SO BEWEGE ICH MICH KOMPETENT UND SICHER IM INTERNET

Landen in Ihrem E-Mail-Postfach hin und wieder Spam-Nachrichten von unbekannten Absender_innen? Haben Sie in einer vermeintlich kostenlosen App schon einmal versehentlich Geld ausgegeben? Begegnen Sie in sozialen Netzwerken gelegentlich hasserfüllten Nachrichten? Zweifeln Sie manchmal an der Glaubwürdigkeit von Online-Nachrichten?

Wer sich im Internet bewegt, steuert zwangsläufig auf **kleinere und größere Hürden der Online-Welt** zu. Zwischen den vielseitigen Potenzialen des World Wide Web verbergen sich leider auch Betrugsfallen, schädliche Computerprogramme, Falschinformationen und viele weitere Gefahrenherde. Die Anonymität des Internets kann Hass und unehrliche Absichten befeuern. Dass wir bei jeder Internetnutzung zudem persönliche Datenspuren hinterlassen, kann Trickbetrüger_innen und Datenkonzernen in die Karten spielen.

Im Folgenden finden Sie **Tipps, wie Sie Ihre persönlichen Daten im World Wide Web schützen und sicher mit anderen Online-Nutzer_innen kommunizieren können**. Auch für Ihre Klient_innen, die aufgrund ihrer Beeinträchtigungen möglicherweise auf besondere Hürden stoßen, ist ein kompetenter Umgang mit dem Internet zentral, um digitale Medien sicher mit Freude nutzen zu können. Um auf eine Auswahl möglicher Gefahrenquellen hinzuweisen, leiten konkrete **Fallbeispiele aus dem heilpädagogischen Arbeitskontext** die nachfolgenden Ratschläge ein. Diese Tipps können Sie gemeinsam mit Ihren Klient_innen aufarbeiten oder im Umgang mit Ihrer Zielgruppe proaktiv anwenden. Das Internet bietet für jede_n – ob mit oder ohne Beeinträchtigung – Stolpersteine. Nehmen Sie die Themen Internetsicherheit und Datenschutz für sich und für Ihre Klient_innen ernst!

Meine Daten und ich – persönliche Informationen schützen

Heutzutage scheint im Internet alles möglich zu sein: Wir können online einkaufen, unsere Bankangelegenheiten im World Wide Web abwickeln, Nachrichten auf Internetseiten lesen und uns digitaler Unterhaltungsmedien zum Filmeschauen oder Musikhören bedienen. Inzwischen gibt es unter dem Schlagwort *Smart Home* sogar digital unterstützte Haushaltsgeräte, die zum Beispiel über WLAN gesteuert werden können. Der Trend der Digitalisierung durchdringt zunehmend alle Lebensbereiche. Dass unser Alltag dadurch stark erleichtert wird, hat jedoch seine Kehrseite: Wir werden zu gläsernen Internetnutzer_innen. Mit jeder Online-Aktivität erzeugen wir Spuren von persönlichen Daten, einen **digitalen Fußabdruck**, der Dritten verrät, wer wir sind und was wir tun. Auch wenn wir uns im Internet womöglich unsichtbar fühlen – unsere Daten sind es nicht. Damit diese nicht von Werbetreibenden, Hacker_innen oder Betrüger_innen missbraucht werden, folgen Ratschläge rund um das Thema Datenschutz.

Wie gut kennen mich Google und Co? – Web-Tracking vermeiden

Beispiel: Natan tut sich aufgrund einer kognitiven Beeinträchtigung schwer, im Internet zurechtzukommen, komplexe Webseiten zu verstehen und Suchmaschinen zu bedienen. Damit der Umgang für ihn leichter wird, möchte er sich ein Sprachassistenzsystem für Zuhause kaufen. Er sucht über Google nach verschiedenen Angeboten. In den nächsten Tagen tauchen in seinem Webbrowser und in seinem Facebook-Account ständig unerwünschte Werbeanzeigen für Sprachassistenzsysteme auf, auch nachdem er schon längst ein Produkt ausgewählt und gekauft hat.

Beim **Web-Tracking** werden unsere Bewegungen im Internet beobachtet. Rufen wir eine Internetseite auf, werden kleine Datenpakete, sogenannte **Cookies**, auf unserem Computer oder Smartphone gespeichert. Bei der nächsten Internetnutzung wird unser Gerät über diese Cookies wiedererkannt, wodurch unsere Daten einander zugeordnet, zu Nutzer_innenprofilen verdichtet und an Dritte, wie etwa Werbetreibende, weitergegeben werden können.

Datenschutzeinstellungen verwalten

- **Cookies einschränken:** Sie können das Speichern von Cookies unter den Datenschutzeinstellungen Ihres Webbrowsers (z.B. Firefox oder Google Chrome) verwalten. Allerdings funktionieren die meisten Internetseiten nur mit Cookies, weshalb das Deaktivieren aller Cookies oft Fehlermeldungen hervorruft. Sie können jedoch für ausgewählte Seiten den Zugriff auf Cookies verweigern oder aber Cookies im Allgemeinen deaktivieren und nur für ausgewählte Seiten erlauben. Sinnvoll ist außerdem, Cookies nur temporär zu nutzen und grundsätzlich einzustellen, dass alle lokalen Daten nach Schließen des Browsers gelöscht werden.
- **Drittanbieter-Cookies:** Deaktivieren Sie über die Browsereinstellungen Cookies von Drittanbieter_innen. Das sind zum Beispiel Cookies von Facebook, die über einen „Gefällt mir"-Button auf anderen Internetseiten eingebunden sind und Facebook das Lesen Ihrer Daten auch außerhalb von Facebook ermöglichen. Wenn eine Internetseite ohne die Berechtigung von Drittanbieter-Cookies nicht funktioniert, können Sie Ausnahmen von dieser Sperre hinzufügen.
- **„Do not track"-Aufforderung:** Unter den Datenschutzeinstellungen Ihres Browsers gibt es das Feld „Do not track". Aktivieren Sie es, um Webseiten mitzuteilen, dass Sie das Tracking Ihres Internetverhaltens nicht wünschen. Zwar ist diese Einstellung aufseiten der jeweiligen Betreiber_innen freiwillig, allerdings kommen viele Internetseiten der Aufforderung nach und spielen Ihnen keine personalisierte sondern von Ihren Webaktivitäten unabhängige Werbung zu.
- **App-Berechtigungen:** Bei der Installation vieler Apps müssen den Betreiber_innen Berechtigungen eingeräumt werden, auf persönliche Daten zuzugreifen, etwa auf den Standort des Geräts, die Kamera oder das Mikrofon. Unter den Einstellungen Ihres Geräts können diese Berechtigungen verwaltet werden. Überlegen Sie kritisch, welche App welche Berechtigungen braucht. Benötigt ein Quiz-Spiel z. B. wirklich Zugriff auf Ihre Kamera? Verweigern Sie alle Berechtigungen, die nicht für das Funktionieren einer App zwingend erforderlich sind.
- **Werbeblocker:** Im Hintergrund laufende Werbefilter bzw. Ad-Blocker können oftmals kostenlos für den eigenen Browser heruntergeladen werden und unterdrücken lästige Werbebanner und Werbevideos.

Existierende Daten löschen

- **Browserverlauf:** Unter „Verlauf" oder „Chronik" in den Browsereinstellungen lassen sich einzelne Elemente oder der gesamte Verlauf Ihrer Suchanfragen löschen.
- **Passwörter:** Sie können Passwörter für bestimmte Internetseiten speichern, damit diese zukünftig automatisch eingegeben werden. Wollen Sie diese Einstellung für ein einmal gespeichertes Passwort wieder löschen, können Sie das über Ihre Browsereinstellungen unter Datenschutz und/oder Browser-Verlauf tun.
- **Auto-Fill-Daten:** Womöglich speichert Ihr Browser persönliche Daten wie etwa Name, Adresse oder Telefonnummer ab, die Sie in digitale Formulare eingeben, und füllt diese bei anderen Formularen automatisch aus. Diese Daten können Sie ebenfalls unter den Datenschutz- und/oder Verlauf-Einstellungen Ihres Webbrowsers löschen.

Voll zugespamt
– Werbebotschaften und Betrugsmaschen erkennen

Beispiel: Lara, eine junge Frau mit Autismus, hat zu ihrem Geburtstag ein Smartphone bekommen. Die Betreuerin ihrer Wohngruppe verwaltet für sie einen Mobilfunkvertrag bei dem Anbieter XXtalk. Eines Tages erhält Lara an ihre private E-Mail-Adresse eine Nachricht vom Absender „rechnungOnline.@XXtalk.de“ mit dem Betreff „Rechnung März“.
Sie lautet: „Guten Tag, mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung von XXtalk. Die Gesamtsumme im Monat Oktober beträgt 55.69 Euro. Details sehen Sie im Anhang. Wenn sie noch weitere Fragen zur Rechnung haben, stehen wir ihnen unter Kundenservice.@XXtalk.de gerne zur Verfügung. Mit freundlichen Grüßen, Ihr XXtalk Kundenservice“
Lara weiß, dass XXtalk ihr Mobilfunkanbieter ist. Sie öffnet das Dokument im Anhang, woraufhin ihr Laptop mit einem Computervirus infiziert wird.

Unter **Spam** versteht man unverlangt zugesendete Nachrichten, meist auf elektronischem Weg. Diese enthalten häufig Werbebotschaften, können aber auch Schadprogramme transportieren (Malware, z. B. Computerviren oder Trojaner) oder persönliche Daten wie Passwörter oder Kontodaten ködern (**Phishing**).

Spam-Mails erkennen

- **Absender_in:** E-Mails von unbekannten Absender_innen sowie merkwürdigen E-Mail-Adressen, die etwa aus willkürlich aneinander gereihten Buchstaben und Zahlen bestehen oder Satzzeichen unüblich einsetzen, sind kritisch zu betrachten.
- **Betreff:** Ist der Betreff reißerisch formuliert (z. B. „Wovon Sie schon immer geträumt haben!“), macht extrem hohe Rabattversprechen oder lässt keine Aussage über den Inhalt der Nachricht zu (z. B. „Wichtig, dringend öffnen!!!“) heißt es: Alarmglocken an!
- **Anrede:** Spam-Mails verwenden meist eine allgemeine Anrede (z. B. „Sehr geehrter Kunde“) statt Sie persönlich mit Ihrem Namen anzusprechen.
- **Inhalte:** Oft dreht sich Spam um Werbung, kostenlose Produkte oder Gewinnspiele. Themen können auch vermeintliche technische Probleme oder Sicherheitslücken an Ihrem Gerät, Wundermedikamente oder finanzielle Mahnungen sein.
- **Handlungsaufforderungen:** Seien Sie misstrauisch bei E-Mails, die Sie dazu drängen, Rechnungen zu bezahlen, Anhänge zu öffnen, auf einen Link zu klicken oder persönliche Daten in ein Formular einzugeben. Häufig werden solche Aufforderungen unter Zeitdruck gestellt (z. B. „Zahlen Sie Ihre Rechnung bis heute Abend!“) sowie Konsequenzen bei Nichtbefolgung angedroht.
- **Stil:** Viele Spam-Nachrichten enthalten Rechtschreib- und Grammatikfehler, sind schlecht formatiert und tarnen sich durch leere Floskeln.
- **Impressum:** Im geschäftsmäßigen E-Mail-Verkehr von Unternehmen, etwa beim Versenden von Angeboten, Auftragsbestätigungen oder Rechnungen, besteht in Deutschland Impressumspflicht.

Mit Spam-Mails umgehen

- **Nicht reagieren:** Gehen Sie auf keinen Fall auf eine E-Mail ein, die Ihnen merkwürdig vorkommt! Erst recht nicht, wenn sie Sie dazu drängt, persönliche Daten zu senden oder Formulare auszufüllen. Antworten Sie nicht, klicken Sie keine Links in der E-Mail an und laden Sie keine Anhänge herunter.
- **Spam-Filter:** Verschieben Sie E-Mails, die Sie als Spam identifiziert haben, in den Spam-Ordner Ihres E-Mail-Programms. Dadurch kann der Spam-Filter dazulernen und ähnliche Nachrichten zukünftig direkt in den Spam-Ordner verschieben.
- **Zweite E-Mail-Adresse:** Um Ihre Haupt-E-Mail-Adresse vor Spam zu schützen, ist es ratsam, eine zweite Adresse etwa für Gewinnspiele, Online-Shopping und Newsletter zu verwenden. Geben Sie Ihre normale E-Mail-Adresse so selten wie möglich an Webseiten und Unternehmen weiter.

Gesehen, geklickt, gezahlt – sicher im Internet einkaufen

Beispiel: Julius spielt gerne Videospiele. Damit er im Gemeinschaftszimmer seiner inklusiven Wohngemeinschaft mit Sound spielen kann, ohne die anderen zu stören, möchte er sich Kopfhörer kaufen. Er sucht im Internet nach Angeboten und findet teure Marken-Kopfhörer stark reduziert auf der Verkaufsplattform Technik-shopping.org. Obwohl die Plattform Julius unbekannt ist und nur eine Zahlung per Kreditkarte zulässt, bestellt er das Produkt. Schon am nächsten Tag wird ihm das Geld vom Konto abgebucht. Die Kopfhörer kommen allerdings nie bei Julius an. Als er versucht, den Kundenservice von Technik-shopping.org zu kontaktieren, muss er feststellen, dass es den Shop gar nicht gibt.

Beim **Online-Shopping** werden Waren oder Dienstleistungen über das Internet ausgewählt, bestellt und bezahlt. Neben seriösen Verkäufer_innen gibt es auch viele gefälschte Online-Shops, die von anderen Portalen kopierte Produktbilder und -informationen verwenden. Sie greifen Kontodaten ab, die im Bezahlvorgang auf der Internetseite angegeben werden, oder liefern ein bestelltes Produkt nach Vorauszahlung nicht.

Kaufentscheidungen durchdenken

- **Keine Impulskäufe:** Kaufen Sie im Internet nicht spontan ein! Oft werden wir durch aufblinkende Werbung oder besondere Aktionen dazu verführt, sofort auf „Kaufen“ zu klicken. Nehmen Sie sich dennoch die Zeit, die Verkaufsplattform zu prüfen und ihren Kaufwunsch zu überdenken.
- **Verkaufsplattform:** Sofern Sie nicht eines der marktführenden, geprüften Verkaufsportale nutzen, informieren Sie sich über einen Online-Shop, bevor Sie einen Kauf abwickeln. Ein Anzeichen für einen unseriösen Shop kann ein fehlendes oder lückenhaftes Impressum sein. Begegnen Sie auch widersprüchlichen Angaben, ungewöhnlich hohen Rabatten und tadellosen, einheitlichen Kund_innenbewertungen skeptisch.

- **Private Verkäufer_in:** Privatpersonen, die beispielsweise über eBay Kleinanzeigen Produkte anbieten, können meist schwerer überprüft werden als Online-Shops. Ein Profil mit persönlichen Angaben, positive Bewertungen von anderen Kund_innen und ein kommunikativer Austausch vor dem Kauf können das Vertrauen jedoch fördern.
- **Vergleichen:** Im Internet gibt es zahlreiche Seiten, auf denen Sie Preise von verschiedensten Produkten vergleichen können. Werfen Sie einen Blick auf die Preisentwicklung sowie auf Angebote von anderen Anbieter_innen. So können Sie ungewöhnlich hohe oder niedrige Preise leichter einschätzen.
- **Rechnung prüfen:** Bevor Sie auf „Kaufen“ klicken, lohnt es sich, die Rechnung noch einmal zu überfliegen. Es kann vorkommen, dass Sie aus Versehen weitere Produkte zu Ihrem Warenkorb hinzugefügt haben oder Versandkosten und Mehrwertsteuern erst im letzten Schritt hinzugerechnet werden.

Sichere Zahlungswege wählen

- **Auf Rechnung:** Bei einer Zahlung auf Rechnung überweisen Sie das Geld erst, wenn die Ware bei Ihnen angekommen ist. Diese Zahlungsweise ist im Vergleich zu 1-Klick-Bestellungen zwar etwas umständlicher, geht aber kein Risiko einer fehlerhaften oder ausbleibenden Lieferung ein.
- **Einzugsermächtigung:** Einem Bankeinzug können Sie innerhalb von acht Wochen, nachdem das Konto belastet wurde, widersprechen. Sie erhalten das Geld von Ihrem Kreditinstitut daraufhin ohne weiteren Aufwand zurück.
- **Käufer_innenschutz:** Einige Internet-Bezahlsysteme, zum Beispiel PayPal, bieten Ihren Kund_innen einen Käufer_innenschutz: Wenn Sie ein bestelltes Produkt nicht oder anders als beworben erhalten, bekommen Sie Ihr Geld zurück. Da Sie Ihre Bankdaten nicht direkt an die Online-Händler_innen übermitteln, sondern der Kauf über das Internet-Bezahlsystem abgewickelt wird, werden Ihre sensiblen Daten außerdem geschützt.
- **Sichere Internetverbindung:** Wenn sie online Ihre Bankdaten eingeben, achten Sie auf eine verschlüsselte Internetverbindung. Sie erkennen diese an dem Kürzel „https“ und einem Schlosssymbol in der Adresszeile des Browsers.

Spielwelt versus Realität – einen klaren Blick in digitalen Spielen behalten

Beispiel: Maria nutzt ihr Smartphone gerne in ihrer Freizeit für Spiele. Gemeinsam mit ihrem heilpädagogischen Betreuer lädt sie ein kostenloses Rätselspiel auf das Gerät. Wenn sie bei einer Rätselaufgabe mal nicht weiterkommt, kann sie mit Spielmünzen der App Hinweise zur Lösung kaufen. Das Spiel schlägt Maria immer wieder vor, mehr Spielmünzen freizuschalten. Maria nimmt diese Vorschläge mehrmals an, bis ihr Betreuer auf der Rechnung des Mobilfunkanbieters Abbuchungen einer fremden Firma entdeckt. Ohne es gemerkt zu haben, hat Maria mehrere In-App-Käufe getätigt.

Gaming und digitale Spiele sind sehr beliebt – ganz gleich ob auf mobilen Endgeräten wie Smartphone oder Tablet, auf Konsolen wie der Playstation oder am PC. Eine Spieloberfläche mit fiktiver Geschichte und fiktiver Währung kann das Gespür für reale Zusammenhänge jedoch schnell trüben.

Kostenfallen umgehen

- **In-Game-Käufe kennen:** Durch In-Game-Käufe (innerhalb von Apps auch In-App-Käufe genannt) können virtuelle Güter oder Leistungen in Spielen erworben werden. Diese Kaufabwicklungen gibt es in kostenlosen wie auch in kostenpflichtigen Spielen. Beispiele sind kostenpflichtige Zusatzinhalte, etwa neue Level oder Spielfiguren, der Erwerb von Spielwährungen durch echtes Geld oder das kostenpflichtige Abschalten von Werbeanzeigen. Bei kostenlosen Spielen gibt es außerdem häufig eine Premiumversion, die gegen Gebühr die Basisversion aufwerten kann.
- **Keine Kreditkarte hinterlegen:** Viele Shops wie der iTunes-Store, in denen Spiele und Apps heruntergeladen werden können, können mit einer Kreditkarte hinterlegt werden. Dadurch werden In-App-Käufe nach einmaliger Eingabe der Kartendaten hürdenlos abgewickelt. Sorgen Sie unbeabsichtigten oder unüberlegten Käufen vor, indem Sie keine Zahlungsweise hinterlegen.
- **Ausgaben im Blick behalten:** Oft sind es nur geringe Beträge, die bei In-Game-Käufen fällig werden. Betrachten Sie Ihre Ausgaben stets in Summe und lassen Sie sich von niedrigen Preisen nicht mitreißen.
- **In-App-Käufe einschränken oder deaktivieren:** Um auf Nummer sicher zu gehen, können Sie In-App-Käufe in den Einstellungen Ihres Geräts oder Ihres App-Stores vollständig ausschalten oder durch Festlegen eines PIN-Codes, der vor jedem Kauf abgefragt wird, besser regulieren. Informieren Sie sich im Internet und halten Sie nach einer Anleitung Ausschau, wie Sie In-App-Käufe für Ihr konkretes Gerät und Betriebssystem verwalten können.

Den Bezug zur Realität bewahren

- **Reflexion:** So schön es auch ist, in einer Spielwelt zu versinken, reflektieren Sie immer mal wieder über die realen Bezüge des Spiels. Denken Sie daran, dass hinter anderen Online-Spieler_innen echte Menschen stecken, dass die Betreiber_innen des Spiels oder der App meist wirtschaftliche Interessen verfolgen und dass exzessives Gaming in realen Schwierigkeiten wie sozialer Isolierung oder Spielsucht münden kann.
- **Pausen:** Um einen kritischen Blick auf digitale Spiele zu bewahren, machen Sie während einer Spielsitzung oder auch zwischen längeren Spielphasen ausreichend Pausen, in denen Sie sich mit anderen Themen und sozialen Kontakten beschäftigen.
- **Ausgleichendes Hobby:** Pflegen Sie neben Ihrer Freude für digitale Spiele auch andere Hobbys. Freizeitbeschäftigungen neben dem Gaming verhindern, dass die Spielwelt zu einer realitätsfernen Zuflucht aus dem Alltag wird. Um das Unterbrechen eines (Online-)Spiels zu erleichtern, kann es hilfreich sein, sich mit den Gaming-Freund_innen zu verabreden.

Die Anderen und ich – souverän online kommunizieren

Internet, Smartphones und der anhaltende technische Fortschritt verändern unsere zwischenmenschliche Kommunikation. Briefe, Telefonate und persönliche Treffen werden ergänzt durch E-Mails, Chats und Videokonferenzen. Online und mobil können wir uns schnell und einfach austauschen. Soziale Medien wie Facebook oder YouTube vernetzen Personen rund um den Globus miteinander und öffnen völlig neue Türen, um fremde Menschen kennenzulernen. Das Internet ist geprägt durch **Schnelllebigkeit**, durch **Öffentlichkeit** und oftmals auch durch **Anonymität**. Dadurch bietet es nicht nur Chancen, sondern auch Betrug und Missbrauch in der Online-Kommunikation einen Raum. Hier finden Sie Tipps, um zentrale Hürden souverän zu meistern.

Ich zeig‘ dir meine Welt – Informationen reflektiert teilen

Beispiel: Phillip hat mehrere Jahre in einer Werkstatt für Menschen mit sogenannter Behinderung gearbeitet. Ein Integrationsfachdienst unterstützt ihn nun beim Übergang in den freien Arbeitsmarkt. Als er einen Vertrag für eine Hilfstätigkeit in einer Gärtnerei unterschreibt, ist er so stolz, dass er diesen Moment mit seinen Freund_innen teilen möchte. Er veröffentlicht ein Bild von seinem Arbeitsvertrag in seiner Instagram-Story und markiert seinen zukünftigen Betrieb. Am nächsten Tag wird er von der Gärtnerei angerufen. Auf dem Foto in Phillips Story waren sensible Unternehmensdaten zu sehen. Zwar bleibt Phillips Handeln bis auf eine Ermahnung der Geschäftsführerin, in Zukunft verantwortungsvoller mit vertraulichen Daten umzugehen, folgenlos. Trotzdem ärgert sich Phillip tagelang über sich selbst, dass er schon vor Arbeitsantritt einen Fehler gemacht hat.

Das Internet ist ein **öffentlicher Raum**. Inhalte, die online geteilt werden, können von anderen Nutzenden angesehen, weitergeleitet und gespeichert werden. Private Inhalte können so in falsche Hände geraten, Spott nach sich ziehen oder sogar Zukunftschancen verbauen.

Keine sensiblen Daten preisgeben

- **Personenbezogene Daten:** Vermeiden Sie es, private Daten wie Ihren vollständigen Namen, Ihre Adresse oder Ihre Telefonnummer in Social-Media-Profilen und in Online-Chats preiszugeben. Besonders bei reinen Internetbekanntschaften sollten Sie keine Informationen weitergeben, durch die Sie zu identifizieren oder aufzufinden sind.
- **Bankdaten:** Gehen Sie vorsichtig mit sensiblen Daten um, die mit Ihren Finanzen zusammenhängen. Kontodaten, Kreditkartennummern und konkrete Auskünfte über ihren Finanzhaushalt sollten möglichst nur beim Online-Banking oder Online-Shopping auf sicheren Internetseiten angegeben werden.

- **Passwörter:** Geben Sie Ihre Passwörter niemals per Online-Kommunikation weiter! Wenn Sie einer vertrauensvollen Person, zum Beispiel einem Familienmitglied, Zugang zu einem Online-Account gewähren wollen, senden Sie die Zugangsdaten nicht per E-Mail oder über einen Chat. Übermitteln Sie das Passwort mündlich oder analog mit Papier und Stift (aber Achtung: Auch ein Zettel kann in falsche Hände geraten!).
- **Intimsphäre schützen:** Egal ob im Profil oder im Chat, es sollten niemals anzügliche, freizügige Bilder oder Nacktaufnahmen über das Internet geteilt werden! Es ist außerdem ratsam, sehr intime Informationen (z. B. über Krankheiten oder Familienprobleme) nicht im Online-Austausch mitzuteilen.

Soziale Netzwerke kritisch nutzen

- **Reichweite reflektieren:** Bevor Sie etwas in sozialen Netzwerken teilen, machen Sie sich bewusst, wer die Information (z.B. Bild, Video, Status) sehen wird. Ist ihr Profil öffentlich oder nur für Freund_innen sichtbar? Wer befindet sich alles in Ihrer Freund_innenliste? Fragen Sie sich stets, ob Sie Ihre Postings (z.B. Urlaubsfotos oder Geschichten aus Ihrem Privatleben) all denjenigen, die Ihr Profil sehen können, auch persönlich zeigen würden. Bei den meisten sozialen Netzwerken können Sie die Sichtbarkeit Ihres gesamten Profils oder einzelner Inhalte verwalten und nur für bestimmte Personengruppen freischalten.
- **Separater Raum für neue Kontakte:** Überlegen Sie: Was gibt es online für Orte zum Austausch? Mit welchen Personen wollen Sie wo in Kontakt treten? Es kann sinnvoll sein, auf unterschiedlichen Plattformen unterschiedlich viele Informationen von sich preiszugeben. Wenn auf Instagram etwa private Fotos mit Freund_innen geteilt werden, sollte das Profil nicht für Fremde offen sein. Nutzen Sie für die Suche nach neuen Kontakten bewährte Kontaktbörsen oder ein separates Profil in sozialen Netzwerken, auf dem nur ausgewählte Informationen öffentlich einzusehen sind.
- **Inszenierungen:** Behalten Sie im Hinterkopf, dass Fotos und Geschichten in sozialen Medien nicht der Wahrheit entsprechen müssen. Fotobearbeitungssoftware und inszenierte Profile können ein verzerrtes, oft idealisiertes Bild vom Leben anderer erzeugen. Machen Sie sich bewusst, dass jede_r mal traurig ist oder langweilige Tage hat, diese Momente aber meist nicht online teilt.

Trolle, Mobbing und Shitstorms – Hass im Netz die Stirn bieten

Beispiel: Martina, ein 16-jähriges Mädchen mit Down-Syndrom, freundet sich in ihrer neuen Schule mit einer Gruppe gleichaltriger Mädchen an. Am Wochenende ist sie zu einer Geburtstagsparty eingeladen, auf der Alkohol ausgeschenkt wird. Um in ihrem neuen Freundinnenkreis nicht anzuecken, trinkt sie zwei Flaschen Bier. Im Laufe des Abends machen sie und ihre Freundinnen einige Fotos. Am nächsten Tag landet ein peinliches Foto von Martina in der WhatsApp-Gruppe ihrer Klasse. Einige ihrer Klassenkamerad_innen machen sich mit gemeinen Kommentaren, die alle in der Gruppe lesen können, über Martina und ihre Behinderung lustig.

Hass im Internet kann viele Formen annehmen: Sogenannte **Trolle** stören absichtlich die Online-Kommunikation und verbreiten provozierende Inhalte. Bestimmte Menschengruppen werden in sozialen Netzwerken immer wieder diskriminiert, angegriffen oder es wird gegen sie zur Gewalt aufgefordert (**Hassrede/Hatespeech**). Viele Heranwachsende wie auch Erwachsene werden zum Opfer von Mobbing-Attacken (**Cybermobbing**) oder bekommen Hasslawinen (**Shitstorm**) ab.

Sich präventiv und im Akutfall schützen

- **Wenig Angriffsfläche bieten:** Teilen Sie öffentlich möglichst keine Informationen, die Sie zur Zielscheibe von Hass machen können (z. B. peinliche Bilder oder kontroverse Standpunkte) und brechen Sie Kontakte, die Ihnen Unwohlsein bereiten, ab.
- **Nicht reagieren:** Wenn Sie Opfer einer Mobbing-Attacke werden, antworten Sie nicht auf Beleidigungen, Drohungen oder Belästigungen! Mobbing-Täter_innen werden durch die Reaktionen ihrer Opfer erst recht befeuert. Mobben Sie nicht zurück, sondern wenden Sie sich an eine Vertrauensperson, eine Hilfestelle oder bei anhaltender Belästigung oder ernsthafter Bedrohung an die Polizei.
- **Beweise sichern:** Machen Sie Screenshots oder Fotos von Hassnachrichten, beleidigenden Kommentaren oder Gewaltandrohungen. Da das Internet sehr schnelllebig ist, können Beweise von Mobbing oder gruppenbezogener Menschenfeindlichkeit nach kurzer Zeit verschwinden und somit konfliktlösende Maßnahmen (z. B. Konfrontation der Täter_innen unter professioneller Begleitung) oder ein gerichtliches Vorgehen verhindern.
- **Weiteren Kontakt unterdrücken:** Um aus dem Kreuzfeuer zu geraten, sollten Sie Mobbing-Täter_innen umgehend blockieren. Wenn Sie in einem sozialen Netzwerk oder Online-Forum vor einem großen Personenkreis bloßgestellt oder gedemütigt wurden, kann es außerdem erleichternd sein, den Nicknamen zu ändern.
- **Melden:** In den meisten sozialen Netzwerken können Sie Nutzende, die sich Ihnen oder anderen Menschen(gruppen) gegenüber unangemessen verhalten, melden. Daraufhin wird das Profil geprüft und womöglich gesperrt. Auch einzelne Inhalte, zum Beispiel beleidigende Postings, können gemeldet und von den Betreiber_innen des sozialen Netzwerks als Folge gelöscht werden.

Gegenrede formulieren

- **Situation einschätzen:** Um Hass und Negativität im Internet nicht dauerhaft das Feld zu überlassen, ist Gegenrede sehr wichtig. Bei gruppenbezogener Menschenfeindlichkeit, Troll-Nachrichten oder Mobbing-Attacken auf andere – Opfer können sich selber oft nicht effektiv zur Wehr setzen – können Sie mit Gegenstrategien eingreifen. Achten Sie jedoch auf Ihren Energiehaushalt: Verstricken Sie sich nicht in endlosen hitzigen Diskussionen und schaffen Sie sich ausgleichende positive Erlebnisse. Schützen Sie außerdem Ihre eigenen Daten und blockieren Sie Täter_innen sofort, wenn diese Sie persönlich angreifen.
- **Sachlichkeit:** Begeben Sie sich nicht auf das Niveau der Täter_innen, sondern fordern Sie eine sachliche, ruhige Diskussion ein und gehen Sie mit gutem Beispiel voran.

- **Argumentieren:** Stellen Sie Verständnisfragen, verlangen Sie konkrete Beispiele, weisen Sie auf Lücken in der Argumentation des Gegenübers hin, nennen Sie Fakten und führen Sie alternative Quellen an. Somit eröffnen Sie neue Perspektiven auf ein Thema oder eine festgefahrene Einstellung. Auch wenn Sie die Täter_innen oft nicht überzeugen können, bieten Sie Mitlesenden Gegenargumente und ermutigen diese im Idealfall, sich ebenfalls einzumischen.
- **Positivität und Humor:** Positive Geschichten und Humor können helfen, um aufgeladene Diskussionen zu entschärfen. Ironischer Widerstand ist außerdem oft eine geeignete Gegenstrategie, wenn sich Täter_innen nicht auf eine sachliche Diskussion einlassen wollen.
- **Gespräch abbrechen:** Brechen Sie Gespräche ab, die auf Dauer nicht zielführend sind und Ihnen nur Nerven rauben.

Real oder inszeniert? – Fake News erkennen

Beispiel: Robert arbeitet in einer inklusiven Werkstatt. In seiner Freizeit ist er viel auf Facebook unterwegs und liest dort aktuelle Nachrichtenmeldungen. Eines Tages liest er auf einer regionalen Facebook-Seite, dass in seiner Stadt aufgrund des starken Schneefalls am nächsten Tag für alle Schüler_innen und alle Arbeitnehmer_innen, die in der Stadt arbeiten, schneefrei ist. Da schon jetzt sehr hoch Schnee liegt und bereits einige Bahnstrecken in seinem Umfeld gesperrt wurden, klingt die Nachricht für Robert plausibel. Ohne mit der Werkstatt Rücksprache zu halten, bleibt er am nächsten Tag zuhause. Gegen Mittag bekommt er einen Anruf von seiner Arbeitsstelle, warum er ungemeldet fehlt. Es stellt sich heraus, dass die Facebook-Nachricht eine Falschmeldung war.

Falschnachrichten, auch **Fake News** genannt, sind Nachrichten, die frei erfunden sind oder eine wahre Meldung verfälschen. Indem sie in sozialen Netzwerken geteilt und an Bekannte weitergeleitet werden, können kritische Informationen oder absurde Geschichten schnell eine hohe Reichweite erlangen und möglicherweise Schaden anrichten.

Quelle prüfen

- **Profil:** Schauen Sie bei Nachrichtenmeldungen in sozialen Netzwerken auf das Profil der verantwortlichen Quelle. Ein bekannter Name (z. B. eines Nachrichtendiensts oder von bekannten Journalist_innen), ein seriöser Auftritt und eine solide Basis an Followern fördern die Glaubwürdigkeit. Behandeln Sie Nachrichten, die von Privatpersonen ohne journalistischen Hintergrund verbreitet wurden, kritisch.
- **Verifizierungszeichen:** In vielen sozialen Netzwerken (z. B. Facebook, Instagram, Twitter und WhatsApp) signalisiert ein kleiner Haken im Profil von Unternehmen, Medienhäuser und bekannten Personen, dass das Profil auf Echtheit geprüft ist.
- **Impressum:** Werfen Sie bei Nachrichtenmeldungen auf Internetseiten einen Blick in das Impressum der Seite. Suchen Sie nach klaren Informationen, wer für die Inhalte verantwortlich ist und an wen Sie sich bei Fragen wenden können. Fehlt ein Impressum, ist das in der Regel ein Hinweis auf eine unzuverlässige Quelle.

- **Internetrecherche:** Suchen Sie im Internet nach der Quelle. Präsentiert sie sich einheitlich und transparent? Je weniger Informationen Sie finden und je undurchsichtiger die Online-Darstellung ist, desto vorsichtiger sollten Sie mit Nachrichten dieser Quelle umgehen.
- **Professionalität:** Verwendet die Quelle einen authentischen, journalistischen Stil in ihrer Nachrichtenmeldung? Bei gehäuften Rechtschreib- und Grammatikfehlern sollten Ihre Alarmglocken läuten. Kritisch zu beurteilen sind außerdem Nachrichten, die sehr einseitig und aufdringlich eine Meinung kundtun, Pauschalisierungen und Schlussfolgerungen ohne plausible Erklärungen treffen oder rassistische, sexistische oder anderweitig diffamierende Ansichten verbreiten. Ein professionelles Medienhaus lässt Texte vor der Veröffentlichung gegenlesen und informiert objektiv und ausgewogen über aktuelle Nachrichten.

Inhalte gegenprüfen

- **Andere Quellen:** Wenn Ihnen Aussagen einer Nachrichtenmeldung merkwürdig vorkommen, recherchieren Sie in Printmedien, Rundfunk und Internet, ob auch andere Quellen die Nachricht aufgreifen und ob es womöglich Abweichungen gibt. Aktuelle, relevante Nachrichten werden nicht nur von einem Medium berichtet.
- **Faktencheck-Seiten:** Auf einigen Faktencheck-Seiten (z. B. *Faktenfinder der Tagesschau*) können Sie bestimmte Informationen gegenprüfen und Tipps für den Umgang mit Fake News im Netz finden.
- **Rückwärtsbildersuche:** Behalten Sie im Hinterkopf, dass auch Bilder, Audiospuren und Videos gefälscht oder in einen falschen Kontext gesetzt sein können. Mit einer Rückwärtsbildersuche (z. B. über *TinEye* oder über die *umgekehrte Bildersuche mit Google Chrome*) können Sie Bilder und ihre ursprünglichen Quellen im Internet auffinden und verifizieren.

Wölfe im Schafspelz – negative Kontakte abblocken

Beispiel: Paula sehnt sich nach einer romantischen Beziehung. Sie hat Lernschwierigkeiten und befürchtet, dass diese bei einem persönlichen Kontakt negativ auffallen. Also meldet sie sich bei einer Dating-App an. Schnell lernt sie einen jungen Mann in ihrem Alter kennen: Tom. Er interessiert sich sehr für Paulas Leben und die beiden schreiben viel miteinander. Nach einigen Tagen drängt Tom darauf, dass Paula ihm Nacktfotos schickt. Verunsichert vertraut sich Paula einer Freundin an. Gemeinsam nehmen sie Toms Profil genauer unter die Lupe. Dabei entdecken sie, dass sein Name und seine Bilder von einem Instagram-Profil eines jungen Mannes aus den USA geklaut sind. Den Tom, den Paula kennengelernt hat, scheint es so nicht zu geben.

In sozialen Netzwerken und Singlebörsen tummeln sich viele **Fake-Profile.** Sie enthalten Lügen, stellen eine erfundene Person dar oder benutzen eine geklaute Identität. Mit einem falschen Profil können Betrüger_innen Daten oder Geld von ihren Opfern abgreifen, sexuell missbräuchliche Handlungen anbahnen oder Mobbing-Attacken hinter einer anonymen Maske verstecken.

Fake-Profile erkennen

- **Makelloses Profil:** Im Internet, ganz besonders im Online-Dating, möchte sich jede_r bestmöglich darstellen. Dementsprechend kann es schwer sein, inszenierte Selbstdarstellungen von Fake-Profilen zu unterscheiden, die oftmals auf sehr attraktive Bilder setzen. Bei Zweifeln an der Authentizität einer Person sollten Sie diese im Internet recherchieren. Hat die Person auch auf anderen sozialen Netzwerken Profile? Bilden diese denselben Menschen ab? Sind die Fotos womöglich von einer anderen Quelle (z. B. aus einem anderen Profil, aus Bilddatenbanken oder von Internetseiten) geklaut? Letzteres können Sie über eine Rückwärtsbildersuche prüfen, genau wie bei einem Verdacht auf Fake News.
- **Sprache:** Anzeichen eines falschen Profils können Nachrichten in fremder Sprache, eine auffällige Häufung von Rechtschreib- und Grammatikfehlern oder ein uneinheitlicher, wechselnder Schreibstil sein.
- **Unerwartete Kontaktanfragen:** Während es auf Dating-Plattformen erwünscht ist, von fremden Personen angeschrieben zu werden, sind unerwartete Kontaktanfragen von Fremden in den klassischen sozialen Netzwerken wie zum Beispiel Facebook eher unüblich. Wer online ernsthaft nach Freundschaften und Beziehungen sucht, nutzt in der Regel entsprechende Single-Börsen.
- **Finanzielle Transaktionen:** Werden Sie hellhörig, wenn eine Internetbekanntschaft um finanzielle Unterstützung oder Vorauszahlungen (z. B. für die Fahrtkosten zu einem persönlichen Treffen) bittet oder Ihnen eine kostenpflichtige Telefonnummer zur Kontaktaufnahme nennt. Überweisen Sie auf keinen Fall Geld, auch keine kleinen Beträge.
- **Pornografisches Material:** Brechen Sie den Kontakt umgehend ab, wenn Sie jemand dazu auffordert, intime Bild- oder Videoaufnahmen zu senden, oder wenn Sie ungefragt pornografisches Material zugesendet bekommen.

Negative Kontakte abbrechen

- **Kontakt kappen:** Wenn eine Internetbekanntschaft Grenzen überschreitet oder als Fake enttarnt wird, sollte der Kontakt sofort abgebrochen werden, um die Gefahr von Betrug oder sexuellen Missbrauchs sowie weiteres emotionales Leid zu verhindern.
- **Blockieren und Melden:** In sozialen Netzwerken können Kontakte blockiert und gemeldet werden. Eine blockierte Person kann nicht mehr auf Ihr Profil zugreifen oder Ihnen private Nachrichten senden. Durch Melden können andere Online-Nutzende außerdem vor ähnlichen Erfahrungen bewahrt werden.
- **Vertrauensperson:** Negative Erfahrungen im Online-Dating oder beim Aufbau neuer Kontakte im Internet können wie im echten Leben schmerzlich sein. Um mit Schwierigkeiten oder Kummer nicht allein zu sein, kann es helfen, sich an eine vertrauensvolle Person zu wenden.

Weiterführende Links zu digitaler Sicherheit und digitalen Kompetenzen:

- Aktionsbund Digitale Sicherheit: *www.aktionsbund.org*
- Bundesamt für Sicherheit in der Informationstechnik: *www.bsi-fuer-buerger.de*
- Deutschland sicher im Netz: *www.sicher-im-netz.de*
- Klicksafe: *www.klicksafe.de*
- Stiftung Digitale Chancen: *www.digitale-chancen.de*
- Informationen über Fake News in einfacher Sprache: Bundeszentrale für politische Bildung über Fake News in einfacher Sprache: *www.bpb.de/politik/grundfragen/politik-einfach-fuer-alle/258073/fake-news*