Inhaltsverzeichnis

12

Datensicherheit ist wichtig. Aber warum eigentlich? Was kann Ihnen passieren?

45

Die Regeln für gute Passwörter ändern sich. Was sollten Sie heute beachten?

118

Google findet für Sie alles – doch wie verdient die Suchmaschine eigentlich Geld?

142

Welche Rechte können Sie dank der Datenschutz-Grundverordnung geltend machen?

151

Ihr Smartphone ist ein wahrer Alleskönner. Was bedeutet das für Ihre Daten?

175

Wie stellen Sie sicher, dass Ihr Sprachassistent nur das hört, was er hören soll?

Sie haben etwas zu verbergen!

Das Internet – unendliche Weiten. Und auch unendliche Mengen von Daten. Wenn Sie eine Seite aufrufen, hinterlassen Sie Spuren. Wenn Sie online etwas kaufen, geben Sie Daten ein. Wenn Sie eine E-Mail verschicken: Daten. Soziale Netzwerke? Daten, Daten, Daten. Es lohnt sich, etwas genauer hinzuschauen: Welche Daten schwirren da draußen herum und was ist deren Nutzen oder Risiko?

Anonymität schafft Privatsphäre

Es gibt nahezu endlos viele Geräte, die miteinander vernetzt sind. Nicht nur PC, Tablet und Smartphone, sondern auch Ihr Fernseher, der Sprachassistent, Ihre Webcam im Ferienhaus und der intelligente Rauchmelder – sie alle sammeln Informationen, oder anders genannt: Daten. Diese Geräte stehen nicht allein da, sondern sie verbinden sich. Über das Internet, im heimischen Netzwerk, durch eigene sogenannte Mesh-Netzwerke. Damit befinden sich Ihre Daten nicht nur an einem Ort, sondern wandern von Gerät zu Gerät, von Speicher zu Speicher. Eines sollten Sie dabei nicht vergessen: Diese Daten gehören Ihnen. Die klassische Aussage „Ich habe nichts zu verbergen“ nehmen viele zurück, sobald ihnen klar wird, wie viel vermeintlich harmlose Daten verraten und für welche Zwecke sie sich verwenden lassen. Sie sollten selbst entscheiden (können), wer welche Daten von Ihnen sieht und nutzt.

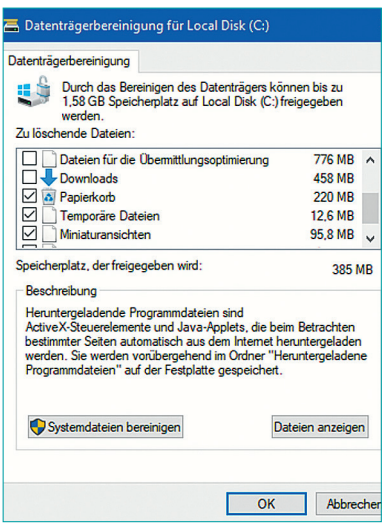
Chance oder Falle?

Die öffentliche Diskussion geht seit einigen Jahren deutlich in eine Richtung: Datenschutz geht vor allem anderen, wer Daten verarbeitet, ist ein potenzieller Bösewicht, und Datenlecks sind ohnehin die Schuld, ja vielleicht sogar Absicht desjenigen, der die Daten gespeichert hat. Die Unternehmen, die Ihre Daten verwenden, haben da eine ganz andere Sicht: Sie bekommen eine Dienstleistung, da-

Wenn Sie Ihre Bibliotheken auf einen externen Datenträger auslagern, sollten Sie eines beachten: Sie müssen den Datenträger beim Hochfahren und beim Herunterfahren angeschlossen lassen. Ist das nicht der Fall, kann Windows die Zuordnung der Verzeichnisse zu den Bibliotheken verlieren!

Die temporären Dateien

Viele Programme und Systemfunktionen von Windows legen sogenannte temporäre Dateien auf der Festplatte ab. Das sind Datenwolken, die eigentlich nur während des laufenden Programms benötigt werden. Dazu kommen noch Ihre aus dem Internet heruntergeladenen Dateien, der Dateiversionsverlauf, wenn Sie eine Datei mehrfach bearbeitet haben, und einiges mehr. Diese Dateien werden nicht sofort gelöscht, sondern bleiben auf der Festplatte liegen, bis Speicher benötigt wird oder Sie die Löschung manuell anstoßen. Sie können diese Datenspeicherung, die ja durchaus auch persönliche Daten enthalten kann, nicht ausschalten, wohl aber regelmäßig die Daten manuell löschen:



1 Starten Sie den Explorer und klicken Sie mit der rechten Maustaste auf das Laufwerk, das Sie bereinigen wollen.

2 Klicken Sie auf *Eigenschaften*, *Bereinigen*.

3 Windows durchsucht jetzt den Datenträger nach temporären Dateien.

4 Wählen Sie zumindest *Downloads*, *Papierkorb*, *Temporäre Dateien*, *Miniaturansichten* und den *Dateiversionsverlauf* aus. Das Löschen aller anderen Einträge (und der Systemdateien, die Sie mit einem Klick auf *Systemdateien bereinigen* löschen können) macht zwar Speicher frei, erhöht Ihre Anonymität aber nicht.

5 Ein Klick auf *OK* löscht diese Dateien vom Datenträger.

Das Passwort: Ein sicherer Schutz?

Seit Jahrzehnten hat sich die Standard-Anmeldemethode für Rechner, diverse Online-Dienste und Konten nicht geändert: das Passwort (oder synonym auch Kennwort). Es handelt sich dabei um eine Kombination aus Ziffern, Buchstaben und Sonderzeichen, die für Sie möglichst einfach zu merken, für den Unbefugten aber möglichst unbestimmbar sein sollte. Ein gutes Passwort sollte selbstverständlich sein. Sollte, denn 2022 waren die häufigsten Passwörter 123456, gefolgt von „password“ und 123456789.

Das „gute“ Passwort

Ein gute Methode, um ein komplexes und trotzdem merkbares Passwort zu erzeugen, ist die Nutzung einer Eselsbrücke, am besten eines Merksatzes. Das funktioniert so:

→ **Passwort mit Merksatz**

Bilden Sie einen Satz, der möglichst auch eine Zahl und ein Wort wie „und“ enthält. Wichtig ist, dass er so nah wie möglich an Ihrem Leben ist, sodass Sie sich blind daran erinnern. Ein Beispiel: „Ich habe gerade vier gute Bücher und Artikel gelesen!“ Aus diesem Satz lässt sich nun ein Passwort bilden, indem Sie die Anfangsbuchstaben der Wörter unter Beachtung der Groß- und Kleinschreibung verwenden. Ein „und“ ersetzen Sie durch das Zeichen +, eine Zahl durch die entsprechende Ziffer. So wird aus dem Satz dieses Passwort: „Ihg4gB+Ag!“

Für sich allein betrachtet könnten Sie sich diese Zeichenkette nie merken. Sie hat keinerlei Bezug zu einem realen Wort und besteht aus einer wilden Mischung aus Zeichen, Ziffern und Buchstaben. Das bedeutet, dass auch sonst niemand dieses Kennwort erraten

ein Einbruchsversuch) wurden festgestellt, ein teurer Einkauf wurde getätigt oder Ihr Konto wurde gesperrt.

Das psychologische Spiel mit der Angst kommt zum Einsatz, weil es Menschen dazu verleitet, schnell und damit unüberlegt zu reagieren. Um dies noch stärker zu unterstützen, finden Sie direkt in der E-Mail einen Link, auf den Sie nur noch klicken müssen, um das Problem sofort zu beheben. Sie gelangen dann (scheinbar) auf die Webseite des Anbieters und melden sich dort an.

→ Der Trick beim Phishing

Erst am Ende der Ereigniskette ist tatsächlich etwas passiert: Eine Phishing-E-Mail leitet Sie nicht auf die echte Anmeldeseite weiter, sondern auf eine täuschend echte Kopie. Wenn Sie dort Ihre Zugangsdaten eingeben, landen diese bei den Betrügern, denen die gefälschte Seite gehört.

Nachdem Sie Ihre Daten eingegeben haben, werden Sie oft sogar auf die echte Seite des Anbieters weitergeleitet, sodass Ihnen gar nichts auffällt. Jetzt haben die Betrüger Ihre Zugangsdaten und können mit Ihrem Konto tun und lassen, was sie möchten, wenn keine weiteren Schutzmaßnahmen eingerichtet sind. Und auch dann liegen viele Ihrer persönlichen Daten offen.

Welche Folgen kann Phishing haben?

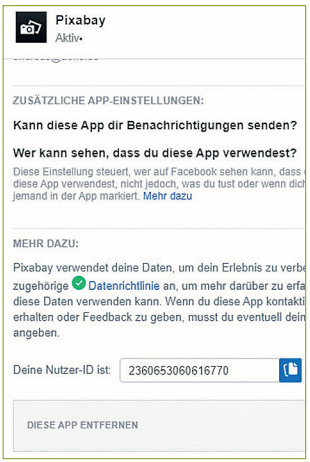
Banken sind spätestens seit der neuen Zahlungsdiensterichtlinie PSD2 (Payment Services Directive2), das heißt seit dem 14. September 2019, dazu verpflichtet, zusätzlich zur Anmeldung auf der Onlinebanking-Webseite jede Transaktion durch eine neu generierte Transaktionsnummer (TAN) abzusichern. Die alte TAN-Liste, die

früher zum Einsatz kam, ist nicht mehr zulässig. Meist wird die TAN, die Sie bei einer Transaktion eingeben müssen, per SMS verschickt oder sie lässt sich auf einem kleinen Code-Gerät ablesen.
Damit lassen sich Transaktionen zwar absichern und das Risiko des Verlusts von Geld wird minimiert. Viele Banken lassen allerdings eine Anmeldung und den Zugriff auf den Kontostand immer noch ohne TAN zu – dazu reichen also die Daten aus, die Sie bei einer Phishing-Attacke verlieren würden.
Stellen Sie sich einmal vor, welche Informationen damit offen liegen: die Zahlung an einen Facharzt, Abbuchungen von verschiedenen, teilweise speziellen Händlern, Geldeingänge von Ämtern für Sozialleistungen, Kindergeld, Pflegegeld und vieles mehr. Teilweise kommen Betrüger auf diesem Weg sogar an Kundennummern, die wiederum missbraucht werden können.
Auch bei einem Onlinehändler ist das Ergebnis nicht besser: Vielleicht schützt Sie eine Zwei-Faktor-Authentifizierung davor, dass Betrüger neue Bestellungen auslösen, aber Ihre Bestellhistorie liegt dennoch für Fremde offen. Besonders bei Händlern mit einem universellen Angebot wie Amazon ist das eine ergiebige Informationsquelle: Bücher geben Aufschluss über Interessen, aber beispielsweise auch über Krankheiten. Die regelmäßige Rum-Bestellung lässt Alkoholismus vermuten, die erste Windelbestellung eine Schwangerschaft und vieles mehr.

Wie schützt man sich vor Phishing?

Im Falle des Phishings sind es weniger die technischen Hilfsmittel wie Virenscanner oder Firewalls, die Ihre Daten schützen, sondern Selbstbeherrschung: Wenn Sie eine verdächtigte E-Mail bekommen, dann unterdrücken Sie die aufkommende Panik und führen Sie einige wenige Schritte durch:

- **Warnmeldungen beachten:** Die meisten Phishing-E-Mails werden von Ihrem E-Mail-Programm als verdächtig eingestuft: Achten Sie auf Meldungen über dem Inhaltsbereich der E-Mail.



Natürlich ist die Verknüpfung Ihres Facebook-Kontos mit den Webseiten (und auch mit Apps, bei denen Sie diese Funktionalität ebenfalls nutzen können) nicht unumkehrbar: Gehen Sie in Facebook in die Privatsphäre-Einstellungen, dann auf *Apps und Websites*. Hier finden Sie alle Verknüpfungen zu Webseiten, können genau sehen, was die Webseiten sehen und verwenden können. In Maßen können Sie hier sogar Änderungen vornehmen. Wenn Sie eine Webseite nicht mehr benutzen wollen oder Ihnen bei der Rückkontrolle deren Datenhunger zu weit geht, dann können Sie den Zugang ganz unten durch einen Klick auf *Entfernen* löschen.

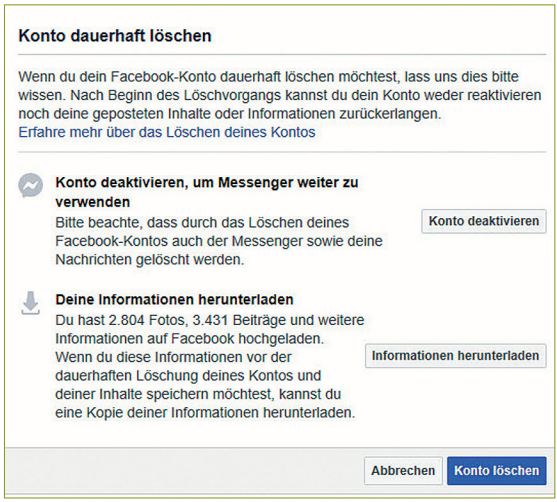
Das Konto löschen

Sie müssen keine sozialen Netzwerke nutzen. Wenn Sie irgendwann die Nase voll haben, dann können Sie Ihr Konto kündigen und verlangen, dass die Daten gelöscht werden. Bei Facebook finden Sie diese Funktion unter *Deine Facebook-Informationen*, *Deaktivierung und Löschung*.

Option: Informationen herunterladen

Vor der Löschanforderung können Sie alle Ihre Daten herunterladen. Diese Option können Sie auch nutzen, um einen Überblick über die von Ihnen bei Facebook eingegebenen Daten zu erhalten. Dieser vermeintliche Service ist der Versuch des Netzwerks, der Vorgabe der EU-Datenschutz-Grundverordnung in Artikel 20 zu entsprechen: Sie haben das Recht, die Sie betreffenden personen-

bezogenen Daten, die ein Unternehmen gespeichert hat, „in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten“.



Sind die Daten wirklich gelöscht?

Informationen darüber, was Facebook aus Ihren Daten extrahiert hat, ob und wie diese mit anderen Daten zusammengeführt wurden usw., werden Sie darin vergeblich suchen. Und wann die Löschanforderung tatsächlich physisch umgesetzt wird, die Daten also wirklich von den Facebook-Servern verwunden sind, das steht in den Sternen. Auch wenn Facebook warnt, dass das Löschen des Kontos unumkehrbar ist: Innerhalb von 30 Tagen können Sie sich weiterhin anmelden und die Löschung stoppen. Mindestens so lange sind die Daten also immer noch verfügbar.

Das ist ein allgemeines Problem, nicht nur bei sozialen Netzwerken: Eine Löschung anfordern ist das eine, einen Nachweis zu haben, dass diese tatsächlich durchgeführt wurde, das andere. Selbst wenn Sie einzelne Beiträge oder Datensätze selbst löschen, bedeutet das nicht, dass diese nicht mehr vorhanden sind. Sie werden Ihnen nur nicht mehr angezeigt. Wenn Sie auf Nummer sicher gehen wollen, ist es also besser, die Daten gar nicht erst preiszugeben.

So machst du das Löschen deines Kontos wieder rückgängig:

1. Melde dich innerhalb von 30 Tagen, nachdem du dein Konto gelöscht hast, bei deinem Konto an.
2. Klicke auf **Löschen abbrechen**.

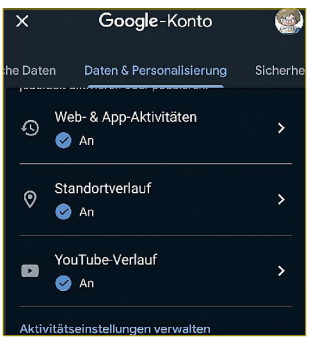
Daten regelmäßig: Wenn Sie das Profil vor Jahren angelegt haben, sind einige dieser Daten vielleicht falsch. Andere waren früher öffentlich sichtbar, können aber heute auf privat gesetzt werden und sind dann nicht mehr allgemein sichtbar. Auf diese Weise können Sie Ihren digitalen Fingerabdruck verkleinern.

Einstellungen auf dem Android-Smartphone

Auch Ihr Android-Smartphone selbst erlaubt es Ihnen, die Datenerfassung einzuschränken. Die Beschreibungen basieren auf Android 14, bei anderen Versionen sind sie aber ähnlich zu erreichen.

Datenschutz bei Android

Sie können die kompletten Privatsphäre-Einstellungen, die beim Google-Konto beschrieben wurden, auch direkt am Telefon einstellen. Dazu gehen Sie in die Einstellungen auf *Google*, dann auf *Google-Konto verwalten*. Unter *Daten und Datenschutz* sowie *Persönliche Daten* können Sie sich die *Datenschutz-Tipps* ansehen und die gewünschten Einstellungen vornehmen.

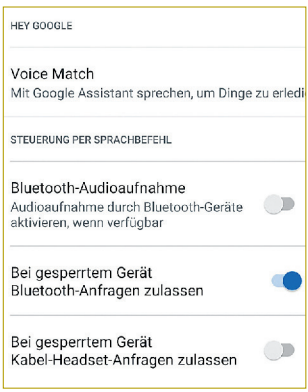


Wenn es Ihnen nur um den Standortverlauf geht, können Sie diesen direkt unter *Einstellungen*, *Standort* deaktivieren.

Zudem finden Sie unter *Einstellungen >Sicherheit und Datenschutz* Hinweise und gegebenenfalls Warnungen, wenn etwas aus Sicht des Systems nicht stimmt. Hier können Sie auch Berechtigungen für alle installierten Apps prüfen.

Spracherkennung ausschalten und Daten löschen

Google verwendet mit dem Google Assistant einen eigenen Sprachassistenten, der wie alle Apps dieser Kategorie sehr neugierig ist. Beim Google Assistant kommt noch hinzu, dass er Ihr Sprachverhalten lernt und bei jeder Aktivierung Ihr Sprachprofil verfeinert. Im Grunde eine nette Idee, leider aber um den Preis einer Audioaufnahme mit Nebengeräuschen, die an Google übermittelt wird.



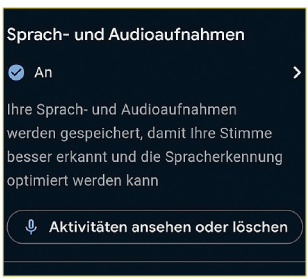
In der Praxis haben die Sprachassistenten ohnehin einen eher eingeschränkten Nutzen. Gerade dann, wenn Sie den Sprachassistenten bisher kaum verwenden, ist es empfehlenswert, einzugreifen. Google ändert die Zugänge zu diesen Funktionen teilweise von Subversion zu Subversion von Android, daher kann es sein, dass diese Beschreibung ein wenig von den konkreten Schritten auf Ihrem Gerät abweicht.

1 Starten Sie den Google Assistant auf Ihrem Android-Gerät, indem Sie die *Assistant*-Taste drücken. Diese unterscheidet sich von Hersteller zu Hersteller, von Gerät zu Gerät.

2 Tippen Sie unten rechts auf das *Kompass*-Symbol.

3 Tippen Sie oben rechts auf Ihr Kontobild, dann auf *Einstellungen* und *Meine Daten bei Assistant*.

4 Rollen Sie dort weiter nach unten auf die *Spracheinstellungen*. Hier können Sie wie bei den anderen Web- und App-Aktivitäten anwählen, dass alle oder nur ältere Aktivitäten gelöscht werden sollen.



Zum Deaktivieren des Google Assistant müssen Sie einen etwas vertrackten Weg gehen (die Vermutung, dass das von Google durchaus so beabsichtigt wurde, ist naheliegend):

1 Starten Sie den Google Assistant auf Ihrem Android-Gerät, indem Sie die *Assistant*-Taste drücken.