

Das Netz

Digicomp



Datenschutz

Sich völlig anonym durch den Alltag zu bewegen, ist heutzutage unmöglich.

Auch im Internet gilt: Einen hundertprozentigen Datenschutz gibt es nicht! Jeder Einstieg ins Web hinterlässt – beabsichtigt oder unbeabsichtigt – Spuren. Leider gibt es viele Versuche, diese Spuren zu lesen und auch illegal zu nutzen.

Für einen großen Teil der verfügbaren Daten über uns sind wir aber selbst verantwortlich, weil wir oft sehr leichtfertig mit Angaben zur eigenen Person umgehen.

Was bedeutet Datenschutz?

Unter Datenschutz versteht man den Schutz der Privatsphäre, aber auch das Recht, selbst zu entscheiden, wer wann welche persönlichen Daten einsehen darf.

Mit persönlichen Daten sind genau genommen personenbezogene Daten gemeint. Dazu gehören alle Daten, die einer konkreten Person zugeordnet werden können (z. B. Ihr Name, Ihr Geburtsdatum oder Ihre Adresse, aber auch Ihre E-Mail-Adresse oder die IP-Adresse Ihres Computers). Als besonders schützenswert gelten sensible Daten. Dazu gehören Informationen über Ihre Gesundheit, politische Einstellung, religiöse oder philosophische Überzeugungen, ethnische Herkunft und Ihr Sexualleben.

Was bedeutet Datenschutz?

Sich völlig anonym durch den Alltag zu bewegen, ist heutzutage so gut wie unmöglich. Ob beim Telefonieren, beim Einkaufen, bei der Urlaubsbuchung, beim Arztbesuch oder beim Surfen im Internet – fast immer werden jede Menge persönliche Daten erfasst, und das oft ohne unser Wissen.

Oftmals gehen wir im Internet aber auch selbst zu freizügig mit Angaben zur eigenen Person um. Das kann unerwünschte Einblicke in unsere Privatsphäre und Datenmissbrauch zur Folge haben. Sie sollten daher genau überlegen, welche Informationen Sie im Internet preisgeben.

Was sagt das Gesetz zum Thema Datenschutz?

Das Recht auf Datenschutz ist als Grundrecht anerkannt. Es steht in der Rechtsordnung über einem normalen Gesetz und kann nicht ohne Weiteres eingeschränkt werden. In der EU-Datenschutz-Grundverordnung (DSGVO) und dem Datenschutzgesetz (DSG) ist geregelt, unter welchen Bedingungen die persönlichen Daten einer Person verwendet und verarbeitet werden dürfen.

Grundsätzlich dürfen persönliche Daten (d. h. alle Informationen, die sich auf eine konkrete Person beziehen) nur dann verarbeitet (d. h. erhoben, gespeichert, geordnet, abgefragt, offengelegt etc.) werden, wenn es eine bestimmte Rechtsgrundlage dafür gibt.

Was sagt das Gesetz zum Thema Datenschutz?

Die Einwilligung der betroffenen Person stellt eine dieser Rechtsgrundlagen dar. In bestimmten Fällen dürfen die persönlichen Daten einer Person aber auch verarbeitet werden, wenn keine Einwilligung vorliegt (z. B. wenn dies zur Erfüllung eines Vertrags erforderlich ist).

Jede Person hat ein Recht auf Auskunft darüber, ob und welche ihrer Daten von jemand anderem verarbeitet werden.

Wenn persönliche Daten ohne Rechtsgrundlage verarbeitet werden, sind im Gesetz empfindliche Strafen vorgesehen.

Warum ist Datenschutz im Internet wichtig?

Im Web ist man nicht so anonym, wie man glaubt.

Alle Inhalte, die Sie ins Netz stellen, sind nicht nur für Personen, die Ihnen nahestehen zugänglich, sondern theoretisch für alle Internetnutzer:innen auf der Welt.

Auch Fremde können Ihre privaten Informationen unter Umständen einsehen und für böse Absichten missbrauchen (z. B. Identitätsdiebstahl, sexuelle Belästigung, Cyber-Mobbing).

Warum ist Datenschutz im Internet wichtig?

Das Internet vergisst nicht!

Einmal veröffentlichte Daten im Web sind weltweit zugänglich, schnell vervielfältigt und oft nicht mehr zu entfernen.

Sie können auch noch Jahre später in anderen Zusammenhängen wieder auftauchen und Ihnen schaden (z. B., wenn ein potenzieller Arbeitgeber exzessive Party-Fotos von Ihnen in einem Sozialen Netzwerk findet).

Warum ist Datenschutz im Internet wichtig?

Der erste Eindruck zählt.

Um mehr über eine Person zu erfahren, nutzen viele Menschen als ersten Weg die Google-Suche. Doch nicht immer vermitteln die online gefundenen Informationen ein realistisches Bild einer Person. Überprüfen Sie daher regelmäßig, was über Sie selbst im Internet steht.

Nicht alles ist, wie es scheint.

Glauben Sie nicht alles, was andere Menschen im Internet behaupten – sich als jemand anderer auszugeben bzw. etwas vorzuspielen, ist im Web besonders einfach und kann für betrügerische Zwecke ausgenutzt werden.

Warum ist Datenschutz im Internet wichtig?

Datensammler haben leichtes Spiel.

Sicherheitslücken – z. B. in Sozialen Netzwerken oder bei E-Mail-Anbietern – können den unerlaubten Zugriff Dritter auf Nutzerdaten ermöglichen.

Die möglichen Folgen:

E-Mail-Adressen und andere private Daten werden z. B. für Spam ausgenutzt, Fotoalben widerrechtlich auf Tauschbörsen zum Download angeboten, Profile weiterverkauft oder Bankdaten von Betrüger:innen missbraucht.

Wie kann ich meine persönlichen Daten im Internet schützen?

Veröffentlichen Sie so wenig personenbezogene Daten wie möglich. Adresse, Telefonnummer, Passwörter etc. gehen Fremde nichts an.

Seien Sie besonders sparsam mit diesen Informationen, wenn Sie sich auf Websites, für Gewinnspiele o. Ä. registrieren.

Nicknames nutzen. Wenn möglich, verwenden Sie anonyme Nicknames anstelle Ihres richtigen Namens.

In Sozialen Netzwerken könnten Sie z. B. Ihren Zweitnamen verwenden.

Wie kann ich meine persönlichen Daten im Internet schützen?

Mehrere E-Mail-Adressen verwenden.

Legen Sie sich bei einem Gratis-Anbieter (z. B. Yahoo, Outlook, Gmail oder GMX) eine E-Mail Adresse an, die keine Rückschlüsse auf Ihre Person zulässt. Verwenden Sie diese Adresse, um sich auf Websites zu registrieren, in Blogs zu posten oder in Foren mitzudiskutieren.

Spam ignorieren.

Antworten Sie niemals auf Spam-E-Mails – auch nicht, um mitzuteilen, dass Sie die lästigen Zusendungen nicht mehr wollen. Damit bestätigen Sie nur, dass es sich um eine gültige E-Mail-Adresse handelt, und bekommen umso mehr Spam.

Wie kann ich meine persönlichen Daten im Internet schützen?

Vorsicht vor Datendiebstahl.

Seien Sie wachsam bei Phishing-E-Mails und geben Sie keine Bank- oder sonstigen Zugangsdaten via Internet oder E-Mail weiter. Wenn Sie unsicher sind, kontaktieren Sie Ihre Hausbank.

Nicht alle Anhänge öffnen.

Öffnen Sie keine unbekannten Dateianhänge aus E-Mails oder via Instant Messenger – sie könnten Viren oder Spyware enthalten, die persönliche Daten auf Ihrem Computer ausspionieren.

Wie kann ich meine persönlichen Daten im Internet schützen?

Online-Verhalten hinterfragen. Überprüfen Sie, ob Ihre Website, Ihr Blog oder Ihre Profile Informationen enthalten, die Sie eigentlich nicht vollkommen öffentlich haben wollen. Bedenken Sie: Alle Inhalte, die Sie ins Internet stellen, sind weltweit frei zugänglich und über Suchmaschinen einfach zu finden.

Sichere Passwörter verwenden.

Verwenden Sie sichere Passwörter und halten Sie diese geheim.

Nutzerprofil einschränken. Nutzen Sie die Privatsphäre-Einstellungen in Sozialen Netzwerken, sodass nur ausgewählte Personen (z. B. „Freunde“) Ihre persönlichen Daten einsehen können.

Wie kann ich meine persönlichen Daten im Internet schützen?

Internet-Browser sicherer machen.

Optimieren Sie die Sicherheitseinstellungen Ihres Browsers (in der Regel unter „Datenschutz und Sicherheit“ o. Ä.) und machen Sie regelmäßige Updates.

Internetspuren regelmäßig beseitigen.

Achten Sie darauf, in den Browsereinstellungen immer wieder die gespeicherten Cookies zu löschen und den Cache sowie Verlauf zu leeren.

Wie kann ich meine persönlichen Daten im Internet schützen?

Anonym surfen.

Nutzen Sie nach Möglichkeit den „Privat-“ bzw. „Inkognito“-Modus Ihres Browsers, der automatisch den Browserverlauf, Cookies, temporäre Dateien etc. löscht. Mit dem TOR Browser, der die IP-Adresse Ihres Geräts versteckt, können Sie gänzlich anonym surfen.

Alternative Suchmaschinen nutzen.

Google ist bekannt dafür, besonders viele Daten zu sammeln. Doch es gibt Alternativen, die mehr Wert auf Datenschutz legen – z. B. DuckDuckGo, Startpage oder Qwant.

Wie kann ich meine persönlichen Daten im Internet schützen?

Computer schützen. Verwenden Sie ein Anti-Viren-Programm und eine Firewall und verschlüsseln Sie Ihre WLAN-Verbindung.

Vorsicht bei der Nutzung öffentlicher Computer und Netzwerke. Seien Sie besonders vorsichtig bei der Nutzung öffentlicher Computer (z. B. in der Schule oder im Internet-Café) und WLAN-Verbindungen.

Allzu sensible Daten (z. B. Bankdaten) sollten Sie hier am besten gar nicht verwenden. Wenn Sie sich auf Websites einloggen, melden Sie sich auch stets wieder ab. Nutzen Sie verschlüsselte Seiten.

Wie kann ich meine persönlichen Daten im Internet schützen?

Achtsame Handynutzung.

Bedenken Sie, dass Ihr Smartphone durch Verlust oder Diebstahl leicht in fremde Hände gelangen kann.

Seien Sie daher besonders sorgsam im Umgang mit sensiblen Daten und machen Sie sich mit den Geräteeinstellungen vertraut, um Ihre persönlichen Daten am Handy zu schützen.

Welche meiner Daten werden online gesammelt?

Grundsätzlich werden zwei Arten von Daten unterschieden:

Inhaltsdaten (z. B. Text und Anhänge einer E-Mail) und Metadaten (im Fall eines E-Mails z. B. Absender:in, Empfänger:in, Betreff, Datum und Uhrzeit, verwendetes Mailprogramm, verwendete Sprache ...).

Welche meiner Daten werden online gesammelt?

Profile in Sozialen Netzwerken.

Hier werden die meisten persönlichen Daten gesammelt!

Neben Postings und hochgeladenen Bildern können das Angaben über Ihren Gefühlszustand, Beziehungen, politische Einstellungen, gefolgte Seiten oder Gruppen etc. sein.

Aber auch Informationen zu genutzten Geräten oder Netzwerken werden gesammelt.

Welche meiner Daten werden online gesammelt?

Besuchte Websites und Online-Shops.

Standardmäßig werden Datum, Uhrzeit, IP-Adresse, ungefährender Ort des Internetanschlusses, verwendetes Betriebssystem, Browsertyp, Sprache und Version der Browsersoftware und die Website, von der Sie zugreifen (z. B. Suchmaschine) erfasst.

Teilweise werden noch viel genauere Daten „geloggt“, etwa wie weit Sie die Website heruntergescrollt oder welche Links Sie angeklickt haben.

Welche meiner Daten werden online gesammelt?

Digitale Kommunikation.

Egal, ob Sie E-Mails, SMS oder Nachrichten über WhatsApp oder andere Messenger verschicken – es wird zumindest mitverfolgt, wann und mit wem Sie kommunizieren (Metadaten).

Die Inhalte selbst sind bei vielen Messengern verschlüsselt – aber eben nicht bei allen.

Welche meiner Daten werden online gesammelt?

Suchmaschinen.

Der Suchmaschinen-Riese Google weiß nicht nur, welche Fragen Ihnen unter den Nägeln brennen, sondern kennt von Nutzer:innen mit Google Account noch viel mehr Details, z. B. oft besuchte Orte oder Ihre Lieblingsvideos auf YouTube.

Unterwegs mit dem Smartphone.

Smartphones versuchen sich ständig zu verbinden, etwa mit WLAN-Netzwerken oder via Bluetooth mit anderen Geräten. Ist Ihre Standortortung aktiviert, entsteht im Laufe des Tages ein detailliertes Bewegungsprofil.

Welche meiner Daten werden online gesammelt?

Apps.

Die kleinen Programme verlangen oft deutlich mehr Zugriffsberechtigungen als notwendig, z. B. auf Standortdaten, Browserverlauf, Geräte-ID, Kontakte im Adressbuch oder Handykamera.

Bezahlen.

Bei der Nutzung von Kreditkarten, Bankomatkarten oder Kundenkarten fallen viele Informationen an, die auch Auskunft über Ihr Kaufverhalten und Ihre Zahlungsfähigkeit geben.

Welche meiner Daten werden online gesammelt?

Internet der Dinge (IoT).

Immer öfter sind Haushaltsgeräte, Heizungen oder Stromzähler („Smart Home“) miteinander vernetzt bzw. mit dem Internet verbunden. Ein Paradebeispiel sind hier digitale Assistenten wie Alexa von Amazon.

Jede Menge Nutzungsdaten sammeln aber auch Kinderspielzeuge, die sich per App bedienen lassen (Smart Toys), sogenannte Wearables (smarte Armbanduhren, Fitnesstracker etc.) oder vernetzte Fahrzeuge.

Welche meiner Daten werden online gesammelt?

Biometrische Daten.

Zum Entsperren von Geräten werden immer häufiger Techniken wie Fingerabdrücke, Iris-Scan oder Gesichtserkennung verwendet.

Biometrische Daten können anders als ein Passwort im Falle eines Diebstahls nicht geändert werden und sind daher besonders sensibel.

Was sind Cookies und Webtracking-Tools?

Wenn Sie eine Website besuchen, können sogenannte Tracking-Tools – meist unbemerkt – eine Vielzahl Ihrer Daten sammeln. Dazu zählen beispielsweise Informationen darüber, welche Seiten Sie besuchen, wo Sie klicken, wie lange Sie auf einer Seite bleiben oder welche Seite Sie zuvor besucht haben. Auch die IP-Adresse – also die eindeutig zuordenbare Adresse Ihres Geräts – wird in der Regel getrackt.

Das passiert oftmals über das Setzen von Cookies. Dabei handelt es sich um kleine Dateien, die beim Erstbesuch einer Website (z. B. Online-Shops, Soziale Netzwerke etc.) auf dem Computer abgelegt werden und danach Informationen sammeln.

Was sind Cookies und Webtracking-Tools?

Besuchen Sie später noch einmal diese Website, weiß der Server dank der Cookies, dass Sie schon einmal hier waren und kann so z. B. Ihre persönlichen Daten automatisch ausfüllen.

Das ist praktisch, aber denken Sie daran, dass dadurch auch andere Computernutzer:innen leicht an Passwörter o. Ä. kommen können.

Außerdem werden Cookies manchmal dazu missbraucht, Sie mit unerwünschter Werbung zu belästigen.

Cookies sind nicht gleich Cookies

Grundsätzlich werden zwei Arten von Cookies unterschieden: technisch notwendige (die für das Funktionieren der Webseite erforderlich sind) und technisch nicht notwendige (z. B. Werbe- und Marketing-Cookies, mit denen Ihr Surfverhalten nachverfolgt wird).

Letztere müssen von Ihnen vorab akzeptiert oder abgelehnt werden.

Das passiert meist über sogenannte Cookie-Banner, die beim Besuch jeder Website aufpoppen und nach Ihrer Einwilligung fragen (Opt-in).

Tracking

Weitere technische Möglichkeiten des Webtrackings sind Zähl- oder Trackingpixel (winzige, unsichtbare Grafiken auf einer Website, die Ihre Nutzungsdaten erfassen), Device Fingerprinting (anhand von Browser-Einstellungen wie Sprache, Version, Zeitzone etc. können Nutzer:innen wiedererkannt werden) oder Analyse-Tools wie z. B. Google Analytics.

Auch wenn Sie etwas in Sozialen Netzwerken liken, können Sie durch einen Klick auf den entsprechenden Button getrackt werden.

Tracking

Hinweis

Da insbesondere Werbetreibende großes Interesse an Ihren Daten haben, können die Cookie-Banner kompliziert und irreführend gestaltet sein.

Klicken Sie sich dennoch stets aufmerksam durch die Cookie-Hinweise, um nicht mehr Daten als gewollt preiszugeben.

In den Einstellungen Ihres Browsers können Sie Cookies zudem generell blockieren und bereits gespeicherte Cookies löschen.

Wie finde ich heraus, was über mich im Internet steht?

Suchen Sie regelmäßig nach Angaben über sich im Internet.

Dazu brauchen Sie nur Ihren eigenen Namen in eine Suchmaschine einzugeben.

Um ein genaueres Suchergebnis zu bekommen, setzen Sie Vornamen und Nachnamen in Anführungszeichen („Maria Meier“).

Die Anführungszeichen verbinden die beiden Wörter zu einer fixen Wortgruppe.

Wie finde ich heraus, was über mich im Internet steht?

Nutzen Sie auch die umgekehrte Bildersuche, um zu überprüfen, wo Ihre Bilder im Umlauf sind.

Sollten unliebsame Bilder auftauchen, können Sie die Website-Betreiber:innen zur Löschung auffordern.

In hartnäckigen Fällen hilft Ihnen die Internet Ombudsstelle kostenlos weiter.

Wie finde ich heraus, was über mich im Internet steht?

Wenn Sie laufend über neue Veröffentlichungen zu Ihrer Person informiert werden wollen, können Sie einen Google Alert einrichten.

Sie erhalten dann automatisch ein E-Mail, sobald die Suchmaschine einen neuen Inhalt über Sie gefunden hat.

Das ist vor allem dann sinnvoll, wenn in der Vergangenheit nachteilige Inhalte über Sie im Umlauf waren (z. B. Nacktaufnahmen) und Sie Sorge haben, dass diese an anderer Stelle wieder im Internet auftauchen könnten.

Wie sieht ein sicheres Passwort aus?

Grundsätzlich gilt

Auch ein langes und kompliziertes Passwort kann geknackt werden – hundertprozentigen Schutz gibt es nicht!

Sie können mögliche Angriffe aber erschweren, indem Sie Ihre Passwörter besonders sicher gestalten.

Wie sieht ein sicheres Passwort aus?

Möglichst lange und kompliziert.

Grundsätzlich sollte ein Passwort mindestens aus acht Zeichen bestehen, besser sind 12- oder sogar 16-stellige Passwörter. Noch wichtiger ist es aber, dass das Passwort kompliziert ist.

Verwenden Sie in Passwörtern daher **keine Informationen**, die leicht zu erraten sind (wie Ihr Geburtsdatum oder den Namen Ihres Lieblingstieres).

Auch einfache Buchstaben- oder Zahlenfolgen wie „1234“ oder „abcd“ bzw. Tastaturmuster (z. B. „asdfgh“) sind nicht ratsam.

Wie sieht ein sicheres Passwort aus?

Nutzen Sie eine **Kombination** aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. - + = ! ? % ^ & * @ # \$ () [] ; : " / , . < > ~).

Verwenden Sie für jedes Konto ein **eigenes Passwort**.

Nutzen Sie einen **Passwort-Manager**. Alternativ können Sie sich Ihre Passwörter aufschreiben, bewahren Sie diese jedoch an einem sicheren Ort auf.

Wie sieht ein sicheres Passwort aus?

Passwort-Satz

Überlegen Sie sich einen Satz, der für Sie persönlich leicht merkbar ist und bilden Sie aus den Anfangsbuchstaben Ihr Passwort:

Aus „Ich fahre morgens am liebsten mit dem Fahrrad ins Büro, um fit zu bleiben“ wird z. B. „IfmalmdFiBufzb“.

Machen Sie das Passwort noch sicherer, indem Sie einzelne Buchstaben durch Zahlen oder Sonderzeichen ersetzen (z. B. „B“ durch „8“ oder „I“ durch „!“).

Wie sieht ein sicheres Passwort aus?

4-Wörter-Methode

Setzen Sie aus vier zufälligen Wörtern ein komplexes und sehr langes Passwort zusammen. Trennen Sie die Wörter mit Zahlen oder Sonderzeichen wie etwa „\$“ oder „ § “ – z. B.
„Babybrei\$Einhorn\$Thomas\$Semmel“.

Sie können auch unterschiedliche Zeichen verwenden (z. B.
„Babybrei&Einhorn2Thomas%Semmel1!“).

Damit schaffen Sie ein schwer zu knackendes Passwort, das dennoch einfach zu merken ist.

Wie sieht ein sicheres Passwort aus?

Diceware-Methode

Eine bekannte und getestete Methode ist auch die sogenannte Diceware-Methode.

Dafür gibt es einen Katalog mit tausenden Wörtern, welche mit einer Zahlenkombination verbunden sind.

Durch Würfeln stellt man sich aus dieser Liste ein Passwort aus mindestens sechs Wörtern zusammen.

Eine Anleitung und die Liste dazu findet man auf Wikipedia.

Wie kann ich Passwörter sicher aufbewahren?

Halten Sie Ihre Passwörter **geheim**.

Geben Sie Passwörter stets **unbeobachtet** von Dritten ein.

Speichern Sie Passwörter nicht im Browser ab – vor allem dann nicht, wenn der Computer bzw. das Smartphone/Tablet von mehreren Personen verwendet wird.

Wie kann ich Passwörter sicher aufbewahren?

Nutzen Sie einen **Passwort-Manager**.

Dieser speichert die unterschiedlichen Passwörter für Ihre Benutzerkonten hinter einem Master-Passwort ab.

So brauchen Sie sich nur noch ein einziges Passwort zu merken.
Bekannte Passwort-Manager sind etwa LastPass, 1Password, Keeper, oder KeePass.

Warum sollte ich unterschiedliche Passwörter verwenden?

Auch wenn es praktisch erscheint, kann die Verwendung eines einzigen Passworts für unterschiedliche Benutzerkonten gefährlich werden:

Wird eines Ihrer Konten gehackt, können die Angreifer auf alle weiteren Accounts zugreifen, für die Sie dasselbe Passwort nutzen.

Oft wird statt eines Benutzernamens die E-Mail-Adresse angegeben, weshalb sich Kriminelle schnell auch Zugang zu Ihrem E-Mail-Konto verschaffen können.

Warum sollte ich unterschiedliche Passwörter verwenden?

Idealerweise sollten Sie daher für jedes Benutzerkonto ein eigenes, sicheres Passwort verwenden.

Ein Passwort-Manager hilft Ihnen bei der Verwaltung der Zugangsdaten.

Vermeiden Sie auch die Verknüpfung mehrerer Online-Dienste über ein und dieselbe E-Mail-Adresse bzw. verwenden Sie nicht Ihren Account in einem Sozialen Netzwerk (z. B. Facebook oder Twitter), um sich für weitere Plattformen zu registrieren.

Was ist die Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung (auch: Zwei-Schritte- oder Zwei-Wege-Authentifizierung bzw. 2FA) ist eine zusätzliche Sicherheitsmaßnahme zum Schutz von Benutzerkonten: Selbst wenn Ihre Passwörter in die falschen Hände gelangen, haben Unbefugte auf diese Weise keinen Zugriff auf Ihre Accounts.

Zusätzlich zum Passwort müssen Sie beim Login eine weitere Sicherheitskomponente eingeben, etwa einen PIN-Code.

Dieser Code wird z. B. an die in Ihrem Konto hinterlegte Handynummer gesendet.

Was ist die Zwei-Faktor-Authentifizierung?

Eine weitere Möglichkeit sind für kurze Zeit gültige Einmalkennwörter, die von sogenannten Authentifizierungs-Apps erstellt werden.

Solche Apps bieten den Vorteil, dass Sie damit Ihre mit 2FA geschützten Konten übersichtlich verwalten können.

Bekannte Apps für die Zwei-Schritte-Authentifizierung sind z. B. Google Authenticator (für iOS/Android), Microsoft Authenticator (für iOS/Android) oder Twilio Authy (für iOS/Android/Desktop).

Was ist die Zwei-Faktor-Authentifizierung?

Die Zwei-Faktor-Authentifizierung wird inzwischen von den meisten großen Online-Diensten unterstützt – von Apple über Google oder Microsoft bis hin zu Twitter, Facebook und Instagram.

Nähere Informationen dazu finden Sie üblicherweise im Hilfebereich des jeweiligen Anbieters.

Was muss ich bei der Nutzung eines öffentl. Computers beachten?

Speichern Sie nie Ihre Login-Daten. Haben Sie sich auf einer Website mit Zugangsdaten eingeloggt, melden Sie sich auch stets wieder ab („Logout“). Es reicht nicht, einfach nur das Browserfenster zu schließen oder eine andere Internetadresse einzugeben. Deaktivieren Sie in jedem Fall auch automatische Anmeldefunktionen (z. B. bei Instant Messengern).

Rufen Sie Ihren Webmail-Dienst nie über eine Suchmaschine auf. Bei öffentlichen Computern besteht immer die Gefahr, dass der PC bereits mit Schadsoftware infiziert ist. Diese kann z. B. die sichere Verbindung (SSL) Ihres E-Mail-Kontos aushebeln, wenn Sie Ihren Webmail-Dienst über eine Suchmaschine aufrufen.

Was muss ich bei der Nutzung eines öffentl. Computers beachten?

Lassen Sie den Computer während der Nutzung niemals unbeaufsichtigt. Wenn Sie fertig sind, melden Sie sich bei allen Websites und Programmen ab und schließen Sie alle Fenster, die vertrauliche Daten enthalten könnten.

Beseitigen Sie Ihre Spuren. Der Browser merkt sich automatisch Passwörter und Websites, die Sie besucht haben, selbst nachdem diese geschlossen wurden und Sie sich abgemeldet haben.

Löschen Sie daher regelmäßig den Browserverlauf.

Was muss ich bei der Nutzung eines öffentl. Computers beachten?

Erzeugen Sie keine Spuren.

Moderne Browser verfügen meist über einen privaten Surfmodus. So werden erst gar keine Informationen (z. B. Cookies, temporäre Internetdateien, Verlauf) auf dem Computer gesammelt.

Lassen Sie niemanden zuschauen.

Achten Sie bei der Nutzung eines öffentlichen Computers immer darauf, dass Ihnen keine fremden Personen über die Schulter schauen, die dabei vertrauliche Daten ausspionieren könnten.

Was muss ich bei der Nutzung eines öffentl. Computers beachten?

Seien Sie generell sparsam mit der Eingabe von persönlichen Daten, denn so sind Sie in jedem Fall geschützt – auch vor Gelegenheitshackern, die eventuell nach Ihnen denselben öffentlichen Computer benutzen.

Bank- oder Kreditkartendaten oder ähnlich vertrauliche Informationen sollten Sie am besten NIE auf einem öffentlichen Computer eingeben.

Was muss ich beachten, wenn ich in einem öffentlichen WLAN surfe?

Deaktivieren Sie die Datei- und Verzeichnisfreigaben für Netzwerke, damit andere nicht unbemerkt auf Ihre Dateien zugreifen können.

Schalten Sie Ihr WLAN nur ein, wenn Sie es tatsächlich verwenden.

Deaktivieren Sie nach Möglichkeit zudem die automatische Anmeldung an bekannten Hotspots bzw. löschen Sie gespeicherte Netzwerke, mit denen sie irgendwann einmal verbunden waren.

Was muss ich beachten, wenn ich in einem öffentlichen WLAN surfe?

Geben Sie Daten ausschließlich über SSL-verschlüsselte Websites ein (erkennbar an "https://" und einem Schloss-Symbol entweder neben der Adressleiste oder am unteren Bildschirmrand).

Über ein VPN („virtuelles privates Netzwerk“) werden Daten verschlüsselt durch das offene WLAN geschickt.

Es gibt inzwischen zahlreiche Anbieter von zum Teil kostenlosen VPN-Programmen, auch viele Anti-Virenprogramme beinhalten solche Tools.

Wie beseitige ich Internetspuren am Computer?

Cookies

Cookies sind kleine Dateien, die beim Erstbesuch einer Website auf dem Computer abgelegt werden und danach unbemerkt Informationen sammeln.

Sie können in den Einstellungen Ihres Browsers (in der Regel unter „Datenschutz und Sicherheit“ o. ä.) die vorhandenen Cookies löschen, Cookies generell zulassen oder blockieren sowie Ausnahmen für bestimmte Websites festlegen.

Wie beseitige ich Internetspuren am Computer?

Cache und Verlauf

Neben einer Liste der zuletzt besuchten Websites („Verlauf“) werden auch Teile dieser Sites („temporäre Internetdateien“) auf der Festplatte im „Cache“ gespeichert, um sie beim nächsten Aufruf schneller anzeigen zu können. Im Browser lässt sich (in der Regel unter „Datenschutz und Sicherheit“ o.ä.) einstellen, dass abgerufene Sites gar nicht erst im Cache gespeichert werden, keine Verlaufsliste erstellt wird oder beides nach jeder abgeschlossenen Sitzung wieder verschwindet. In jedem Fall sollten Sie die automatisch gespeicherten Browserinformationen in regelmäßigen Abständen entfernen, damit andere Computernutzer:innen nicht nachverfolgen können, was Sie im Internet gemacht haben.

Wie beseitige ich Internetspuren am Computer?

„Unsichtbares“ Surfen

Moderne Browser bieten die Möglichkeit, privat zu surfen. Beim Privaten Modus (Mozilla Firefox), Inkognitomodus (Google Chrome) oder InPrivate-Browsen (Microsoft Edge) werden deutlich weniger Informationen auf dem Computer gesammelt. Der Browser speichert z. B. nicht mehr, welche Webseiten Sie besucht haben und Formulare werden nicht mehr automatisch vervollständigt. Sobald Sie den Browser schließen, werden auch die Cookies gelöscht. Der Private Modus macht Sie im Internet allerdings nicht anonym – Ihr Browser „vergisst“ einfach mehr Daten.

Wie lösche ich meine Festplatte richtig?

Beim Löschen von Dateien werden in der Regel nur die Einträge im Inhaltsverzeichnis der Festplatte gelöscht. Die Daten selbst bleiben so lange bestehen, bis sie überschrieben werden. Eine Wiederherstellung ist mit verschiedenen Tools einfach möglich.

Selbst das Formatieren der Festplatte löscht Dateien nicht endgültig.

Bevor Sie Ihre Festplatte weitergeben oder entsorgen, sollten Sie daher einen „Datenshredder“ verwenden (z. B. das Gratis-Programm Eraser).