Kommunikation im Netz

MODUL 07

verbraucherzentrale Berlin

SMART SURFER

Fit im digitalen Alltag

Lernhilfe für aktive Onliner:innen

Gebündelte Kompetenz rund um die Themen: Datensicherheit, Verbraucherschutz, Digitalisierung, Unterhaltung und digitale Ethik

Seit 2011 bietet das medienpädagogische Ausbildungskonzept „Silver Surfer – Sicher online im Alter“ eine digitale Grundbildung für aktive Onliner:innen. 2020 wurde das Konzept neu aufgelegt. Dafür sind einzelne Themenbereiche erheblich erweitert und einige neue hinzugefügt worden. Zusätzlich wurde auch der Titel der Lernhilfe angepasst: „Smart Surfer – Fit im digitalen Alltag“.

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ wurde gemeinsam von Mitarbeiter:innen der Verbraucherzentrale Rheinland-Pfalz e.V., der Medienanstalt Rheinland-Pfalz, des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz und der Stiftung MedienKompetenz Forum Südwest sowie der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der Katholischen Hochschule Mainz erstellt.

verbraucherzentrale Rheinland-Pfalz

Medienanstalt Rheinland-Pfalz

Der Landesbeauftragte für den DATENSCHUTZ und die INFORMATIONSFREIHEIT Rheinland-Pfalz

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST STIFTUNG

Katholische Hochschule Mainz
Clearingstelle Medienkompetenz

Das Projekt wird gefördert durch:

RheinlandPfalz
MINISTERIUM FÜR FAMILIE, FRAUEN, KULTUR UND INTEGRATION

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz

Baden-Württemberg
MINISTERIUM FÜR LÄNDLICHEN RAUM UND VERBRAUCHERSCHUTZ

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

LAND BRANDENBURG
Ministerium für Soziales, Gesundheit, Integration und Verbraucherschutz

LFK: Die Medienanstalt für Baden-Württemberg

BERLIN
Senatsverwaltung für Justiz, Verbraucherschutz und Antidiskriminierung

Wie Sie diese Lernhilfe benutzen

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ bietet viele Informationen rund um das Thema Internet. Sie soll gleichzeitig als Nachschlagewerk dienen.

Seit dem Jahr 2020 wird die Lernhilfe in digitaler Form angeboten. Sie können die PDF-Dateien zu den einzelnen Modulen über Ihren PC/Laptop sowie Ihr Tablet nutzen.

In einer PDF-Datei können Sie gezielt nach Stichwörtern suchen. Mit einem Klick auf eine Internetadresse gelangen Sie direkt auf die jeweilige Website, vorausgesetzt, Sie lesen dieses PDF über ein internetfähiges Gerät. Natürlich können Sie sich diese PDF-Datei ausdrucken. Weitere Informationen zum Thema „Wie nutze ich ein PDF?“ finden Sie unter:
www.silver-tipps.de/was-bedeutet-eigentlich-pdf

Die Lernhilfe „Smart Surfer – Fit im digitalen Alltag“ besteht aus 9 Modulen:

- Modul 1: Was ist das Internet?
- Modul 2: Wie man das Internet nutzt
- Modul 3: Unterhaltungsmöglichkeiten im Internet
- Modul 4: Wie man Risiken im Netz vermeidet
- Modul 5: Die Welt des mobilen Internets
- Modul 6: Datenschutz im Internet
- **Modul 7: Kommunikation im Netz**
- Modul 8: Soziale Medien im Netz
- Modul 9: Ein Blick in die Zukunft des Internets

Mehr Informationen zum Projekt „Smart Surfer“ und alle PDF-Dateien zum Download finden Sie unter: *www.verbraucherzentrale-berlin.de/smart-surfer-be*

Alle Informationen der Lernhilfe haben wir nach bestem Wissen und Gewissen geprüft.
Wir freuen uns stets über kritische Anmerkungen, die helfen, diese Lernhilfe noch besser zu machen. Sie möchten Kritik äußern? Dann zögern Sie nicht, uns zu kontaktieren (per E-Mail an: smartsurfer@vz-bln.de).

In der Lernhilfe finden sich unterschiedliche Symbole:

Weiterführendes: Das entsprechende Thema wird an einer anderen Stelle der Lernhilfe erneut aufgegriffen und umfangreicher dargestellt.

Silver Tipps: Auf der Onlineplattform *www.silver-tipps.de* finden sich viele weiterführende Informationen rund um das Thema Sicherheit im Internet.

Link: Über die eingefügten Links sind weiterführende Informationen und andere Internetquellen zum Thema zu finden.

Fakt: Interessante Fakten werden im Text gesondert hervorgehoben.

Paragraf: Wer sich im rechtlichen Bereich weiterführend informieren will, findet an dieser Stelle die genauen Gesetzesbezeichnungen.

Begriffe, die mit einem Pfeil (➔) markiert sind, werden im Anschluss an den Text in einem Glossar näher erläutert.

Gender-Hinweis: Gendergerechte Sprache ist ein wichtiges Thema. Deshalb wurde in der Lernhilfe mit der Gender-Schreibweise der Verbraucherzentrale Berlin gearbeitet und der Gender-Doppelpunkt (:) genutzt, um alle Leser:innen gleichermaßen anzusprechen.

MODUL 07

Kommunikation im Netz

Das Internet steckt voller Kommunikationsmöglichkeiten. Wir können mit Freund:innen und Familie E-Mails austauschen, über Messenger kommunizieren und videotelefonieren. Nicht zuletzt die Corona-Pandemie zeigte wieder, wie wichtig digitale Teilhabe für alle Altersgruppen ist. Denn durch das Internet konnte man auch in Zeiten des Social Distancings miteinander in Verbindung bleiben. Über Messenger wurde Nachbarschaftshilfe organisiert und Videotelefonie bot eine Möglichkeit, die Verwandtschaft zu sehen, ohne sich gegenseitig dem Risiko einer Ansteckung auszusetzen.

Welche Kommunikationsmöglichkeiten bietet das Netz und welche passen am besten zu Ihnen? Was hat es mit Fake News auf sich? Und wie schützen Sie sich vor sogenanntem digitalen Stress? Das und mehr erfahren Sie im Modul 7. Im Interview spricht Anne Spiegel, Ministerin für Familie, Frauen, Jugend, Integration und Verbraucherschutz Rheinland-Pfalz, außerdem über ihre persönliche Einstellung zu den heutigen digitalen Kommunikationsmöglichkeiten.

Pro Sekunde werden ca. 3 Mio E-Mails versendet.

Das Internet in Zahlen: https://s.rlp.de/1hlL0

7.1 E-Mailing

Neben dem Surfen im World Wide Web ist das Senden und Empfangen von E-Mails nach wie vor einer der am häufigsten genutzten Dienste im Internet. Weltweit werden pro Sekunde etwa drei Millionen E-Mails versendet (Stand 2020). Der Grund: Mit einer E-Mail kann man die adressierte Person jederzeit kontaktieren und neben Texten in unbegrenzter Länge auch Anhänge wie Bilder, Videos und Dokumente beifügen. Eine E-Mail erreicht den:die Empfänger:in meist innerhalb weniger Sekunden, auch wenn diese Person gerade nicht online ist.

Die digitale Post: Wie funktioniert der E-Mail-Verkehr?

Damit eine E-Mail ihre:n Absender:in verlassen und ihre:n Empfänger:in erreichen kann, benötigt man auf beiden Seiten eine Art elektronischen Briefkasten, auf Englisch → „Mailbox“ genannt. Dafür sucht man sich einen Anbieter wie beispielsweise web.de, gmail.com oder t-online.de und richtet dort ein E-Mail-Konto ein. Bei der notwendigen Registrierung verlangen die Anbieter neben Angaben wie Name, Adresse und Telefonnummer auch die Vergabe eines → Passworts, mit dem man in Zukunft auf seine Mailbox zugreifen kann. Für den Fall, dass die Zugangsdaten verloren oder vergessen werden, kann meist eine zweite E-Mail-Adresse oder eine Telefonnummer hinterlegt werden, über die das Konto dann wiederhergestellt werden kann. Wie viele Daten man bei der Kontoeröffnung preisgeben möchte, entscheidet die oder der Einzelne. Der Name mag hier durchaus noch sinnvoll sein, allerdings sind Adress- und Telefonangaben sowie das echte Geburtsdatum nicht unbedingt erforderlich. Ein wenig Erfindungsreichtum schützt die privaten Daten meist am sichersten.

Technisch betrachtet ist die E-Mail eine digitale Datenübertragung von einem Standort zum anderen. Benötigt werden hierbei neben einer bestehenden Internetverbindung Protokolle wie POP3, IMAP und SMTP. Diesen Abkürzungen begegnet man beispielsweise, wenn man Hilfsdienste zum Abrufen der E-Mails wie Outlook oder Thunderbird einrichten möchte. Jede E-Mail-Adresse ist einzigartig und existiert nur einmal. Ähnlich wie eine Webadresse setzt sie sich aus bestimmten Bestandteilen zusammen.

Der Weg einer E-Mail: https://s.rlp.de/3Lmu4

name	@	anbieter.de	
Name	Trenn-zeichen	Domäne	Domänen-endung

Aufbau einer E-Mail-Adresse

Bei E-Mail-Adressen wird nicht zwischen Groß- und Kleinschreibung unterschieden. Umlaute wie „ä“ werden meist zu „ae“ usw. Mittlerweile können jedoch auch Umlaute in E-Mail-Adressen verwendet werden – es gilt allerdings zu bedenken, dass diese auf ausländischen Tastaturen unter Umständen nicht vergeben sind.

Zugriff auf E-Mail-Konten

Modul 2.2: Der Browser

Es gibt verschiedene Arten, auf das eigene E-Mail-Konto zuzugreifen. Der einfachste Zugriff erfolgt direkt über einen Internetbrowser auf der jeweiligen Webseite des Anbieters. Abgesehen vom Browser ist bei dieser Variante keine separate Software erforderlich. Der Zugriff ist außerdem geräteunabhängig, funktioniert also sowohl auf jedem PC und Laptop als auch auf mobilen Geräten wie Smartphones oder Tablets. Alles, was gebraucht wird, ist die Eingabe der Zugangsdaten. Diese Zugriffsart ist besonders geeignet für Nutzer:innen, die eher gelegentlich Nachrichten empfangen und verschicken und wenig Wert auf detaillierte Verwaltungsoptionen für ihr Postfach legen.

Vielschreiber:innen, die ihre E-Mails gerne verwalten und mit mehreren Geräten arbeiten, sind mit einem E-Mail-Verwaltungsprogramm gut beraten. Ob man sich für eine kostenlose oder eine kostenpflichtige Variante entscheidet, hängt von den eigenen Bedürfnissen und Vorlieben ab.

Kostenlose Programme sind teilweise werbefinanziert (t-online.de, gmail.com, web.de, gmx.de etc.), das heißt, sie müssen zwar nicht gekauft werden, finanzieren sich aber durch Werbung, die den Nutzer:innen eingeblendet wird. Zudem bieten solche Programme oft weniger Funktionen als kostenpflichtige, wie etwa das Erstellen beliebig vieler Unterordner, das Einrichten von Zugangspasswörtern und von regelmäßigen Sicherheitskopien (sogenannten Back-ups) oder E-Mail-Verschlüsselungen. Einige Programme kommen zwar ebenfalls mit begrenzten Funktionalitäten, aber immerhin ohne Werbeeinblendungen aus, wie zum Beispiel Windows Live Mail und Thunderbird.

Mit Blick auf deutsche beziehungsweise europäische Datenschutzgesetze gilt, dass meist nur deutsche Anbieter garantieren, dass die Daten auch ausschließlich auf deutschen Servern gespeichert werden. Wichtig ist heutzutage, dass bei der Auswahl der E-Mail-Programme sowohl die Nutzung auf dem Computer als auch auf den mobilen Geräten mitgedacht wird. Aktuelle Nutzerzahlen zeigen, dass immer mehr Menschen vor allem auf dem Smartphone E-Mails schreiben.

Im Ergebnis lässt sich festhalten: Wer großen Wert auf vielfältige Verwaltungsoptionen legt und frei von Werbeeinblendungen arbeiten möchte, dem ist die Nutzung kostenpflichtiger Dienste anzuraten, wie beispielsweise Outlook, das in Microsoft 365 enthalten ist oder einzeln bezogen werden kann. Zu diesem Ergebnis kommt auch die Stiftung Warentest, die die Anbieter mailbox.org und Posteo als Testsieger auszeichnete. Egal ob kostenfreier oder kostenpflichtiger Dienst, stets empfiehlt es sich, verschiedene Anbieter zu vergleichen und insbesondere, deren Seriosität zu prüfen.

Tipp

Die Stiftung Warentest testet im Jahr Tausende Produkte. Dazu nimmt sie Dienstleistungsuntersuchungen, Schnelltests und Marktübersichten vor und erstellt untersuchungsgestützte Reporte: *www.test.de*

Sicherheitseinstellungen

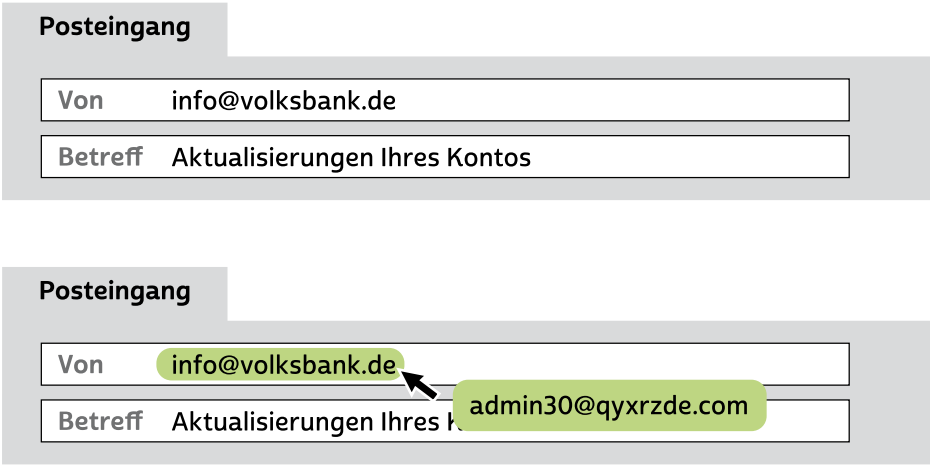
Diese Einstellungen helfen, unerwünschte Nachrichten wie sogenannte Spam- oder Junk-Mails herauszufiltern. Diese weisen etwa auf günstige, aber gefälschte Pharmaprodukte hin, versprechen dubiose Gewinne und locken mit fragwürdigen Reiseangeboten. Es gibt Angaben, nach denen fast sieben von zehn weltweit versandten E-Mails elektronischer Müll sind.

Tipp

Für alle E-Mails mit unbekanntem oder nicht vertrauenswürdigem Absender gilt: Löschen! Und auf keinen Fall angegebene Links anklicken!

Ein Link ebenso wie ein:e E-Mail-Absender:in können sich auch anders nennen, als sie tatsächlich heißen. Denn der:die Absender:in einer E-Mail hat die Möglichkeit, im Postfach die eigentliche Adresse zu verschleiern und so zu tun, als handle es sich um eine reguläre E-Mail, zum Beispiel die eines Kundenservice.

Das Gleiche gilt bei Internetadressen. So kann sich hinter einer angegebenen Bankadresse eine völlig andere Internetadresse verstecken, die aber in ihrer grafischen Darstellung der Originalseite sehr ähnelt. Wenn diese Seite nun ein Log-in hat und nach Anmeldedaten fragt, können Benutzernamen und Passwörter in die falschen Hände gelangen. Man spricht in solchen Fällen von Phishing, da die Daten wortwörtlich „abgefischt“ werden.



Gängiges Beispiel für gefälschte E-Mail-Adressen

Je nach E-Mail-Anbieter gibt es unterschiedlich zu bedienende und unterschiedlich wirksame Methoden, sich vor dieser unerwünschten Post zu schützen. In der Grundeinstellung arbeitet bei aktiviertem Spam-Filter ein Algorithmus, der E-Mails anhand bekannter Auffälligkeiten (bereits gemeldete Absenderadresse, massenhafte Verwendung von Großbuchstaben und Sonderzeichen, reißerische Aussagen etc.) herausfiltert und in einen gesonderten Junk- oder Spam-Ordner verschiebt. Um unerwünschte E-Mails in einen solchen Ordner aufzunehmen, markiert man sie mit den Funktionen „Als Spam markieren“, „Als Junk melden“ oder „Zum Spam hinzufügen“ und verschiebt sie. Auch in Zukunft wird dann keine E-Mail von diesem:dieser Absender:in mehr in den Posteingang gelangen. Allerdings gibt es eine unbegrenzte Anzahl an Absenderadressen, weshalb Werbetreibende und Kriminelle immer wieder neue Spam-E-Mails versenden können, die

dann nicht erkannt werden. Ein Spam-Filter kann allerdings auch dazu führen, dass „normale“ E-Mails fälschlicherweise im Spam-Ordner landen. Ein prüfender Blick in den Spam-Ordner von Zeit zu Zeit kann also nicht schaden.

Was ist an Spam gefährlich?

Grundsätzlich ist der reine Erhalt von Spam nicht gefährlich. Dennoch können Links und Anhänge in solchen E-Mails Risiken bergen. Beispielsweise kann der Absender die Empfängerin auffordern, einen im Text angegebenen Link anzuklicken und sich die dortige Information anzuschauen. Durch einen einfachen Klick können jedoch nicht nur Webseiten geöffnet, sondern auch Programme gestartet werden, die weitere Software installieren oder Sicherheitseinstellungen außer Kraft setzen. Im schlimmsten Fall holt man sich so Schädlinge auf den heimischen Computer, die auch von Virenscannern nicht erkannt werden.

Tipp

Niemals bei verdächtigen E-Mails Anhänge öffnen!

Gerade bei Anhängen ist Vorsicht geboten: Hinter einer harmlosen Bezeichnung kann sich wiederum Schadsoftware verstecken, zum Beispiel eine ausführbare Datei (mit „.exe“ als Dateiendung). Selbst als Bilder oder andere Dateitypen getarnte Anhänge können Risiken beinhalten, wenn sie geöffnet werden. Nicht selten locken Kriminelle gezielt mit dringlich erscheinenden Beschreibungen, auf die man aber nicht hereinfallen sollte. So wird etwa im Text einer E-Mail, die angeblich von einem Inkassodienst oder der Polizei stammt, eine erfundene hohe Summe gefordert, für deren Legitimation man die angehängte Rechnung lesen solle. In solchen und vergleichbaren Fällen sollten die E-Mails einfach gelöscht und niemals die Anhänge geöffnet werden.

Tipp

Bringen Sie bei der Wahl des Anbieters schon vorher in Erfahrung, wie man seine Daten und sein Konto einfach, sicher und kostenfrei wieder löschen kann.

Eine weitere Tücke der E-Mail-Nutzung beinhaltet das Löschen des gesamten Benutzerkontos. Im Gegensatz zur Kontoerstellung, die gut sichtbar auf der Hauptseite platziert ist, muss für eine Kontolöschung oft umständlich ein (häufig kostenpflichtiger) Anruf getätigt oder das Kleingedruckte gelesen werden.

Virenbefall, Trojaner-Angriff und Co.

Modul 5.7: Back-ups

Um Computerschädlingen wie Viren, Trojanern und Würmern vorzubeugen, helfen regelmäßige Sicherheitskopien und ein Antivirenprogramm. Ein solches sollte generell installiert sein und immer auf dem neuesten Stand gehalten werden. Es gibt viele unterschiedliche Anbieter auf dem Markt, einige hiervon bieten „abgespeckte“ Varianten ihrer Software mit einem geringeren Funktionsumfang kostenlos zur Nutzung an. Wer mehr Funktionen haben möchte, muss die kostenpflichtige Vollversion erwerben.

Ob kostenlose oder kostenpflichtige Anwendung – einen hundertprozentigen Schutz gegen Viren, Trojaner und Würmer gibt es nicht. Allerdings kann man es digitalen Schädlingen zumindest sehr schwer machen, Schaden auf dem Computer anzurichten. Sicherheit bedarf regelmäßiger Kontrolle von Sicherheitseinstellungen, tagesaktuellen Updates von Antivirensoftware und häufigen Aktualisierungen des Betriebssystems.

Verschlüsselung

Normalerweise lässt sich eine E-Mail mit einer Postkarte vergleichen: Ohne großen Aufwand kann sie gelesen und ausgewertet werden. Sicherer wird die E-Mail durch Verschlüsselung. Dabei wird der Klartext in einen unkenntlichen Text umgewandelt. Beim Entschlüsseln wird aus dem unleserlichen Text wieder der Klartext. Um das Mitlesen des E-Mail-Verkehrs im Internet zu verhindern, beispielsweise wenn

man häufig unsichere Netzwerke wie das WLAN in Hotels oder Cafés nutzt, ist die Nachrichtenverschlüsselung ein gutes Mittel. Meist muss die Verschlüsselung manuell aktiviert werden, bei einigen E-Mail-Anbietern wird sogar automatisch verschlüsselt.

Die eigenen E-Mails wirklich gründlich zu schützen, ist allerdings leider immer noch relativ kompliziert. Nur wenige Dienste und Programme, die zuverlässig verschlüsseln, sind auch einfach in der Anwendung.

Kostenloses oder kostenpflichtiges E-Mail-Programm?

Mit kostenlosen E-Mail-Programmen kommt man schon sehr weit. Wer jedoch keine Werbung, mehr Funktionalitäten und ein hohes Datenschutzniveau möchte, greift besser auf kostenpflichtige Dienste zurück. Vor der Auswahlentscheidung sollte man sich angemessen mittels seriöser Testberichte informieren, etwa bei der Stiftung Warentest.

Mit Blick auf den Schutz vor Kriminellen und Schadsoftware im Postfach gilt: Besonders wichtig ist ein aufmerksames und überlegtes Verhalten im Internet. So sollten beispielweise Links in E-Mails oder Downloads nur angeklickt werden, wenn man sich über die Echtheit der E-Mail und die Seriosität des:der Absenders:in wirklich sicher ist. Aus gleichem Grund empfiehlt sich eine gesunde Portion Misstrauen gegenüber E-Mail-Anhängen von unbekannten Absender:innen.

Im Zweifel gilt die Grundregel, dass man, wenn man den:die Absender:in nicht mit ausreichender Sicherheit identifizieren kann, lieber davon ausgeht, dass es sich um eine Schad-E-Mail handelt, die man ignoriert oder löscht. Soll die E-Mail vorgeblich von einem:einer seriösen Absender:in stammen, man ist sich aber nicht sicher, so kann man bei der Person nachfragen, ob diese die fragliche E-Mail versandt hat. Leider kommt es immer wieder vor, dass Kriminelle Accounts (E-Mail-Konten, aber auch Social-Media-Profile und Messenger-Konten) von Personen knacken und fälschlicherweise im Namen dieser Personen agieren. Wenn man also eine E-Mail von einer bekannten Person bekommt, die man als fragwürdig empfindet, sollte man der Person sicherheitshalber auf anderem Weg eine Textnachricht zukommen lassen, beispielsweise über einen Messenger-Dienst.

7.2 Instant Messenger

Das Internet bietet Nutzer:innen einzigartige Möglichkeiten, mit anderen zu kommunizieren. Neben der klassischen E-Mail kann man sich über Instant Messenger mit Freund:innen und Bekannten austauschen, Urlaubsbilder verschicken oder Geburtstage organisieren und vieles mehr.

WhatsApp, Threema, Signal und Co.

Von unterwegs aus ein Foto an Freund:innen und Bekannte schicken, sich mit den Kindern und Enkel:innen in einer Familiengruppe über das anstehende Wochenende austauschen oder im Urlaub kostenlos per Telefon oder sogar per Videoanruf mit der Familie in Kontakt bleiben – dank Instant-Messenger-Diensten ist all das heute möglich. Die Programme für Smartphones, Tablets und teilweise auch für PCs ermöglichen es, Nachrichten, Bilder und Videos nahezu in Echtzeit über den ganzen Globus zu schicken. Genutzt werden dabei die Datenautobahnen des Internets und des Mobilfunknetzes.

Im Grunde ist „Instant Messaging“, zu Deutsch „sofortige Nachrichtenübermittlung“, eine weitere Form des Chats. Das Wort „chat“ kommt aus dem Englischen, ist ursprünglich ein Verb und bedeutet nichts anderes als „plaudern“. Und genau darum geht es bei Instant Messengern: Zwei oder mehr Personen können sich in einem virtuellen Raum miteinander unterhalten, Neuigkeiten austauschen und digitale Inhalte wie Bilder und Videos teilen.

Prinzipiell sind Instant Messenger nicht öffentlich, das heißt Nutzer:innen haben eine Liste aus Freund:innen und Bekannten, die zum Beispiel von einer App wie WhatsApp, Threema oder Signal automatisch aus der Kontaktliste des Smartphones angelegt wurde. Andere, unbekannte Nutzer:innen werden nicht in dieser Liste angezeigt.

Für die Nutzung eines Instant Messengers beispielsweise auf dem Smartphone oder dem Tablet ist die Installation einer separaten App notwendig.

Tipp

Bevor man sich für ein bestimmtes Programm entscheidet, ist es sinnvoll herauszufinden, welchen Dienst der eigene Freundeskreis überwiegend nutzt. Hier hilft auch ein Blick in die Familie: Da viele junge Menschen heute Instant Messenger nutzen, lohnt es sich, die eigenen Kinder und Enkel:innen zu fragen, welches Programm sie verwenden. Denn ohne Freund:innen in der Freundesliste kann ein Instant Messenger seinen Zweck nicht erfüllen. Auch bei Fragen zur Benutzung können eventuell Kinder und Enkel:innen weiterhelfen.

Modul 5.5: Risiken und Nebenwirkungen von Apps

Die Installation eines Instant Messengers auf dem Smartphone oder Tablet

Instant Messenger für Smartphones oder Tablets kann man als App aus dem jeweiligen Anbietershop, also in der Regel Google Play oder App Store, herunterladen. Nach der Installation eines Instant Messengers wird Nutzer:innen eine einmalige Nummer zugewiesen, über die sie von anderen Teilnehmer:innen erreicht werden können – in aller Regel ist das die eigene Telefonnummer oder eine andere einmalige Identifikationsnummer.

Instant Messenger wie WhatsApp, Threema oder Signal gleichen bei der ersten Anmeldung ab, welche Kontakte im Telefonbuch vorhanden sind und ob diese auch das entsprechende Programm installiert haben. Alle Kontakte werden dann in eine Kontaktliste aufgenommen. Indem man auf eine Freundin oder einen Freund klickt oder tippt und dann eine Nachricht in ein separates Fenster eingibt, nimmt man Kontakt mit ihr oder ihm auf.

Wichtig ist auch, nach dem ersten Öffnen des Programms die Privatsphäre-Einstellungen anzupassen, also anzugeben, wer welche persönlichen Daten wie Telefonnummern, E-Mail-Adressen, das Profilbild, den Namen, Lesebestätigungen und den Status sehen darf. Bei den meisten Programmen sind bereits Einstellungen vorgegeben, häufig sind diese aber so gewählt, dass alle Daten für alle Nutzer:innen sichtbar sind. Die Privatsphäre-Optionen finden sich häufig unter dem Menüpunkt „Einstellungen“ oder → „Profil“.

Tipp

Auch hier gilt bezüglich persönlicher Daten: so viel wie nötig und zugleich so wenig wie möglich bei der Anmeldung preisgeben. Komplette Adresssätze mit Straße, Wohnort, Telefonnummer oder gar persönlichen Vorlieben sollten Sie nur angegeben, wenn Sie auch möchten, dass andere Nutzer:innen und der Anbieter selbst diese Daten sehen können. Bei der Nutzung eines Instant Messengers sollte man sich zudem bewusst sein, dass man nicht nur eigene Daten preisgibt, sondern auch die Daten anderer, zum Beispiel über den Abgleich der Kontakte oder beim Versand von Texten, Bildern und Videos.

Grundlegender Aufbau und Funktionen von Instant Messengern

Oftmals haben die verschiedenen Instant Messenger eine ähnliche Struktur mit Kontaktlisten, Nachrichtenfenstern und Einstellungsmöglichkeiten. Die meisten von ihnen erlauben neben dem klassischen Austausch von Textnachrichten, Dateien, Bildern und Videos auch Internet- oder Videotelefonie innerhalb der eigenen Kontakte. Im Weiteren unterscheiden sich die einzelnen Instant Messenger unter anderem in den Nutzungsoptionen, den Sicherheitseinstellungen, in Fragen der Datenübertragung, im Aussehen der Oberfläche oder im Personenkreis, der dort angemeldet ist.

Das eigene Profil und das Einstellungsmenü: Jeder Instant Messenger bietet die Möglichkeit, das eigene Profil zu bearbeiten. Hier kann man zum Beispiel ein Profilbild einstellen, Datenschutzeinstellungen vornehmen und die Darstellung der App ändern. Auch Benachrichtigungsoptionen, also zum Beispiel wann und ob man über neue Nachrichten auf dem Startbildschirm informiert wird, und wo empfangene Bilder auf dem Gerät abgelegt werden, lassen sich hier einstellen.

Tipp

Wenn man Bilder oder Videos von Kontakten geschickt bekommt, werden diese in aller Regel sofort auf dem eigenen Gerät gespeichert. Gerade Videos haben oftmals eine enorme Datenmenge und sorgen dafür, dass das Datenvolumen im Mobilfunknetz schnell aufgebraucht ist. Es empfiehlt sich daher, Videos nur über eine WLAN-Verbindung herunterzuladen. Über die Einstellungen der App kann man bestimmen, dass empfangene Dateien wie Bilder und Videos nicht automatisch gespeichert werden.

Kontaktlisten: Mit wem man über einen Messenger-Dienst Kontakt aufnehmen kann, erfährt man in der Kontaktliste. Hier werden alle Personen aufgelistet, die ein Instant Messenger erfolgreich abgleichen konnte, die also dieselbe App benutzen. Klickt man auf den Kontakt, wird ein Chat geöffnet.

Tipp

Öffnet man einen Kontakt im Telefonbuch des Smartphones, dann sieht man im Eintrag oft, welche Instant Messenger ein Kontakt nutzt.

Chats: Möchte man Kontakt mit jemandem aufnehmen, öffnet man ein Chatfenster, indem man auf einen Eintrag in der Kontaktliste tippt. Nun kann man zum Beispiel eine Textnachricht eingeben, ein Bild oder Video verschicken oder einen (Video-)Anruf starten. Die meisten Messenger-Dienste bieten zudem die Möglichkeit, dass man mit mehreren Kontakten einen Gruppenchat eröffnet. Wird ein Beitrag hierin verfasst, sehen ihn alle, die in der Gruppe sind. Ein Gruppenchat eignet sich besonders gut, um zum Beispiel einen Geburtstag zu planen oder mit der ganzen Familie in Kontakt zu bleiben, denn Termine, Fotos oder Videos müssen dann nur an einer Stelle und nicht in vielen unterschiedlichen Einzelchats versendet werden.

Tipp

Wie man eine Gruppe in WhatsApp erstellt, Gruppenmitglieder hinzufügt und Nachrichten an alle verschickt, wird als Kurzanleitung und als Video bei Silver Tipps erklärt:
https://s.rlp.de/PgdCM

Texte, Bilder und Videos versenden: Im Chatfenster können Texte verfasst sowie Bilder und Videos verschickt werden. Auch das Versenden von Dateien und des aktuellen Standorts ist bei den meisten Instant Messengern möglich. Anhand von kleinen Symbolen neben der Nachricht, meist links unten, erkennt man, ob die Nachricht vom angeschriebenen Kontakt empfangen und gelesen wurde. Meist sind dies zwei Häkchen, die sich einfärben. Die sogenannte Lesebestätigung kann von Nutzer:innen aber auch abgestellt werden.

Erhält man eine Nachricht, wird eine Benachrichtigung angezeigt. Dies geschieht meist in Form einer kleinen Zahl direkt im App-Symbol oder im betreffenden Chat. Neben der kleinen Anzeige gibt es auch Benachrichtigungen auf dem Startbildschirm des Smartphones oder Tablets beziehungsweise einen Ton oder eine Vibration. Die Art der Benachrichtigung kann über die Einstellungen der App individuell festgelegt oder sogar für einzelne Chats abgestellt werden.

Tipp

Wie man Bilder und Nachrichten mit einem Messenger verschickt, zeigt Digital-Botschafterin Helga Handke im Video „Mit WhatsApp in Verbindung bleiben“ auf Silver Tipps:
https://s.rlp.de/4vsnt

Emoticons: Bei der Kommunikation über Instant Messenger fehlen Gestik und Mimik. Auch ist es schwer, Gefühle auszudrücken und die Reaktion des Gegenübers richtig einzuschätzen. Deshalb gibt es in Instant Messengern → Emoticons, auch → Emojis genannt. In Form kleiner Abbildungen, etwa eines lachenden oder zwinkernden Smileys oder eines noch oben zeigenden Daumens, steht Nutzer:innen neben der textlichen auch eine bildliche Ausdrucksebene zur Verfügung. Die meisten Messenger-Apps wie WhatsApp, Threema und Co. bieten eine

Emoticons können als Tastenkombination :-) oder im Bild dargestellt werden.

Vielzahl unterschiedlicher Emoticons aus den verschiedensten Kategorien an. Von Schiffen über Früchte bis hin zu Sportaktivitäten sind bildhafte Darstellungen aus vielen Bereichen vorhanden. Emoticons kann man entweder in eine Textnachricht einbauen oder einzeln verschicken. Einfügen kann man die Bildchen durch das Tippen auf das Smiley-Symbol links neben dem Nachrichtenfeld.

(Video-)Telefonie: Viele Instant Messenger bieten die Möglichkeit, dass man mit Personen in der Kontaktliste telefoniert oder sogar einen Videoanruf startet. Am Smartphone oder Tablet werden dann die eingebaute Kamera und das Mikrofon genutzt. Einen Anruf startet man mit dem Klick auf den Telefonhörer direkt im Einzel- oder auch im Gruppenchat. Bei Letzterem werden dann alle Gruppenmitglieder über Video angerufen. Da Telefonate und Videochats, wenn sie im Instant Messenger vorgenommen werden, über das Internet getätigt werden, kann zum Beispiel auch vom Ausland aus zu Hause angerufen werden, ohne dass Telefonkosten entstehen. Wichtig ist aber, dass man in einem WLAN angemeldet ist.

Tipp

Nicht jeder Instant Messenger bietet die Möglichkeit zur Videotelefonie. Nutzt man solche Dienste von unterwegs aus, kann schnell das monatliche Datenvolumen aufgebraucht sein. Man sollte also nach Möglichkeit mit einem WLAN verbunden sein.

Wer einen Instant Messenger nutzt oder nutzen möchte, sollte sich ein paar wichtige Fragen stellen:

Wer nutzt den Instant Messenger ebenfalls?
Ein Instant Messenger erfüllt seinen Zweck erst, wenn Kontakte, wie die Familie, Bekannte, Freund:innen oder Kolleg:innen, darüber auch erreichbar sind. Oft wählen Nutzer:innen populäre Produkte wie WhatsApp, um einen möglichst großen Kreis an Personen kontaktieren zu können. Generell bieten aber auch andere Anbieter wie Signal, Threema oder Wire Produkte, die einen großen Personenkreis erreichen. Für die Nutzung eines Instant Messengers beispielsweise auf dem Smartphone oder dem Tablet ist die Installation einer separaten App notwendig. Einige Messenger-Anbieter geben die Möglichkeit, die App auch über den PC/Laptop zu nutzen.

Wie wird verschlüsselt?
Die zentrale Frage beim Thema Verschlüsselung ist: Wer kann eine Nachricht lesen? Im Idealfall nur die Partei(en), für die die Nachricht auch bestimmt ist. Der Goldstandard hier nennt sich Ende-zu-Ende-Verschlüsselung. Dabei werden Nachrichten direkt vom Absendergerät verschlüsselt, und zwar so, dass nur das Gerät des:der Empfängers:in sie auch wieder entschlüsseln kann. Viele Instant Messenger sind heute auf diese Weise verschlüsselt. So ist es Dritten, etwa Unternehmen oder staatlichen Stellen, nicht möglich, Inhalte mitzulesen.

Kostenlos oder kostenpflichtig?
Nicht alle Instant Messenger sind kostenlos. Das ist darin begründet, dass die Entwicklung von Programmen und deren Unterhalt in Form von Servern, Personal etc. mit enormen Kosten verbunden ist. Wenn man sich für einen Instant Messenger entscheidet, sollte man auch darauf achten, welchem Dienst man seine Daten anvertraut und wie dessen Finanzierung erfolgt.

Gibt es die Möglichkeit von Back-ups?
Back-ups sind Sicherungskopien. Im Falle von Instant Messengern werden zum Beispiel die Chatverläufe, Bilder, Dateien und Videos gespeichert, um diese beim Verlust, beim Wechsel oder bei Beschädigung des Smartphones wiederherstellen zu können. Einige Instant Messenger bieten die Möglichkeit, Daten lokal, das heißt direkt auf dem Gerät, oder im Internet, zum Beispiel in einer Cloud, zu speichern und bei Bedarf das Nutzerkonto und die Chatverläufe wiederherzustellen. Bei lokalen Sicherungen sollte immer bedacht werden, dass bei Verlust oder Beschädigung des Gerätes die Back-ups ebenfalls verloren sind und diese deshalb am besten auch auf einem anderen Gerät, zum Beispiel einem Laptop, gespeichert werden sollten.

In der folgenden Tabelle sind Beispiele für Instant Messenger aufgeführt, kurz beschrieben und in ihren Besonderheiten dargestellt.

Beispiele für Instant Messenger

Instant Messenger	Kurzbeschreibung	Besonderheiten
Signal 	Signal ist ein kostenloser amerikanischer Instant Messenger, der als App für Android wie auch für Apple erhältlich ist. Texte, Bilder, Videos etc. werden verschlüsselt verschickt. Zudem können Nachrichten lokal verschlüsselt als Back-up gesichert werden. Allerdings haben Gruppenchats keine Videofunktion.	• finanziert von der Signal-Stiftung • standardmäßige Verschlüsselung der Kommunikation • Auto-Löschfunktion für Nachrichten kann eingestellt werden • lokale Back-ups mit Verschlüsselung möglich
Telegram 	Der russische Instant Messenger Telegram ist kostenlos als App für Android wie auch für Apple erhältlich. Standardmäßig verschlüsselt Telegram Chats nur vom Sender zum Server. Dort werden die Daten zentral abgespeichert. Eine Ende-zu-Ende-Verschlüsselung gibt es nur in „geheimen Chats“, die separat angelegt werden müssen.	• aktuell finanziert aus dem Privatvermögen eines Entwicklers • Nachrichten können in nicht geheimen Chats gelöscht werden
Threema 	Threema ist ein kostenpflichtiger Schweitzer Instant Messenger, der auf Smartphones und Tablets, Apple wie Android, genutzt werden kann. Neben Textnachrichten können zum Beispiel Bilder oder Videos hin- und hergeschickt werden. Neben einer Ende-zu-Ende-Verschlüsselung bietet Threema die Möglichkeit, den Dienst ohne eine Telefonnummer zu nutzen und Kontakte anonym abzugleichen.	• kostenpflichtig: einmalig 3,99 € • standardmäßige Verschlüsselung der Kommunikation • ohne Telefonnummer nutzbar • keine Speicherung von Metadaten • lokale verschlüsselte Back-ups möglich

Beispiele für Instant Messenger

Instant Messenger	Kurzbeschreibung	Besonderheiten
Wire 	Wire ist ein Instant Messenger, der sowohl für Android als auch für iOS verfügbar ist. Hauptsitz der Firma ist in den USA. Wire ist in der Grundversion kostenlos, für Unternehmen beispielsweise gibt es aber kostenpflichtige Abonnements (Wire Pro), die weitere Funktionen wie Gruppenvideotelefonie etc. ermöglichen. Wire verschlüsselt Chats standardmäßig Ende-zu-Ende.	• Videokonferenzen nur in der kostenpflichtigen Pro-Version • standardmäßige Verschlüsselung der Kommunikation • Auto-Löschfunktion für Nachrichten kann eingestellt werden • lokale verschlüsselte Back-ups möglich (nur iOS), Android-Back-ups sind unverschlüsselt
WhatsApp 	Mit dem zu Facebook gehörenden kostenlosen Instant Messenger lassen sich Texte, Bilder, Dateien oder Videos von einem mobilen Endgerät zu einem anderen schicken. Außerdem kann man Kontakte direkt über WhatsApp auch per Video anrufen, auch in Gruppen. Nachrichten werden standardmäßig Ende-zu-Ende verschlüsselt. Back-ups können verschlüsselt lokal oder über eine Cloud wie Google Drive oder iCloud erstellt werden.	• sehr großer Nutzer:innenkreis • standardmäßige Verschlüsselung der Kommunikation • keine Ende-zu-Ende-Verschlüsselung bei Back-ups • WhatsApp sammelt Metadaten, die analysiert und mit Facebook geteilt werden

Tipp

Eine detaillierte Analyse und Auflistung verschlüsselter Messenger gibt es auf der Internetseite von mobilsicher.de: *https://s.rlp.de/fQgzt*

Für absolute Anfänger:innen in Sachen Instant Messaging ist zu empfehlen, sich Unterstützung innerhalb der eigenen Familie, bei Bekannten oder Freund:innen zu suchen. Gemeinsam geht es eben oft besser, und wenn man den Dreh einmal raus hat, kommt man schon bald ohne Unterstützung klar.

7.3 Videotelefonie

Gerade in Zeiten der Corona-Pandemie im Jahr 2020 standen viele Menschen vor der Frage, wie sie mit Angehörigen, Freund:innen und auch Kolleg:innen in Kontakt bleiben können. Die persönlichen Begegnungen wurden entweder auf ein Minimum beschränkt oder waren teilweise gar nicht mehr möglich. Der Anruf per Telefon ist zwar eine bewährte Möglichkeit der Kontaktaufnahme, aber Menschen zu sehen und die Reaktion des Gegenübers unmittelbar mitzubekommen – das kann ein Telefonat nicht leisten. Durch Geräte wie Smartphones, Tablets und Laptops lässt sich über das Internet hingegen ein digitales Miteinander realisieren.

Was bietet Videotelefonie?

Sich gegenseitig per Video sehen, die Stimmen der anderen hören und das Gefühl haben, nah beieinander zu sein: Das ermöglichen Videotelefondienste wie Skype, Jitsi oder Zoom. Die Nutzung ist in aller Regel kostenlos und einfach einzurichten. Es ist sogar möglich, mit mehr als einer Person gleichzeitig auch per Video zu telefonieren. So kann man trotz großer Distanz mit Freund:innen sprechen, Kolleg:innen kontaktieren oder gemütlich am Familientreffen teilnehmen und gemeinsam Kaffee trinken.

Alles, was man für Videotelefonie benötigt, sind ein Gerät wie ein Smartphone, ein Tablet oder ein Laptop, eine Kamera und ein Mikrofon. In den meisten Geräten sind Kamera und Mikrofon heute bereits standardmäßig verbaut. Natürlich muss man auch ein Programm oder eine App installieren – wobei manche Dienste, wie etwa Jitsi, nicht einmal das unbedingt voraussetzen, da die Videokonferenzen auch direkt über den Browser funktionieren.

Tipp

Für eine bessere Verständlichkeit sorgt meist ein Headset. Das ist ein Kopfhörer mit eingebautem Mikrofon, der direkt an den PC, das Smartphone oder das Tablet angeschlossen wird und präziser die eigenen Worte aufnimmt, weil das Mikrofon näher am Mund ist. Auch die Verständlichkeit der anderen ist meist besser, da der Ton direkt am Ohr wiedergegeben wird. Headsets bekommt man schon für wenig Geld im Elektrofachmarkt oder in Onlineshops.

Grundlegende Elemente und Funktionen einer Videokonferenz

Das Treffen von Teilnehmenden in einer Videokonferenz ist im Grunde ein Treffen in einem virtuellen Raum. In einem beliebigen Programm wird eine Videokonferenz eröffnet und andere Teilnehmende treten dann diesem Raum bei. Das funktioniert zum Beispiel über eine Einladung, die per E-Mail oder Instant Messenger an die anderen Teilnehmenden verschickt werden kann. Für einige Programme ist eine separate Installation notwendig.

So funktioniert die Bedienung von Videokonferenzen:

- **Videofenster:** Mittig im Bild sind die Videos der Teilnehmenden zu sehen. Wie die Videos angeordnet sind, also ob zum Beispiel nur die oder der aktuell Sprechende zu sehen ist, lässt sich von Nutzer:innen individuell einstellen.

- **Funktionsbuttons:** In allen Videokonferenzprogrammen kann über ein Hörersymbol die Teilnahme begonnen oder beendet werden, das Symbol ist dann entweder grün für „teilnehmen“ oder rot für „Konferenz verlassen“ eingefärbt. Zudem kann die Übertragung des eigenen Videobildes und des Tons an- und ausgeschaltet werden. Das ist zum Beispiel dann gut, wenn andere reden und der eigene Ton störend ist oder man das eigene Bild nicht übertragen möchte.

- **Liste der Teilnehmenden:** Alle Personen, die an einer Videokonferenz teilnehmen, werden in einer Teilnehmerliste angezeigt. Meistens können hier öffentliche, also für alle sichtbare, oder auch private Chats zwischen einzelnen Personen begonnen werden.

- **Chat:** In den meisten Videokonferenzprogrammen gibt es die Möglichkeit eines Chats, um sich mit einzelnen oder allen Teilnehmenden gleichzeitig in Textform auszutauschen.

- **Bildschirm teilen:** In vielen Videokonferenzprogrammen kann man seinen Bildschirm teilen. Die anderen Teilnehmenden sehen dann das, was die Person, die ihren Bildschirm freigegeben hat, auch sieht. Das ist zum Beispiel dann praktisch, wenn man eine Präsentation halten möchte, gemeinsam an einem Dokument arbeitet, aber auch, um die Bilder vom letzten Urlaub zu zeigen. Einige Programme bieten zudem die Möglichkeit, Dokumente zu öffnen oder YouTube-Videos zu teilen. Die Bildschirm-Teilen-Funktion eignet sich auch dafür, aus der Ferne Hilfe zu leisten.

- **Sich „melden“:** Wer mit vielen Personen in einer Videokonferenz ist, bemerkt schnell, dass es manchmal chaotisch werden kann. Teilnehmende fallen einander ungewollt ins Wort, und wer als Nächstes spricht, ist oft nicht klar. Um diese Herausforderung zu lösen, gibt es die Möglichkeit, virtuell die Hand zu heben. Dafür drückt oder tippt man einfach auf zum Beispiel das Handsymbol. Andere sehen dann, dass man sprechen möchte. Kleiner Tipp: Oft hilft es auch, sich mit allen darauf zu einigen, dass nur die- oder derjenige das Mikrofon eingeschaltet hat, die oder der auch spricht. Eine weitere Möglichkeit sind sogenannte Videokonferenzkarten, die man zum Beispiel hier herunterladen kann: *https://s.rlp.de/JLOfMs*

- **Einstellungen:** Videokonferenzprogramme bieten die verschiedensten Einstellungen. So kann zum Beispiel die Qualität des eigenen Videos bestimmt werden, um bei einer schlechten Verbindung keine Abbrüche der Übertragung zu riskieren. Hier kann ebenfalls gewählt werden, welche Kamera und welches Mikrofon genutzt werden sollen, also zum Beispiel das im Gerät verbaute Mikrofon oder das Headset.

Aufbau eines Videokonferenzsystems

Tipp

Videokonferenzen sind sehr datenintensiv, da viele Informationen, wie Video, Audio und Bildschirmpräsentationen, an alle Teilnehmenden übertragen werden müssen. Es ist daher wichtig, eine stabile und durchsatzstarke Internetleitung zu nutzen, da ansonsten Videos stehen bleiben, der Ton unverständlich werden oder Konferenzen einfach abbrechen können. In jedem Fall empfiehlt es sich, nicht über das Mobilfunknetz, sondern immer über (W-)LAN an Videokonferenzen teilzunehmen, weil das mobile Datenvolumen sonst schnell aufgebraucht sein kann. Um Datenvolumen zu sparen, kann es günstiger sein, das Videobild der Teilnehmenden abzustellen und lediglich über das Audiosignal zu kommunizieren. Wer wissen möchte, wie schnell die eigene Internetverbindung ist, kann einen Test bei der Bundesnetzagentur machen: *www.breitbandmessung.de*

In der folgenden Tabelle sind Beispiele für Videokonferenzprogramme aufgeführt, kurz beschrieben und in ihren Besonderheiten dargestellt.

Beispiele für Videokonferenzprogramme

Programm	Kurzbeschreibung	Anleitungen und weiterführende Infos
Cisco Webex	Cisco Webex Meetings ist ein professionelles Videokonferenzsystem von Cisco Systems mit Sitz in den USA. Die kostenlose Variante erlaubt eine unbegrenzte Anzahl an Videokonferenzen mit der Option der Bildschirmfreigabe und bis zu 50 Teilnehmende mit einer Länge von bis zu 40 Minuten.	*https://s.rlp.de/d0G0c*
Google Meet	Der von Google entwickelte Videokonferenzdienst, früher Google Hangouts und Google Chat, lässt sich kostenlos über ein bestehendes Google-Konto nutzen. Nachdem ein Videokonferenzraum eröffnet wurde, können Teilnehmende eingeladen werden. Google Meet bietet die Möglichkeit, den Bildschirm zu teilen und auch via Tablet und Smartphone an Konferenzen teilzunehmen.	*https://s.rlp.de/6FEQe*
Jitsi	Jitsi ist ein freies, quelloffenes Videokonferenzsystem, das über den Browser oder eine App kostenlos genutzt werden kann. Im Gegensatz zu anderen Programmen benötigt man zur Nutzung keine Registrierung und kein Benutzerkonto.	*https://s.rlp.de/7dHxe*
Skype	Skype ist ein Programm, das von Microsoft angeboten wird. Der Dienst bietet die Möglichkeit, Videotelefonie zu nutzen, Daten zu übertragen und den Bildschirm zu teilen. Skype kann über den Browser oder über eine App auf verschiedenen Endgeräten genutzt werden.	*https://s.rlp.de/Wkbv2*

Beispiele für Videokonferenzprogramme

Programm	Kurzbeschreibung	Anleitungen und weiterführende Infos
WhatsApp 	Mit dem zu Facebook gehörenden kostenlosen Instant Messenger lassen sich Kontakte per Video anrufen, auch in Gruppen. Nachrichten werden standardmäßig Ende-zu-Ende verschlüsselt.	*https://s.rlp.de/8OI3c*
Zoom 	Zoom wird von Zoom Video Communications Inc. mit Sitz in den USA angeboten. In der kostenlosen Variante können Gruppen bis zu 100 Personen an Videokonferenzen über Smartphone, Tablet oder PC teilnehmen. Die maximale Gesprächsdauer beträgt in der Gratisversion 40 Minuten.	*https://s.rlp.de/SNF9d*

Tipp

Auch bei Videokonferenzprogrammen spielt das Thema Verschlüsselung eine wichtige Rolle. Welche Dienste die Kommunikation wie verschlüsseln, hat die Redaktion von mobilsicher.de in einem Beitrag zusammengestellt: *https://s.rlp.de/9qSr1*

7.4 Foren

Der Klassiker unter den Kommunikationsmöglichkeiten im Internet ist das Forum. Das Wort „Forum“ kommt aus dem Lateinischen und bedeutet „Marktplatz“. Und entsprechend kann man sich auch die Idee hinter einem Internetforum vorstellen: Menschen treffen sich auf einem virtuellen Marktplatz. Allerdings betreiben sie dort keinen Handel mit Waren, sondern mit Informationen. Das Internetforum ist ein Ort der Diskussion sowie des Meinungs- und Erfahrungsaustausches.

Im Vergleich zum Chat oder Instant Messaging ist das Forum eine zeitversetzte Kommunikationsform. Nutzer:innen schreiben etwas in einen Beitrag und bekommen zu einem späteren Zeitpunkt Antwort

von anderen Nutzer:innen oder Moderator:innen. Diese Konversation ist meist öffentlich und von allen frei einsehbar. Ein Internetforum hat also durchaus Ähnlichkeiten mit einem Schwarzen Brett. Im Internet gibt es unzählige Foren, jedes davon mit einem bestimmten Oberthema. Es gibt Foren, die sich mit Technik beschäftigen, andere haben Gartenarbeit zum Thema, um nur zwei Beispiele zu nennen.

Der große Vorteil an Foren ist, dass Internetnutzer:innen sich dort (größtenteils kostenlos) Hilfe holen können. Um Beiträge lesen zu können, muss man meistens weder im jeweiligen Forum angemeldet sein, noch ein bestimmtes Programm auf dem Smartphone, Tablet oder Laptop installieren. Möchte man aktiv mitdiskutieren, ist oft ein Benutzerkonto nötig. Die Anzahl der sogenannten Hilfeforen im Netz ist riesig. Häufig sind Einträge in Foren auch für eine lange Zeit archiviert und werden von Suchmaschinen gefunden. Genau darin liegt aber zugleich auch die Schwierigkeit: Informationen in Foren sollten immer mit Vorsicht genossen werden, denn zum einen könnten sie bereits veraltet, zum anderen lediglich Halbwahrheiten oder schlichtweg falsch sein. Denn nicht jede:r, die oder der etwas schreiben darf, weiß immer auch tatsächlich Rat.

Tipp

Wenn man Foreneinträge von ihrem Beginn an durchliest, kann man ganz gut abschätzen, wie viel Wahrheitsgehalt in den einzelnen Einträgen steckt.

Generell sind Foren so strukturiert, dass es ein bestimmtes Oberthema, englisch „Topic“, gibt, unter dem dann weitere einzelne Einträge, englisch → „Postings“, hinterlassen werden können. Diese hierarchische Struktur erleichtert die Suche nach Informationen. Auch viele Hersteller von technischen Geräten bieten sogenannte Support-Foren („Unterstützungsforen“) an, in denen Kund:innen Fragen zu Produkten stellen können. Dieser Typ von Forum ist meist kostenlos und moderiert, das heißt, geschulte Mitarbeiter:innen des jeweiligen Anbieters beantworten die Fragen und geben Hilfestellungen.

7.5 Fake News

Zeitungsente, Falschmeldung oder Fehlinformation – all diese Begriffe meinen das Gleiche: Nachrichten, die nicht der Wahrheit entsprechen. Über soziale Netzwerke wie Facebook und Twitter werden die sogenannten Fake News schnell verteilt und sind zunächst oft nicht von echten Nachrichten zu unterscheiden. Umso wichtiger ist es, eine solide Informationskompetenz zu gewinnen, um nicht auf Fake News hereinzufallen.

Modul 8:
Soziale Medien im Netz

Fake oder Fakt – was macht Fake News aus?

Als Fake News werden Nachrichten oder Meldungen bezeichnet, die nicht der Wahrheit entsprechen. Diese befassen sich hauptsächlich mit aktuellen Themen, die meist weit verbreitet werden und viel Aufsehen in der Gesellschaft erregen. In Deutschland sind das beispielsweise Themen wie die Flüchtlingskrise, Politiker:innen und Parteien, aber auch internationale Geschehnisse oder Verschwörungsmythen. Verbreitet werden Fake News über soziale Netzwerke wie Facebook, Instagram, YouTube, WhatsApp oder Twitter. Dort geschieht die Verbreitung oft ungefiltert, da anders als im klassischen Journalismus niemand nachprüft, ob Meldungen der Wahrheit entsprechend dargestellt werden. Denn ein wichtiger Bestandteil der Arbeit von Journalist:innen ist die Prüfung und Bewertung von Fakten. Im → Web 2.0 ist es jedoch jeder Person, die beispielsweise einen Social-Media-Account hat, möglich, Nachrichten mit der Welt zu teilen.

Das Einmaleins, um Fake News zu erkennen

Es gibt ein paar Hinweise, die einen beim Lesen von Nachrichten stutzig machen sollten und helfen, Fake News zu enttarnen:

- Es werden reißerische Überschriften verwendet, die beim Lesen starke Gefühle bei Leser:innen verursachen.
- Der Beitrag ist in einem sehr emotionalen, manchmal reißerischen Ton formuliert. Er kann zum Beispiel besonders rührselig oder aufregend sein.
- Der Beitrag hat keine oder eine fehlerhafte Quellenangaben.
- Der Beitrag ist nicht auf anderen Seiten im Netz zu finden.

- Das Benutzerkonto, unter dem der Beitrag zum Beispiel auf Facebook, Twitter oder Instagram veröffentlicht wurde, hat nur wenige oder keine Follower:innen.
- Das Bild passt nicht zum Text oder ist offensichtlich bearbeitet.
- Der Beitrag ist nicht aktuell.

Tipp

Es gibt im Internet bereits einige Angebote, die dazu genutzt werden können, Fake News zu entlarven oder das eigene Bewusstsein für solche Falschnachrichten zu schärfen. Die ARD greift auf ihrer Internetseite www.tagesschau.de/faktenfinder unter dem Hashtag #faktenfinder Nachrichten, die im Netz kursieren, auf und überprüft diese auf die tatsächliche Faktenlage. Mit dem SWR FakeFinder kann das eigene Wissen über Fake News spielerisch geprüft werden: *www.swrfakefinder.de*

Wer verbreitet Fake News?

Falschnachrichten haben unterschiedliche Formen. Außer in Gestalt von Artikeln können sie auch auf diesen Kanälen auftauchen:

- **Kettenbriefe:** Nachrichtenketten, die über Instant Messenger wie WhatsApp oder Plattformen wie Facebook verteilt werden, nerven nicht nur, sondern können auch Panik schüren und Angst verbreiten. Zu Beginn der Corona-Pandemie wurden so zum Beispiel Falschnachrichten über das Virus verbreitet.

- **Kommentare auf sozialen Netzwerken:** Über die Kommentarfunktion auf Social-Media-Kanälen verbreiten sogenannte Trolle eine meist sehr radikale Meinung. Ziel ist es, für möglichst viel Aufregung zu sorgen, damit viele Menschen mit ihnen in die Diskussion einsteigen und das Thema öffentliches Interesse bekommt. Das sorgt nicht nur für Wirbel, sondern füttert den Anzeige-Algorithmus und die Falschmeldungen werden großflächig verteilt.

- **Social Bots:** Für Unruhe in den Kommentaren können auch sogenannte Social Bots verantwortlich sein. Das sind im Unterschied

zu den Trollen keine echten Menschen, sondern eine Art Roboter. Meinungsmache ist der Grund ihrer Existenz, und darin sind sie dank einer durchdachten Programmierung besonders gut.

Was macht Fake News gefährlich?

Vorurteile schüren, Wahlen beeinflussen und Ängste verbreiten: Die Absicht von Fake News ist es, Menschen in eine bestimmte Richtung zu manipulieren. Klar ist, Fake News dürfen nicht ignoriert werden, da sie darauf ausgelegt sind, die freie Meinungsbildung zu korrumpieren und das Vertrauen der Menschen in seriöse Quellen und Medien zu beschädigen. Dies ist eine ernst zu nehmende Gefahr, wenn wir weiterhin in einer demokratischen Gesellschaft leben möchten, in der Entscheidungen auf der Grundlage von Fakten und nicht von Unwahrheiten getroffen werden.

Was kann man tun, wenn man eine Falschnachricht entlarvt hat?

Betreiber wie Facebook, Twitter und Co. sind bemüht, Fake News von ihren Seiten zu nehmen, wenn diese gemeldet werden. Nach dem Netzwerkdurchsetzungsgesetz besteht eine Löschungspflicht nur bei bestimmten Fallgruppen. Deshalb ist es wichtig, eine entdeckte Falsch-nachricht beim Anbieter zu melden. Sollte auf einer anderen Seite die Falschmeldung bereits aufgedeckt und widerlegt worden sein, kann dieser Beitrag geteilt werden. Aber Vorsicht: Nicht die gefundene Falschmeldung mit einem Hinweis im Original teilen. Dies sorgt dafür, dass sich die Meldung weiterverbreiten kann.

Tipp

Auf der Website Hoaxsearch (*www.hoaxsearch.com*) können bereits bekannt gewordene Fake News gesucht werden. Einfach ein Schlagwort oder eine gesamte Überschrift in die Suchzeile eingeben und prüfen, ob es sich um eine Falschmeldung handelt. Der angegebene Link führt dann zu einem Beitrag, in dem die Meldung widerlegt wird.

7.6 Datentausch im Internet

Datenaustausch per E-Mail

Modul 7.1:
E-Mailing

Der Versand von Dateien über E-Mail ist eine der klassischsten Methoden, um Dateien zu verschicken und zu empfangen. Voraussetzung für beispielsweise die Absenderin wie für den Empfänger sind ein E-Mail-Programm und ein Benutzerkonto. Egal ob am PC, Laptop oder Smartphone: Dateien können dann als Anhang mit einer E-Mail verschickt werden. Der Versand per E-Mail eignet sich gut, um kleinere Dateien zu versenden, wie Textdokumente und Bilder mit kleiner Dateigröße. Für große Dateien, wie etwa Foto- oder Videodateien mit großer Datenmenge, eignet sich der Versand per E-Mail weniger gut, da die E-Mail-Anbieter meist eine maximale Dateigröße von 10–15 MB zulassen.

Datenaustausch per Messenger

Modul 7.2:
Instant Messenger

Der Versand von Dateien über Messenger wie WhatsApp, Threema, Signal und Co. auf dem Smartphone ist eine der meistgenutzten Möglichkeiten, um schnell Bilder und Videos untereinander auszutauschen. Denn inzwischen nutzt eine große Mehrheit der Personen in Deutschland ein Smartphone und speichert darauf ihre digitalen Fotoalben. Voraussetzung ist, dass Sender:in und Empfänger:in die gleiche Messenger-App auf dem Smartphone nutzen. Der Vorteil ist unter anderem, dass man mehrere Dateien auf einmal verschicken kann und die Bedienung sehr einfach ist. Auch am PC/Laptop lassen sich über den Browser Messenger-Dienste nutzen und so Bilder und Dateien verschicken. Ein Nachteil ist, dass manche Anbieter Bilder und Videos beim Versand komprimieren, sie also kleiner machen, und dadurch die Qualität etwas schlechter ist als beim Original.

Datenaustausch per Filesharing-Dienst

Filesharing-Dienste wie WeTransfer, WeSendIt und Schicks' digital haben sich auf den Versand großer Dateien wie beispielsweise Videos oder große Präsentationen spezialisiert. Die Dienste lassen sich auf den Internetseiten der Anbieter über den Browser am PC oder Laptop nutzen. Mithilfe der Dienste können kostenlos Dateien mit einer Größe von 2–3 GB verschickt werden. Optional bieten die Anbieter auch eine Bezahloption, um noch größere Dateien zu versenden.

Die Funktionsweise ist bei allen Diensten gleich: Man lädt eine Datei, die sich auf der Festplatte befindet, mit einem Klick hoch und gibt die E-Mail-Adresse des:der Empfängers:in ein. Durch den Versand erhält die Person einen Download-Link, über den die Datei, je nach Dienst, in den folgenden 7–14 Tagen heruntergeladen werden kann. Danach werden die Dateien von den Anbietern wieder gelöscht. Der Vorteil ist, dass man sich nicht registrieren und kein Programm installieren muss. Allerdings sollte man hier mit dem Versand sensibler Dateien aufpassen, da nicht alle Anbieter die Dateien verschlüsselt übertragen.

Datenaustausch per Cloud

Als „Cloud“ oder auch „Webspace“ wird eine Art Festplatte im Internet bezeichnet, auf der Daten gespeichert und abgerufen werden können. Auf diese Festplatte kann man anderen Personen Zugriff geben, um Dateien auszutauschen. Bekannte Anbieter sind Dienste wie Dropbox, Google Drive oder die MagentaCLOUD von Telekom. Der große Vorteil einer Cloud: Sie bietet von vielen Geräten Zugriff auf einen zentralen Speicher. Darin liegt aber auch ein großer Nachteil. Daten können von Servern im Internet verloren gehen und die Anbieter haben, zumindest potenziell, die Möglichkeit, auf die Dateien zuzugreifen. Es gibt auch Anbieter wie Tresorit und luckycloud, die sich auf Privatsphäre und Sicherheit spezialisiert haben und die Dateien verschlüsseln, sodass der Anbieter selbst keinen Zugriff auf die Dateien hat. Für die Nutzung benötigt man in der Regel ein Benutzerkonto. In der kostenlosen Version ist die Speicherkapazität meist auf wenige Gigabyte beschränkt.

Tipp

Bevor Sie eine Datei verschicken, sollten Sie sich immer überlegen, was Sie verschicken möchten, wie groß die Datei ist und wer sie empfangen soll. So fällt es leichter, sich für eine angemessene Art des Datentausches zu entscheiden.

Verschlüsselung von Daten

Ähnlich wie schon bei der Verschlüsselung von E-Mails gesehen, kann Verschlüsselung auch bei Dateien oder sogar ganzen Laufwerken eingesetzt werden, um diese zu schützen. Insbesondere bei sehr sensiblen Dateien wie Rechnungen, Kontoauszügen, offiziellem Schriftverkehr und Ähnlichem ist es äußerst empfehlenswert, diese gesondert vor dem Zugriff von Unbefugten zu schützen. Und dieser ungewollte Zugriff kann leider schneller passieren, als einem lieb ist, auch wenn das Gerät niemals aus der Hand gegeben wurde – etwa wenn sich Kriminelle per Schadsoftware aus einem E-Mail-Anhang Zugang zum Computer verschaffen und die dort gespeicherten Daten abgreifen. Solche sensiblen Informationen haben im Internet auf kriminellen Datentauschbörsen einen echten Marktwert und werden dort wie andernorts begehrte Waren gehandelt.

Einmal im Netz verbreitet, können die Informationen für weitere Taten missbraucht werden – etwa Identitätsbetrug, wenn mit erbeuteten Bankdaten eingekauft wird, oder Erpressungen, wenn Kriminelle von Opfern Geld fordern, damit sie erbeutete sensible Informationen nicht veröffentlichen usw. Hiervor kann man sich zum Glück wirksam schützen, indem man besagte sensible Dateien verschlüsselt und sie so quasi in einem digitalen Tresor wegschließt. Können sich Kriminelle nun Zugriff auf den Computer verschaffen, so gelangen sie wenigstens nicht an die Daten im Tresor, solange sie nicht den Schlüssel haben. Damit man weiß, wie man dabei korrekt vorgeht, sollte die Funktionsweise der Verschlüsselung zumindest in groben Zügen verstanden werden.

Das Prinzip ist stets dasselbe – egal ob Datei, ganzes Laufwerk auf einem Computer oder dem Speicherbereich auf einem cloudbasierten Internetspeicherdienst – bei jeder Verschlüsselung werden stets die digitalen Informationen zunächst unkenntlich gemacht, indem sie mithilfe eines komplexen Algorithmus in ein schier unauflösbar erscheinendes Zeichenknäuel aus endlos aneinandergereihten Zahlen, Buchstaben und Sonderzeichen verwandelt werden. Nur wer den „Schlüssel“ kennt, ist in der Lage, das Knäuel zu entwirren.

Praktisch kann man sich das folgendermaßen vorstellen: Will man eine Datei verschlüsseln, bedient man sich dazu eines Verschlüsselungsprogramms, das die Codierung der Datei übernimmt und über welches man das gewünschte Mittel zur Entschlüsselung festlegt. Meist wird als Mittel ein sicheres Passwort gewählt, es sind jedoch auch andere Mittel möglich, wie biometrische Daten (Fingerabdruck, Gesichtsscan) oder auch ein Softwarezertifikat, ein sogenannter → Token.

Für was man sich auch entscheidet: Der Schlüssel sollte getrennt vom Tresor an sicherer Stelle aufbewahrt werden. So nutzt die beste Verschlüsselung nichts und die Täter freuen sich, wenn sie im selben Ordner, in dem die verschlüsselte Datei liegt, ein Textdokument mit dem Passwort finden.

Verschlüsselung von Daten

Bei der Auswahl des jeweils infrage kommenden Verschlüsselungsprogramms kann man sich grundsätzlich von denselben Erwägungsgründen leiten lassen, die bereits bei der Auswahl des E-Mail-Programms maßgeblich waren:

- Am Anfang sollte eine sorgfältige Recherche stehen, bei der man sich auch über die eigenen Anforderungen und Bedürfnisse klarwerden sollte. Möchte man geräteübergreifend auf die verschlüsselten Daten zugreifen und sollen sie bei einem Clouddienst gespeichert sein, oder sollen sie nur lokal auf einem bestimmten einzelnen Gerät liegen? Will man das Risiko eingehen, dass auch alle Daten verloren sind, wenn man den Schlüssel verliert, oder wünscht man sich eine Rückversicherung? Welchen Stellenwert hat es, dass die Daten auf deutschen Servern liegen, etc.?
- Generell bieten kostenpflichtige Verschlüsselungsprogramme meist mehr Funktionalitäten und Bedienkomfort als kostenlose Programme. Bei kostenlosen Programmen sollte insbesondere genau darauf geachtet werden, dass es sich um einen seriösen Dienst und nicht um einen verkappten Datendieb handelt.
- In immer mehr Cloudspeicherdienste integrieren die Anbieter aufgrund der gestiegenen Nachfrage eigene Softwarelösungen zur Dateiverschlüsselung als Bestandteil des angebotenen Service. Ein Beispiel ist die „Fault“ in Microsoft One Drive. Ob dies für die eigene Nutzung infrage kommt, sollte zumindest einen Blick wert sein, auch wenn man sich darüber im Klaren sein muss, dass man damit Kontrolle abgibt und dem jeweiligen Anbieter sehr weitreichendes Vertrauen entgegenbringt.

7.7 Digitaler Stress

Digitale Technik zwischen Entlastung und Belastung

Digitale Medien, insbesondere das Smartphone, besitzen einen hohen Stellenwert im Leben vieler Menschen. Erhebungen bestätigen, dass vier von fünf Personen in Deutschland ein Smartphone in Gebrauch haben (Stand 2020). Dabei ermöglicht das mobile Internet einen nahezu zeit- und ortsunabhängigen Zugriff, der von drei Vierteln der Menschen genutzt wird. Insgesamt nimmt der Digitalisierungsgrad in der Bevölkerung stetig zu, der Zuwachs ist am größten bei Menschen ab 60 Jahren.

Es ist mit Vorteilen verbunden, dass heute viele Menschen über digitale Medien verfügen. Informationen austauschen, E-Mails verschicken, Nachrichten abrufen – das lässt sich mit dem Smartphone oft schnell und komfortabel auch mal zwischendurch erledigen. Mehr noch

Gut 80 Prozent der Deutschen nutzen ein Smartphone.

D21 Digital Index 19/20: https://s.rlp.de/tNeNY

sorgen elektronische Anwendungen in vielfältiger Weise dafür, dass man in Echtzeit mit Bild und Ton kommunizieren kann, und leisten darüber hinaus viele nützliche Dienste im Alltag und im Beruf, zum Beispiel, indem sie an Termine erinnern. Das macht das Smartphone heute zum ständigen Begleiter. Neben der Erleichterung und den vielen Annehmlichkeiten der digitalen Technik verursachen der andauernde Zugriff und die Erreichbarkeit aber auch zunehmend Stress und Belastung mit Folgen für das Wohlbefinden und die Gesundheit der Menschen.

Heute ist es durch digitale Technik möglich, dass an fast jedem Ort und zu jeder Zeit gearbeitet und gleichzeitig auf eine Fülle von Informationen zugegriffen werden kann. Umgekehrt kann die ständige Erreichbarkeit auch dazu führen, dass auf Dauer außerhalb der regulären Arbeitszeiten berufliche Tätigkeiten ausgeübt werden. Damit verschwimmen die Grenzen zwischen Berufs- und Privatleben.

Tipp

Stress kann entstehen, wenn äußere oder innere Anforderungen und die Fähigkeiten, diese zu bewältigen, ins Ungleichgewicht geraten.

Eine starke Nutzung digitaler Technik und Medien geht vor allem im Beruf mit erhöhten Anforderungen einher. Vor diesem Hintergrund lassen sich häufige Belastungsgründe benennen, die in der privaten wie in der beruflichen Nutzung digitaler Endgeräte erkennbar sind.

Belastungs-gründe im Alltag	Betroffene Nutzer:innen	Belastungs-gründe im Beruf	Betroffene Nutzer:innen
Soziale Verpflich-tung, sofort auf eingehende Nach-richten reagieren zu müssen	Ältere Menschen leiden mehr unter der Nachrichtenflut als jüngere.	Gefühl von Leis-tungsüberwachung durch die einfache Erfassung und Vergleichbarkeit von Leistungsdaten durch digitale Technik	Die Altersgruppe der 25- bis 34-Jäh-rigen fühlt sich am stärksten unter Druck.
Befürchtung, etwas Wichtiges zu ver-passen		Beeinträchtigung der Privatsphäre durch die Nutzung digitaler Technik und Medien	
„Multitasking“-Nut-zung von Online-inhalten, während zeitgleich andere Tätigkeiten ausgeübt werden	Ältere Menschen sind weniger anfäl-lig für Stress durch „Internet-Multitas-king“.	Unzuverlässigkeit von digitaler Technik am Arbeitsplatz, hervorgerufen durch Fehlfunktio-nen oder instabile Systeme	

Folgen von digitalem Stress

Wie sich die Folgen von gefühltem Druck durch andauernde digitale Informationsfülle und ständige Erreichbarkeit im Alltag auf das Wohl-befinden der Menschen auswirken, das lässt sich bislang nicht ein-deutig beschreiben.

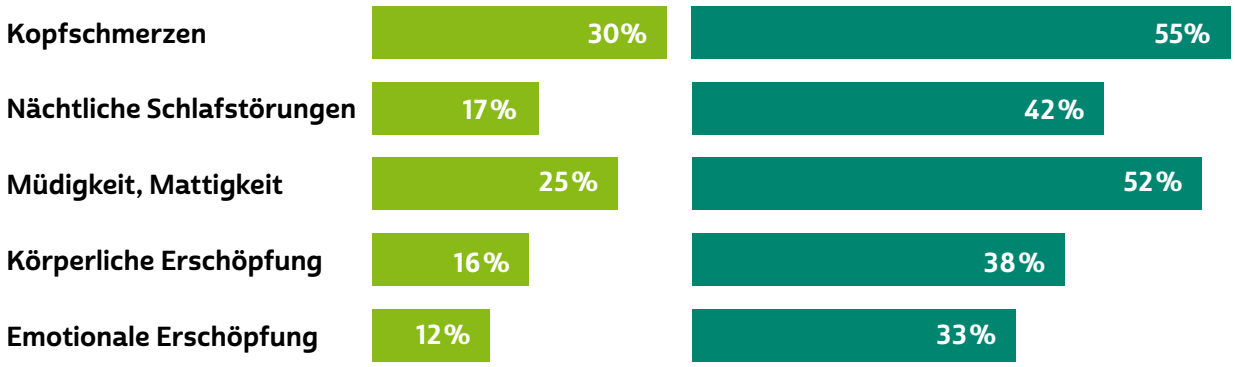
Im Berufsleben haben Beschäftigte die gesundheitlichen Auswir-kungen bereits mit dem wahrgenommenen digitalen Stress in Verbin-dung gebracht und benannt.

Silver Tipps!

Always on?:
https://s.rlp.de/U40r6

Technik macht Kopfschmerzen

So häufig sind Beschwerden bei Beschäftigten mit **niedrigem** und **hohem** Digitalstress:



Modul 8:
Soziale Medien im Netz

Wie sich digitaler Stress vermeiden lässt

Kommt es häufig zu einer oder mehreren der genannten Beschwerden, dann kann es angezeigt sein, das eigene Nutzungsverhalten digitaler Medien(inhalte) oder Anwendungen zu hinterfragen.

In der Studie „Digitaler Stress in Deutschland“ (Prof. Dr. Henner Gimpel u. a., 2018) wurde untersucht, welche Verhaltensweisen bereits erfolgreich zur Bewältigung von digitalem Stress bei der Arbeit eingesetzt wurden.

Am häufigsten wurden **fünf Verhaltensweisen** von Betroffenen genannt:

1. die Dinge von einer positiveren Seite betrachten,
2. aktiv handeln, um die Situation zu verbessern,
3. die Dinge mit Humor nehmen,
4. sich einen Plan überlegen,
5. lernen, mit der Situation zu leben.

Dabei wird darauf hingewiesen, dass Betroffene nicht nur eine, sondern viele verschiedene Vorgehensweisen wählen, um Stressbelastungen zu reduzieren.

Wer dauerhaft digitalen Stress im Alltag verringern will, kommt nicht umhin, seine Gewohnheiten zu hinterfragen und diese bewusst zu ändern.

Tipp

Gewohnheiten kann man sich durch Selbstbefragung bewusst machen:

- Geht der erste Griff am Morgen zum Smartphone?
- Wie schnell werden eingehende Nachrichten überprüft?
- Werden Nachrichten sofort beantwortet?
- Wie oft am Tag werden E-Mails gecheckt?
- Wird das Smartphone genutzt, um Langeweile zu überbrücken?
- Dient die Beschäftigung mit dem Smartphone der Entspannung?
- Geht der letzte Griff vor dem Einschlafen zum Smartphone?

Gewohnheiten zu ändern, das braucht ein gewisses Maß an Selbstdisziplin und ist dann einfacher, wenn man alte Gewohnheiten durch neue ersetzt, die zu mehr Wohlbefinden und guter Gesundheit führen.

Tipp

Anstatt sich am Morgen vom Smartphone wecken zu lassen und so gleichzeitig den Blick auf den Messenger-Dienst zu riskieren, könnte man sich am Abend einen analogen Wecker stellen. Das ersetzt dann auch den letzten Griff zum Smartphone vor dem Einschlafen.

„Zeit ist eine der wertvollsten Ressourcen. Deshalb braucht es einen bewussten Umgang mit den neuen digitalen Möglichkeiten.“

INTERVIEW MIT

Anne Spiegel

ehemalige Ministerin für Familie, Frauen, Jugend, Integration und Verbraucherschutz des Landes Rheinland-Pfalz 2016–2021

Nie konnte man so vielfältig kommunizieren wie heute. Was sind Ihrer Meinung nach die Vorteile dieser Möglichkeiten?

Anne Spiegel: Die Digitalisierung eröffnet in bisher nicht gekannter Weise Zugang zu Wissen und Informationen. Clouddienste ermöglichen, dass wir jederzeit und von überall auf digitale Dokumente zugreifen können. Shopping, Rezepte, Banküberweisung – Apps erleichtern viele Dinge und sparen Zeit. Das Web 2.0 bietet eine Vielzahl von Mitsprache- und Kommunikationsmöglichkeiten. Unzählige Foren eröffnen neue Möglichkeiten für den gesellschaftlichen Dialog. Die sozialen Netzwerke mit ihren individuellen Funktionen ermöglichen es, leicht an relevante Informationen zu gelangen, neue Kontakte zu knüpfen, sich auszutauschen und zu vernetzen. E-Mail, Echtzeitkommunikation über Instant Messenger und Videoanrufe können dazu beitragen, Beziehungen zu intensivieren und den Kontakt beispielsweise zu weit entfernt lebenden Kindern oder anderen Familienangehörigen lebendig zu halten.

Die ständige Abrufbarkeit und Erreichbarkeit setzt viele Menschen unter Druck. Wie geht man am besten mit diesem Stress um?

Anne Spiegel: Es stimmt – Zeit ist eine der wertvollsten Ressourcen. Deshalb braucht es einen bewussten Umgang mit den neuen digitalen Möglichkeiten. Wie können wir heute über das Internet kommunizieren

und seine Angebote für uns nutzen, ohne uns dabei zu stressen? Denn die ständige Erreichbarkeit und die Flut von Informationen sind auch anstrengend. Wichtig ist, den „digitalen Konsum“ im Blick zu behalten. Das kann man mithilfe von Apps machen, die die sogenannte Bildschirmzeit messen. Oder man legt einfach Zeiten fest, in denen man das Smartphone nicht zur Hand nimmt.

Als Ministerin muss ich natürlich fast immer erreichbar sein. Ich nehme mir aber auch bewusst Auszeiten, in denen ich Zeit mit meiner Familie verbringe. Mir ist es wichtig, mich bei Gesprächen voll und ganz meinen Gesprächspartner:innen widmen zu können, ohne ständig aufs Handy zu schauen. Da möchte ich auch ein Vorbild für meine Kinder sein.

Wie viel Zeit verbringen Sie täglich in sozialen Netzwerken?

Anne Spiegel: Soziale Netzwerke haben mich nie gereizt. Daher bin ich dort so gut wie nie unterwegs. Ich lese lieber Zeitung oder ein gutes Buch. Nach einem Tag mit vielen Terminen, Telefonaten, zahlreichen Akten und E-Mails, die bearbeitet werden müssen, bleibt am Abend sowieso wenig Zeit, um noch im Internet zu surfen.

Als Familienministerin weiß ich aber durchaus, dass dies ein Thema in vielen Familien ist. Manche Eltern verbringen viel Zeit online. Kinder und Jugendliche sind oft bereits in sehr jungem Alter in den sozialen Medien unterwegs. Mir ist es wichtig, dass auch die Kinder lernen, wie sie einen bewussten Umgang mit den sozialen Medien finden können. Das gilt natürlich nicht nur für die Bildschirmzeit, sondern auch für die Inhalte, die in den Apps geteilt werden. Da spielt Datenschutz ebenso eine große Rolle wie ein respektvolles Miteinander.

Glossar

Account: Ein Account ist ein Benutzerkonto für einen Onlinedienst, zum Beispiel für einen E-Mail-Service oder eine Videoplattform. Meistens gewährt dieses Benutzerkonto Zugang zu gespeicherten persönlichen Informationen oder zu sonst nicht frei zugänglichen Bereichen einer Internetseite oder eines Internetdienstes.

Algorithmus: Algorithmen sind komplexe mathematische Formeln, die miteinander verknüpft sind und im Ergebnis eine Kette von Regeln oder Anweisungen bilden, die zum Beispiel Grundlage einer computergesteuerten Entscheidung sein können.

App: Die Abkürzung „App“ steht für das englische Wort „**App**lication“, was so viel wie „Anwendung“ bedeutet. Diese Anwendungen sind nichts anderes als Programme, die je nach Funktionalität mal größer und mal kleiner im Datenumfang sind. Der Begriff „Apps“ ist in seiner Verwendung sehr eng an Smartphones und Tablet-Computer gebunden. Apps bezieht man über spezielle Stores (virtuelle Einkaufsläden), am sichersten über den Anbieter des geräteeigenen Betriebssystems.

Betriebssystem: Das Betriebssystem ist die Schaltzentrale eines PCs, Smartphones oder Tablets. Es verwaltetet alle verbauten Komponenten wie Festplatten, Grafikkarten oder Arbeitsspeicher und stellt den Nutzer:innen eine grafische Oberfläche zur Verfügung, mit der Programme aufgerufen und Dateien verwaltet werden können. Bekannte Betriebssysteme für PCs sind Windows, macOS oder Linux, für mobile Geräte Android und iOS. Damit keine Schädlinge auf den Computer gelangen und Sicherheitslücken von Kriminellen genutzt werden können, ist es wichtig, das Betriebssystem immer auf dem aktuellen Stand zu halten und regelmäßig Aktualisierungen (Updates) vorzunehmen.

Browser: Egal ob am Laptop oder Smartphone: Browser sind der Dreh- und Angelpunkt des Internetgebrauchs. Das Wort „Browser“ kommt aus dem Englischen, das Verb „to browse“ bedeutet „durchstöbern“. Browser machen das Anschauen von Internetseiten erst möglich. Sie können den sogenannten Quelltext, der auf Websites hinterlegt ist, lesen und grafisch darstellen. Bekannte Browser sind Microsoft Edge,

der auf den meisten Computern mit Windows als Betriebssystem vorinstalliert ist, Mozilla Firefox und Google Chrome, die oft separat installiert werden müssen. Auf Smartphones mit Android als Betriebssystem ist Google Chrome häufig standardmäßig als Browser eingerichtet. Der Standardbrowser für Apple-Geräte ist Safari.

Chat: Der Begriff „Chat" kommt vom englischen Verb „to chat", was so viel wie „plaudern" heißt. Gemeint ist eine textbasierte Kommunikationsform in Echtzeit mit anderen Nutzer:innen in einem virtuellen Raum. Ein Chat kann auch durch Telefonie und Videoübertragung ergänzt werden. Man spricht dann zum Beispiel von einem Videochat.

Datenvolumen: Als Datenvolumen wird die Menge an Daten bezeichnet, die ein internetfähiges Gerät braucht, sobald auf das Internet zugegriffen wird. In Internetverträgen für Smartphones wird häufig ein festgelegtes Datenvolumen zur Verfügung gestellt, sodass auch ohne eine WLAN-Verbindung eine Internetverbindung aufgebaut werden kann. Wird diese Menge überschritten, steht nur noch ein gedrosselter, das heißt verlangsamter Internetzugriff zur Verfügung.

Download: Bei einem Download werden Daten aus dem Internet auf den heimischen Computer oder mobile Endgeräte wie Smartphones und Tablets heruntergeladen, also übertragen.

Emojis: Da bei der oft kurz gehaltenen schriftlichen Kommunikation im Internet Gefühle nur schwer ausgedrückt werden können und man die Reaktion des Gegenübers nicht sehen kann, werden häufig Emojis genutzt. Das sind kleine Abbildungen, mit denen Gefühle und Mimik in einem Text bildnerisch ausgedrückt werden sollen. Bekannte Beispiele sind lachende Gesichter wie Smileys ☺. Besonders beliebt sind Emojis oder Emoticons in der Nutzung von Instant Messengern.

Emoticon: siehe *Emoji*

Follower:innen: Als „Follower" (zu Deutsch „Folgende") werden Nutzer:innen bezeichnet, die bestimmte Personen oder Inhalte in sozialen Netzwerken abonniert haben. Dadurch erhält man automatisch regelmäßig Neuigkeiten zu diesen Personen oder Themen.

Hashtag: Hashtag (von englisch „hash“ für das Rautenzeichen „#“ und dem Verb „to tag“ für „markieren“) ist die Verschlagwortung von Beiträgen und wird häufig in sozialen Netzwerken genutzt. Hierbei werden Wörter oder Sätze mit einem vorangestellten „#“ markiert, zum Bespiel „#SilverTipps“. Die Beiträge werden so in sozialen Netzwerken leichter auffindbar. Wer alle Nachrichten zu einem bestimmten Thema sehen möchte, kann einfach nach dem entsprechenden Hashtag suchen.

Instant Messenger: Instant Messenger sind Programme oder Dienste zur sofortigen Nachrichtenübermittlung über das Internet. Genutzt werden sie vor allem mobil auf Smartphones und Tablets, aber auch stationär auf Computern und Laptops. Die bekanntesten Programme dieser Kategorie sind WhatsApp, Threema, Telegram und Signal. Instant Messaging ist eine weitere Form des Chats.

Internet: Das Internet ist ein weltweit zwischenverbundenes Computernetzwerk (englisch „**Inter**connected **Net**work“). Das bedeutet, dass viele einzelne Netzwerke, etwa von Firmen, öffentlichen Einrichtungen und privaten Nutzer:innen, in einem Netzwerkverbund stehen.

Junk: siehe *Spam*

LAN: Die Abkürzung „LAN“ steht für den englischen Begriff „**L**ocal **A**rea **N**etwork“ (zu Deutsch „lokales Netzwerk“). Router und PC sind über ein Kabel miteinander verbunden. Ist dies nicht der Fall, ist das Netzwerk also kabellos (englisch „wireless“), nennt man es „**W**ireless **L**ocal **A**rea **N**etwork“, abgekürzt „WLAN“.

Link: Der Begriff stammt vom englischen Verb „to link“, was „verbinden“ bedeutet. Unter einem Link versteht man einen digitalen (Quer-)Verweis auf eine andere Stelle innerhalb einer Website, auf eine externe Internetseite, auf eine Datei oder eine Anwendung innerhalb des Internets. Links sind zentrale Strukturelemente des Internets.

Log-in: Als „Log-in“ bezeichnet man den Vorgang, bei dem ein:e Benutzer:in sich mithilfe des Benutzernames und Passworts in den gesicherten Bereich einer Website begibt (einloggt). Beispiele hierfür sind der Zugang zum E-Mail-Konto oder zum Onlinebanking.

Mailbox: Die Mailbox ist ein digitales Postfach im Internet. Beispielsweise haben E-Mail-Konten eine Mailbox, in der neue Nachrichten eingehen und ältere gespeichert werden können.

Passwort: Passwörter sind Losungswörter, mit denen der Zugang zu einem bestimmten Bereich im Internet gewährt wird. E-Mail-Konten, Onlinebanking und viele andere Benutzerkonten werden in der Regel mit einem Passwort versehen, damit nicht jede:r darauf zugreifen kann. Passwörter sollten mindestens acht Stellen haben und aus Buchstaben, Sonderzeichen sowie Ziffern bestehen.

Phishing: Beim Phishing geht es darum, mit gefälschten E-Mails und anderen Nachrichtenformen an Daten von Nutzer:innen zu kommen. Dabei werden Nutzer:innen auf gefälschte Websites gelockt, um dort ihre Daten preiszugeben. Beispielsweise erhält man eine E-Mail, in der man dazu aufgefordert wird, die eigenen Bankdaten auf einer Website anzugeben. Die entsprechende Seite sieht der Originalseite der Bank sehr ähnlich, ist allerdings eine Betrugsseite. Der Begriff „Phishing“ setzt sich zusammen aus den Wörtern „fishing“ (zu Deutsch „angeln“) und „Passwort“. Phishing ist also das Angeln nach Passwörtern.

Posting: Postings (kurz: Posts) sind Mitteilungen in einem Forum, auf einem Blog, im Kommentarfeld, in einem sozialen Netzwerk oder einem Chat.

Profil: Profile im Internet sind vergleichbar mit einem Steckbrief. Sie dienen dazu, Informationen über eine:n Nutzer:in anzuzeigen. In sozialen Netzwerken können Profile selbst angelegt und bearbeitet werden. In anderen Anwendungen wie Personensuchmaschinen werden von der Suchmaschine selbst Profile von Nutzer:innen angelegt, die aus Daten gewonnen werden, die bereits im Internet zu finden sind.

Server: Wie die Bezeichnung „Server“ (zu Deutsch „Diener“ oder „Zusteller“) schon andeutet, liegt die Funktion eines Servers in der Bereitstellung von Daten oder Anwendungen für die Teilnehmenden eines Netzwerks wie dem Internet. Ein Server kann entweder ein Computer selbst oder auch nur ein Programm sein.

Smartphone: Der auch im deutschen Sprachraum genutzte Begriff „Smartphone“ bedeutet „intelligentes oder geschicktes Telefon“. Die Funktionalität von Smartphones geht dabei weit über die eines reinen Telefons hinaus. Smartphones sind Minicomputer, die die Nutzung von vielen Programmen wie Kalender, E-Mail oder anderen Internetdiensten ermöglichen. Besondere Merkmale der Smartphones sind hochauflösende Displays (Anzeigen), zahlreiche Sensoren wie GPS und die Bedienung über Touchscreen.

Social Bot: Social Bots sind Programme, mit deren Hilfe in sozialen Netzwerken eine echte Person simuliert werden soll. Kommentare, die von diesen Programmen verfasst werden, dienen meistens dazu, ein bestimmtes Ziel zu verfolgen, wie beispielsweise die Verbreitung einer bestimmten Meinung, politischer Propaganda oder auch zu Werbezwecken. Insbesondere auf der Plattform Twitter sind Social Bots aktiv, da die kurzen Postings gut dazu geeignet sind, von einer Software simuliert zu werden. Social Bots sind durch die voranschreitende Technik immer schwerer zu erkennen und bergen die Gefahr, durch gezielten Einsatz das Meinungsbild der Internetgemeinschaft zu verzerren.

Software: Als Software bezeichnet man Programme wie das Betriebssystem eines Computers, Tablets oder Smartphones. Die Software bildet die Ergänzung zur sogenannten Hardware, also den technischen Bauteilen des Computers, und ist für die Steuerung von Prozessen innerhalb der Komponenten eines Computers zuständig.

Spam: Der Begriff „Spam“ ist abgeleitet von „**Sp**iced H**am**“, einem Dosenschinken. Die britische Comedy-Gruppe Monty Python nutzte das Wort Spam so häufig, dass es als nervend und unerwünscht empfunden wurde. Unerwünschtes, also auch unerwünschte E-Mails, bezeichnet man seitdem als Spam.

Tablet: Ein Tablet ist ein internetfähiges Gerät, dessen Größe zwischen Smartphone und Laptop liegt. Der englische Begriff „Tablet“ meint im Deutschen einen „Schreibblock“ oder eine „kleine Tafel“. Für den tragbaren Computer haben sich im deutschen Sprachgebrauch aber auch die Begriffe „Tablet-Computer“ und „Tablet-PC“ durchgesetzt. Im Vergleich zu Smartphones haben Tablets oft keinen SIM-Karten-Slot und

sind damit auf eine WLAN-Verbindung angewiesen, um ins Internet zu gehen. Wer ein Tablet auch mobil nutzen möchte, der sollte darauf achten, ein Gerät mit einem SIM-Karten-Slot für den Zugang zum Mobilfunknetz zu kaufen.

Token: Als „Token" wird in der IT eine Erkennungsmarke bezeichnet, die beispielsweise die Trägerin als Inhaberin einer Berechtigung ausweist.

Trojaner: Trojaner sind Schadprogramme, die sich als harmlose, oft auch bekannte Programme tarnen, aber tatsächlich gezielt Daten ausspionieren. Der Begriff „Trojaner" entstammt der Geschichte des Krieges um Troja, in dem das Trojanische Pferd eingesetzt wurde, um Soldaten der Belagerer unbemerkt in die gegnerische Stadt zu schmuggeln.

Trolle: Als „Trolle" werden Personen im Internet bezeichnet, deren Beiträge einzig darauf zielen, andere Nutzer:innen emotional zu provozieren. Damit soll eine Reaktion anderer Personen hervorgerufen werden. Neben einer reinen Provokation kann auch versucht werden, die eigene Meinung beziehungsweise Propaganda zu verbreiten.

Update: Bei einem Update wird ein Programm auf den aktuellen Stand gebracht. Hierfür muss in den meisten Fällen das Programm selbst mittels einer Internetverbindung auf einen Rechner der Herstellerfirma zugreifen können, um dort die Version des Programms auf dem heimischen Computer mit der auf dem Computer des Herstellers abzugleichen und gegebenenfalls zu aktualisieren. Updates sollten regelmäßig vorgenommen werden.

Web 2.0: Während beim Web 1.0, also dem Internet der ersten Generation, von einigen wenigen Programmierer:innen Inhalte für eine große Menge an Internetnutzer:innen erstellt wurden, werden beim Internet der zweiten Generation, beim Web 2.0, die Inhalte durch viele Nutzer:innen produziert. Das Web 2.0 ist damit ein Sammelbegriff für die Mitmachmöglichkeiten im Internet, wozu beispielsweise Wikis, Blogs und soziale Netzwerke gehören.

WLAN: siehe *LAN*

Autor:innen

Hannah Ballmann studierte Soziale Arbeit und Sozialpädagogik an der Katholischen Hochschule in Mainz und ist seit 2018 Mitarbeiterin bei der Stiftung MedienKompetenz Forum Südwest. Sie betreut die Inhalte auf der Website *www.silver-tipps.de* und leitet die Silver-Tipps-Redaktion.

Fabian Geib arbeitet als Referent für Medienkompetenz bei der Stiftung MedienKompetenz Forum Südwest. Er koordiniert das Projekt Digital-Botschafterinnen und -Botschafter Rheinland-Pfalz und ist Teil der Silver-Tipps-Redaktion.

Maximilian Heitkämper leitet den Fachbereich Digitales und Verbraucherrecht bei der Verbraucherzentrale Rheinland-Pfalz. Bereits im juristischen Studium waren Digitalisierung und wettbewerbsrechtliche Themen sein inhaltlicher Fokus. Zunächst als Rechtsreferent im Projekt Marktwächter Digitale Welt angestellt, übernahm er 2019 schließlich den neu geschaffenen Fachbereich.

Anja Naumer ist im Bereich Medienförderung der Medienanstalt RLP beschäftigt. Einer ihrer Arbeitsschwerpunkte liegt bei Medienprojekten für Senior:innen, dazu zählt die Durchführung von Expertenrunden für ältere Menschen zum Umgang mit digitaler Technik und Medieninhalten.

Dr. Florian Tremmel arbeitet als Referent für Offene Kanäle und Medienkompetenz bei der Medienanstalt Rheinland-Pfalz und ist pädagogischer Leiter des Projekts Digital-Botschafterinnen und -Botschafter für Rheinland-Pfalz. Zudem ist er Mitentwickler und Redaktionsmitglied des Projekts Silver Tipps – mit Freude online!.

Impressum

Titel:
Smart Surfer – Fit im digitalen Alltag
Lernhilfe für aktive Onliner:innen

Projektkoordination:
Verbraucherzentrale Rheinland-Pfalz e.V.
Laura Muth
Seppel-Glückert-Passage 10, 55116 Mainz
www.verbraucherzentrale-rlp.de

Lektorat:
WORDS IN FLOW
Julia Gilcher
Schillerplatz 18, 55116 Mainz
www.wordsinflow.de

Gestaltung:
alles mit Medien
Anke Enders
Freiherr-vom-Stein-Straße 10, 55576 Sprendlingen
www.allesmitmedien.de

Bildnachweis:
Cover: Laura Muth, Malin Günther (Liv Liv Design);
Portrait Anne Spiegel: MFFJIV; Portrait Hannah Ballmann, Maximilian Heitkämper, Dr. Florian Tremmel: Laura Muth;
Portrait Fabian Geib: Maresa Getto; Portrait Anja Naumer: Backofen

Autor:innen:
Dr. Julia Gerhards, Michael Gundall, Maximilian Heitkämper, Jennifer Kaiser und Miriam Raic von der Verbraucherzentrale Rheinland-Pfalz e.V.; Hannah Ballmann und Fabian Geib von der Stiftung MedienKompetenz Forum Südwest; Anja Naumer und Dr. Florian Tremmel von der Medienanstalt Rheinland-Pfalz; Helmut Eiermann, Timo Göth und Sonja Wirtz als Mitarbeiter:innen des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz; Andreas Büsch von der Clearingstelle Medienkompetenz der Deutschen Bischofskonferenz an der KH Mainz.
Ehemalige Autor:innen: Christian Gollner und Barbara Steinhöfel von der Verbraucherzentrale Rheinland-Pfalz e.V.; Christian Wedel und Jeanine Wein, freiberufliche Medienpädagog:innen; Annette Thunemann vom Medienkompetenz Netzwerk Mainz-Rheinhessen.

Diese Lernhilfe wurde erstellt von:

Das Projekt wurde gefördert durch:

Dank:
Wir danken unseren Förderern, die ein solches länderübergreifendes Projekt möglich gemacht haben. Unser Dank gilt auch allen weiteren Multiplikatoren, die uns helfen, dieses Wissen an die interessierten Onliner:innen weiterzutragen.
Ein besonderer Dank gilt zudem allen Autor:innen und Interview-Partner:innen, den Coverfoto-Modellen und allen weiteren Unterstützer:innen des Projekts.

Herausgeber:
Verbraucherzentrale Berlin e.V.
Ordensmeisterstr. 15-16
12099 Berlin
verbraucherzentrale-berlin.de

Bezugsadressen:
Verbraucherzentrale Berlin e.V.
Ordensmeisterstr. 15-16
12099 Berlin
verbraucherzentrale-berlin.de/smart-surfer-be

Smart Surfer | 2021