungen aus der Einzelarbeit ab, indem Sie in Kleingruppen nach verschiedenen Apps in App- oder Play-Stores suchen, zum Beispiel nach Fremdsprachen, Lexika, Kamera- und Foto-Apps oder Apps für Reisen.

2 Finden Sie in der Gruppe heraus: Welche Programme sind auf dem PC installiert? Wofür können Sie sie nutzen? Überlegen Sie gemeinsam, welche Programme häufig von Ihnen genutzt werden und welche nie.

PRAXIS

STATION 5

Onlinedienste sicher nutzen

Vieles, was wir im Internet machen, ist darauf ausgelegt, Dinge mit anderen zu teilen oder gemeinsam an Inhalten zu arbeiten. Viele Onlinedienste sind Cloud-Dienste, das heißt, dass Sie über das Internet jederzeit und von jedem Ort auf diese zugreifen können. Ein beliebter Cloud-Dienst ist zum Beispiel ein Onlinespeicher, bei dem Sie Daten wie Ihre Texte, Fotos oder sonstigen Dateien hinterlegen und diese von verschiedenen Endgeräten aufrufen oder sie mit anderen teilen können. Einige Anbieter ermöglichen es Ihnen auch, Ihre Daten mit online ausführbaren Anwendungen zu bearbeiten, etwa mit einem Programm zur Textbearbeitung. Die Anwendung muss dafür nicht auf Ihrem Rechner installiert sein. Stattdessen können die gespeicherten Dateien über einen Browser direkt in der Cloud bearbeitet werden. Jedoch bedeutet das auch, dass ein Dritter – in diesem Fall der Cloud-Diensteanbieter – unter Umständen Zugang zu nichtveröffentlichten Dokumenten wie Entwürfen erhalten kann.

Als weiteres Beispiel kann auch Web-Mail als Cloud-Dienst realisiert werden. Anbieter stellen Ihnen online ein Postfach für Ihre E-Mails zur Verfügung. Die Nachrichten Ihres Onlinepostfachs befinden sich dabei auf Servern des Anbieters. Sie können von jedem Ort aus und mit jedem internetfähigen Gerät auf Ihre E-Mails zugreifen.

Zunehmend mehr Menschen nutzen auch Geräte wie Smartwatches oder Fitnesstracker (internetfähige Geräte für das Handgelenk), die ihre Aufzeichnungen je nach Einstellung mit cloudbasierten Onlinediensten synchronisieren. Dabei müssen Sie sich bewusst machen, dass Sie gegebenenfalls Gesundheitsdaten an die Anbieter übermitteln. Diese können die Daten automatisiert nach bestimmten Kriterien auswerten.

Auch Video- oder Musik-Streaming-Plattformen sind Cloud-Dienste. Bedenken Sie, dass der Anbieter eines Streamingdienstes über die Analyse des jeweiligen Nutzerverhaltens die Möglichkeit hat, Auswertungen zu erstellen und so zum Beispiel zielgerichtet Werbung einzublenden oder ihre politischen und religiösen Einstellungen in Erfahrung zu bringen.

Weitere Informationen erhalten Sie im Kompetenzteil unter:
Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen

Lernziel Cloud-Angebote kennenlernen und nutzen.

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Stellen Sie sich vor, Sie haben in Ihrem Urlaub viele Videos aufgenommen. Sie wollen diese nun Freund/-innen oder Familienmitgliedern zukommen lassen. Es sind aber zu viele und zu große Dateien, um sie per E-Mail zu versenden. Welche Möglichkeiten haben Sie? Entscheiden Sie sich für eine Cloud? Wenn ja, wie gehen Sie vor?

2 Fitnesstracker sind kleine Geräte, ähnlich einer Uhr, die Sie um das Handgelenk tragen und die Ihre Bewegungsaktivitäten aufzeigen. Aber was passiert mit den Daten? Werden diese auf der Uhr gespeichert? Recherchieren Sie.

Tipp: Digitalisierte Bücher nennt man übrigens E-Books. Kennen Sie Buchhändler/-innen im Internet, die E-Books anbieten? Welche Vorteile haben E-Books gegenüber Büchern aus Papier? Welche Nachteile? Wo würden Sie Ihre E-Books abspeichern, wenn Sie mit verschiedenen Geräten, zum Beispiel zu Hause mit Ihrem Tablet und unterwegs mit Ihrem Smartphone, das E-Book immer an der Stelle weiterlesen möchten, bei der Sie zuletzt aufgehört haben?

ÜBUNGEN
FÜR SCHULUNGSGRUPPEN

PRAXIS

1 Machen Sie eine Umfrage: Gibt es bereits Teilnehmer/-innen, die Cloud-Dienste nutzen? Wenn ja, wofür und warum? Was ist bei der Nutzung der jeweiligen Cloud-Dienste zu beachten? Erstellen Sie gemeinsam eine Liste.

Datenschutz bei Onlinediensten

Wollen Sie einen Onlinedienst nutzen, müssen Sie wissen, dass in der Regel auch personenbezogene Daten bei der Anmeldung erhoben werden, wie zum Beispiel Ihr Name, Ihre Kontodaten (zum Beispiel, wenn der Dienst kostenpflichtig ist), Ihre Adresse und nahezu immer Ihre E-Mail-Adresse.

Für den EU-Raum gilt: Bei der Nutzung des Onlinedienstes treten Sie in ein Rechtsverhältnis mit dem jeweiligen Anbieter. Daraus ergeben sich für Sie Rechte. So haben Sie beispielsweise das Recht zu erfahren, wie Ihre personenbezogenen Daten beim Anbieter gespeichert, verarbeitet und ob, wann und an wen sie gegebenenfalls weitergeleitet werden. Solche Informationen finden Sie in der Datenschutzerklärung des Onlinedienstes. Darin werden Sie über den Zweck, die Dauer, die Art und Weise und die Weitergabe Ihrer Daten aufgeklärt.

Seit Mai 2018 bildet die EU-Datenschutz-Grundverordnung (DSGVO) zusammen mit weiteren nationalen Vorschriften den gültigen rechtlichen Rahmen für Ihren Datenschutz.

Darüber hinaus wird in der EU zusätzlich zu den Regeln der DSGVO an einer ePrivacy-Verordnung (ePVO) gearbeitet, die unter anderem den Umgang mit der Speicherung von Cookies regeln soll.

DAMIT DER EINSTIEG INS NETZ SICHER GELINGT, LESEN SIE MEHR ZU FOLGENDEN EMPFEHLUNGEN IM KOMPETENZTEIL:

- Schutz persönlicher Informationen und Daten auf den eigenen Geräten, zu Hause und unterwegs

  Kompetenzteil 1 > Sichere Interneteinstellungen

- Verständnis von Datenübermittlung und -speicherung im Netz

  Kompetenzteil 4 > Daten schützen und sichern

- Sichere Grundeinstellungen von Software und Geräten

  Kompetenzteil 2 > Geräte und Software sicher einrichten und pflegen

Lernziel

Lernen Sie die Möglichkeiten der Datenschutzeinstellungen bei Onlinediensten kennen.

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Stellen Sie sich folgende Fragen: Wie gehe ich mit Datenschutzerklärungen um? Lese ich sie? Klicke ich sie nur weg? Warum verhalte ich mich so?

2. Erstellen Sie eine Liste mit Ihren persönlichen Informationen, die Sie nicht im Internet veröffentlichen wollen. Wenn Sie unsicher sind, beantworten Sie sich folgende Frage: Würden Sie wollen, dass diese Information in der Zeitung steht?

3. Nutzen Sie dann eine Suchmaschine und prüfen Sie, welche Informationen frei über Sie frei im Internet verfügbar sind.

REFLEXION + VERTIEFUNG

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Besuchen Sie unterschiedliche Webseiten, finden Sie auf diesen die Datenschutzerklärungen, lesen oder überfliegen Sie diese und fassen Sie sie kurz zusammen. Vergleichen Sie Ihre Ergebnisse mit denen der weiteren Teilnehmer/-innen.
Welche Gemeinsamkeiten und Unterschiede stellen Sie fest? Kennen Sie Beispiele für aus Ihrer Sicht nutzerfreundliche Datenschutzerklärungen?

REFLEXION + VERTIEFUNG

Linktipps

Vernetzte Öffentlichkeit
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: YouTube-Video zum Thema Big Data

Wie viel weiß das Internet?
Herausgeber: Klicksafe (EU-Initiative) in Kooperation mit dem YouTube-Kanal „Tomatolix“
Beschreibung: Video zum Thema Privatsphäre und Datenspuren im Internet

Datenschutz und Spuren im Netz
Herausgeber: Landesmedienzentrum Baden-Württemberg
Beschreibung: Informationsportal zu verschiedenen Themen rund um den Datenschutz

Sicherheit und Anonymität bei der Internetnutzung
Herausgeber: Karsten Neß (German Privacy Foundation e. V.)
Beschreibung: Das „Privacy-Handbuch“ gibt unter anderem Tipps zum spurenarmen Surfen

Datenschutz geht zur Schule
Herausgeber: Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V. in Zusammenarbeit mit Klicksafe (EU-Initiative)
Beschreibung: Zusammenstellung zahlreicher Angebote zum Thema Datenschutz in der Schule
Zielgruppe: Vor allem Lehrkräfte

Cookies – Was Sie über die kleinen Dateien wissen sollten
Herausgeber: VFR Verlag für Rechtsjournalismus GmbH
Beschreibung: Technisches und Rechtliches rund um Cookies

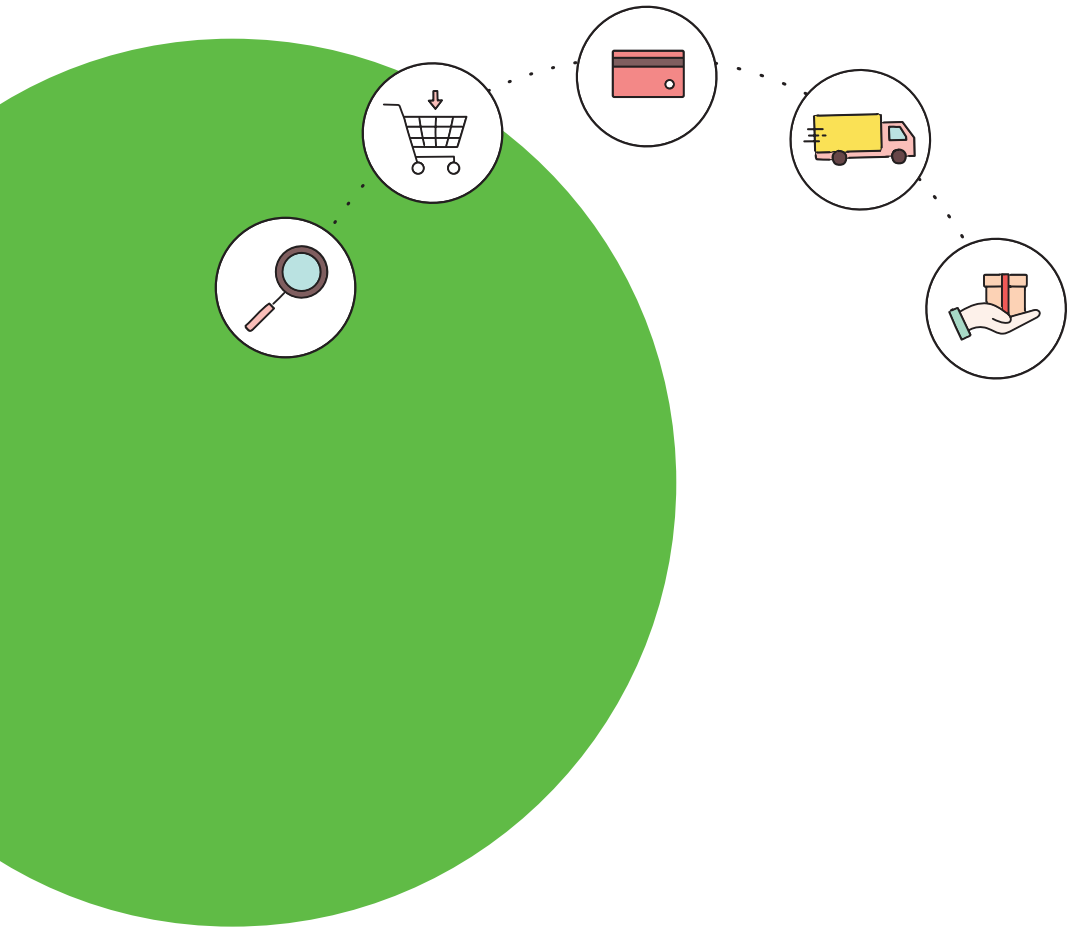
Privatsphäre und Big Data
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Schulungsmaterialien und Arbeitsblätter von Klicksafe

Deine Daten. Deine Rechte.
Herausgeber: Digitale Gesellschaft e. V.
Beschreibung: Informationsportal zum neuen EU-Datenschutzrecht

Datenschutz – das bleibt privat!
Herausgeber: Internet-ABC e. V. bei der Landesanstalt für Medien NRW
Beschreibung: Online-Lernmodul zum Thema Datenschutz
Zielgruppe: Vor allem Lehrkräfte an Grundschulen

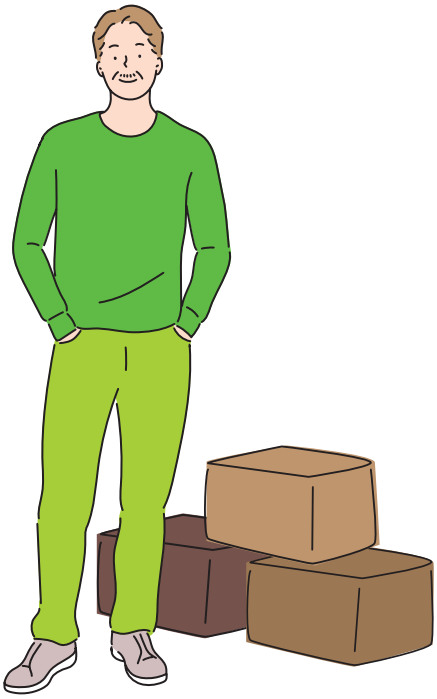
Datensatz – Datenschatz? Warum Datenschutz und Datensicherheit wichtig sind
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Handbuch mit Übungsaufgaben und Arbeitsblättern
Zielgruppe: Vor allem Lehrkräfte

Webcode: 2 1 1 8



LEBENSWELT 2
Online einkaufen und bezahlen

Onlineshopping hat viele Vorteile: Unabhängig von Öffnungszeiten können Sie bequem vom Sofa aus bestellen, statt in langen Warteschlangen zu stehen. Wer bestellt, hinterlegt in den meisten Fällen personenbezogene Daten wie Name, Bankdaten, Adresse oder Telefonnummer. Deswegen ist es wichtig, vertrauenswürdige Anbieter zu finden und zu verstehen, wie Bezahlverfahren funktionieren. Die digitale Lebenswelt „Online einkaufen und bezahlen“ bietet einen Einstieg in das Onlineshopping – von der Angebotssuche über Kauf und Verkauf von Produkten bis hin zum Bezahlen via Onlinebanking.



IN DER LEBENSWELT „ONLINE EINKAUFEN UND BEZAHLEN“ LERNEN SIE,

- was Onlineshopping ist und wie Sie passende Angebote im Internet finden,
- was Profilbildung und personalisierte Werbung ist,
- wie Sie Onlineplattformen sicher nutzen,
- wie Onlinebanking und andere Bezahlverfahren per App funktionieren.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.

STATION 1

Rund um die Uhr digital einkaufen

Was ist Onlineshopping?

Einkaufen, ohne vor die Tür gehen zu müssen? Preise direkt von zu Hause aus vergleichen können? Onlineshopping ist der Oberbegriff für die Einkaufswelt im Netz – oder anders gesagt: Darunter versteht man den Erwerb von Waren und Dienstleistungen über das Internet. Fast jedes Produkt lässt sich dabei auf unterschiedlichen Wegen erwerben. Neben dem direkten Kauf können Sie beispielsweise an Onlineauktionen teilnehmen, Dinge oder Leistungen tauschen oder etwas ausleihen.

Die Kaufrecherche

Wer ein neues Produkt kaufen möchte, kann sich vorab im Internet informieren. Eine solche Kaufrecherche lohnt sich gerade bei teureren Produkten wie einem Kühlschrank oder längerfristigen Dienstleistungen wie einem Stromanbieter.

So gibt es beispielsweise Preisvergleichsportale, die die Preise unterschiedlicher Shopping-Portale auflisten oder in denen sich Privat-

personen austauschen, ihre Erfahrungen teilen und Produkte empfehlen. Diese ermöglichen eine höhere Preistransparenz und einen Überblick über das beste Preis-Leistungs-Verhältnis.

Viele Onlineshops bieten zudem eigene Bewertungsmöglichkeiten zu den jeweiligen Produkten an. Interessierte können so die Meinungen und Hinweise anderer Käuferinnen und Käufer lesen. Beachten Sie aber: Nicht jede Bewertung, die online steht, muss echt sein. Es gibt auch Bewertungen durch Personen, die von Herstellern dafür bezahlt werden, das Produkt möglichst zufriedenstellend zu bewerten. Deswegen ist ein Vergleich zwischen mehreren Portalen und Artikeln ratsam. Außerdem gibt es die Option, journalistische Warentests oder Artikel zu den jeweiligen Produkten zurate zu ziehen.

Linktipps

Online einkaufen und Onlinebanking: Sicher im Internet bestellen und bezahlen
Herausgeber: Deutschland sicher im Netz e. V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Handreichung #5 des Digital-Kompasses
Zielgruppe: Vor allem Senior/-innen

Worauf beim Online-Einkauf zu achten ist
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Sicherheitstipps und Hintergrundinformationen

Ein Produkt suchen und auswählen
Herausgeber: Deutschland sicher im Netz e. V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Übungsblatt des Digital-Kompasses zum Thema „Bestellen und bezahlen – das Internet-Kaufhaus hat immer geöffnet“
Zielgruppe: Vor allem Senior/-innen

Webcode: 2211

Lernziel **Erkunden Sie die Vor- und Nachteile des Online-Einkaufs.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Welche Vorteile hat ein Online-Einkauf für Sie? Welche Nachteile? Erstellen Sie eine Tabelle und prüfen Sie: Überwiegen die Vor- oder die Nachteile?

2. Wägen Sie die Vor- und Nachteile noch einmal in einer weiteren Tabelle ab, nun aber für bestimmte Geschäfte (zum Beispiel Bäckerei, IT-Fachmarkt, Baumarkt, Blumenladen, Möbelfachgeschäft, Textilwarengeschäft oder Supermarkt). Welche Unterschiede stellen Sie zur ersten Tabelle fest? Gibt es Produkte, die Sie zukünftig nur noch selten oder gar nicht online einkaufen werden?

REFLEXION

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Erstellen Sie in Kleingruppen Tabellen, wie in den Aufgaben für die Einzelarbeit beschrieben. Vergleichen Sie Ihre Listen mit weiteren Gruppen. Diskutieren Sie in der großen Gruppe die Gründe für Unterschiede und Gemeinsamkeiten.

2 Suchen Sie auf mehreren Webseiten Produkte (mögliche Beispiele: Staubsauger, Körperwaage, Toaster). Definieren Sie zunächst die von Ihnen gewünschten Eigenarten und Funktionen des Produkts. Ermitteln Sie im Anschluss, welcher Hersteller das beste Preis-Leistungs-Verhältnis in dem von Ihnen festgelegten Funktionsrahmen anbietet. Erfahren Sie bei internetfähigen Geräten etwas über deren Cybersicherheit?

Personalisierte Werbung

Kennen Sie das? Gerade haben Sie nach einem bestimmten Produkt gesucht und im nächsten Moment wird Ihnen auf einer anderen Webseite genau dieser oder ein ähnlicher Artikel in einer Werbeanzeige dargestellt. Wer beispielsweise zuvor nach den Symptomen einer Pollenallergie recherchierte, bekommt nun womöglich auf der nächsten aufgerufenen Webseite Werbung für ein Antiallergikum angezeigt.

Die Platzierung personalisierter Anzeigen ist ein Bestandteil vieler Geschäftsmodelle von Webseiten. Beim Onlineshopping werden in vielen Fällen die persönlichen Suchbegriffe, die Sie auf Shopping-Webseiten eingegeben haben, und Einkäufe, die Sie tätigen, über einen längeren Zeitraum so analysiert, dass detaillierte Profile über Ihre Kaufgewohnheiten und -interessen entstehen. Dieses Verfolgen von Ihren Spuren im Internet nennt man Tracking. Es ermöglicht den Werbetreibenden, gezielt und individualisiert Produkte auf Webseiten bekannt zu machen.

Lernziel **Erkennen und reflektieren Sie personalisierte Werbung.**

PRAXIS + REFLEXION

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Haben Sie bereits bei einem Onlineshop eingekauft, der Ihnen Kaufempfehlungen anzeigt? Wenn ja: Welche Produkte werden Ihnen zum Kauf empfohlen? Erkennen Sie Zusammenhänge zu Ihren Bestellungen?

2. Falls Sie gerade ein Produkt im Internet gekauft haben: Nutzen Sie eine Suchmaschine und suchen Sie irgendeinen Begriff. Surfen Sie auf verschiedenen Webseiten. Welche Werbung wird Ihnen angezeigt? Erkennen Sie Zusammenhänge zu dem von Ihnen bestellten Produkt?

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1. Gibt es Teilnehmer/-innen, die die oben beschriebene Erfahrung bereits gemacht haben? Machen Sie eine Umfrage: Welches Produkt oder welche Produkte haben Sie gekauft und welche Werbeanzeigen wurden Ihnen daraufhin angezeigt?

2. Machen Sie eine Umfrage: Gibt es Teilnehmer/-innen, die sich von personalisierter Werbung inspirieren lassen und tatsächlich weitere Produkte kaufen?

3. Interessante Kaufanregung oder nervige Werbung? Diskutieren Sie in der Gruppe Vor- und Nachtteile personalisierter Werbung.

Onlineplattformen

Über Onlineplattformen und -portale ist beispielsweise das Geschäft mit gebrauchten, aber auch neuen Gegenständen sowie käuflich erwerblichen Dienstleistungen so einfach wie noch nie. Das gilt sowohl für professionelle Händlerinnen und Händler als auch für Privatpersonen.
Wichtig ist es, sich vorab mit den Allgemeinen Geschäftsbedingungen (AGB) der Portale zum Kauf und zur Rückgabe zu befassen. So ist die Abgabe eines Angebots auf einer Auktionsplattform immer ein verbindliches Kaufangebot. Werden Bieterinnen oder Bieter nicht von einer weiteren Person überboten, sind sie verpflichtet, die Waren zum gebotenen Preis abzunehmen und zu bezahlen. Was die Rückgabe betrifft, so sind private Verkäufer und Verkäuferinnen nicht verpflichtet, Waren wieder zurückzunehmen.

BERÜCKSICHTIGEN SIE BEI IHREM KAUF DESHALB DIE FOLGENDEN TIPPS:

- Viele Onlineportale arbeiten mit einem Bewertungssystem. Schauen Sie sich die Meinungen anderer zu dem Verkäufer oder der Verkäuferin vor einem möglichen Kauf an. Bewerten Sie selbst ehrlich. Falls Sie selbst Bewertungen abgeben, seien Sie sich darüber bewusst, dass diese für die Öffentlichkeit einsehbar sind. Wenn Ihnen Bewertungen unseriös vorkommen, können Sie das dem Plattformbetreiber melden.

- Insbesondere bei privaten Käufen und Verkäufen auf Kleinanzeigenportalen ist es sinnvoll, den Schriftverkehr zu dokumentieren, beispielsweise durch Screenshots. Das sind Aufnahmen Ihres Bildschirmfensters oder eines Teils davon.

- Achten Sie bei einer Überweisung darauf, dass der Name des Verkäufers beziehungsweise der Verkäuferin und der des Kontoinhabers beziehungsweise der Kontoinhaberin identisch sind. Vermeiden Sie Auslandsüberweisungen an Unbekannte.

- Bezahlsysteme der Plattformen haben einen Vorteil: Die unkomplizierte Rückerstattung. Mehr dazu erfahren Sie in **Lebenswelt 2, Station 2 > Einfach und sicher im Netz bezahlen.**

- Wenn es sich um einen Kauf unter Privatpersonen handelt, ist ein Kaufvertrag sinnvoll.

Linktipps

So schützen Sie sich vor Betrug auf eBay-Kleinanzeigen
Herausgeber: T-Online
Beschreibung: Artikel mit Tipps zum Schutz vor Betrug auf der beliebten Handelsplattform

eBay: So schützt ihr euer Konto mit einer Zwei-Faktor-Authentifizierung
Herausgeber: Netzwelt
Beschreibung: Bebilderte Anleitung zum Schutz Ihres eBay-Kontos

Webcode: 2 2 1 2

Lernziel Nutzen Sie Online-Handelsplattformen.

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Machen Sie eine Umfrage: Warum nutzen Ihre Freund/-innen, Familienmitglieder oder Bekannten Online-Handelsplattformen und Auktionsportale, um Produkte zu kaufen oder zu verkaufen? Welche Vorteile sehen Sie gegenüber Ladengeschäften oder Flohmärkten?

2. Sie wollen ein Buch kaufen. Wo würden Sie es online bestellen? Begründen Sie Ihre Entscheidung.

3. Suchen Sie auf einer Handelsplattform Ihrer Wahl nach einem beliebigen Produkt. Lesen Sie die Bewertungen und schauen Sie sich die Sprache, die Darstellung des Produktes, Kritikpunkte etc. an. Woran erkennen Sie, ob die Bewertung möglicherweise von einem echten Käufer beziehungsweise einer echten Käuferin stammt oder ob es sich um versteckte Werbung handeln könnte?

PRAXIS + REFLEXION + VERTIEFUNG

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Machen Sie die Umfrage aus der Einzelarbeit in der Gruppe der Teilnehmenden. Diskutieren Sie über die Vor- und Nachteile der jeweiligen Plattformen.

2 Besuchen Sie in kleinen Gruppen verschiedene Onlineplattformen, suchen Sie Ihre Lieblingsprodukte und lesen Sie die Bewertungen. Wie wird das Produkt in den verschiedenen Plattformen bewertet? Sind die Bewertungen ähnlich oder gibt es auf bestimmten Plattformen Bewertungen, die hinsichtlich ihrer Sprache (sehr positive Darstellung, keine Kritikpunkte etc.) eher einer Werbung gleichen?

PRAXIS + REFLEXION + VERTIEFUNG

STATION 2

Einfach und sicher im Netz bezahlen

Sicheres Bezahlen im Internet

Die Mehrheit der Onlineshops und -portale bietet unterschiedliche Bezahlverfahren an, darunter beispielsweise Lastschrift, Kreditkarte und Rechnung, aber auch sofortige Überweisungen. Es ist dabei immer wichtig, die Sicherheit des Bezahlverfahrens in den Blick zu nehmen und einige Sicherheitsvorkehrungen zu treffen **Kompetenzteil 6 > Sichere Transaktionen**.

Generell ist die wohl sicherste Art, Onlinekäufe zu tätigen, der Kauf auf Rechnung. Hierbei haben Sie in der Regel eine Zahlungsfrist von 14 Tagen. Die Rechnung liegt der Ware bei oder wird gesondert versandt. Sind Sie zufrieden, begleichen Sie diese. Entspricht die Ware nicht Ihren Vorstellungen, ist sie fehlerhaft oder kaputt, gelten die Regelungen der Rückgabe. Standardmäßig gilt: Sie haben bei gewerblichen Verkäufern ein 14-tägiges Widerrufsrecht, sofern Sie beim Bestellvorgang nicht anklicken, dass Sie von diesem Recht zurücktreten.

Linktipps

Welche Zahlungsmethoden sind im Internet sicher?
Herausgeber: Verbraucherzentrale
Beschreibung: Artikel über sichere Zahlungsmethoden und Zusatzkosten

Bezahlen im Internet
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Die wichtigsten Sicherheitstipps zum Bezahlen im Internet

Bestellen und bezahlen – Ihr Internet-Kaufhaus hat immer geöffnet
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Anleitung und Präsentationsfolien des Digital-Kompasses

Sicher im Internet bestellen und bezahlen
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Übungsblätter zur Handreichung #5 des Digital-Kompasses

Sicheres Einkaufen und Bezahlen im Netz
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Video und weitere Informationen für Verbraucher/-innen

Webcode: 2 2 1 3

Lernziel **Nutzen Sie die Möglichkeiten des sicheren Einkaufens online.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

Besuchen Sie eine Shopping-Plattform, die bei Ihren Familienmitgliedern, Bekannten oder Freund/-innen sehr beliebt ist. Suchen Sie auf der Webseite nach den Allgemeinen Geschäftsbedingungen (AGB).
Lesen oder überfliegen Sie diese.

1. Welche Richtlinien werden dort angegeben?
2. Welche Möglichkeiten der Bezahlung werden aufgelistet?
3. Gibt es die Möglichkeit, die Ware als Neukunde oder Neukundin auf Rechnung zu zahlen?
4. Welche Richtlinien der Rückgabe werden angeboten? Wird auf das 14-tägige Widerrufsrecht hingewiesen?

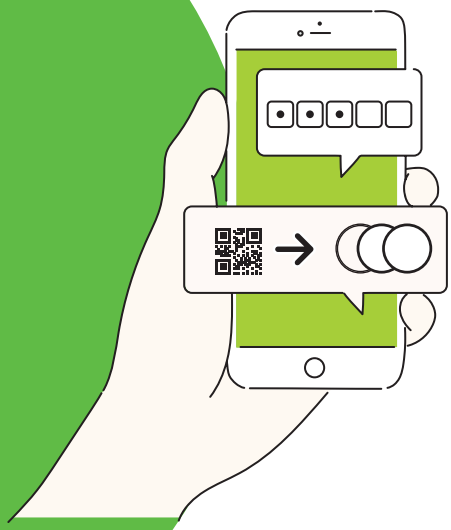
Tipp: Sollten Sie digitalisierte Produkte zum Herunterladen (Download) kaufen (zum Beispiel E-Books, digitale Musik oder Software), wird Ihnen angeboten, auf das 14-tägige Widerrufsrecht zu verzichten. Damit wird Ihnen die Möglichkeit eingeräumt, das Produkt sofort in vollen Umfang zu benutzen. Gleichzeitig kann man nicht mehr vom Vertrag Abstand nehmen. Manchmal befindet sich der Hinweis auch in den AGB.

PRAXIS

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Verteilen Sie die zuvor genannten Fragen auf verschiedene Kleingruppen. Alternativ können Sie auch in den Kleingruppen verschiedene Shopping-Plattformen untersuchen und die verschiedenen AGB vergleichen.

PRAXIS



Onlinebanking

Banken und Sparkassen bieten ihren Kundinnen und Kunden die Möglichkeit des Onlinebankings an, also die Abwicklung von Bankgeschäften über das Internet. So können Sie von Ihren Geräten, zum Beispiel Ihrem PC aus, den Kontostand oder einzelne Umsätze abfragen, Überweisungen durchführen und Daueraufträge anlegen. Wenn Sie diesen Service nutzen wollen, erkundigen Sie sich bei Ihrer Bank, ob Sie sich einmalig anmelden und freischalten lassen müssen oder ob Ihnen das Onlinebanking automatisch zur Verfügung steht. Die wichtigsten Unterlagen erhalten Sie per Post, insbesondere eine Benutzerkennung und eine PIN zum Login in das Onlinebanking.

Seit September 2019 haben alle Banken gemäß der neuen Zahlungsdiensterichtlinie PSD2 (Payment Services Directive2) die „starke Kundenauthentifizierung“ eingeführt. Das Ziel dieser europäischen Richtlinie ist es, Verbraucher und Verbraucherinnen besser zu schützen, wenn sie online bezahlen.

Die TAN-Liste auf Papier wurde im September 2019 abgeschafft und durch verschiedene sichere elektronische Verfahren ersetzt. Zurzeit sind nur noch TAN-Verfahren erlaubt, bei denen für jede Transaktion jeweils eine neue TAN speziell generiert wird, die mit dem Betrag, dem Zahlungsempfänger etc. verbunden ist (sogenanntes dynamisches TAN-Verfahren).

HIER EIN ÜBERBLICK ÜBER DIE TAN-VERFAHREN:

- **TAN-Generatoren:** TAN-Generatoren generieren auf Knopfdruck die Transaktionsnummern und zeigen sie auf einem eingebauten Bildschirm an.

- **Signaturverfahren:** Dabei bestätigen die Anwender/-innen eine Transaktion nicht mit einer TAN, sondern mithilfe eines digitalen Schlüssels, der auf einer Chipkarte gespeichert ist. Die Daten – etwa für eine Überweisung – werden in eine Finanzsoftware eingegeben, die Signaturkarte in das Lesegerät gesteckt und ein festgelegter PIN eingegeben. Die Signaturkarte „unterschreibt" und verschlüsselt die Transaktion.

- **TAN-Verfahren per SMS:** Bei jeder Überweisung wird automatisch eine mobile TAN generiert und per SMS auf das vorher registrierte Mobilgerät gesendet. Dieses mTAN-Verfahren ist zwar praktisch und benutzerfreundlich, birgt aber leider auch einige Risiken. Unter Umständen können Kriminelle die zur Authentisierung verschickten SMS-Nachrichten abfangen oder umleiten.

Achten Sie nicht nur beim Onlinebanking unbedingt auf einen höchstmöglichen Schutz beim Login **Kompetenzteil 3 > Sichere Logins nutzen**.

Linktipps

Onlinebanking – Sicherheitstipps
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Sicherheitsmaßnahmen beim Onlinebanking

Sicherheit im Onlinebanking
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Die wichtigsten Infos zu den verschiedenen TAN-Verfahren

Bankgeschäfte online – bequem von zu Hause aus
Herausgeber: Deutschland sicher im Netz e.V
Beschreibung: Anleitung und Präsentationsfolien des Digital-Kompasses
Zielgruppe: Senior/-innen

Online einkaufen und Onlinebanking: Sicher im Internet bestellen und bezahlen
Herausgeber: Deutschland sicher im Netz e.V
Beschreibung: Handreichung #5 des Digital-Kompasses
Zielgruppe: Senior/-innen

Demo-Konto Onlinebanking
Herausgeber: Deutschland sicher im Netz e.V
Beschreibung: Übungsblatt des Digital-Kompasses zum Thema „Bankgeschäfte online – bequem von zu Hause aus“ zum Erproben der Onlinebanking-Funktionen
Zielgruppe: Senior/-innen

Webcode: 2214

Lernziel **Lernen Sie die Möglichkeiten des Onlinebankings kennen.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Überlegen Sie sich, ob Sie das Onlinebanking Ihrer Bank nutzen wollen. Recherchieren Sie im Internet nach „Demo-Konto Onlinebanking“. Wählen Sie aus der Ergebnisliste einen Treffer aus, der offensichtlich zu einem Test eines Onlinebanking-Zugangs führt. Nutzen Sie den Testzugang und verschaffen Sie sich einen Überblick, welche Möglichkeiten das Onlinebanking bietet. Finden Sie alle Funktionen, die Sie für Ihre Bankgeschäfte benötigen (zum Beispiel Kontostand, Überweisungen, Daueraufträge)?

Tipp: Ein Beispiel finden Sie im Übungsblatt des Digital-Kompasses zum Thema „Bankgeschäfte online – bequem von zu Hause aus“ (siehe Linktipps).

PRAXIS

ÜBUNGEN
FÜR SCHULUNGSGRUPPEN

1 Nutzen Sie in Kleingruppen die verschiedenen Demo-Konten der Sparkassen und Banken. Können Sie Unterschiede bei den angebotenen Funktionen feststellen? Finden Sie alle Funktionen, die Sie für Ihre Bankgeschäfte benötigen (zum Beispiel Kontostand, Überweisungen, Daueraufträge)?

Bezahlsysteme

Nicht alle Onlineshops bieten den Kauf auf Rechnung an, insbesondere wenn es sich um neue Kundinnen und Kunden handelt oder solche ohne Registrierung („Kauf als Gast“). Einige Anbieter erwarten Zahlung auf Vorkasse, was beispielsweise per Online-Überweisung oder mittels Bezahlsystemen möglich ist **Kompetenzteil 6, Station 2 > Online Geld bezahlen**.

Onlinebezahlsysteme erfreuen sich mittlerweile großer Beliebtheit: Nach einer Registrierung beim jeweiligen Bezahldienst können Sie dort Geld oder Ihre Kontodaten hinterlegen. Durch diese Verknüpfung erfolgt die Abbuchung bei einer Bestellung automatisch und schnell.

Einige Bezahlsysteme werben damit, unter gewissen Voraussetzungen das Geld zurückzuerstatten, sollte die bestellte Ware nicht geliefert werden oder tatsächlich nicht dem Angebot des Onlineshops entsprechen. Den besten Schutz bieten Bezahldienste, die die Überweisung des Kaufpreises dann so lange zurückhalten, bis die Ware versendet ist.

Bezahlen und Banking per App

Es gibt einige Apps, bei denen Sie ein Produkt sofort zahlen und erwerben können. So können Sie beispielsweise eine Fahrkarte für den öffentlichen Nahverkehr mit Ihrem Smartphone bezahlen. Das kann praktisch sein, wenn Sie kein Kleingeld dabeihaben.

Beim Onlinebanking nutzen Sie die entsprechende App Ihrer Bank. Achten Sie darauf, eine solche App nur aus einer vertrauenswürdigen Quelle herunterzuladen. Sie finden Sie in den offiziellen App-Stores und Markets. In vielen Fällen werden Sie auch von der Webseite Ihrer Bank direkt dorthin

weitergeleitet. Bei der Einrichtung der Apps ist es wichtig, einen sicheren Zugangsschutz einzustellen, zum Beispiel durch ein sicheres Passwort und eine Zwei-Faktor-Authentisierung. Dabei geben Sie in der Regel nicht nur ein Passwort ein, sondern auch eine weitere Information, zum Beispiel eine Zugangsnummer, die Ihnen beispielsweise per SMS zugesendet wird **Kompetenzteil 3 > Sichere Logins nutzen**. Bei eventuellen Schwierigkeiten hilft Ihnen der Kundenservice Ihrer Bank.

Darüber hinaus sollte das Smartphone oder Tablet mit einem Sperrcode geschützt werden. Zahlungsvorgänge, bei denen Zugangsdaten eingegeben werden, müssen immer über verschlüsselte Verbindungen erfolgen. Diese erkennen Sie an Adressen im Browser, die mit https:// beginnen. Tätigen Sie keine Onlinegeschäfte über öffentliche WLAN-Netzwerke. Die Gefahr, dass andere im gleichen WLAN-Netzwerk Informationen abfangen, ist hierbei zu groß **Kompetenzteil 1, Station 2 > Sichere Interneteinstellungen für unterwegs**.

Linktipps

Goldene Regeln für die sichere Nutzung des Mobile Banking
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Empfehlungen für die sichere Abwicklung von Bankgeschäften im Internet

Phishing-Radar
Herausgeber: Verbraucherzentrale
Beschreibung: Aktuelle Meldungen über Gefährdungen und Betrugsstrategien

Webcode: 2215

Lernziel **Lernen Sie Bezahlmöglichkeiten und die Gefahren des Phishings kennen.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Lesen Sie aktuelle Meldungen über Gefährdungen und Betrugsstrategien. Nutzen Sie dazu zum Beispiel auch den „Phishing-Radar“ der Verbraucherzentrale. Die Webseite finden Sie als Link in den Linktipps. Entdecken Sie Meldungen, die sich auch auf von Ihnen genutzte Onlinedienste beziehen? Oder haben Sie in letzter Zeit weitere Phishing-Nachrichten erhalten?

2 Prüfen Sie auf verschiedenen Shopping-Seiten, welche Bezahlmöglichkeiten angeboten werden. Tipp: Schauen Sie diebezüglich auch in die AGB.

ÜBUNGEN
FÜR SCHULUNGSGRUPPEN

1 Recherchieren Sie in Gruppen nach verschiedenen Shopping-Portalen und prüfen Sie, welche Bezahlmöglichkeiten angeboten werden. Vergleichen Sie Ihre Ergebnisse in der großen Runde. Begründen Sie, für was Sie sich entscheiden.

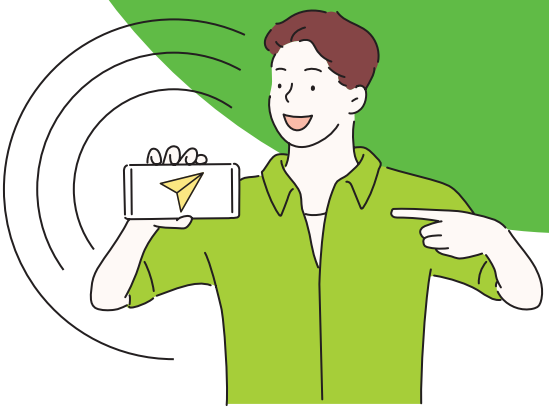
2 Gibt es in der Gruppe bereits Erfahrungen mit Phishing? Berichten Sie von dem Problem und wie dies gelöst werden konnte.

DAMIT DAS EINKAUFEN UND BEZAHLEN IM INTERNET SICHER GELINGT, LESEN SIE MEHR ZU FOLGENDEN EMPFEHLUNGEN IM KOMPETENZTEIL:

- Onlinebanking-Konto absichern
  - **Kompetenzteil 6, Station 1 > Onlinebanking**
- Bezahlsysteme sicher nutzen
  - **Kompetenzteil 6, Station 2 > Online Geld bezahlen**
- Betrügerische Mails erkennen
  - **EXTRA 02: Onlinebetrug**

LEBENSWELT 3
Online vernetzen und austauschen

Urlaubsfotos im Familienchat teilen, die Beförderung in sozialen Netzwerken bekannt machen oder eine E-Mail mit medizinischen Unterlagen versenden: Informationen jeder Art werden heute über das Internet kommuniziert. Doch was passiert mit Daten, die einmal veröffentlicht sind? Wie gut sind Sie geschützt? Wer kann Informationen sehen oder gar darauf zugreifen? In der Lebenswelt „Online vernetzen und austauschen" erhalten Sie einen Überblick, wie Kommunikationsdienste funktionieren und worauf Sie bei der digitalen Kommunikation besonders achten sollten. Zu den Austauschdiensten zählen sowohl die klassische E-Mail-Kommunikation als auch soziale Netzwerke, in denen Sie mit weiteren Personen über ein Thema, zum Beispiel einen geteilten Beitrag, unterhalten können. Eine weitere Austauschmöglichkeit sind Messenger – Programme, mit denen Sie sich unter anderem mit Familienmitgliedern oder Freund/-innen einzeln oder in Gruppen digital kommunizieren und Fotos oder Videos teilen können.



IN DER LEBENSWELT „ONLINE VERNETZEN UND AUSTAUSCHEN“ LERNEN SIE,

- welche verschiedenen Arten der Onlinekommunikation es gibt,
- was mit Ihren Daten passiert, wenn Sie diese veröffentlichen,
- was soziale Netzwerke sind und worauf Sie bei der Nutzung achten sollten.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.

STATION 1

Mit E-Mails beruflich und privat sicher kommunizieren

Wenn Sie an Kommunikation im Netz denken, kommt Ihnen sicherlich zuallererst die E-Mail in den Sinn. Kein Wunder, ist sie doch eine der ältesten Formen der Onlinekommunikation. Die Mail ist, einfach gesprochen, eine briefähnliche Nachricht, die auf elektronischem Weg in Computernetzen übertragen wird.

Eine E-Mail besteht stets aus verschiedenen Elementen: Zunächst müssen Sie sich klar darüber werden, an wen Sie die Nachricht verschicken wollen. Dafür brauchen Sie – analog zum Brief – eine Adresse. Diese können Sie in einem digitalen Adressbuch speichern und verwalten. Wenn Sie beispielsweise zu einer Party einladen, können Sie auch eine Nachricht gleichzeitig an eine Gruppe von Personen verschicken.

E-Mail-Adressen von Personen, die nicht direkt adressiert sind, aber trotzdem über die Kommunikation mit dem Empfänger oder der Empfängerin in Kenntnis gesetzt werden sollen, setzen Sie in die Zeile CC Ihres E-Mail-Programms.

Wenn Sie nicht möchten, dass die Empfänger/-innen alle Adressen sehen, die Sie angeschrieben haben, können Sie mit verdeckten Empfängerlisten arbeiten, indem Sie die Mailadressen in das BCC-Feld einfügen.

Jede Mail sollte einen aussagekräftigen Betreff haben wie „Einladung zum 50. Geburtstag“. Dieser ist wichtig, damit der oder die Adressierten sofort wissen, um was es geht. Der Inhalt entspricht in etwa einem Brief. Begleitend dazu lassen sich zudem noch Dateien beliebiger Art, beispielsweise Dokumente, Fotos und Videos, versenden. Diese werden als Anhang bezeichnet. Jedoch gibt es pro E-Mail ein Limit für eine bestimmte Dateigröße. Wer die Dateigröße überschreitet, bekommt eine entsprechende Fehlermeldung und kann die Mail nicht versenden. Zum Teilen oder Versenden großer Dateien können stattdessen unter Umständen Cloud-Speicher hilfreich sein.

Beim Einrichten Ihres E-Mail-Accounts sollten Sie einige grundsätzliche Sicherheitsvorkehrungen treffen. In allen Fällen ist ein starkes Passwort ein grundlegender Schutz. Zudem ist es sehr wichtig, für jedes Konto ein eigenes zu erstellen **Kompetenzteil 3, Station 1 > Einrichtung sicherer Passwörter**. Nutzen Sie wenn möglich eine Zwei-Faktor-Authentisierung. Das bedeutet, dass Sie sich neben dem Login mittels Benutzerkennung und Passwort mit einem weiteren Faktor identifizieren. Es handelt sich dabei beispielsweise um einen Zahlencode, den Ihnen Ihr E-Mail-Account-Anbieter per SMS zusendet. Dies gilt insbesondere dann, wenn Sie Ihren E-Mail-Account nutzen, um sich bei anderen Onlinediensten wie Onlineshops oder sozialen Netzwerken zu registrieren. Denn haben Cyberkriminelle Zugriff auf Ihr E-Mail-Konto, können diese sich darüber die Passwörter von anderen Diensten zurücksetzen lassen und erhalten somit Zugriff darauf.

Auch empfiehlt es sich, eine Transportverschlüsselung einzurichten – bei vielen E-Mail-Anbietern mittlerweile eine Standardeinstellung. E-Mails mit sensiblen Inhalten sollten außerdem von der versendenden Person mit einer Ende-zu-Ende-Verschlüsselung versehen werden. Die E-Mail kann dann nur von dem Empfänger oder der Empfängerin persönlich mit einem individuellen privaten Schlüssel entschlüsselt werden **Kompetenzteil, 5, Station 1 > Nachrichten verschlüsseln**.

Sie können unter zahlreichen E-Mail-Anbietern auswählen, um sich ein Postfach mit einer dazugehörigen Adresse einzurichten. Um anschließend Nachrichten schreiben, empfangen oder lesen zu können, gibt es mehrere Wege: Sie können sich auf der Seite Ihres Anbieters über den Browser anmelden oder Sie installieren ein E-Mail-Programm auf Ihrem PC oder eine App auf Ihrem Mobilgerät.

Es gibt sowohl kostenlose als auch kostenpflichtige Angebote. Bei der Auswahl sollten Sie abwägen: Viele E-Mail-Anbieter finanzieren sich durch Werbung. In der Regel werden dabei auch Nutzerdaten verwendet. Vergleichen Sie daher die Allgemeinen Geschäftsbedingungen (AGB) und Datenschutzerklärungen der Anbieter.

BEI DER AUSWAHL KÖNNEN SIE SICH FOLGENDE FRAGEN STELLEN:

- Werden personenbezogene Daten erhoben?
- Wenn ja, wie werden diese Daten verwendet oder werden sie gar weitergeleitet?
- Wird eine Verschlüsselung angeboten?
- Ist eine Zwei-Faktor-Authentisierung möglich?
- Räumt sich der Anbieter das Recht ein, auf den Inhalt Ihrer E-Mail zuzugreifen?

Wer einen E-Mail-Account hat, macht in den meisten Fällen Erfahrungen mit Spam, also unerwünschten oder sogar betrügerischen E-Mails. Diese können unbekannte Links und Anhänge enthalten, die Schadprogramme mit sich führen oder auf gefälschte Webseiten hinleiten, auf denen Sie vielleicht aufgefordert werden, sensible Daten, zum Beispiel Passwörter, einzutragen – was Sie auf keinen Fall tun sollten. Bei solchen Betrugsversuchen spricht man von Phishing

Kompetenzteil, 5 > Sicher digital kommunizieren,
EXTRA 01: Schadprogramme,
EXTRA 02: Onlinebetrug.

Linktipps

Datenschutz und Verschlüsselung bei E-Mails
Herausgeber: Verbraucherzentrale
Beschreibung: Artikel über Risiken beim Empfangen und Senden von E-Mails

E-Mail und Newsletter – Post für dich
Herausgeber: Internet-ABC e. V. bei der Landesanstalt für Medien NRW
Beschreibung: Online-Lernmodul für junge Netzeinsteiger/-innen
Zielgruppe: Lehrkräfte in Grundschulen

E-Mail und Messenger sicher nutzen
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Erklärvideo und Informationen für Verbraucher/-innen

Online-Quiz: E-Mail-Sicherheit
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Kurzer Wissenstest mit sechs Fragen

Onlinekommunikation – E-Mails, Messenger und Videotelefonie
Herausgeber: Deutschland sicher im Netz e. V. mit Unterstützung von BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Handreichung #3 des Digital-Kompasses

Sichere E-Mail-Kommunikation
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Übungsblätter zur Handreichung #3 des Digital-Kompasses

Webcode

Linktipps

E-Mail – Ein Konto einrichten und nutzen am Beispiel Yahoo
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Anleitung des Digital-Kompasses

E-Mail – Ein Konto einrichten und nutzen am Beispiel GMX
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Anleitung des Digital-Kompasses

E-Mail – Ein Konto einrichten und nutzen am Beispiel T-Online
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Anleitung des Digital-Kompasses

Webcode: 2 3 1 1

Lernziel **Nutzen Sie anlassbezogen E-Mails, um in Kontakt zu bleiben. Prüfen Sie die Angebote.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

VERTIEFUNG + PRAXIS

1. In welchen Kontexten benutzen Sie bereits eine E-Mail-Adresse? Welche Angelegenheiten klären Sie per E-Mail?

2. Warum gibt es kostenfreie und kostenpflichtige E-Mail-Angebote im Netz? Was unterscheidet die Dienste? Prüfen Sie zur Klärung der Fragen den Funktionsumfang der Angebote im Netz. Achten Sie dabei darauf, bei welchen Anbietern in E-Mails Werbung angezeigt wird, wie groß der Speicherplatz ist, wie groß Dateianhänge sein dürfen und welche weiteren Gründe es gibt, einen kostenpflichtigen Anbieter zu wählen.

3. Spielen Sie das Spiel „Spam-Detektiv“ in den Übungsblättern zur Handreichung #3 des Digital-Kompasses.
Diese finden Sie in der Linkliste.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1. Fragen Sie in die Gruppe: Zu welchen Anlässen oder Zwecken nutzen Sie E-Mails? Erstellen Sie gemeinsam eine Liste. Klären Sie dabei auch, wann eine Kommunikation per E-Mail nicht sinnvoll ist und zu welchen Anlässen oder Zwecken andere Kommunikationsmittel wie zum Beispiel Telefon oder Chat sinnvoller erscheinen.

2. Wie bewahren Sie E-Mail-Adressen von Bekannten, Freund/-innen und Familienmitgliedern auf? Auf Papier? Im Adressverzeichnis Ihres E-Mail-Anbieters? In den Kontakten Ihres Handys? Diskutieren Sie in der großen Runde, welche Möglichkeit die sicherste ist.

STATION 2

Mit Instant Messengern schnell und direkt Kontakte pflegen

Freundinnen und Freunde oder die Familie schnell mal auf den neuesten Stand bringen? Mit Instant Messaging (auf Deutsch: sofortige Nachrichtenübermittlung) können Nachrichten über das Internet nahezu in Echtzeit zwischen Personen oder geschlossenen Gruppen übermittelt werden, die denselben Messenger verwenden. Die entsprechende Software oder App müssen Sie herunterladen und auf dem PC, Tablet oder Smartphone installieren. Instant-Messaging-Dienste bieten die Möglichkeit, Fotos oder Videos zu übertragen **Kompetenzteil 5, Station 3 > Kommunizieren über Messenger**. Nachrichten können generell kostenfrei übertragen werden. Jedoch ist der Download einiger Messenger einmalig kostenpflichtig.

Weit verbreitete Messenger-Dienste in Deutschland sind WhatsApp, Facebook und iMessage. Es gibt aber auch Alternativen wie Telegram, Threema und Signal. Die Dienste unterscheiden sich teils darin, welche Daten ihrer Nutzerinnen und Nutzer sie erheben und speichern.

INFORMIEREN SIE SICH VOR DER ENTSCHEIDUNG FÜR EINEN MESSENGER, WAS MIT IHREN DATEN PASSIERT, WENN SIE EINEM KONTAKT SCHREIBEN.

- Werden Verschlüsselungsmethoden angeboten? Wenn ja, welche? (zum Beispiel Ende-zu-Ende-Verschlüsselung)
- Welche Berechtigungen räumt sich die Messenger-App beim Installieren ein?
- Sind diese Berechtigungen notwendig? **Kompetenzteil 2, Station 4 > Software auswählen und sicher einrichten**
- Auch sollten Sie klären, ob Sie gegebenenfalls Ihre Nutzungsrechte an den hochgeladenen Fotos und Videos an den Anbieter des Messengers abgeben. Einige Anbieter halten sich das Recht frei, Ihre Texte, Bilder oder Videos zum Beispiel für Werbezwecke zu verwenden.

Über die Sicherheitseinstellungen des Messengers können Sie Ihre Privatsphäre schützen. Beispielsweise können Sie bestimmen, wer Ihren Onlinestatus oder Ihr Profilfoto sehen darf und ob unbekannte Personen, die nicht aus Ihrem eigenen Kontaktverzeichnis stammen, Ihnen Nachrichten senden dürfen. So sind Ihre Daten nicht für alle einsehbar.

Doch selbst wenn Sie diese Privatsphäre-Einstellungen restriktiv umgesetzt haben und Ihre Nachrichten Ende-zu-Ende verschlüsselt sind, können Anbieter Ihre Metadaten festhalten. Zu den Metadaten zählen die Kennung des Absenders, häufig in Form der Telefonnummer, die Kennung des Adressaten, das Datum und die Uhrzeit. Auch weitere Angaben sind

möglich. Solche Daten dienen nicht nur der korrekten Zuleitung der Nachricht, sondern können auch zur Analyse von Vorlieben und Ähnlichem genutzt werden. Auf diese Weise lassen sich Nutzerprofile erstellen, die für personalisierte Werbung auf Webseiten verwendet werden können. Zudem lässt sich daraus ableiten, wer beispielsweise mit wem gut befreundet ist oder wer wann und mit welchen Geräten online ist. So ist auch die Auswahl des Messengers entscheidend dafür, wie viele digitale Spuren Sie hinterlassen werden.

Bitte beachten Sie: Bei Messengern gelten ganz ähnliche Sicherheitsregeln wie bei den E-Mails: Betrügerische Nachrichten können unbekannte Links und Anhänge enthalten, die Schadprogramme mit sich führen oder auf gefälschte Webseiten hinleiten **Kompetenzteil 5 > Sicher digital kommunizieren,**
EXTRA 01: Schadprogramme:
EXTRA 02: Onlinebetrug.

Linktipps

Messenger-Apps für Kinder
Herausgeber: Schau hin
Beschreibung: Kindgerechte Alternativen zu WhatsApp, Messenger-Vergleich im Überblick
Zielgruppe: Eltern

Aktuelle Infos über Messenger
Herausgeber: iRights e. V.
Beschreibung: Diese Seite bietet verschiedene Artikel zum Thema Messenger und Sicherheit

Messenger und Sicherheit: Wie sicher chattest du?
Herausgeber: Handysektor (Landesanstalt für Kommunikation Baden-Württemberg)
Beschreibung: Informationen zum Thema Datenschutz
Zielgruppe: Jugendliche

Instant Messenger
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Sicherheitsrelevante Informationen für alle Bürger

Einfach WhatsApp
Herausgeber: Bundeszentrale für politische Bildung
Beschreibung: Leitfaden in leichter Sprache
Zielgruppe Menschen mit Behinderung

Sicher unterwegs in WhatsApp
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Informationen für Kinder und Jugendliche zum Schutz der Privatsphäre

Webcode: 2 3 1 2

Lernziel **Nutzen Sie sichere Messenger. Beachten Sie dabei Ihre Privatsphäre.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

VERTIEFUNG

1. Zu welchen Zwecken oder Anlässen wollen Sie einen Messenger nutzen? Welche Gründe sind für Sie persönlich entscheidend? Erstellen Sie eine Liste.

2. Suchen Sie im Internet nach verschiedenen Messengern. Vergleichen Sie: Welche Konditionen der Nutzung werden genannt? Was sagen die Anbieter zum Datenschutz und zu Ihrer Sicherheit?

3. Wählen Sie den Messenger aus, der Ihnen am sichersten erscheint und installieren Sie diesen auf Ihrem Handy.

4. Erstellen Sie ein Profil. Finden Sie dann die Sicherheitseinstellungen Ihres Messengers und wählen Sie aus, welche Daten Sie preisgeben wollen und welche nicht. Klären Sie für sich vorher folgende Fragen: Wer darf mein Profil sehen? Wer kann mein Profilbild beziehungsweise meinen Status sehen, wenn ich sie ändere? Gibt es Anlässe, bei denen ich meinen Standort preisgeben sollte? Will ich nur Nachrichten per Text senden, Bilder hochladen, Sprachnachrichten und Videoanrufe tätigen? Wenn Letzteres, dann überlegen Sie, ob Sie dem Messenger den Zugriff auf Ihre Fotos, Ihr Mikrofon oder Ihre Kamera erlauben oder nicht.

5. Informieren Sie Bekannte und Freunde über die Installation des Messengers und fragen Sie diese, ob sie Sie als Kontakt hinzufügen können.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Installieren Sie in verschiedenen Kleingruppen jeweils einen anderen Messenger. Erstellen Sie in jeder Gruppe pro Person ein Profil und versuchen Sie sich in der Kleingruppe gegenseitig zu finden. Was erfahren Sie über die anderen Personen? Vergleichen Sie Ihre Ergebnisse mit denen der anderen Kleingruppen. Wie bewerten Sie die Ergebnisse hinsichtlich des Datenschutzes beziehungsweise Ihrer Privatsphäre?

2 Erstellen Sie in der gesamten Gruppe gemeinsam eine Liste von unsicheren und sicheren Messengern anhand der Konditionen. Nutzen Sie dafür die Hinweise des Bundesamts für Sicherheit in der Informationstechnik aus den Linktipps.

VERTIEFUNG

STATION 3

In sozialen Netzwerken austauschen

Das eigene Profil in den verschiedenen sozialen Netzwerken ist für viele heute eine wichtige private und berufliche Visitenkarte. Über soziale Netzwerke können Nutzerinnen und Nutzer sich präsentieren und schnell und einfach Inhalte teilen und mit anderen in Kontakt treten. Bekannte Plattformen sind beispielsweise Twitter, Facebook, YouTube, Instagram, aber auch berufliche Netzwerke wie LinkedIn oder Xing. Für die Nutzung dieser Plattformen müssen Sie sich in den meisten Fällen mit Ihrer E-Mail-Adresse und einem Passwort registrieren. Achten Sie hier auf sichere Logins mit einem starken Passwort und melden Sie sich nach der Nutzung ab, um Risiken wie Identitätsdiebstahl vorzubeugen

Kompetenzteil 3 > Sichere Logins nutzen.

Nach der Registrierung können Sie in den Netzwerken ein eigenes Profil erstellen. Sie entscheiden, welche Angaben Sie machen zu Benutzernamen, Hobbys, Interessen, Geburtsdatum, Wohnort oder Beruf und welches Profilbild Sie einstellen. Außerdem können Sie Ihre Privatsphäre schützen, indem Sie verkürzte oder anonymisierte Nutzernamen sowie Profilfotos ohne erkennbare Personen verwenden.

Ausgestaltet wird dieses eigene Profil mit dem regelmäßigen „Posten“ von Inhalten: Das können Wortbeiträge, Fotos, Videos oder Links sein. Zudem haben Sie die Möglichkeit, andere Beiträge zu kommentieren. Viele soziale Netzwerke bieten auch an, zu Veranstaltungen einzuladen oder sich in Gruppen gezielt über ein Thema auszutauschen. Wenn Sie etwas von sich preisgeben, machen Sie sich bewusst, wer die Veröffentlichung sehen kann: nur eine ausgewählte Person, Ihr Bekanntenkreis oder alle Internetnutzerinnen und -nutzer? Passen Sie vorab Ihre Privatsphäre-Einstellungen an, um beispielsweise den Kreis der Personen einzuschränken, der Ihre Inhalte einsehen und mit Ihnen in Kontakt treten darf. Daneben ist es oft zusätzlich möglich, privat über integrierte Messenger oder Chats Nachrichten an nur eine Person zu verschicken.

Mithilfe der sozialen Netzwerke können sich Menschen über regionale und internationale Grenzen hinweg austauschen. Alte Freundschaften können wiederbelebt und neue geschlossen werden. In den meisten Fällen bekommen Sie dafür eine Kontaktanfrage. Behalten Sie dabei immer im Hinterkopf, dass es auch Fake-Profile gibt. Bei diesen machen Menschen falsche Angaben über sich selbst, indem sie beim Geburtsjahr lügen oder ein Foto aus dem Internet nutzen. Einige sind auch komplett frei erfunden. Deswegen bleiben Sie immer skeptisch: Kennen Sie diesen Menschen bereits? Warum möchte er mit Ihnen Kontakt aufnehmen? Im Zweifel können Sie die Anfrage ablehnen. Einmal angenommene Kontakte können Sie zudem jederzeit wieder ablehnen oder blockieren. Sollten Sie über die sozialen Netzwerke belästigt werden, ist es ratsam, diesen Vorfall auch dem Anbieter zu melden **EXTRA 04: Belästigung und Beleidigung**.

BEACHTEN SIE EIN PAAR GRUNDREGELN DES AUSTAUSCHS:

- Gehen Sie bewusst vorsichtig mit der Preisgabe persönlicher Informationen um, zu denen auch Fotos von Ihnen, von Ihren Freund/-innen und Ihrer Familie zählen. Gerade bei Informationen, die auch etwas über Ihre Kontakte aussagen, sollten Sie sich sicher sein, dass diese damit einverstanden sind.

- Achten Sie auch auf die Persönlichkeitsrechte anderer sowie auf Urheber- und Nutzungsrechte beim Veröffentlichen fremder Bilder. Insbesondere bei Kinderbildern gilt ein besonders sensibler Umgang – aber auch bei allen anderen Fotos und persönlichen Daten von anderen Menschen.

Der Preis des Kostenlosen

Viele soziale Netzwerke bieten eine kostenfreie Nutzung an, zumindest in einer Basisversion. Verdienen die Anbieter kein Geld über erweiterte Funktionen und Abonnements, geschieht dies in der Regel über den Verkauf von Anzeigen. Zur Einblendung der Werbung verwenden die Plattformanbieter gesammelte Daten, die ihre Nutzerinnen und Nutzer bewusst oder unbewusst preisgeben. So kann Ihnen zielgerichtete, personalisierte Werbung angezeigt werden.

Dabei haben es Verbraucherinnen und Verbraucher nicht immer selbst in der Hand, wie viel der Dienst über sie erfährt: Andere Kontakte, mit denen das eigene Profil beispielsweise über Freundeslisten verknüpft ist, fließen ebenfalls in die Analyse zur personalisierten Werbung mit ein, da befreundete Personen oft ähnliche Interessen und Vorlieben teilen.

Betreiber sozialer Netzwerke sind gesetzlich verpflichtet, Sie über die Sammlung, Speicherung und Verwendung Ihrer Daten in einer Datenschutzerklärung zu informieren. Dabei setzt die Nutzung der Daten eine Einwilligung in die Datenschutzerklärung voraus. Diese wird gesondert neben den Allgemeinen Geschäftsbedingungen (AGB) veröffentlicht, denen Sie bei der Anmeldung zusätzlich zustimmen müssen.

Linktipps

Schau Hin: Die Chancen der sozialen Netzwerke für Kinder
Herausgeber: Projektbüro SCHAU HIN! bei WE DO communication GmbH GWA
Beschreibung: Informationen für Eltern

Was ist ein Fake-Profil?
Herausgeber: Hochschule für Angewandte Wissenschaften
Beschreibung: Internetratgeber „Netzdurchblicker“ für Jugendliche gibt Orientierung bei Fake-Profilen

Wie erkennen Sie Fake-Profile?
Herausgeber: Watchlist Internet (Österreichisches Institut für angewandte Telekommunikation, ÖIAT)
Beschreibung: Zusammenstellung von Fällen von Fake-Profilen und Möglichkeiten des Erkennens von falschen Profilen in sozialen Netzwerken

Soziale Netzwerke
Herausgeber: MedienNetzwerk SaarLorLux e. V., Landesmedienanstalt Saarland
Beschreibung: Schulungsbroschüre der Kampagne „Onlinerland Saar“ (2012)

Broschüre Soziale Netzwerke
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: 10 Tipps zur sicheren Nutzung von sozialen Netzwerken

Sicher in sozialen Netzwerken aktiv
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Informationen und Erklärvideo

Webcode

Linktipps

Chatten ohne Risiko
Herausgeber: jugendschutz.net gGmbH
Beschreibung: Der „kompass-social.media“ bewertet die beliebtesten Onlinedienste in puncto Sicherheit. Mithilfe des praktischen Ampelsystems erhält man schnell einen Überblick

Herz verloren, Identität gestohlen:
Digitale Sicherheit beim Online-Dating
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Das BSI klärt über Risiken bei der Suche nach einem Partner oder einer Partnerin im Internet auf

Soziale Netzwerke im Internet – Miteinander in Kontakt bleiben
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Handreichung #4 des Digital-Kompasses

Freundschaftsbörsen – Begegnungen in der digitalen Welt
Herausgeber: Deutschland sicher im Netz e.V.
Beschreibung: Übungsblatt des Digital-Kompasses

Mein Profil im Netz: Soziale Netzwerke beim Einstieg in das Berufsleben reflektieren und sicher nutzen
Herausgeber: Stiftung Medienpädagogik Bayern
Beschreibung: Schulungsmaterialien des Medienführerscheins Bayern

Datenschutz in sozialen Netzwerken: Meine Daten gehören mir
Herausgeber: iRights.info und Klicksafe (EU-Initiative)
Beschreibung: Rechtsfragen im Netz, einfach erklärt

Webcode: 2 3 1 3

Lernziel **Nutzen Sie soziale Netzwerke – anlassbezogen und sicher.**

PRAXIS

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Überlegen Sie sich drei Beiträge aus Ihrem Alltag, die Sie in einem sozialen Netzwerk veröffentlichen würden. Das können zum Beispiel Erlebnisse aus Ihrem Alltag, eine interessante Neuigkeit oder Fotos sein. Überlegen Sie, ob diese Beiträge Rückschlüsse auf Ihre persönlichen Daten wie zum Beispiel Wohnort oder Name zulassen.

2 Suchen Sie in einem oder mehreren sozialen Netzwerken die Accounts einer berühmten Persönlichkeit. Was erfahren Sie über ihr Leben? Würden Sie diese Informationen auch preisgeben?

3 Laden Sie sich den Leitfaden „Datenschutz in sozialen Netzwerken“ von Klicksafe (EU-Initiative) herunter. Einen Link finden Sie in der Linkliste. Gehen Sie die Schritt-für-Schritt-Anleitungen für das soziale Netzwerk durch, das Sie nutzen möchten.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Durchsuchen Sie in verschiedenen Kleingruppen die Accounts verschiedener berühmter Persönlichkeiten nach privaten Informationen (zum Beispiel Wohnort, Geburtsort, Hobbys, Urlaubsaktivitäten, Berufsleben etc.). Was erfahren Sie? Welche dieser Informationen würden Sie von sich oder von Bekannten, Freund/-innen oder Familienmitgliedern niemals veröffentlichen, weil diese zu privat sind? Erstellen Sie dann in der Gruppe eine Liste.

Beleidigungen und Belästigungen

Die Kommunikation mit Freund/-innen, Familie und Bekannten in den sozialen Netzwerken ist für viele Menschen ein wichtiger Bestandteil ihres Lebens geworden. Wie jeder Raum, in dem verschiedene Personen mit unterschiedlichen Motivationen zusammenkommen, hat aber auch dieser virtuelle Raum seine Schattenseiten. In den sozialen Medien kann es immer wieder zu Verleumdungen und Beleidigungen kommen. Digitale Nötigungen und Diffamierungen sind unter dem Begriff Cybermobbing (oder Cyberbullying) bekannt. Dazu kann zum Beispiel ein Account angelegt werden, der den Eindruck erweckt, vom Opfer angelegt worden zu sein. Anschließend werden beispielsweise in einem sozialen Netzwerk im Namen des vermeintlichen Kontoinhabers beziehungsweise der vermeintlichen Kontoinhaberin unangemessene Nachrichten geschrieben, unterstellte politische Ansichten gepostet, angebliche sexuelle Vorlieben behauptet oder unangenehme Fotos hochgeladen

EXTRA 04: Belästigung und Beleidigung.

DAMIT DAS DIGITALE KOMMUNIZIEREN SICHER GELINGT, LESEN SIE MEHR ZU FOLGENDEN EMPFEHLUNGEN IM KOMPETENZTEIL:

- Sicheres Passwort und Zwei-Faktor-Authentisierung für Online-Accounts und Benutzerkonten
  Kompetenzteil 3 > Sichere Logins nutzen

- Privatsphäre-Einstellungen in sozialen Netzwerken bewusst vornehmen **Kompetenzteil 5, Station 4 > Kommunizieren über soziale Netzwerke**

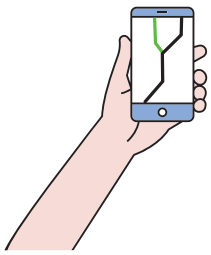
- Anhänge und Links in E-Mails und Nachrichten prüfen
  EXTRA 02: Onlinebetrug

- Mit Daten bewusst und möglichst sparsam umgehen
  Kompetenzteil 4, Station 3 > Datensparsamkeit

LEBENSWELT 4

Online Reisen planen und vernetzt mobil sein

Den Stau umfahren dank Routenplaner, einen E-Roller mit dem Smartphone mieten, den Urlaub online planen oder per App die schnellste Verbindung mit dem Bus heraussuchen: In unserer vernetzten Welt gibt es eine Vielzahl neuer Möglichkeiten und Chancen, um mobil zu sein. Die digitale Lebenswelt „Online Reisen planen und vernetzt mobil sein“ zeigt Ihnen, worauf Sie bei der Nutzung digitaler Mobilitätsangebote achten sollten und wie diese Ihren Alltag erleichtern können.



IN DER LEBENSWELT „ONLINE REISEN PLANEN UND VERNETZT MOBIL SEIN“ LERNEN SIE,

- wie Sie von zu Hause aus online Ausflüge und Reisen planen,
- wie Sie dabei Bewertungs- und Buchungsportale optimal nutzen,
- wie Sie Ihren Standort digital bestimmen,
- wie Apps Ihnen Ihre Reise angenehmer machen,
- was gemeinschaftliche Fahrzeugnutzung ist und wie sie funktioniert.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.

STATION 1

Online Reisen und Urlaub planen

Digitale Mobilität fängt bereits zu Hause an: Unabhängig von Öffnungszeiten in klassischen Reisebüros können Sie rund um die Uhr alle Informationen, die Sie für Ihre Reise brauchen, aus einer Vielzahl von Angeboten zusammensuchen. Welches ist die beste Reisezeit? Wie sehen Unterkünfte vor Ort aus? Ist die Pauschalreise preiswerter oder ist es besser, Flug und Unterkunft separat zu buchen?

Haben Sie Ihre Reise online gebucht, können Sie in vielen Fällen über Ihr eigenes Profil oder Kundenkonto bequem von jedem internetfähigen Gerät auf Unterlagen wie Buchungsbestätigungen und Flugtickets zugreifen. Außerdem gibt es spezielle Seiten und Apps, die Preise für verschiedene Verkehrsmittel vergleichen und die beste Verbindung zum günstigsten Preis anzeigen. Diese Vergleichsportale gibt es beispielsweise für Mitfahrgelegenheiten, Bus-, Zug- und Flugverbindungen.

Bewertungs- und Buchungsportale

Wer eine Reise buchen möchte, kann im Netz zahlreiche Webseiten nutzen, um Pauschalangebote, Hotelübernachtungen oder Flugreisen zu buchen. Auch Onlineplattformen für Unterkünfte bei Privatpersonen und Gastfamilien sind sehr beliebt. Vergleichs- oder Buchungsportale stellen die Angebote vieler Anbieter gegenüber und helfen so, den Überblick zu behalten. Auf diversen Bewertungsplattformen können zudem Berichte und Fotos von Gästen eingesehen werden, die oftmals einen Anhaltspunkt geben, ob das Hotel wirklich den Beschreibungen der Touristikunternehmen entspricht.

Hier gilt es, bei abgegebenen Kritiken von Nutzerinnen und Nutzern genau hinzuschauen: Nicht immer wurden sie tatsächlich von Reisenden erstellt, sondern womöglich vom Unternehmen selbst (oder von dessen Konkurrenz), um die Bewertung zu manipulieren. Achten Sie deshalb auf überschwänglich positive und negative Beiträge und schenken Sie lieber Rezensionen Aufmerksamkeit, die sachlich geschrieben sind.

Linktipps

Reiseplanung im Internet
Herausgeber: Deutschland sicher im Netz e. V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Handreichung #6 des Digital-Kompasses
Zielgruppe: Vor allem Senior/-innen

12 goldene Regeln für Reisebuchungen im Internet
Herausgeber: Verbraucherzentrale NRW, Klicksafe (EU-Initiative), Landesmedienanstalt NRW
Beschreibung: Praktische Tipps für Online-Reisebuchungen

Der DB-Navigator – Mobil suchen und buchen
Herausgeber: Deutschland sicher im Netz e. V., BAGSO – Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V.
Beschreibung: Anleitung des Digital-Kompasses, die Grundkenntnisse im Umgang mit der Navigator-App der Deutschen Bahn vermittelt
Zielgruppe: Vor allem Senior/-innen

Webcode: 2 4 1 1

Lernziel Buchen Sie eine Reise online.

ÜBUNGEN
FÜR DIE EINZELARBEIT

PRAXIS

1 Stellen Sie sich vor, Sie planen eine Reise. Wollen Sie fliegen, mit dem Bus oder lieber mit dem Zug fahren? Wollen Sie in einem Hotel oder einer privaten Unterkunft übernachten? Vielleicht ist Ihnen auch eine Pauschalreise lieber? Machen Sie eine Liste der Entscheidungen, bevor Sie ins Internet gehen und entsprechend Ihrer Vorlieben weiter recherchieren.

2 Suchen Sie nun eine Unterkunft entsprechend Ihrer Vorstellungen im Internet. Vergleichen Sie gegebenenfalls die Preise der Unterkunft auf unterschiedlichen Portalen mit den Angeboten direkt auf der Webseite der Unterkunft. Wo finden Sie den günstigeren Preis zu welchen Konditionen? Welche weiteren Informationen über die Unterkunft erhalten Sie auf den unterschiedlichen Seiten? Welche Möglichkeiten der Stornierung werden zum Beispiel angeboten?

3 Finden Sie heraus, welche Züge, Busse oder welche Flüge zu welchen Preisen angeboten werden. Nutzen Sie dafür die Portale der Bahn-, Bus- oder Flugunternehmen.

4 Schreiben Sie eine fiktive Bewertung über Ihre Reise. Überlegen Sie, ob Sie diese auch anonym veröffentlichen könnten. Achten Sie in Ihrem Text genau darauf, auf private Angaben zu Ihnen und anderen (z. B. Personal) zu verzichten.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Einigen Sie sich in der Schulung auf ein Reiseziel, auf eine Art der Unterkunft (Hotel, Pension etc.) und auf die Dauer der Reise. Teilen Sie sich in Gruppen auf und erstellen Sie jeweils ein Reiseangebot hinsichtlich Übernachtung sowie Hin- und Rückfahrt. Stellen Sie Vermutungen über Möglichkeiten an, im Internet einen günstigen Preis zu finden. Sind Portale sinnvoller oder die Direktbuchung auf der Seite der Unterkunft? Was ist günstiger: Bus, Flugzeug oder Bahn?

PRAXIS

STATION 2

Im Netz Routen finden und sicher navigieren

Auch wenn Sie Ihre Reise bereits im Voraus zu Hause geplant haben, müssen Sie manchmal spontan nachschauen, wo Sie sich befinden oder wie Sie von A nach B kommen – digitale Endgeräte sind dabei mittlerweile zu wertvollen Helfern geworden. Mithilfe von Karten-Apps können Sie in Echtzeit die eigene Position bestimmen und den schnellsten Weg zum gewünschten Ziel ermitteln.

Apps zur Navigation können mit jedem Smartphone genutzt werden. Wollen Sie einen bestimmten Ort erreichen, können Sie sich eine Route errechnen lassen. Die App generiert für Sie entsprechende Vorschläge und errechnet, welche Strecke Sie zurücklegen müssen und wie lange Sie dafür brauchen werden. Dabei können Sie die Routenplanung von der Art Ihrer Fortbewegung abhängig machen, je nachdem, ob Sie mit dem Auto, dem Fahrrad, zu Fuß oder mit öffentlichen Verkehrsmitteln unterwegs sind. Autofahrern und Autofahrerinnen stehen darüber hinaus mobile oder fest im Fahrzeug installierte Navigationsgeräte zur Verfügung.

Wenn Sie in Echtzeit, also während Sie unterwegs sind, navigieren möchten, muss die Standortbestimmung Ihres mobilen Geräts eingeschaltet sein. Diese Dienste basieren in der Regel auf Satellitennavigationssystemen wie zum Beispiel GPS (Global Positioning System), Glonass oder Galileo, aber auch auf den Daten der jeweiligen Mobilfunkzellen und den Signalen von WLAN-Netzwerken.

Wenn Sie den Zugriff auf die Standortdaten freigeben, können diese Aufschluss über regelmäßig zurückgelegte Strecken und die jeweilige Tageszeit sowie über längere Aufenthalte geben. Mit diesen Informationen ist es für einige Anbieter unter Umständen möglich, den Arbeitsplatz und die Wohnung zu identifizieren, ohne dass diese Adressen direkt als solche angegeben wurden. Ihre Standortdaten können zudem für weitere Zwecke verwendet werden wie das Bewerben von Geschäften oder Restaurants in Ihrer unmittelbaren Nähe. Je nachdem, wie viele Informationen Sie preisgeben möchten, sollten Sie sich bewusst für eine Einstellung entscheiden. Wer nicht auf entsprechende Dienste verzichten möchte, kann die Apps so anpassen, dass eine Übermittlung der Daten nur bei der aktiven Nutzung des Dienstes erfolgt – und diese nicht im Hintergrund weiterläuft, obwohl die App geschlossen ist. Dies lässt sich üblicherweise für alle Apps in den Datenschutz-Einstellungen des Smartphones regulieren.

Linktipps

Standortdaten: Bequemes Feature oder Überwachung?
Herausgeber: VFR Verlag für Rechtsjournalismus GmbH
Beschreibung: Datenschutz.org klärt über Standortdaten auf

Die Standortbestimmung beim Smartphone – überall auffindbar?
Herausgeber: Initiative D21 e. V.
Beschreibung: Online-Artikel der Initiative D21

Aktuelle Infos zum Thema Standort
Herausgeber: iRights e. V.
Beschreibung: Diese Seite bietet verschiedene Artikel zum Thema

Navi-Apps im Check
Herausgeber: iRights e. V.
Beschreibung: Mobilsicher.de hat beliebte Apps geprüft

Webcode: 2 4 1 2

Lernziel Lernen Sie, online zu navigieren.

PRAXIS

ÜBUNGEN
FÜR DIE EINZELARBEIT

1. Finden Sie heraus, wo in Ihrem Smartphone die Übermittlung standortbasierter Daten ausgestellt werden kann. Erstellen Sie für sich Kriterien, wann Sie standortbasierte Daten preisgeben wollen und wann Sie sie deaktivieren.

2. Stellen Sie sich vor, Sie suchen eine Jogging- oder Wanderroute in Ihrer Umgebung. Finden Sie Seiten oder Apps, die sie per GPS anleiten? Ist das aus Ihrer Sicht eine nützliche Funktion? Stellen Sie Vor- und Nachteile zusammen.

ÜBUNGEN
FÜR SCHULUNGSGRUPPEN

1. Machen Sie in Kleingruppen eine kleine Exkursion zu einem nächstgelegenen Standort (zum Beispiel einem Supermarkt, Restaurant o. Ä.) und zurück. Nutzen Sie zur Navigation Ihr Smartphone.

2. Sammeln Sie in der Gruppe Vor- und Nachteile der Navigation online. Überwiegen am Ende die Vor- oder Nachteile?

3. Prüfen Sie in Kleingruppen an verschiedenen Geräten (Handy, Tablet, Laptop, PC), wo die Übermittlung des Standorts abgeschaltet werden kann. Erklären Sie dies den anderen Kleingruppen.

STATION 3

Mit Apps buchen und reisen

Spontan eine Fahrkarte lösen oder eine Übernachtung von unterwegs buchen? Viele Anbieter verfügen über eine eigene App, mit der Sie schnell und einfach Unterkünfte, Fahrten und Flüge suchen und buchen können. Doch Sie sollten jede App vor dem Herunterladen genau prüfen – vor allem, wenn Sie dort Zahlungsdaten hinterlegen wie bei Bahn-, Flug- oder Hotelbuchungen. Hier gelten die gleichen Sicherheitsvorkehrungen wie für das generelle Onlineshopping **Lebenswelt 2 > Online einkaufen und bezahlen und** **Kompetenzteil 6 > Sichere Transaktionen**. Zudem ist es wichtig, die Apps aus den offiziellen App-Stores herunterzuladen.

Ein praktischer Vorteil der Buchung über die App ist, dass Sie die Buchungsbestätigung beziehungsweise das Ticket direkt auf dem Smartphone haben. Das spart Papier und lästiges Drucken, was unterwegs auch nicht so einfach ist. Wenn Sie ein Handyticket nutzen, sind Sie allerdings auch dafür verantwortlich, dass Sie es vorzeigen können. Achten Sie also darauf, dass der Akku Ihres Smartphones ausreichend geladen ist.

Um bereits gebuchte Tickets oder die Möglichkeit weiterer Buchungen auf Ihrem Gerät im Falle eines Diebstahls zu schützen, sollte es über Sperrmechanismen verfügen. Es sollte mindestens die Eingabe einer PIN oder der Fingerabdruck notwendig sein, um darauf zuzugreifen. Beim Zugriff auf Onlinedienste ermöglichen viele Anbieter eine Zwei-Faktor-Authentisierung. Das heißt, dass neben den eigentlichen Login-Daten (Nutzername und Kennwort) noch ein weiterer Faktor eingesetzt werden muss. Das kann die Verknüpfung mit einem zweiten Gerät sein, auf dem der Zugriff bestätigt werden muss **Kompetenzteil 3 > Sichere Logins nutzen und** **Kompetenzteil 6 > Sichere Transaktionen**.

Linktipps

Urlaub mit dem Smartphone
Herausgeber: iRights e. V.
Beschreibung: Mobilsicher.de nennt drei Tipps für den Urlaub mit Smartphone
Webcode: 2413

STATION 4

Fahrzeuge clever teilen und vernetzt unterwegs sein

Insbesondere in Großstädten haben sich im Zuge der digitalen Vernetzung neue und kreative Formen der Fortbewegung entwickelt, die uns auf eine Vielzahl von Verkehrsmitteln zurückgreifen lassen. Sharing Economy heißt wörtlich übersetzt „Wirtschaft des Teilens“ und bezeichnet im Bereich der Mobilität die gemeinschaftliche Nutzung von Fahrrädern, Rollern oder Autos. Das Prinzip ist so simpel wie praktisch: Ein Unternehmen stellt Fahrzeuge in einem bestimmten Einsatzgebiet zur Verfügung und Nutzer sowie Nutzerinnen können über eine App sehen, wo das nächste freie Fahrzeug bereitsteht. Dieses kann direkt über die App reserviert, freigeschaltet, entsichert und bezahlt werden. Nach Ende der Benutzung kann man das Fahrzeug einfach wieder im Einsatzgebiet abstellen. Sharing-Dienste können einerseits die Umwelt und den eigenen Geldbeutel schonen – andererseits werden Standortdaten minutiös an die Anbieterfirma übermittelt. Schauen Sie sich deswegen gut die Allgemeinen Geschäftsbedingungen (AGB) des Unternehmens und die erforderlichen Berechtigungen der entsprechenden App an, um zu klären, wann welche Daten zu welchem Zweck übermittelt und gespeichert werden und wer diese Daten einsehen und verwenden darf. Prüfen Sie auch unterschiedliche Preise. In der Regel ist das Ausleihen von E-Bikes teurer als das Ausleihen gewöhnlicher Fahrräder. Manche Anbieter verlangen auch eine Kaution oder eine Gebühr beim Überschreiten bestimmter Ortsgrenzen.

Linktipps

Wieso wir ein neues Verständnis von Kapazität im motorisierten Individualverkehr (Pkw) brauchen
Herausgeber: Martin Randelhoff
Beschreibung: Ein Artikel von Zukunft Mobilität zum Thema Effizienz von Ridesharing

Carsharing – Bleibt der Datenschutz auf der Strecke?
Herausgeber: intersoft consulting services AG
Beschreibung: Online-Artikel von datenschutzbeauftragter.info

Smart City: Intelligent vernetzter Verkehr
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Intelligente Fahrzeuge und vernetzter Verkehr: Die Zukunft der Mobilität stellt viele Fragen an IT-Sicherheit und Datenschutz

Eine Typologie der Mobilitätsgesellschaft von morgen
Herausgeber: ADAC e. V.
Beschreibung: Eine Studie des ADAC zeigt die verschiedenen Mobilitätstypen der Zukunft auf

Die Evolution der Mobilität
Herausgeber: ADAC e. V.
Beschreibung: Eine Studie des Zukunftsinstituts und des ADAC zur Mobilität im Jahr 2040

Die Zukunft der Mobilität
Herausgeber: FOX NETWORKS GROUP GERMANY GmbH
Beschreibung: Ein Artikel des „National Geographic“ zum Thema Mobilität in Städten der Zukunft

Webcode: 2414

Lernziel **Erfahren Sie mehr über die Vorteile der vernetzten Mobilität.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Fragen Sie in Ihrem Familien-, Freundes- oder Bekanntenkreis nach den Erfahrungen mit Carsharing, aber auch mit dem digitalen Teilen von E-Rollern oder Fahrrädern. Welche Erfahrungen wurden gemacht? Gab es Probleme? Was sind die Vorteile aus Sicht der Befragten?

2 Machen Sie den Check: Könnte Carsharing in Ihrem Leben zu einer Verbesserung führen? Ist es denkbar, bestimmte Wege mit dem E-Bike zu fahren oder den Roller zu nehmen? Welche Vor- oder Nachteile hätte Carsharing für Sie persönlich?

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Tauschen Sie sich über Ihre eigenen Erfahrungen aus: Welche Angebote der vernetzten Mobilität nutzen Sie bereits? Wo sehen Sie Vorteile einer vernetzten Verkehrswelt und wo lauern womöglich Sicherheitsrisiken? Erstellen Sie gemeinsam eine Liste der Vor- und Nachteile.

REFLEXION + VERTIEFUNG

UM MOBILITÄTSANGEBOTE SICHER UND SELBSTBESTIMMT ZU NUTZEN, LESEN SIE UNSERE EMPFEHLUNGEN IM KOMPETENZTEIL:

- Anbieter von Software und Apps vergleichen
  - **Kompetenzteil 2, Station 4 > Software auswählen und sicher einrichten**
- Sichere Bezahlverfahren verwenden
  - **Kompetenzteil 6, Station 2 > Online Geld bezahlen**
- Daten sparsam angeben
  - **Kompetenzteil 4, Station 3 > Datensparsamkeit**
- Accounts und Konten sicher anlegen
  - **Kompetenzteil 3 > Sichere Logins nutzen**
- Öffentliches WLAN sicher nutzen
  - **Kompetenzteil 1, Station 2 > Sichere Internet-einstellungen für unterwegs**

LEBENSWELT 5
Online sein in Haus und Freizeit

Vernetzung ist ein wesentliches Kennzeichen der Digitalisierung. Letztere erhält in Form des Internets der Dinge zunehmend Einzug in deutschen Haushalten: Seien es Sprachassistenten, die auf Zuruf den Wetterbericht vortragen, Smart-TVs, über die Sie Serien streamen, oder vernetzte Haushaltsgeräte, die automatisch Lebensmittel nachbestellen können. Doch trotz vieler Vorzüge dürfen das Bewusstsein für Datensicherheit sowie entsprechende Schutzmaßnahmen nicht auf der Strecke bleiben – gerade im eigenen Zuhause, wo zum Teil sehr persönliche Informationen preisgegeben werden können. Wie genau diese „smarten“ Alltagshelfer funktionieren, welchen Nutzen sie bringen, wie sie eingerichtet werden und wie Sie Onlinespiele zu Hause nutzen können, darüber klärt die digitale Lebenswelt „Online sein in Haus und Freizeit“ auf.

IN DER LEBENSWELT „ONLINE SEIN IN HAUS UND FREIZEIT“ LERNEN SIE,

- was das Internet der Dinge ist und wie ein Smart Home funktioniert,
- was digitale Sprachassistenten sowie Smart Toys sind,
- wie Sie herausfinden, welche Datenspuren Sie hinterlassen,
- was Sie bei Onlinespielen beachten sollten.

Die Übungen in den einzelnen Abschnitten ermöglichen es Ihnen auf einfache Weise, Ihr Wissen auch an andere weiterzugeben.

STATION 1

Im Smart Home leben

Das Internet der Dinge (oder Internet of Things, kurz IoT) steht für eine vernetzte Welt aus smarten Geräten. Ein smartes Gerät kann sich in der Regel mit anderen Geräten und dem Internet vernetzen sowie aus der Ferne gesteuert werden. Alle smarten Geräte zu Hause bilden das Smart Home. So können Sie beispielsweise mit einer vernetzten Haussteuerung einstellen, dass die Heizung beim Verlassen des Hauses automatisch heruntergeschaltet wird und sich umgekehrt wieder anschaltet, sobald Sie oder ein Familienmitglied sich dem Haus nähert. Haus- und Wohnungsschlösser können per Smartphone geschlossen oder geöffnet werden und Systeme erkennen automatisch, ob der Herd ab- oder die Waschmaschine angeschaltet wurde. Über Apps auf dem Tablet oder Smartphone können Sie die Systeme steuern – auch von unterwegs. Smart-Home-Systeme können nicht nur Zeit und Energie sparen, sondern eröffnen auch neue Möglichkeiten zum Beispiel für körperlich beeinträchtigte Menschen, die dadurch selbstbestimmter leben können.

Der Router ist meist der Knotenpunkt für die Kommunikation aller vernetzten Geräte zu Hause. Er wacht darüber, welche Daten das Heimnetzwerk verlassen und wer von außen Zugriff auf das Netzwerk erhält. Er verbindet Geräte untereinander sowie mit dem Internet. Ein sicherer Router ist somit das Fundament für die IT-Sicherheit zu Hause.
Smarte Geräte müssen geschützt werden, um fremde Zugriffe auf das eigene Netzwerk zu verhindern. Für sie gelten dieselben Risiken und Schutzmaßnahmen wie bei herkömmlichen internetfähigen Computern oder Smartphones. Das betrifft vor allem eine sichere Internetverbindung sowie den Schutz der einzelnen Geräte durch individuelle starke Passwörter und regelmäßige Updates (Softwareaktualisierungen), um Sicherheitslücken zu schließen ☞ **Kompetenzteil 1 > Sichere Internet-einstellungen und ☞ Kompetenzteil 2 > Geräte und Software sicher einrichten und pflegen**.

Wenn der Saugroboter die Wohnung kartiert oder man sich den Kühlschrankinhalt beim Einkaufen via App in Echtzeit anzeigen lässt, dann werden teils sehr persönliche Daten verarbeitet. Erkundigen Sie sich deswegen vor dem Kauf eines Gerätes, welche Daten gesammelt, gespeichert

und verarbeitet werden – zum Beispiel in den Allgemeinen Geschäftsbedingungen (AGB) und in der Datenschutzerklärung. Seien Sie insbesondere dann skeptisch, wenn eine Erhebung oder eine Verarbeitung persönlicher Daten stattfindet, jedoch nicht für die Ausführung der Dienste erforderlich ist **Kompetenzteil 2 > Geräte und Software sicher einrichten und pflegen**. Oftmals liegen die Daten in einer Cloud. Erkundigen Sie sich, wie diese geschützt werden **Kompetenzteil 2, Station 5 > Cloud-Nutzung abwägen**. Achten Sie außerdem darauf, dass Ihre vernetzten Geräte persönliche Daten, sofern notwendig, nicht unverschlüsselt versenden, denn Angreifer/-innen könnten diese Daten abfangen und auslesen.

Linktipps

Smart Home
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Das BSI hat die wichtigsten Sicherheitstipps zusammengefasst, auch als informatives Video.

Smart Home – Ist das sicher?
Herausgeber: Landeskriminalamt Niedersachsen
Beschreibung: Das LKA klärt ausführlich über Stolperfallen im Smart Home auf.

Vernetztes Wohnen
Herausgeber: iRights e. V.
Beschreibung: Das Projekt „ANNA – Das vernetzte Leben“ bietet unterhaltsame und informative Inhalte wie Kurzfilme und Podcasts zum vernetzten Zuhause.

Internet der Dinge: Sicheres Smart Home
Herausgeber: Deutschland sicher im Netz e. V.
Beschreibung: Der Online-Artikel beschreibt, wie wichtig IT-Sicherheit im intelligenten Zuhause ist.

Webcode: 2 5 1 1

Lernziel **Gestalten Sie Ihre digitale Zukunft – mit einem Smart Home. Wägen Sie Vor- und Nachteile ab.**

ÜBUNGEN
FÜR DIE EINZELARBEIT

REFLEXION

1. Versuchen Sie sich einen Tag in einem Smart Home vorzustellen: Welche automatischen Abläufe würden Sie sich wünschen? Recherchieren Sie, welche Ihrer Wünsche sich bereits jetzt realisieren lassen und welche (noch) nicht.

2. Welche Vor- und Nachteile hätten bestimmte Anwendungen, die es bereits jetzt schon gibt, wie zum Beispiel die Fernsteuerung der Waschmaschine per App? Welche Entlastungen, aber auch welche neuen Belastungen kämen auf Sie oder andere zu?

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Diskutieren Sie in Kleingruppen die Vor- und Nachteile eines vernetzten Zuhauses. Präsentieren und vergleichen Sie die Ergebnisse in der großen Gruppe. Gibt es unterschiedliche Einstellungen in den jeweiligen Kleingruppen?

2 Sammeln Sie in der Gruppe eine Liste von Gegenständen, die als Roboter Ihren Arbeitsalltag erleichtern könnten. Unter welchen Umständen würden Sie solche Roboter einsetzen?

REFLEXION

Digitale Sprachassistenten

Online unterwegs ohne eine Tastatur zu benutzen? Digitale Sprachassistenten sind Programme, die mithilfe von Künstlicher Intelligenz (KI) gesprochene Anweisungen erkennen und entsprechende Aktionen durchführen. Per Sprachbefehl können Sie unter anderem Suchanfragen im Internet stellen, aktuelle Nachrichten abrufen oder den Kalender aktualisieren und Erinnerungen setzen. Diese Systeme sind oft auch mit Komponenten der Unterhaltungselektronik vernetzt und steuern etwa die heimweite Nutzung von Video- und Audio-Inhalten, sodass Sie zum Beispiel über die Sprachsteuerung Ihre Lieblingsmusik wiedergeben können.

Linktipps

Was macht einen Sprachassistenten klug?
Herausgeber: iRights e. V.
Beschreibung: Auf der Seite „ANNA – Das vernetzte Leben“ finden sich Informationen darüber, wie Künstliche Intelligenz und maschinelles Lernen bereits in den Alltag eingezogen sind

Welche Daten sammeln Sprachassistenten?
Herausgeber: iRights e. V.
Beschreibung: Mögliche Sicherheitslücken der Sprachassistenten erklärt das Angebot „ANNA – Das vernetzte Leben“

Sprachassistenten: Sichere Einstellungen nutzen
Herausgeber: Surfen:ohne:Risiko
Beschreibung: Die pädagogischen Expert/-innen erklären anhand von Screenshots, wie man Sprachassistenten insbesondere für Kinder im Haushalt sicherer macht

Webcode: 2 5 1 2

Lernziel **Reflektieren Sie den Einsatz von Sprachassistenten.**

REFLEXION

ÜBUNGEN
FÜR DIE EINZELARBEIT

1 Gibt es in Ihrem Bekannten-, Freundes- oder Familienkreis jemanden, der einen digitalen Sprachassistenten nutzt oder nutzen Sie selbst einen? Wenn ja, wofür? Erstellen Sie anhand der Antworten eine Liste, welche Funktionen Sprachassistenten haben können. Ergänzen Sie diese durch eine Recherche im Internet.

ÜBUNGEN
FÜR SCHULUNGS-GRUPPEN

1 Diskutieren Sie in Kleingruppen die Vor- und Nachteile von digitalen Sprachassistenten. Wie könnten diese den Alltag erleichtern? Präsentieren und vergleichen Sie die Ergebnisse in der gesamten Gruppe. Gibt es unterschiedliche Einstellungen in den jeweiligen Kleingruppen?

Vernetztes Spielzeug

Smart Toys, also digital vernetzte Spielzeuge, zeichnen sich dadurch aus, dass sie ihre Umgebung erkennen und auf sie reagieren, indem sie mit Menschen, Tieren oder anderen digitalen Geräten interagieren. Es gibt sowohl Smart Toys, die sich mit dem Internet oder untereinander verbinden können, als auch solche, die offline funktionieren. Smarte Spielzeuge eröffnen neue Möglichkeiten des spielerischen Lernens. Sie greifen unter anderem auf das Internet als große Wissensdatenbank zu und können – mit entsprechender Unterstützung – Kinder frühzeitig an einen kompetenten Umgang mit der digitalen Welt heranführen.

Smartes Spielzeug im Kinderzimmer birgt allerdings auch gewisse Risiken: Die Geräte können ungewollt Gespräche aufzeichnen, die Aufschluss über regelmäßige Aufenthaltsorte sowie Gewohnheiten und Interessen von Kindern und anderen Familienmitgliedern geben. So werden möglicherweise Wünsche und Fantasien, welche Kinder mit ihrem Spielzeug teilen, aufgezeichnet und weitergegeben. Sind die Daten auf den Servern der Anbieter nicht ausreichend gesichert, besteht die Gefahr, dass bereits Kinder Opfer von Identitätsdiebstählen werden. Darüber hinaus kann über eine ungesicherte Verbindung, zum Beispiel über eine Bluetooth-Schnittstelle (erkennbar am entsprechenden Symbol), unter Umständen vernetztes Spielzeug von Dritten ferngesteuert oder missbraucht werden. Fremde könnten so Kontakt zu einem Kind aufnehmen. Um Ihre Familie und insbesondere Ihre Kinder zu schützen, empfiehlt es sich daher, vor einer Anschaffung genau zu prüfen, wie die drahtlosen Verbindungen abgesichert sind und welche Daten von wem zu welchen Zwecken aufgezeichnet und verarbeitet werden **Kompetenzteil 2 > Geräte und Software sicher einrichten und pflegen**.

Linktipps

Smarte Spielzeuge – Lernhilfen oder Spione?
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Infos zur Sicherheit von Smart Toys

Vernetztes Spielzeug – Datenschutzrisiko im Kinderzimmer
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Informationen über Risiken für die Privatsphäre von Kindern durch vernetztes Spielzeug

Vorsicht bei Smart Toys: Die Risiken von vernetztem Spielzeug
Herausgeber: Verbraucherzentrale Nordrhein-Westfalen
Beschreibung: Marktüberblick zu Sicherheitsrisiken von Smart Toys

(K)ein Kinderspiel?! Vernetztes Spielzeug birgt Risiken
Herausgeber: Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e. V. (vzbv)
Beschreibung: Die Marktwächter informieren auf ihrer Internetseite.

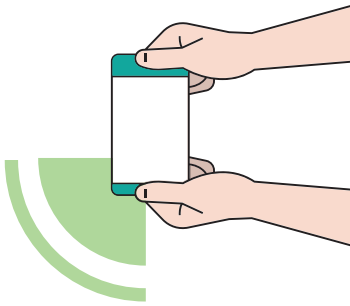
Webcode: 2 5 1 3

STATION 2

Im Netz spielen und Freizeit verbringen

Laut Jahresreport der deutschen Games-Branche 2019 spielen über 34 Millionen Menschen in Deutschland Computer- und Videospiele. So vielfältig wie die Spielerinnen und Spieler in diesem Bereich sind auch die verschiedenen Genres: Es gibt Abenteuer- und Rollenspiele, Kriegsspiele, Sport- und Bewegungsspiele, Singspiele, Knobelspiele, Gedächtnistraining und vieles mehr. Am populärsten ist aktuell das Spielen am Smartphone, gefolgt von der Konsole und dem Computer. Die meisten Spiele profitieren von einer Anbindung an das Internet. Das hat beispielsweise den Vorteil, dass Sie im Multiplayer-Modus mit anderen Menschen spielen oder dass Inhalte kontinuierlich erweitert und verbessert sowie Fehler überarbeitet werden können.

Spielen am Smartphone oder Tablet: Bei mobilen Endgeräten kaufen Sie die Spiele-Apps in den Stores der Hersteller. In manchen Fällen sind die Anwendungen kostenlos. Dann kann es aber sein, dass das heruntergeladene Spiel Werbung enthält oder dass Sie bestimmte Funktionen nur in Anspruch nehmen können, wenn Sie dafür innerhalb der App zahlen (In-App-Käufe).



Spielen an der Konsole: Bei Spielekonsolen haben Sie, ähnlich dem Computer, die Wahl zwischen Käufen in den digitalen Stores und dem Kauf von Datenträgern in einem Geschäft. Entscheiden Sie sich für den Kauf in einem digitalen Store, wird das Spiel, nachdem Sie den Kauf bestätigt haben, auf die Konsole heruntergeladen. Es kann, abhängig von Ihrem Internetanschluss, nach einigen Minuten bis Stunden gestartet werden. Bei physischen Datenträgern (wie Blu-ray-Discs) legen Sie den Datenträger in die Konsole ein und das Spiel wird installiert. Dieser Vorgang dauert oft nur wenige Augenblicke. Allerdings werden auch beim physischen Datenträger häufig aktuellere Daten für das Spiel aus dem Internet heruntergeladen. In den Erklärungen zum Spiel auf der Verpackung oder im Netz finden Sie bereits vor dem Kauf heraus, ob zum Starten des Spiels eine Internetverbindung notwendig ist.

Spielen am Computer: Computerspiele können auf Datenträgern (zum Beispiel DVDs oder Blu-ray-Discs) in Elektronikmärkten sowie über digitale Stores gekauft werden. Einige Hersteller und Plattformen bieten unterstützend auch Launcher an. Das sind Programme, die bei der Installation sowie beim Verwalten Ihrer Spieledaten unterstützen. Zudem können Launcher Ihnen durch das Herunterladen von Updates aus dem Internet dabei helfen, die Spieledaten aktuell zu halten.

EGAL, MIT WELCHEM GERÄT SIE ONLINE SPASS HABEN WOLLEN, ACHTEN SIE DARAUF, IHRE DATEN ZU SICHERN. IM KOMPETENZTEIL ERFAHREN SIE MEHR ZU DEN BASIS-EMPFEHLUNGEN:

- **Account schützen:** Für die meisten Computer- und Konsolenspiele benötigen Sie ein Benutzerkonto. Um die hinterlegten Zahlungsdaten oder weitere sensiblen Informationen Ihres Accounts zu schützen, sollten Sie ein sicheres Passwort hinterlegen **Kompetenzteil 2, Station 2 > Benutzerkonten sicher einrichten**. Achten Sie darauf, dass jeder Spiel-Account ein anderes Passwort bekommt. Bei der Verwaltung der verschiedenen Passwörter helfen beispielsweise Passwortmanager **Kompetenzteil 3, Station 2 > Einrichtung eines Passwortmanagers**.

- **Software aktuell halten:** Installieren Sie immer die aktuellen Updates für Geräte, Software und Spiele. Dies kann in den meisten Fällen sogar automatisch vom Gerät übernommen werden **Kompetenzteil 2, Station 1 > Software aktuell halten**.

- **Sicherer Download:** Informieren Sie sich beim Onlinekauf vorab über die Seriosität des Anbieters, damit Sie sich beispielsweise beim Download der Spieldateien nicht mit Schadsoftware infizieren. Laden Sie Spiele und andere Software nur aus vertrauenswürdigen Quellen wie den offiziellen Stores der Hersteller herunter. Nutzen Sie keinesfalls illegal bezogene Spiele, da diese ebenfalls Schadsoftware enthalten können **EXTRA 01: Schadprogramme**.

Linktipps

Jahresreport der deutschen Games-Branche 2019
Herausgeber: game – Verband der deutschen Games-Branche e. V.
Beschreibung: Der Dachverband der deutschen Games-Branche ermöglicht einen Gesamtblick auf die Videospiellandschaft in Deutschland

Digitale Spiele
Herausgeber: Klicksafe (EU-Initiative)
Beschreibung: Informationen sowie diverse Broschüren und Flyer unter anderem für Eltern, Schule, Kinder- und Jugendhilfe zum Download

Gaming für Senioren: Spiele trainieren das Gedächtnis
Herausgeber: Norddeutscher Rundfunk (NDR)
Beschreibung: Das Video des NDR stellt positive Wirkungen des Spielens für Seniorinnen und Senioren vor

Videospiele im Alter: Warum immer mehr Senioren spielen
Herausgeber: game – Verband der deutschen Games-Branche e. V.
Beschreibung: Der Dachverband der deutschen Games-Branche stellt „Silver Gamer“ und ihre Motive vor

Heart of Gaming – Mit Sicherheit gewinnen!
Herausgeber: Bundesamt für Sicherheit in der Informationstechnik
Beschreibung: Das BSI setzt sich mit Sicherheitsfragen bei Videospielen auseinander

Webcode: 2514

DAMIT SIE DAS DIGITALE ZUHAUSE SICHER NUTZEN KÖNNEN, LESEN SIE FOLGENDE EMPFEHLUNGEN IM KOMPETENZTEIL NACH:

- Router sicher einrichten

  Kompetenzteil 1, Station 1 > Sichere Interneteinstellungen für zu Hause

- Verständnis von vernetzter Haustechnik entwickeln

  Kompetenzteil 2, Station 6 > Das smarte Zuhause sicher einrichten

- Accounts und Konten sicher einrichten

  Kompetenzteil 2, Station 2 > Benutzerkonten sicher einrichten

- Spiele nur aus vertrauenswürdigen Quellen herunterladen

  Kompetenzteil 2, Station 4 > Software auswählen und sicher einrichten

- Für die Gefahren von Cybermobbing oder Cybergrooming sensibilisiert sein

  EXTRA 04: Belästigung und Beleidigung

Glossar

BEGRIFF	ERKLÄRUNG
Add-on	Kleine Erweiterung zum Browserprogramm, um bestimmte Funktionalitäten hinzuzufügen.
Account	Ein Account ist ein Benutzerkonto bei einem Dienste-anbieter, das eine Zugangsberechtigung erfordert.
Algorithmus	Definierte Handlungsvorschrift zur Lösung eines Problems oder einer bestimmten Art von Problemen. In der Infor-matik: Verarbeitungsvorschrift, die so eindeutig formuliert ist, dass sie durch ein maschinell ausführbares Programm wiedergegeben werden kann.
Antiviren-programm	Siehe Virenschutzprogramm.
App	Eine Applikation, kurz App, ist eine Anwendungssoftware. Der Begriff App wird oft im Zusammenhang mit Anwendun-gen für Smartphones oder Tablets verwendet.
Authentifizierung	Bei der Authentifizierung wird der bei der Authentisierung vorgelegte Identitätsnachweis einer Person überprüft. Erst nach erfolgreicher Authentifizierung erfolgt dann eine Autorisierung.
Authentisierung	Bei der Authentisierung legt eine Person einen Nachweis über ihre Identität vor, um ihn von einem System über-prüfen zu lassen. Dies kann u. a. durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen, die Authentisierung von Daten z. B. durch kryptographische Signaturen.

BEGRIFF	ERKLÄRUNG
Autorisierung	Bei der Autorisierung werden für eine bereits erfolgreich authentifizierte Person die ihr auf einem System eingeräumten Rechte freigeschaltet.
Avatar	„Virtueller Stellvertreter“, Grafik oder Animation, die im Internet – beispielsweise in Chatrooms – zur Darstellung einer Person genutzt wird.
Backup	Ein Backup ist eine Sicherung der Daten zum Schutz vor Datenverlust. Es werden dabei Kopien von vorhandenen Datenbeständen erstellt.
Bluetooth	Bluetooth ist ein Industriestandard für die Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik.
Browser	Der Browser ist ein spezielles Programm, um im Internet zu surfen. Das englische Wort „to browse“ bedeutet so viel wie „blättern“ oder „durchstöbern“.
Botnetz	Als Botnetz wird ein Verbund von Systemen bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind.
Cache	Pufferspeicher, der Daten schneller zur Bearbeitung bereitstellt. Zum Beispiel: Lokales Verzeichnis für beim Surfen im Internet besuchte Seiten, die so nicht neuerlich geladen werden müssen.
Chat	Über bestimmte Programme oder auf bestimmten Internetseiten ist mit dem Chat eine schnelle, direkte Kommunikation in Echtzeit möglich.
Cloud	Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Dabei wird nicht mehr auf die Rechenleistung oder den Speicher der eigenen Geräte zurückgegriffen, sondern die Rechenleistung eines Cloud-Anbieters genutzt.

BEGRIFF	ERKLÄRUNG
Cookie	Zeichenfolge, die mit einer Web-Seite vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird. Sinn ist, unter anderem Besucher wiederzuerkennen, so dass es beispielsweise nicht erforderlich ist, Nutzerdaten neu einzugeben.
Cybergrooming	Cybergrooming bezeichnet die Kontaktaufnahme von Erwachsenen zu Kindern und Jugendlichen über das Internet mit dem Ziel, sexuelle Handlungen oder Kontakte anzubahnen.
Cybermobbing	Cybermobbing steht für verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen über das Internet. Das Opfer wird durch aggressive oder beleidigende Texte, kompromittierende Fotos oder Videos angegriffen oder der Lächerlichkeit ausgesetzt.
Cyberstalking	Cyberstalking (auch Digital Stalking oder Onlinestalking) bezeichnet das Nachstellen, Verfolgen und auch Überwachen einer Person mit digitalen Hilfsmitteln. Dies geschieht insbesondere in Beziehungen, beispielsweise überwacht ein Partner seinen aktuellen Partner oder Ex-Partner.
Datenleak	Bei einem Datenleak geraten Daten in falsche Hände. Cyberkriminelle können über eine kompromittierte Webseite an diese Daten kommen oder über eine Panne, bei der ein Unternehmen die sensiblen Daten ungeschützt aufbewahrt. Teilweise werden die sensiblen Daten dann auch veröffentlicht. Leak heißt auf Deutsch „undichte Stelle“.
Datensicherung	Siehe Backup.

BEGRIFF	ERKLÄRUNG
DoS-/DDoS-Angriffe	Denial-of-Service-Angriffe, kurz DoS, richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.
Download	Übertragung von Daten von einem fremden Rechner auf den eigenen Rechner, zum Beispiel die aktuelle Version des eigenen Browsers aus dem Internet.
Doxing	Beim so genannten Doxing sammeln Täter/-innen personenbezogene Daten, die sie bündeln und öffentlich verfügbar machen.
Echokammer-Effekt	Siehe Filterblase.
E-Mail	Elektronische Post.
Fake News	Fake News sind Falschmeldungen, die teils irrtümlich, teils bewusst im Internet verbreitet werden, insbesondere in den sozialen Medien.
Fake-Shops	Fake-Shops bezeichnen gefälschte Internet-Shops, hinter denen sich Betrüger bzw. Betrügerinnen verbergen. Nach Erhalt der Bezahlung wird keine Ware ausgeliefert.
Filterblase	Filterblase beschreibt einen Effekt aus den Medienwissenschaften: Weil Webseiten oder soziale Netzwerke versuchen, algorithmisch vorauszusagen, welche Informationen der Benutzer oder die Benutzerin auffinden möchte, werden vermehrt Inhalte gezeigt, die der eigenen Meinung entsprechen. Das führt dazu, dass Leser nicht mehr mit Informationen konfrontiert werden, die den bisherigen Ansichten widersprechen. Auf diese Weise können die eigenen Auffassungen auch nicht mehr überprüft und eventuell relativiert werden.

BEGRIFF	ERKLÄRUNG
Firewall	Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen Netzwerk und dem externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden, wie die, die hinein wollen.
GPS	GPS steht für „Global Positioning System“. Es handelt sich um ein globales Navigationssatellitensystem zur Positionsbestimmung.
Hoax	Der Begriff Hoax bezeichnet eine Falschmeldung (Gerücht oder Scherz), die über E-Mail, Messenger-Programme, SMS oder MMS verbreitet wird.
http	Die Abkürzung steht für Hypertext Transfer Protocol und bezeichnet ein Übertragungsprotokoll für Webseiten.
https	Die Abkürzung steht für Hypertext Transfer Protocol over SSL und bezeichnet ein Protokoll zur verschlüsselten Übertragung von Webseiten.
Instant Messenger	Siehe Messenger.
Internet der Dinge	Im Gegensatz zu „klassischen“ IT-Systemen umfasst das Internet der Dinge „intelligente“ Gegenstände, die zusätzliche „smarte“ Funktionen enthalten. Diese Geräte werden in der Regel an Datennetze angeschlossen, in vielen Fällen drahtlos, und können sogar oft auf das Internet zugreifen und darüber erreicht werden.
Internet of Things (IoT)	Siehe Internet der Dinge.
IP-Adresse	Eine Adresse, unter der ein Rechner innerhalb eines Netzwerks nach dem Internetprotokoll erreichbar ist. Eine IP-Adresse besteht aus vier Byte, die durch Punkte getrennt sind: z. B. 194.95.179.205.

BEGRIFF	ERKLÄRUNG
Junk/Junk-Mail	Bedeutet übersetzt „Abfall-Mail“. Als Junk-Mails bezeichnet man Massenmails, die einem Empfänger ungewollt zugestellt werden und meistens Werbeangebote enthalten.
LAN	LAN steht für Local Area Network und bezeichnet ein lokales Netz. So wird beispielsweise das hausinterne Netz eines Unternehmens genannt.
Leak	Siehe Datenleak.
Login	Anmeldevorgang für die Nutzung eines PC, von einzelnen auf dem PC installierten Programmen oder von Online-diensten.
Malware	Siehe Schadprogramm.
Messenger	Instant-Messaging bedeutet „sofortige Nachrichtenüber-mittlung“. Ein Messenger ist ein Service für Online-Chats und das Versenden kurzer Nachrichten. Dabei ist vorab keine Verabredung nötig – die Anwesenheit von Gesprächs-partnern/-innen wird automatisch signalisiert.
NFC	NFC steht für Near Field Communication und ermöglicht unter anderem das kontaktlose Zahlen. Durch die NFC ist es möglich, auf sehr kurze Distanz kleine Datenmengen zu übertragen. Dazu zählen Zugangs-, Bezahldaten oder Daten-pakete, die beispielsweise Passwörter oder andere Codes enthalten.
Onlinebanking	Bankgeschäfte (z. B. Überweisungen oder Aktienhandel) über das Internet.
Passwortmanager	Programm, beispielsweise als Bestandteil eines Internet-browsers, das bei der Verwaltung von Passwörtern hilft und diese archiviert. Es unterstützt dabei, für jeden Dienst ein seperates Passwort zu nutzen.

BEGRIFF	ERKLÄRUNG
Patch	Ein Patch („Flicken“) ist ein Softwarepaket, mit dem Softwarehersteller Sicherheitslücken in ihren Programmen schließen oder andere Verbesserungen integrieren.
Patch-Management	Als Patch-Management bezeichnet man Prozesse und Verfahren, die helfen, verfügbare Patches für die IT-Umgebung möglichst rasch erhalten, verwalten und einspielen zu können.
Phishing	Das Wort setzt sich aus „Password“ und „Fishing“ zusammen, zu Deutsch „nach Passwörtern angeln“. Beim Phishing wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen.
PIN-/TAN-Verfahren	Verfahren zur Authentisierung, besonders beim Onlinebanking. Hierbei sind für den Zugang zum Konto neben der Konto- oder Kundennummer die geheime PIN (Personal Identification Number) und für Transaktionen (z. B. Überweisungen) zusätzlich eine TAN (Transaktionsnummer) anzugeben.
Plug-in	Ein Plug-in ist eine Zusatzsoftware oder ein Softwaremodul, das in ein Computerprogramm eingebunden werden kann, um dessen Funktionalität zu erweitern.
Ransomware	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom“) wieder freigeben.
Router	Der Router verbindet das Heimnetzwerk und das Internet. Er bildet den Knotenpunkt für die Kommunikation der internetfähigen Geräte und verbindet neben dem Computer auch den smarten Fernseher und teilweise die intelligente Haustechnik mit dem Internet.

BEGRIFF	ERKLÄRUNG
Schadprogramme	Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Sie bezeichnen Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen.
Server	Typischerweise bezeichnet ein Server einen Rechner, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.
Signatur	Eine digitale Signatur (=Unterschrift) besteht aus Daten in elektronischer Form. Die Signatur wird an andere elektronische Daten angehängt, um den Verfasser bzw. die Verfasserin von Informationen klar zu identifizieren und zu belegen, dass die Daten nach dem Signieren nicht mehr verändert wurden. Dokumente, Programme usw. können signiert werden.
Social Engineering	Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren.
Software	Sammelbegriff für Betriebssysteme, Anwendungs- und Dienstprogramme.
Spam	Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden.
Streaming	Streaming (englisch „strömen“) bezeichnet das Abspielen von Video- und Audioinformationen, ohne sie dauerhaft auf dem Gerät zu speichern. Das Streaming wird durch eine spezielle Software (Plug-ins oder Wiedergabeprogramme) ermöglicht, die in der Regel kostenlos angeboten werden. Durch Streaming gelangen Videobilder und -töne live auf den Bildschirm des Computers.

BEGRIFF	ERKLÄRUNG
Suchmaschine	Eine Suchmaschine ermöglicht die Recherche von Inhalten, die im Internet oder in einem Computer gespeichert sind.
TAN	Siehe PIN-/TAN-Verfahren.
Update	Neue Version bzw. Ergänzung einer Software, die Programmmängel korrigiert oder Programmverbesserungen enthält. Updates werden in der Regel in elektronischer Form zum Herunterladen aus dem Internet zur Verfügung gestellt.
URL	Eine URL gibt eine Adresse im Internet an. Sie besteht aus dem Protokoll (z. B. http://), dem Rechnernamen (z. B. www.bund.de) und ggf. auch aus der Angabe des Ports (z. B. :80) und der Pfadangabe (z. B. /startseite.html).
USB-Stick	Mobiles Speichermedium, das an den USB-Port angeschlossen wird.
Virenschutzprogramm	Ein Virenschutzprogramm überprüft neue Dateien (zum Beispiel Anhänge von E-Mails) und den gesamten Computer auf Schadsoftware. Dazu vergleicht es in erster Linie die Daten auf dem Rechner mit den „Fingerabdrücken“ bekannter Schadprogramme.
VPN	VPN steht für Virtual Private Network. Es verschlüsselt die Datenkommunikation zwischen zwei Endpunkten – zum Beispiel zwischen einem Endgerät und einem VPN-Server. Auf diese Weise kann die Kommunikation nicht ohne weiteres mitgelesen oder verändert werden.
Webbrowser	Siehe Browser.
WLAN (Wireless Local Area Network)	WLAN steht für Wireless Local Area Network und bezeichnet drahtlose Funknetzwerke, die kabelfreie Kommunikation zwischen mehreren lokalen Computern ermöglichen. Es wird häufig genutzt, um unterwegs mit dem Computer oder Smartphone ins Internet zu gehen.

BEGRIFF	ERKLÄRUNG
Zwei-Faktor-Authentisierung	Die Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Faktoren aus den drei Bereichen Wissen (zum Beispiel Passwort), Besitz (zum Beispiel Chipkarte) und Biometrie (zum Beispiel Fingerabdruck).