DATENSCHUTZ

SICHER IM NETZ

mecodia | AKADEMIE

Inhaltsverzeichnis

Datenschutz am Computer 6
Der richtige Schutz für den Internetbrowser 6
Im Inkognito- Modus surfen 6
Browserverlauf löschen 6
„Do-not-track“-Funktion aktivieren 7
Ad-Tracking Deaktivieren 8
Anti-Tracking-Add-Ons installieren 8
Cookies löschen 8
Skripte blockieren 9
Der richtige Schutz für den Computer 9
Kamera und Mikrofon abschalten 9
Virenschutzprogramm installieren 10
Automatische Bildschirmsperre 10
Windows Firewall aktivieren 10
Weitere Hinweise 11
Den richtigen Passwortschutz verwenden 11
Tipps für E-Mails 11
Weitere Tipps 11
Datenschutz fürs Smartphone 12
Smartphone einrichten 12
Doppelter Passwortschutz: SIM-Pin und Bildschirmsperre aktivieren 12
Ortungsdienste deaktiveren 12
IMEI notieren 12
Passwortschutz für In-App-Käufe 12
Ad-Tracking deaktivieren 13
Google-Standortverlauf deaktivieren 14
Automatische Datenbackups deaktivieren 15
Google-Aktivitäten abschalten bei Android 16
Virenschutz 17
Externe Sperr- und Löschmöglichkeiten fürs Smartphone 18
Daten bei falscher Pin-Eingabe löschen 18
Daten verschlüsseln (Android) 18
Regelmäßige Checks 19
Regelmäßige Updates 19
App-Berechtigungen überprüfen 19
Browserverlauf regelmäßig löschen 20
Google-Suchverlauf löschen 20
Datenaustausch im Hintergrund einschränken 20
Tipps für Apps und Soziale Medien 22
Tipps für WhatsApp 22
Zuletzt Online-Funktion deaktivieren 22
Lesebestätigung deaktivieren 23
Profilbild und Status deaktivieren oder nur für Freunde sichtbar machen 23
Personen blockieren 23
WhatsApp-Konto löschen 24
Tipps für Facebook 24
Online-Status bei Facebook verbergen 24
Personen blockieren bei Facebook 24
Facebook-Konto löschen 25
Privatsphäre-Einstellungen 26
Werbetracking deaktivieren 26
App-Unternehmen vom Profil löschen 27
Tipps für Instagram 27
Privates Konto 27
Tipps für Snapchat 27
Privatsphäre schützen 27
Tipps für Twitter 28
App-Tracking deaktivieren 28
Zukünftige Entwicklungen 28
Smarte Sache 28
Videoüberwachung 29
Fazit 29

Hallo lieber Nutzer von Smartphones, Computern und neuen Medien

Geräte und Dienste geben uns an vielen Stellen tatsächlich die Möglichkeit, die Datensammlung einzuschränken. Doch die richtigen Einstellungen vorzunehmen ist aufwändig und kostet Zeit. Wir raten ihnen: Nehmen sie sich diese Zeit, es lohnt sich!“

Egal ob wir in sozialen Netzwerken unsere Daten preisgeben, oder Firmen und Organisationen unsere persönlichen Daten sammeln und zusammenführen – in Summe entsteht ein erschreckend genauer digitaler Fußabdruck von uns.

Durch die Nutzung von Smartphones, Smart-TVs oder die Nutzung unseres Browsers hinterlassen wir unzählige Datenspuren. Diese werden gesammelt, ausgewertet und mit Nutzerprofilen verknüpft. So können unsere Daten für personalisierte Werbung oder sogar für die Weitergabe an staatliche Behörden verwendet werden. Unternehmen wie Facebook, Google, Apple und Co. arbeiten hier nach einem ganz einfachen Prinzip: Je mehr sie über uns wissen, desto besser können sie dieses Wissen vermarkten und damit Geld verdienen. Und wir dienen dabei als Datenlieferanten, die nicht wissen, was mit ihren Daten geschieht. Stück für Stück werden wir so zum „gläsernen Menschen“. Die Methoden und Tricks, um unsere Nutzerdaten zu tracken, werden dabei immer ausgefeilter. Hinzu kommen politisch oder finanziell motivierte Hacker, die sich mittels Viren und Trojanern Zugang zu unseren PCs und Smartphones verschaffen. Ein Großteil des potentiellen Schadens kann aber verhindert werden, wenn der Nutzer bestimmte Datenschutzmaßnahmen trifft.

Dieser Leitfaden zeigt die besten Tipps für den Datenschutz am Smartphone und PC.

Datenschutz am Computer

Der richtige Schutz für den Internetbrowser

Im Inkognito-Modus surfen

Das Surfen im Inkognito-Modus ist vor allem dann sinnvoll, wenn du an einem fremden Computer eingeloggt bist. Du kannst aber auch zu Hause an deinem eigenen Computer in diesem Modus surfen, wenn du nicht möchtest, dass andere Benutzer deines Computers den Internetverlauf, die Downloads oder die Autofill-Dateien einsehen können. Autofill bedeutet, dass dein Internet-Browser sich merkt, wie beispielsweise bei auf bestimmten Portalen dein Nutzername lautet. Tippst du den ersten Buchstaben deines Nutzernamens ein, so wird der vollständige vorgeschlagen und du musst ihn nur noch anklicken. Der Inkognito-Modus eignet sich zudem, wenn man seine Surfaktivitäten geheim halten möchte oder man an einem öffentlichen Computer wegen der Sicherheit und Privatsphäre besorgt ist. In allen gängigen Browsern kann der Inkognito-Modus aktiviert werden.

Bei **Google Chrome** das Menü über die drei Punkte öffnen, anschließend auf „neues Inkognito-Fenster“.

Bei **Mozilla Firefox** das Menü über die drei Striche öffnen, „neues Privates Fenster“ wählen.

Im **Internet Explorer** auf das Einstellungen-Zahnrad und dann Sicherheit klicken. Dort „InPrivate-Browsen“ auswählen.

Browserverlauf löschen

Der Browserverlauf speichert alle besuchten Seiten und bietet dadurch viele Informationen über den Benutzer und sein Surfverhalten. Deshalb sollte der Browserverlauf ab und zu gelöscht werden.

In **Google Chrome** im Menü auf „Verlauf“ klicken. Oben links können die Browserdaten gelöscht werden.

In **Firefox** auf Einstellungen und dann „Chronik“ klicken. Dort „neuste Chronik löschen“ auswählen und den Zeitraum bestimmen, der gelöscht werden soll.

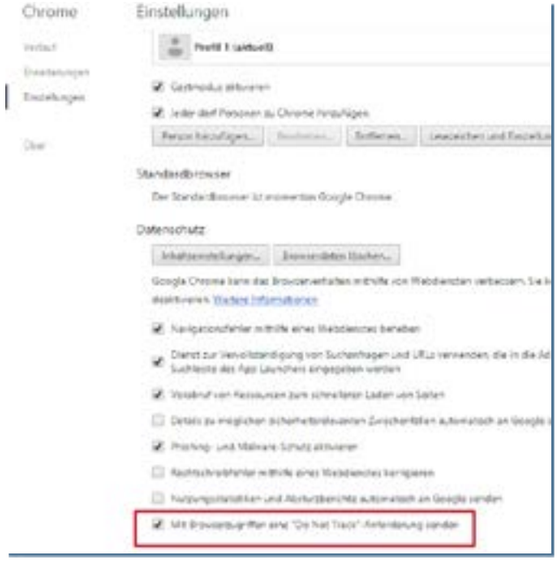
Im **Internet Explorer** die Einstellungen aufrufen und auf „Sicherheit“ klicken. Dort „Browserverlauf löschen“ wählen. Hier gibt es die Möglichkeit den Browserverlauf und auch alle Cookies nach jedem Beenden zu löschen. Hierfür in den Browser-Einstellungen „Internetoptionen“ wählen und die Registerkarte „Allgemein“ öffnen. Unten bei „Browserverlauf nach Beenden löschen“ ein Häkchen setzen und Entscheidung mit „OK“ bestätigen.

„Do-not-track“-Funktion aktivieren

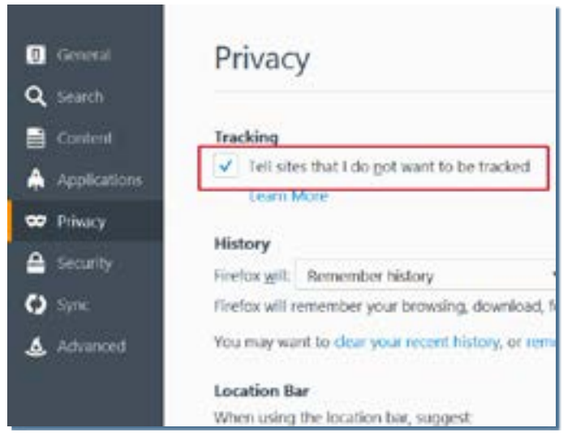
Die „Do-not-track“-Funktion sendet beim Aufrufen einer Webseite eine Bitte an die Seite, kein Nutzungsprofil über den Besuch eines Nutzers zu erstellen.

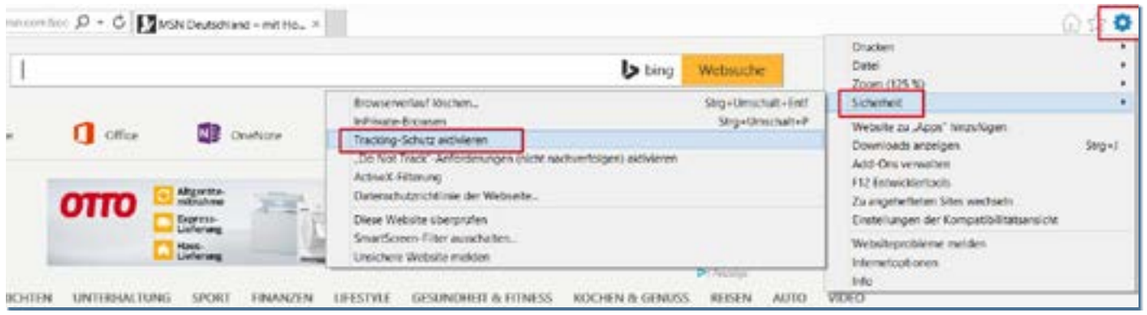
Die Funktion kann man aktivieren, indem man in **Google Chrome** die Einstellungen über das Menü aufruft, dort nach ganz unten scrollt und auf „erweiterte Einstellungen“ klickt. Unter „Datenschutz“ gibt es das Feld „Mit Browserzugriffen eine „Do-Not-Track“-Anforderung senden“. Dort einen Haken setzen und das erscheinenden Feld mit „Ok“ bestätigen.

Im Browser **Mozilla Firefox** kann man ebenfalls die „Do-not-track“-Option einstellen. Dafür muss man in den Einstellungen auf „Datenschutz“ gehen und dann in das Kästchen „Websites mitteilen, meine Aktivitäten nicht zu verfolgen“ ein Häkchen setzen.



Klicke im **Internet Explorer** auf das Zahnrad oben rechts. Dadurch öffnen sich die Einstellungen. Anschließend auf „Sicherheit“ und im





nächsten Menü auf „Do-not-track-Anforderungen (nicht nachverfolgen)" klicken.

Da es sich bei der Funktion „Do-not-track" lediglich um eine Bitte an die Webseite handelt, kann nicht sichergestellt werden, ob ein Nutzerprofil erstellt wurde oder nicht.

Ad-Tracking deaktivieren

Bei jedem Klick im Internet werden Informationen zu Interessen und Vorlieben des Nutzers gesammelt. Diese werden dann zum Anzeigen von passenden Suchergebnissen aber eben auch zur Anzeige interessenbezogener Werbung verwendet. Manche Suchanfragen sind aber möglicherweise sehr privat oder intim. Der Tracking-Schutz sorgt dafür, dass keine interessenbezogene Werbung angezeigt wird.

Wer das Ad-Tracking in **Google Chrome** abstellen will, muss sich mit seinem Google-Konto anmelden und folgende Seiten aufrufen: www.google.de/settings/ads/authenticated und www.google.de/settings/ads/anonymous. Dort kann die interessenbezogene Werbung innerhalb und außerhalb von Google-Webseiten deaktiviert werden.

Klicke im **Internet Explorer** auf das Zahnrad oben rechts, dadurch öffnen sich die Einstellungen. Wähle „Sicherheit" und im nächsten Menü auf „Tracking-Schutz aktivieren" klicken.

Anti-Tracking-Add-Ons installieren

Um den Trackingschutz zu optimieren, können zusätzlich spezielle Browser Add-ons wie „Ghostery", „Disconnect" oder „Privacy" installiert werden, die das Tracking blockieren.

Cookies löschen

Cookies sind Datensätze, die von einer Webseite auf deinem Computer gespeichert werden. Sie enthalten unter anderem Anmeldeinformationen und Daten zu persönlichen Seiteneinstellungen. In deinen Browser-Einstellungen kannst du Cookies löschen oder blockieren. In Bezug auf das User-Tracking spielen Cookies dennoch nur eine geringe Rolle. In der Praxis werden verschiedenste Tracking-Verfahren angewendet und kombiniert, um eine detaillierte Analyse der Anwender zu erreichen.

Skripte blockieren

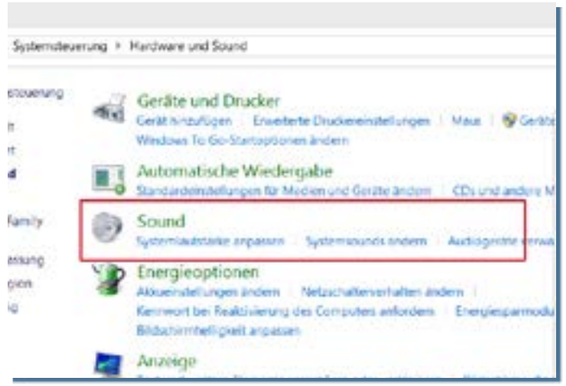
Skripte können Sicherheitslücken ausnutzen, um fremde Skripte in einen vermeintlich sicheren Bereich einer Webseite laufen zu lassen. Darüber können sensible Daten wie zum Beispiel Passwörter oder benutzerspezifische Daten abgegriffen werden. Auch das Erstellen digitaler Fingerabdrücke des Systems und des Browsers ist mit Skripten deutlich einfacher als ohne. Gegenmaßnahmen sind z. B. Add-Ons wie „NoScript", mit dem man alle Skripte generell blockieren und gezielt für vertrauenswürdige Seiten freigeben kann.

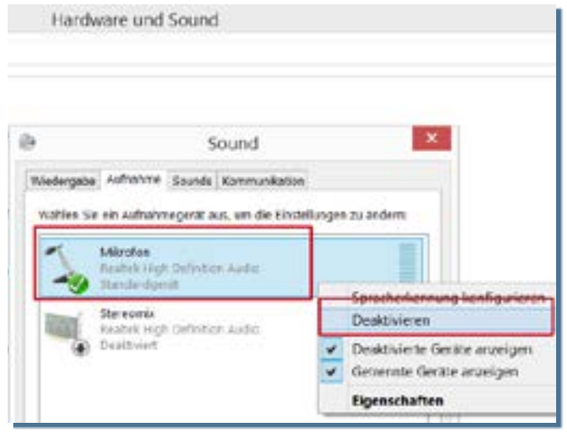
Der richtige Schutz für den Computer

Kamera und Mikrofon abschalten

Wenn der Verdacht besteht, dass der Computer abgehört wird, kann man das **Mikrofon ausschalten**. Hierfür die System-Steuerung öffnen und die Kategorie „Hardware und Sound" wählen. Zu dem Punkt „Sound" wechseln und „Aufnahme" klicken. Hier ein Rechtsklick auf dem Mikrofon ausführen und deaktivieren wählen. Entscheidung mit OK bestätigen.

Um die **Kamera zu deaktivieren**, den Geräte-Manager aufrufen (am besten im Windows-Suchfeld „Geräte-Manager" eingeben und auf dem Computer danach suchen). Dann „Bildverarbeitungsgeräte" wählen. Dort wird die Webcam angezeigt. Mit einem Rechtsklick drauf klicken und „deaktivieren". Alternativ kannst du deine Kamera auch mit einem Stück Papier überkleben.





Virenschutzprogramm installieren

Um sich vor Schadsoftware zu schützen und diese zu erkennen, empfiehlt es sich, ein Virenschutzprogramm zu installieren. Wer sich ein Antiviren-Programm installieren möchte, sollte sich davor über die Software und die Kosten informieren – z. B. auf der Webseite der Computerzeitschrift chip.de oder unter av-test.org

Automatische Bildschirmsperre

Mit der rechten Maustaste auf eine freie Stelle des Bildschirms klicken und im Menü die Option „anpassen“ wählen. In dem sich öffnenden Fester auf „Bildschirmschoner“ klicken und im Menü einen Bildschirmschoner auswählen. Zeit einstellen, nach der der Bildschirmschoner aktiviert werden soll. Haken setzen bei „Anmeldeseite bei Reaktivierung“. Sobald der Bildschirmschoner erscheint, wird man automatisch ausgeloggt und der PC gesperrt. Mit der Tastenkombination “Win +L“ kann der Bildschirm beim Verlassen des PCs auch manuell gesperrt werden.

Windows Firewall aktivieren

Eine Firewall schützt den Computer vor Angriffen aus dem Internet. Diese ist meist bereits schon im Router eingebaut, kann aber am PC zusätzlich installiert und aktiviert werden. Dazu die Systemsteuerung öffnen, im Suchfeld „Firewall“ eingeben und „Windows-Firewall“ auswählen. Links im Menü auf „Windows-Firewall ein- oder ausschalten“ klicken und ggf. per Passwort bestätigen. Wenn die Firewall alle Programme an der Kommunikation hindern soll, dann im Kontrollkästchen auf „Alle eingehenden Verbindungen blockieren, einschließlich der in der Liste zugelassenen Programme“ klicken. Falls nur einzelne Netzwerkadressen geschützt werden sollen, bei den einzelnen Adressen die Windows-Firewall aktivieren und mit OK bestätigen.

Weitere Hinweise

Den richtigen Passwortschutz verwenden

Nach wie vor ist es wichtig, dass der Computer mit einem Passwort gesichert ist, sodass niemand unbefugt auf die Daten zugreifen kann. Auch Online-Zugänge etc. müssen mit einem Passwort gesichert sein. Dabei ist wichtig, das Passwort nicht zu speichern, sondern es immer wieder neu einzugeben. Für das Erstellen eines sicheren Passworts gibt es ein paar Regeln, die beachtet werden sollten. Das Passwort sollte mindestens zwölf Zeichen lang sein, Großbuchstaben und Kleinbuchstaben, Zahlen und Sonderzeichen enthalten. Weiter sollte es keine Begriffe enthalten, die mit einer Person oder einem selbst in Verbindung stehen. Aber nicht jedes Passwort, dass diese Anforderungen erfüllt, ist auch sicher: Ein einfaches Passwort wie z.B. Backofen1! Kann trotzdem noch schnell geknackt werden.

Mehr zu einem sicheren Passwort gibt es auch in unserem Passwort-Leitfaden.

Tipp: Auf der Webseite checkdeinpasswort.de kann die Sicherheit von Passwörtern geprüft werden.

Tipps für E-Mails

E-Mails von unbekannten Absendern können Viren oder Malware enthalten und sollten nicht geöffnet werden. Falls die Mail trotzdem geöffnet wurde, keine Links in der Mail anklicken und nicht darauf antworten. Genauso sollten unbekannte Anhänge nicht geöffnet werden.

Weitere Tipps

- Für Zugriff auf E-Mails, Online-Banking oder beim Online-Shopping auf eine verschlüsselte Verbindung achten. Diese beginnen mit „https“ – das „s“ steht hierbei für „secure“.
- Regelmäßige Backups durchführen, damit die Daten gesichert sind, falls die Festplatte oder der Computer kaputt gehen sollte.
- Das WLAN mit einem modernen Verschlüsselungsstandard (z. B. WPA2) verschlüsseln und den Router bei Nicht-Gebrauch ausschalten.
- Die aktuelle Version des Browsers verwenden und Plugins wie Java oder Flash aktuell halten.
- Verschiedene Suchmaschinen verwenden. Beispielweise stellen metager.de, ixquick.de und startpage.com eine datenschutzfreundliche Alternative zu Google dar. Diese speichern weder IP-Adressen noch sammeln sie Suchanfragen und setzen keine Tracking-Cookies.

Datenschutz fürs Smartphone

Smartphone einrichten

Doppelter Passwortschutz: SIM-PIN und Bildschirmsperre aktivieren.

Ein Zugriffsschutz sollte auch beim Smartphone nicht fehlen. Hier ist sogar ein doppelter Passwortschutz möglich und empfehlenswert. Neben der SIM-Karte sollte auch eine Bildschirmsperre eingerichtet werden, damit niemand unbefugt auf Inhalte zugreifen kann.

Android: In den Einstellungen unter „Sicherheit“ SIM-PIN-Optionen wählen und SIM-Karten-PIN eingeben. Die Bildschirmsperre unter „Sperrbildschirm“ aktivieren.

iOS: In den Einstelllungen unter „Telefon“ den SIM-PIN eingeben. Für die Bildschirmsperre unter Einstellungen auf „Touch ID & Code“ tippen, dort „Einfacher Code“ deaktivieren, den Code einstellen und aktivieren.

Am besten geeignet sind Zahlenkombinationen oder Passwörter, die nicht in Verbindung mit einem selbst stehen. Bei Mustern (z. B: 1234, 4444 oder 2580) besteht die Gefahr, dass der Code leicht erraten werden kann. Ebenso verraten hinterlassenen Fettspuren auf dem Display das Smartphones schnell den Code.

Ortungsdienste deaktivieren

Über Ortungsdienste wie GPS aber auch über WLAN und Bluetooth kann nachverfolgt werden, wo man sich aufhält. Außerdem können die Funk-Verbindungen genutzt werden, um auf Daten des Smartphones zuzugreifen. Deswegen sollten sie deaktiviert werden, wenn man sie nicht braucht.

Android: Den oberen Bildschirmrand herunterziehen und dort die Dienste abschalten. Alternativ Dienste in den Einstellungen abschalten.

iOS: Dienste in den Einstellungen deaktivieren.

IMEI notieren

Android & iOS: In der Telefon-App mit der Tastenkombination *#06# die IMEI abrufen und extern notieren. Diese Identifikationsnummer ist bei jedem Gerät einzigartig und hilft, das Smartphone zu identifizieren, wenn es nach einem Verlust wiedergefunden wird. Bei manchen Netzbetreibern kann man das Handy auch über diese Nummer sperren lassen.

Passwortschutz für In-App-Käufe

Android: Im Play Store die Menü-Taste antippen, um zu den Einstellungen zu gelangen. Dort unter „Authentifizierung für Käufe erforderlich“ „Für alle Käufe wählen.“ Anschließend das Passwort des Google-Kontos eingeben.

iOS: In den Einstellungen unter „Allgemein“ „Einschränkungen“ auswählen. Dort einen Code festlegen (und merken), der vor unautorisierten Käufen im App Store schützt.

Ad-Tracking deaktivieren

Smartphones unterstützen die Werbeindustrie und sammeln Informationen welche Apps wie lange und wie häufig genutzt werden. Dadurch kann auf Vorlieben und Interessen geschlossen und passgenaue Werbung angezeigt werden. Auf dem Smartphone kann das Ad-Tracking ganz einfach deaktiviert und zurückgesetzt werden.

Android: In den Einstellungen die Google-Einstellungen auswählen. Dort auf „Anzeigen“ gehen und die interessenbezogenen Werbung deaktivieren. Die Werbe-ID kann hier ebenfalls zurückgesetzt werden.

Bei neueren Android-Versionen in den Google-Einstellungen auf „Persönliche Daten & Privatsphäre / Einstellungen für Werbung“ (öffnet im Browser) und dort auf „Einstellungen für Werbung verwalten“ klicken. Danach interessenbezogene Werbung deaktivieren und zurücksetzen.

iOS: Die Einstellungen aufrufen und auf Datenschutz klicken. Dort „Werbung“ auswählen, „Kein Ad-Tracking“ aktivieren sowie die Ad-ID zurücksetzen.

Google-Standortverlauf deaktivieren

Android: Je nach Android-Version gibt es unterschiedliche Möglichkeiten die Standortdaten für die Google-Suche zu deaktivieren.

Erste Möglichkeit: Einstellungen öffnen, Standortdienste wählen und „Standort und Google-Suche“ deaktivieren. In neueren Android-Versionen „Google-Standortverlauf“ deaktivieren.

Zweite Möglichkeit: Einstellungen öffnen, Google-Einstellungen wählen, Standortdienste wählen und deaktivieren.

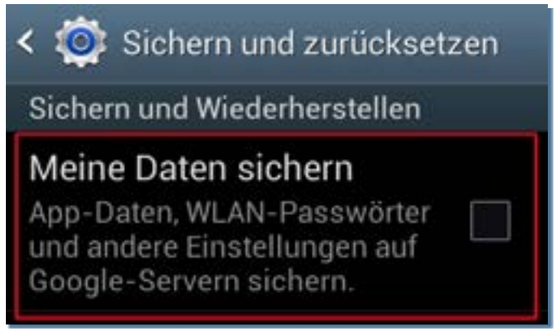
Dritte Möglichkeit: Die Google-App öffnen, auf Einstellungen gehen, Konten & Datenschutz wählen, Standort und Sicherheit klicken und „GPS-Satelliten verwenden“ deaktivieren.

iOS: Einstellungen öffnen und Datenschutz wählen. Dort Ortungsdienste für Google deaktivieren. Oder: In den Einstellungen für die Google-App Standort-Zugriff auf „nie“ stellen.

Automatische Datenbackups deaktivieren

iCloud und Google speichern automatisch Daten des Geräts, wenn man dies nicht unterbindet. Mit wenigen Klicks kann das abgeschaltet werden.

Android: Über die Einstellungen auf „Sichern und zurücksetzen“ tippen und dann „Meine Daten sichern“ deaktivieren. Je nach Modell und Android-Version kann es auch in den Einstellungen über „Sichern und zurücksetzen“ und „meine Daten sichern“ deaktiviert werden.



iOS: Über die Einstellungen auf „iCloud“ tippen und dort das Backup deaktivieren. Wer Apple nicht alle Daten preisgeben möchte, kann auswählen, dass nur die wichtigsten Daten gesichert werden. Dafür in den Einstellungen unter „iCloud“ die Sicherung der entsprechenden Daten aktivieren bzw. deaktivieren.

Auf eine vollständige Datensicherung sollte aber keinesfalls verzichtet werden. Im Fall eines Verlusts oder Defekts des Smartphones wären Daten ansonsten verloren. Daher empfiehlt es sich, beispielsweise über USB-Kabel eine Datensicherung auf dem PC zu erstellen.

Google-Aktivitäten abschalten bei Android

Insbesondere Android-Telefone sind dem Datenhunger von Google ausgeliefert. Google greift auf Aktivitäten zu, um das Nutzungsverhalten zu durchleuchten und die Suchergebnisse und Apps zu personalisieren. Jeder Suchverlauf, egal ob in der Google-Suche, Maps, YouTube oder im Browser wird gespeichert und ausgewertet. Der Zugriff auf Aktivitäten kann jedoch beschränkt werden.

Über die Google-App die Einstellungen aufrufen. In den Einstellungen „Konten & Datenschutz“ wählen. Die Ansicht kann hier je nach Version und Smartphone anders sein. „Google-Kontoverlauf“ wählen und alle Aktivitäten auf „pausiert“ setzen.

Virenschutz

Ein Virenschutz ist auch auf dem Smartphone wichtig. Er schützt das Smartphone vor Viren und Trojanern und hat meist noch weitere praktische Funktionen wie z. B. die Ortung des Smartphones, wenn es verloren geht oder geklaut wurde. Im Folgenden stellen wir einige Apps für Android vor.

Hinweis: Für iOS gibt es nur wenige Virenschutz-Pograme. Apple sorgt im Gegensatz zu Android besser für den Schutz des Smartphones. Achte deswegen stets darauf, dass du die aktuelleste iOS-Version auf deinem iPhone verwendest.

- **Avast Mobile Security für Android**
  Der Virenscanner „Avast Mobile Security“ arbeitet schnell und bremst das System nicht. Er ist mit einem Surfschutz, einem Anruf- und SMS-Filter gut ausgestattet. Außerdem hilft die App auch weiter, wenn das Smartphone gestohlen oder verloren wurde.
  https://play.google.com/store/apps/details?id=com.avast.android.mobilesecurity&hl=de
- **DroidWall**
  Eine Firewall für Android braucht nicht jeder, die App DroidWall ist aber für Nutzer

gerooteter Geräte einen Blick wert. Die App schützt vor Angriffen und hilft den Internet-Zugriff der installierten Apps zu regulieren. Hier gibt es getrennte Regeln für WLAN und 3G, sodass man gezielt den mobilen Datentraffic schonen kann.
https://play.google.com/store/apps/details?id=com.googlecode.droidwall.free&hl=de

- **McAfee Antivirus & Security**
  Diese App bietet Schutz für Smartphones und Tablets. Neben einer Antivirus –Funktion verfügt sie auch über die Möglichkeit der Geräteortung, einen App Schutz und die Möglichkeit zur Leistungsoptimierung.
  https://itunes.apple.com/us/app/mcafee-security-privacy-vault/id724596345?mt=8
  https://play.google.com/store/apps/details?id=com.wsandroid.suite

Externe Sperr- und Löschmöglichkeiten fürs Smartphone

Android: Mit der App „Android-Geräte-Manager“ bzw. über den Google-Account, kann das Smartphone vom PC aus geortet, gesperrt und die Daten gelöscht werden.

iOS: Mit der App „Mein iPhone suchen“ bzw. über die iCloud kann das Gerät geortet, gesperrt oder gelöscht werden.

Daten bei falscher Pin-Eingabe löschen

Falls das Smartphone gestohlen wird, sollen die Daten nach mehrfacher falscher Eingabe des Bildschirm-PINs gelöscht werden. Dies setzt allerdings eine regelmäßige Datensicherung voraus.

iOS: In den Einstellungen auf Code und dann „Daten löschen“ aktivieren. Für Android existiert diese Möglichkeit nicht.

Daten verschlüsseln

Bei neuen **Android-Smartphones** ab Android Version 5 ist der Speicher automatisch verschlüsselt. Bei älteren Geräten müssen Nutzer die Daten auf dem Gerät und (falls vorhanden) einer SD-Karte selbst verschlüsseln. Falls das Smartphone verloren geht, kann der Finder nicht auf die Daten zugreifen. Um die Daten zu verschlüsseln, in den Einstellungen auf „Sicherheit“ tippen. Dort die Punkte SD-Karte und Gerät verschlüsseln auswählen.

Um das Gerät zu verschlüsseln muss zunächst ein Passwort angelegt werden. Außerdem muss der Akku aufgeladen sein, am besten ist es, wenn das Gerät während der Verschlüsselung am Ladekabel hängt. Die Verschlüsselung der Daten dauert mindestens eine Stunde, man sollte also genug Zeit einplanen. Wenn die Verschlüsselung unterbrochen wird, kann es passieren, dass Daten verloren gehen.

Bei iOS-Geräten sind die Daten automatisch auf dem internen Speicher verschlüsselt, sobald man eine Bildschirmsperre eingerichtet hat.

Regelmäßige Checks

Regelmäßige Updates

Regelmäßige Updates von Apps und Betriebssystem sind sinnvoll, um eine hohe Sicherheit zu gewährleisten.

Android: Updates werden in der Regel vom Play Store gemeldet oder automatisch durchgeführt. Ansonsten im Play Store im Menü unter „Meine Apps“ nachschauen, ob Updates verfügbar sind und diese dann installieren. Ein Update für das Betriebssystem wird normalerweise automatisch gemeldet. Andernfalls in den Einstellungen unter dem Punkt Geräteinformationen nachschauen, ob ein Software-Update verfügbar ist.

iOS: App-Updates können automatisch durchgeführt werden. Dazu in den Einstellungen unter „iTunes & App Store“ „Updates“ aktivieren. Alternativ im App Store nach Updates suchen. Das Gerät meldet, wenn ein neues Betriebssystem verfügbar ist. Ansonsten in den Einstellungen unter „Allgemein“ und „Softwareaktualisierungen“ nachschauen.

App-Berechtigungen überprüfen

Apps fordern viele Zugriffe auf bestimmte Teile des Smartphones. So sammeln sie jede Menge empfindlicher Daten wie Kontaktdaten, E-Mails, persönliche Bilder, den Standort oder Informationen zu Telefonanrufen.

Android (ab Version 6): Nutzer können die App-Berechtigungen selbst verwalten. Neue Apps fragen dich vor dem Zugriff auf bestimmte Funktionen (Kamera, Standort usw.), ob du den Zugriff erteilen möchtest. Einmal erteilte

Berechtigungen können später in der App-Übersicht in den Einstellungen wieder entzogen werden.

Android (bis Version 5): Beim Herunterladen aus dem Google Play Store werden die Berechtigungen, die eine App verlangt, vor der Installation angezeigt. Hier sollte man abwägen, ob man der App die Berechtigungen erteilen möchte oder ob man sie lieber nicht installiert. Für installierte Apps kann man die Berechtigungen im Anwendungsmanager in den Einstellungen anschauen. Der Entzug von Berechtigungen ist jedoch nicht möglich.

iOS: Die App-Berechtigungen werden vor der Installation nicht angezeigt, stattdessen frägt die App beim Datenzugriff um Erlaubnis. Man kann die Befugnisse aber auch nachträglich in den Einstellungen unter „Datenschutz“ anschauen und der App Berechtigungen entziehen.

Browserverlauf regelmäßig löschen

Android: Die Chrome-App öffnen und die Einstellungen aufrufen. Dort „Datenschutz“ wählen und ganz unten auf „Browserverlauf löschen“.

iOS: Auf Einstellungen gehen, Safari wählen und „Verlauf und Websitedaten löschen“ klicken.

Google-Suchverlauf löschen

Android: Über die Google-App in die Google-Einstellungen gehen. „Konten & Datenschutz“ wählen. „Google-Kontoverlauf“ wählen. Dort werden die App-Aktivitäten angezeigt. Jede einzelne Aktivität anklicken und auf „Verlauf verwalten“ klicken. Beim Google-Konto anmelden und über die drei Menüpunkte die Löschoptionen wählen. Dort die Daten löschen.

iOS: Google-App öffnen und auf Einstellungen gehen. Dort auf Datenschutz und anschließend auf Verlauf klicken. Hier gibt es die Option „Verlauf auf Gerät löschen.“ Außerdem kann man den Verlauf für das Gerät komplett deaktivieren. So werden erst gar keine Suchanfragen gespeichert.

Datenaustausch im Hintergrund einschränken

Android: In den Einstellungen auf Datennutzung gehen. Dort die (linke) Menütaste drücken. Dadurch öffnet sich ein neues Menü, in dem man die Hintergrunddaten deaktivieren kann.

iOS: In den Einstellungen unter „Allgemein“ den Punkt Hintergrundaktualisierung wählen. Dort kann die Hintergrundaktualisierung für einzelne Apps oder komplett deaktiviert werden.

Hinweis: Wenn die Hintergrunddaten, bzw. Hintergrundaktualisierung deaktiviert werden, ist es möglich, dass manche Apps nicht mehr wie gewünscht funktionieren, wenn das Smartphone nicht mit einem WLAN verbunden ist.

Weitere Hinweise

- Bitte sensible Daten nicht über Hot Spots oder freies WLAN abrufen oder verschicken. Die Verbindung könnte nicht sicher sein und Dritte könnten auf die Daten zugreifen. Wichtige Daten deshalb vom heimischen WLAN oder über die mobile Datenverbindung abrufen und versenden.
- Bei Verlust des Smartphones die SIM-Karte sperren lassen. Das geht meist über den Netzanbieter. So kann verhindert werden, dass Fremde auf deine Kosten telefonieren.
- Merkwürdige Seiten beim mobilen Surfen sofort verlassen
- Keine Mails von unbekannten Absendern öffnen oder unbekannte Anhänge herunterladen. Solche Mails enthalten oft Viren und Trojaner.
- Auf Kostenfallen achten: Nicht auf fremde SMS antworten und Lockanrufe ignorieren. (Mehr Tipps und Informationen zu Kostenfallen auf www.handysektor.de/abo-abzocke)
- PIN und Passwörter nicht speichern, sondern immer neu eingeben.

Tipps für Apps und soziale Medien

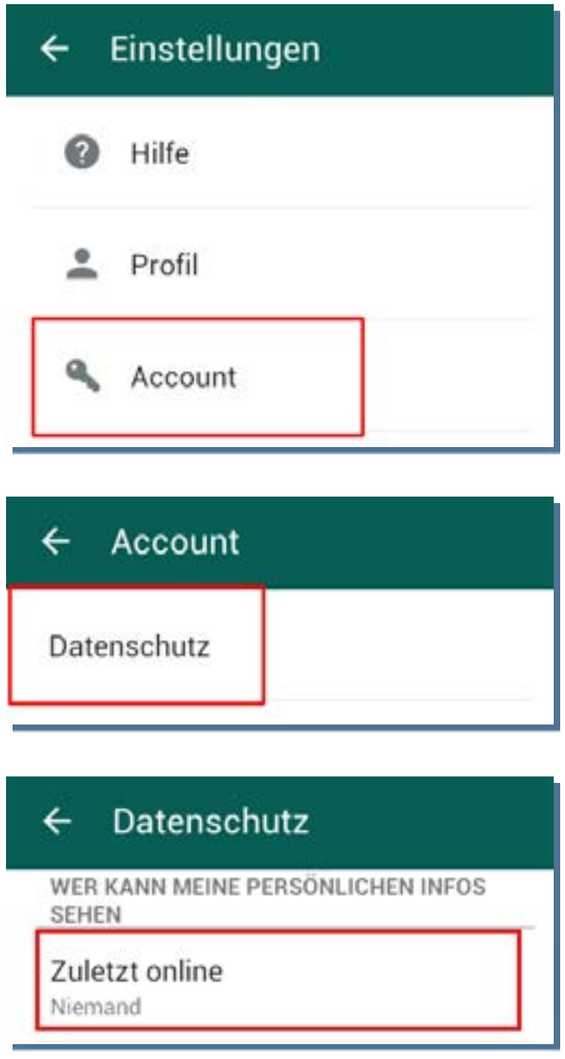
In sozialen Netzwerken gibt es einige Möglichkeiten, die eigene Privatsphäre zu schützen. Es ist wichtig, in den Privatsphäre-Einstellungen die Standardeinstellungen des Anbieters zu ändern, damit nicht jeder alle Bilder, Spiele, Posts usw. sehen kann. Wenn man etwas in einem sozialen Netzwerk veröffentlicht, sollte man darauf achten, dass dies nur von Freunden oder entsprechend geeigneten Kontakten gesehen werden kann. Außerdem sollte gründlich überlegt werden, wie Fremde auf diesen Inhalt reagieren könnten. Es ist sicher nicht von Vorteil, wenn ein Arbeitgeber die Fotos von der letzten Party sehen kann oder private Nachrichten lesen kann.

Tipps für WhatsApp

Nicht jedem ist bewusst, dass auch über WhatsApp verfolgt werden kann, was man gerade tut. Auch hier sollte man auf eine ordentliche Selbstdarstellung achten und beispielsweise nicht ein Partyfoto als Profilbild samt passendem Trinkspruch als Status haben. Denn wenn der Arbeitgeber die Handynummer hat, kann er Status, Bild und Zuletzt-Online-Zeitpunkt sehen. So kann er überprüfen, ob man während der Arbeitszeit in WhatsApp war oder gestern Nacht erst spät nach Hause gekommen ist. Diese Funktionen kann man aber auch ausschalten.

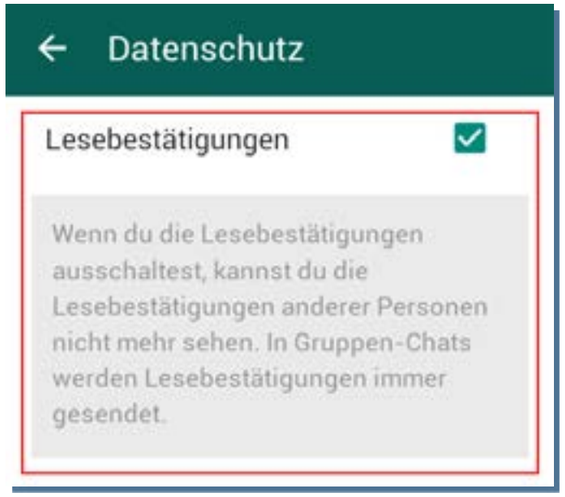
Zuletzt Online-Funktion deaktivieren

Wenn man die Zuletzt Online-Funktion deaktiviert, kann niemand sehen, wann man zuletzt online war. Dafür in den WhatsApp-Einstellungen auf „Account“ und dann „Datenschutz“ gehen. Bei „zuletzt online“ „niemand“ auswählen.



Lesebestätigung deaktivieren

Die blauen Häkchen in WhatsApp zeigen an, dass die Nachricht gelesen wurde. Wenn das Gegenüber erst einmal gesehen hat, dass die Nachricht gelesen wurde, steht man schnell unter Zwang die Nachricht zu beantworten. Diese Lesebestätigung kann man abschalten, indem man in den WhatsApp-Einstellungen auf „Account“ geht und dann auf Datenschutz tippt. Dort nach unten scrollen und die Lesebestätigung abschalten.



Profilbild und Status deaktivieren oder nur für Freunde sichtbar machen

Wer nicht möchte, dass eine fremde Person das Profilbild oder den WhatsApp-Status sehen kann, klickt in den WhatsApp-Einstellungen unter Account den Punkt Datenschutz an. Dort lässt sich einstellen, dass das Profilbild entweder ganz deaktiviert oder nur von Freunden gesehen werden kann. Das gleiche gilt für den WhatsApp-Status.

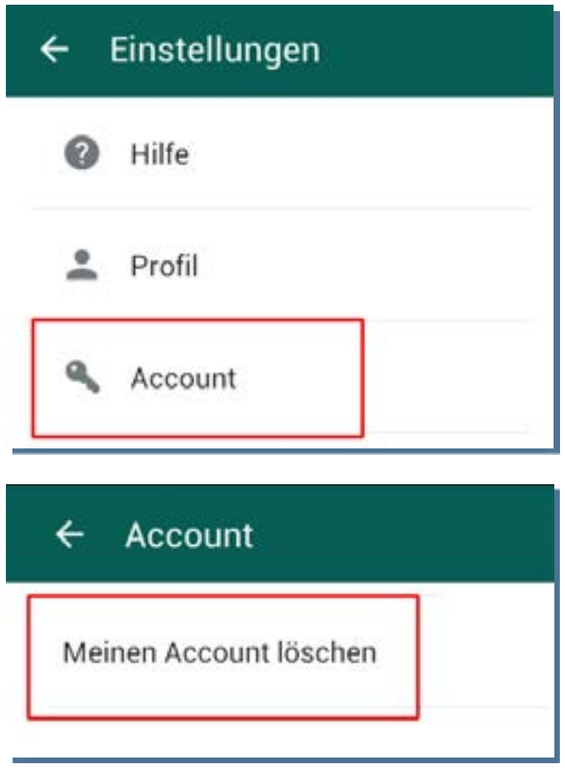
Personen blockieren

Wer sich von Personen auf WhatsApp belästigt fühlt und keine weiteren Nachrichten von ihnen erhalten möchte, kann diese blockieren. Dazu WhatsApp öffnen und die Menütaste drücken. Einstellungen wählen. Auf „Account“ und dann „Datenschutz“ klicken. Dann „blockierte Kontakte“ auswählen. Die Seite zeigt alle Kontakte an, die blockiert wurden. Über den Button oben rechts, kann ein Kontakt zur Liste hinzugefügt werden. Die Funktion, einen Kontakt zu melden, bietet WhatsApp leider noch nicht an.

Hinweis: Da der blockierte Nutzer aber immer noch die Handynummer weiß, kann er trotzdem weiterhin per SMS oder Anruf Kontakt aufnehmen. Daher immer gut überlegen, wem die Handynummer ausgehändigt wird.

WhatsApp-Konto löschen

Um das WhatsApp-Konto zu löschen, WhatsApp öffnen und die Menütaste drücken. In den Einstellungen auf „Account“ klicken und dann „meinen Account löschen“. Jetzt nur noch die Telefonnummer eingeben (Achtung: Vollständig im internationalen Format) und dann auf „meinen Account löschen“ tippen.



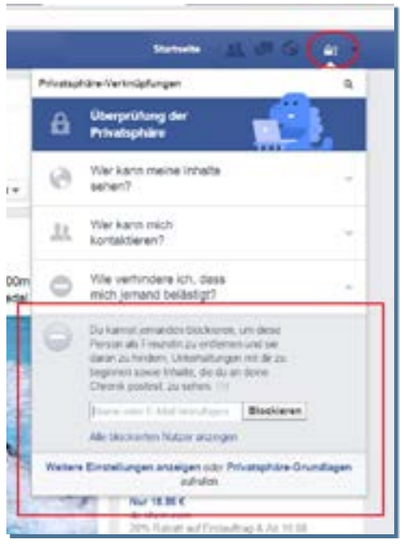
Tipps für Facebook

Online-Status bei Facebook verbergen

Wenn man den Online-Status in Facebook verbirgt, kann im Chat niemand sehen, dass man online ist. Dazu in Facebook einloggen und im Chatfenster unten auf das kleine Zahnrad-Symbol gehen. Im sich öffnenden Menü den Menüpunkt „Chat deaktivieren“ auswählen. Hier kann ausgewählt werden für wen der Chat deaktiviert wird. Der Chat kann für einzelne Personen, aber auch für alle Facebook-Freunde deaktiviert werden. Die Nachrichten werden dann an das Facebook-Postfach gesendet, wo man sie trotzdem lesen kann.

Personen blockieren bei Facebook

Um bei Facebook Personen zu blockieren, die einen belästigen, muss man oben in der Menüleiste auf das Schlosszeichen gehen. Dort die Frage „wie verhindere ich, dass mich jemand belästigt?“ auswählen und den Nutzer hinzufügen, den man blockieren will.

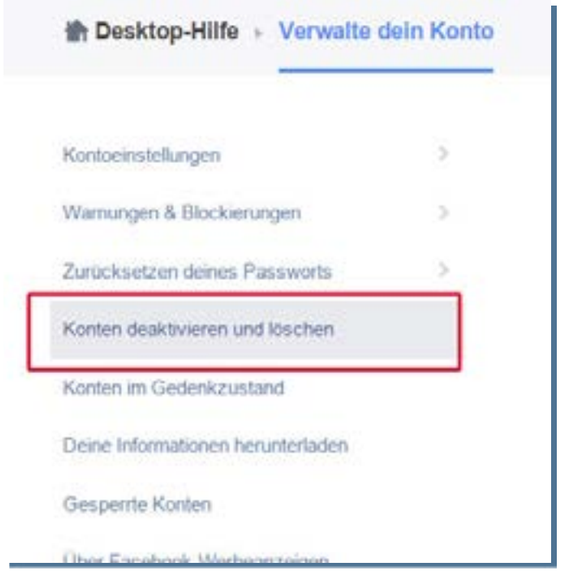


Facebook-Konto löschen

Bei Facebook im Menü „Hilfe“ wählen.

Über den Link „Besuche den Hilfebereich“ unten links im Menü kommt man auf eine Übersichtsseite.

In der Navigationsleiste „Verwalte dein Konto“ wählen.



Dann auf „Konten deaktivieren und löschen“ gehen.

Rechts auf die Frage „Wie lösche ich mein Konto dauerhaft?“ klicken. Dann auf den entscheidenden Link am Ende des ersten Absatzes „Teile es uns mit“ klicken. Ein letzter Klick

auf „Mein Konto löschen“ leitet den Löschvorgang schließlich ein. Dein Facebook-Konto wird nicht sofort gelöscht, sondern erst innerhalb der nächsten zwei Wochen. Wenn du dich in dieser Zeit einloggst, kann der Löschauftrag widerrufen werden.

Privatsphäre-Einstellungen

Bei Facebook kann man seine Privatsphäre-Einstellungen überprüfen. Dazu geht man auf sein eigenes Profil und wählt die drei Punkte neben „Aktivitätenprotokoll anzeigen“ auf dem Titelbild. Dort gibt es die Option „Anzeigen aus der Sicht von“. Hier kann man überprüfen wie Fremde oder Freunde das eigene Profil sehen.
Möchte man die Privatsphäre-Einstellungen ändern und Zugriffe auf die Daten entsprechend einschränken, geht dies unter Einstellungen bei „Privatsphäre“. Einen ausführlichen Leitfaden zur Privatsphäre im sozialen Netzwerk-Facebook findest du unter www.mecodia.de/tipps.

Soziale Werbung deaktivieren

Deine Profilinformationen werden von Facebook für zielgerichtete Werbung genutzt und auch du wirst zum Werbeträger für Unternehmen, die dir gefallen, in den Neuigkeiten deiner Freunde. Doch du kannst das unterbinden: In der obersten Leiste deiner Facebook-Seite auf den kleinen Pfeil nach unten klicken, um in die Einstellungen zu gelangen. Dort gehst du in die Rubrik „Werbeanzeigen“ und klickst im Feld „Werbeanzeigen in meinen sozialen Handlungen“ auf „Bearbeiten“. Wähle hier die Option „Niemand“ aus.

App-Unternehmen vom Profil löschen

Hast du dich einmal mit deinem Facebook-Profil bei einer App angemeldet, so kann diese Zugriff auf bestimmte persönlichen Daten erhalten. Um das zu steuern, gehst du in die Einstellungen deiner Facebook-Seite und wechselst in die Rubrik „Apps“. Dort wird dir nun die Liste der Anwendungen angezeigt, mit denen du über Facebook angemeldet bist. Klickst du auf eine App, so hast du die Möglichkeit, die Einstellungen zu ändern oder die App komplett zu löschen. Wenn du weiter nach unten scrollst, siehst du die Option „Von anderen Personen verwendete Apps“. Dort kannst du sehen, welche Daten deine Freunde von dir sehen können. Genau diese Daten bekommen auch alle Apps angezeigt, die deine Freunde nutzen. Hebst du die Markierungen der Boxen auf, kannst du das problemlos unterbinden.

Tipps für Instagram

Privates Konto

Aktivierst du „Privates Konto“ in den Einstellungen deines Kontos, können nur noch von dir bestätigte Personen die Inhalte deines Profils sehen. Möchte dir jemand folgen, so erhältst du automatisch eine Anfrage, die du bestätigen oder ablehnen kannst. Wir empfehlen dir, diese Einstellung vorzunehmen, um deine Bilder und Videos vor fremden Augen zu schützen!

Auf Bildern markieren

Zudem kannst du verhindern, dass Bilder auf denen du markiert wirst, automatisch in deinem Profil angezeigt werden. Gehe dazu auf dein Profil und wähle die Seite „Fotos von dir“. Über die drei Punkte kannst du „manuell hinzufügen“ auswählen. Weitere Informationen zu Instagram kannst du im Instagram-Leitfaden unter mecodia.de/tipps nachlesen.

Tipps für Snapchat

Privatsphäre schützen

In den Einstellungen kannst du deine Handynummer verschleiern, so dass dich andere Nutzer darüber nicht finden können. Deine Freunde können dich aber weiterhin über deinen Nutzernamen oder Snapcode adden.
Damit deine Geschichten privat bleiben, kannst du die Sichtbarkeit in den Einstellungen einschränken. So können nur noch deine ausgewählten Freunde die Inhalte deiner Snapchat-Geschichten sehen.
Pass immer darauf auf, welche Fotos du an andere verschickst. Snaps haben zwar ein Ablaufdatum, dennoch können andere Nutzer jederzeit Screenshots von deinen Bildern erstellen!
Ausführlichere Informationen zum Thema findest du auf der Seite: handysektor.de/snapchat

Tipps für Twitter

App-Tracking deaktivieren

Twitter betreibt App-Tracking, um herauszufinden, welche anderen Apps sich auf deinem Smartphone befinden. Dadurch möchte Twitter in deinem Feed Tweets anzeigen, die deinen Präferenzen entsprechen. Diese Funktion kannst du in der Twitter-App ganz einfach ausschalten.

Android: Gehe in die Einstellungen und wähle den Account aus, für den du die Einstellungen vornehmen willst. Unter Sonstiges kannst du den Haken bei „Twitter anhand meiner Apps anpassen“ entfernen.

iOS: Wähle den Account aus, für den du die Einstellungen vornehmen willst, entferne unter Datenschutz den Haken bei „Twitter anhand meiner Apps anpassen“.

Zukünftige Entwicklungen

Smarte Sache

Smarte Uhren, Autos und Häuser – einiges hat man darüber schon gehört, manches benutzt du vielleicht sogar schon. Generell geht es um Objekte, die durch die Zuführung von Informationstechnologien über Fähigkeiten verfügen, die über ihre übliche Bestimmung hinausgehen. So kannst du beispielsweise die Heizung deines Hauses mit deinem Smartphone von unterwegs steuern oder dein Kühlschrank scannt die in ihm enthaltenen Lebensmittel und kann fehlende Produkte einfach nachbestellen. Auch smarte Autos gewinnen immer mehr an Zustimmung. Diese können unter anderem mit dem Smartphone geöffnet werden, haben Einparkhilfen sowie eine Notbrems- und Fernlichtassistenz. Gegenüber dem Komfort hat das Konzept aber ebenfalls eine Schattenseite: Es ist Angreifern schon gelungen, die Software der Autos zu hacken. Auch kann das Fahrverhalten der Autofahrer analysiert und bewertet werden. So könnte das eigene Auto zum Zeugen für eine schlechte Fahrweise mutieren und Anonymität wäre nicht mehr gewährleistet.

Smarte Objekte erfordern eine weitreichende Vernetzung und erzeugen riesige Datenmengen, die auch als Big Data bezeichnet werden. Hier verbirgt sich die Gefahr, dass deine persönlichen Daten in die falschen Hände geraten, vor allem weil einige deiner Geräte miteinander vernetzt sind. Achte darauf, stets vorsichtig zu sein, auch wenn smarte Objekte das Leben um einiges erleichtern und die Gefahren eigentlich nicht erkennbar sind.

Videoüberwachung

Nicht nur an Gebäuden sind Überwachungskameras zu finden. Mittlerweile fliegen sie an Drohnen durch die Luft oder sind in Autos eingebaut. Eine Drohne eignet sich besonders gut, um Fotos und Videos von Landschaften zu machen. Dabei sollte aber darauf geachtet werden, dass private Grundstücke und Personen auf den Videos nicht zu erkennen sind. Videos von Autokameras können als Beweismittel für Unfälle dienen, dennoch ist die durchgehende Nutzung der Kamera verboten. Außerdem dürfen selbst aufgenommene Videos nicht veröffentlicht werden.

Fazit

Das Thema Datenschutz ist und bleibt sehr wichtig. Durch die stetig wachsende Digitalisierung, kann dem Thema nicht genug Aufmerksamkeit gewidmet werden. Schließlich können Hacker ganze Identitäten stehlen und dadurch gravierende Schäden verursachen. Man kann es nicht oft genug wiederholen: Sei achtsam und überlege genau, welche Daten du wo hinterlässt!

Noch Fragen?

Weitere Leitfäden von mecodia mit praktischen Tipps zu allem rund um die Neuen Medien gibt‘s unter **http://mecodia.de/tipps**

10 Tipps für ein perfektes Selfie

Fotos machen kann jeder. Schöne Fotos machen nur die Profis. Beleuchtung, Hintergrund, Blickwinkel, Bildkomposition und die Nachbearbeitung spielend dabei eine große Rolle. Damit du mit deinem Selfie beeindruckst, haben wir dir hier noch ein paar Tipps vom Jugendportal **www.handysektor.de**.

mecodia GmbH
Neckartailfinger Straße 1
72631 Aichtal

07127 799 042

mail@mecodia.de