Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Soziale Netzwerke sicher nutzen

10 Tipps und Hinweise zum richtigen Umgang und den Gefahren

Sichere Nutzung sozialer Netzwerke

Über soziale Netzwerke können Sie mit Freundinnen und Freunden, Familie, Kolleginnen und Kollegen oder Bekannten kommunizieren, Ihre Fotos und Videos teilen und vieles mehr. Die Gefahren sozialer Netzwerke sollten Sie aber nicht unterschätzen. So drohen beispielsweise Identitätsdiebstahl oder das Ausspähen privater Informationen. Wir haben für Sie zehn wichtige und leicht umsetzbare Sicherheitstipps für das soziale Leben im Internet zusammengestellt.
Weitere Hinweise und Hilfestellungen bieten wir auf unserer Website bsi.bund.de/soziale-netzwerke an.

Hier haben wir die wichtigsten Tipps zum sicheren Umgang mit sozialen Netzwerken für Sie zusammengefasst. Ausführliche Informationen finden Sie auf den nachfolgenden Seiten dieser Broschüre.

① Verwenden Sie stets nur sichere Passwörter.
② Nutzen Sie eine Zwei-Faktor-Authentisierung.
③ Seien Sie vorsichtig bei der zusätzlichen Installation von Apps, Add-ons oder Plug-ins in sozialen Netzwerken.
④ Sorgen Sie für einen guten Basisschutz Ihrer mobilen Geräte, wenn Sie soziale Netzwerke über diese nutzen.
⑤ Seien Sie wählerisch bei Kontaktanfragen und nehmen Sie grundsätzlich nur Personen in Ihre Freundesliste auf, die Sie kennen.
⑥ Klicken Sie nicht unüberlegt auf Links oder Buttons in Ihrem sozialen Netzwerk, auch wenn diese von Freunden stammen.
⑦ Schützen Sie Ihre Privatsphäre. Machen Sie sich mit den Sicherheitseinstellungen vertraut. Bedenken Sie auch die enge Verzahnung der Betreiber sozialer Netzwerke mit anderen Internetdiensten. Geben Sie nicht zu viel von sich preis. Je weniger personenbezogene Daten von Ihnen veröffentlicht sind, desto weniger fällt auf Sie zurück.

(8) Melden Sie Cyberstalker und Hasskommentare dem Betreiber des sozialen Netzwerkes, der Polizei und den Betroffenen.
(9) Löschen Sie Ihren Account, wenn Sie ihn nicht mehr benötigen.
(10) Machen Sie sich mit den AGB und den Bestimmungen zum Datenschutz gründlich vertraut – und zwar bevor Sie ein Profil anlegen. Überlegen Sie zudem vor Veröffentlichung, ob Sie die Rechte an Ihren Bildern, Videos oder Texten teilen möchten. Achten Sie auch darauf, dass Sie nur Inhalte veröffentlichen, über deren Rechte Sie verfügen.

1

Sichere Passwörter sind ein wichtiger Schutz

Verwenden Sie unterschiedliche und komplexe Passwörter für die Anmeldung bei sozialen Netzwerken. Für ein sicheres Passwort gilt:

- Sie müssen sich ein Passwort gut merken können.
- Je länger das Passwort ist, desto besser.
- Das Passwort sollte mindestens acht Zeichen lang sein.
- Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.
- Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster kommen ebenfalls als sicheres Passwort nicht in Frage.

- Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert.

Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern. Dabei handelt es sich um eine Anwendung, die sichere Passwörter für Ihre Online- und Benutzerkonten verwaltet und diese auch generieren kann. Sie benötigen für die Nutzung ein sogenanntes Masterpasswort. Damit können Sie auf den Passwortmanager zugreifen. Es sollte daher ein sicheres Passwort sein, das Sie sich merken können. Unter keinen Umständen sollten Sie Ihr Passwort an Dritte weitergeben.
Weitere Informationen zu sicheren Passwörtern:
bsi.bund.de/account-schutz

2

Nutzen Sie eine Zwei-Faktor-Authentisierung

Nutzen Sie für den Zugriff auf Ihre Benutzerkonten bei sozialen Netzwerken eine Zwei-Faktor-Authentisierung. Das bedeutet: Als erster Faktor kommt ein sicheres Passwort zum Einsatz. Als zweiter Faktor kommt für die zusätzliche Authentisierung z. B. eine Hardware-Komponente zum Einsatz, die als Schlüssel fungiert. Das können das Smartphone, eine Chipkarte oder ein spezieller USB-Stick sein. Auch eine vom Anbieter versendete SMS mit einem Einmalcode kann genutzt werden. Damit besteht ein wesentlich besserer Schutz für Ihr Nutzerkonto. Für einen unautorisierten Zugang müssten Dritte über beide Faktoren verfügen, also sowohl über das Wissen des Passworts als auch den Besitz des Gerätes.

3

Seien Sie vorsichtig bei der Installation von Apps, Add-ons oder Plug-ins

Viele soziale Netzwerke erlauben es, Anwendungen von Drittanbietern zu installieren, beispielsweise Spiele. Je nach Netzwerk ist dann von Apps, Add-ons oder Plug-ins die Rede. Gemeinsam haben sie alle, dass Sie Ihr Profil so um zusätzliche Funktionen erweitern oder an Ihre persönlichen Bedürfnisse anpassen können.

Doch auch Onlinekriminelle erstellen oder kapern solche Anwendungen und nutzen sie, um Zugriff auf Ihr Profil zu erhalten. Prüfen Sie deshalb Anbieter und Quellen auf ihre Vertrauenswürdigkeit.

Tauschen Sie sich beispielsweise vor der Installation mit Freundinnen und Freunden darüber aus oder informieren Sie sich im Internet, welche Apps, Add-ons oder Plug-ins empfehlenswert sind oder nicht.

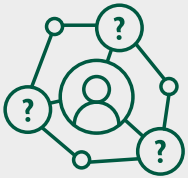
4

Seien Sie bei mobiler Nutzung besonders vorsichtig

Soziale Netzwerke werden oft über mobile Geräte wie Smartphones oder Tablets genutzt. Sorgen Sie daher für einen guten Basisschutz Ihrer mobilen Geräte. Für den Zugang stellen die Betreiber oder Drittanbieter Apps zur Verfügung. Diese greifen häufig auf sensible Daten zu, die auf dem Mobilgerät vorhanden sind. Dazu zählen unter anderem das Adressbuch, Fotos, Videos oder Standortangaben. Womöglich wollen Sie diese Daten nicht preisgeben. Außerdem bleiben Sie in der Regel nach der ersten Anmeldung stets automatisch in dem sozialen Netzwerk angemeldet. Bei Verlust Ihres Gerätes kann dies ausgenutzt werden, indem sich jemand anderes als Sie ausgibt. Schützen Sie daher den Zugriff auf Ihr mobiles Gerät

mit einem Sperrcode, einer PIN- oder Passwort-Eingabe, dem Fingerabdruck oder der Gesichtserkennung. Weitere Informationen zum Basisschutz mobiler Geräte: bsi.bund.de/smartphone-sicherheit

5



Seien Sie wählerisch bei Kontaktanfragen

Identitätsdiebstahl gehört zu den Risiken des digitalen Zeitalters. Kriminelle übernehmen die Identität einer anderen Person, um sich als diese auszugeben, in ihrem Namen zu kommunizieren oder diese möglicherweise für Straftaten oder illegale Onlinegeschäfte zu missbrauchen. Dafür reicht es oftmals schon aus, das Profilbild sowie den Namen einer Person zu kopieren und ein neues Benutzerkonto zu erstellen. Unbekannte Dritte können sich also auch als Personen ausgeben, die Sie vermeintlich kennen. Wenn Sie zweifelhafte Kontaktanfragen von Bekannten erhalten, erkundigen Sie sich außerhalb sozialer Netzwerke nach der Echtheit dieser Nachrichten.

Nehmen Sie nur Personen in die Freundes- oder Kontaktliste auf, bei denen Sie sicher sind, dass es sich um authentische Nutzerprofile handelt. Das Alter eines Profils und die bisherigen Veröffentlichungen können hierfür ein Anhaltspunkt sein. Personen und Organisationen, die in der Öffentlichkeit stehen, sind oft erkennbar durch die Plattformen verifiziert.

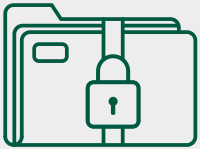
6

Klicken Sie nicht unüberlegt auf Links oder Buttons

Onlinekriminelle nutzen soziale Netzwerke, um Nutzerinnen und Nutzer mit Beiträgen oder Links in Chats auf präparierte Webseiten zu locken, über die sie Zugangsdaten abgreifen oder Geräte mit Schadsoftware infizieren können.
Ein unbedarftes Klicken kann dazu führen, dass sich Schadsoftware auf Ihrem Gerät installiert. Diese kann beispielsweise von Ihnen unbemerkt die Kamera Ihres Gerätes einschalten, Ihre Gespräche durch das Mikrofon aufzeichnen oder auch Ihren Standort abfragen. Auch Ihr Adressbuch, Ihre Fotos oder Ihre Videos können unbemerkt in fremde Hände gelangen. Seien Sie daher bei Nachrichten von Fremden ganz besonders misstrauisch und klicken Sie keine Links an.

Auch die Nutzerkonten von bekannten Kontakten können missbräuchlich genutzt werden, wenn Dritte zum Beispiel durch Identitätsdiebstahl Zugriff zu diesen erhalten haben.

7



Schützen Sie Ihre Privatsphäre und geben Sie nicht zu viel von sich preis

Jedes soziale Netzwerk bietet zahlreiche Einstellungen zum Schutz Ihrer Privatsphäre. Machen Sie sich mit den möglichen Einstellungen vertraut und nutzen Sie diese zum Schutz Ihrer Privatsphäre, insbesondere wenn nur Ihre Freundinnen und Freunde Ihr Profil und Ihre Beiträge sehen sollen. Sie können dort auch einstellen, dass Suchmaschinen Ihr Profil ignorieren. Oder Sie legen fest, welche der Informationen in Ihrem Konto öffentlich einsehbar sind. Wenn Sie beispielsweise Ihre E-Mail-Adresse nicht in Ihrem Profil anzeigen lassen, erschwert das die Suche nach Ihnen in Suchmaschinen.
Bedenken Sie auch die enge Verzahnung der Betreiber sozialer Netzwerke mit anderen Internetdiensten. Es kann dadurch ein sehr umfangreiches Profil über Sie erstellt werden. Führen Sie ab und zu eine Online-Suche nach Ihrem Namen oder

dem von Familienmitgliedern durch, um zu erfahren, welche Informationen über Sie oder gegebenenfalls Ihre Kinder im Netz auffindbar sind.
Prüfen Sie zudem in regelmäßigen Abständen die Sicherheitseinstellungen Ihrer Benutzerkonten in sozialen Netzwerken. Achten Sie dabei insbesondere auf die Verknüpfung zu anderen Konten. Anbieter sozialer Netzwerke könnten diese Einstellungen von sich aus ändern.

Sehr persönliche Informationen gehören nicht ins Netz. Denn einmal im Internet veröffentlichte Informationen können schnell ein Eigenleben entwickeln und lassen sich nur sehr schwer oder nie wieder löschen. Prüfen Sie kritisch, welche persönlichen Informationen Sie daher veröffentlichen wollen und schränken Sie den Empfängerkreis entsprechend ein.

Je weniger personenbezogene Daten von Ihnen veröffentlicht sind, desto weniger fällt auf Sie zurück. Dies gilt auch für vertrauliche Informationen über Ihren Arbeitgeber und Ihre Arbeit. Informationen über Tätigkeiten und Personen am Arbeitsplatz sollten – wenn überhaupt – nur nach Rücksprache mit dem Arbeitgeber veröffentlicht werden.

8

Melden Sie Cyberstalker und Hasskommentare

Melden Sie dem Betreiber des sozialen Netzwerkes Personen, die Sie oder andere Nutzerinnen und Nutzer belästigen oder beleidigen. Die Betreiber können dem Missbrauch nachgehen und unseriöse Profile löschen. Ebenso können Sie Posts mit bedenklichen Inhalten melden. Lassen Sie sich bei offensichtlichen oder vermuteten Straftaten von der Polizei beraten, informieren Sie Betroffene und erstatten Sie gegebenenfalls Anzeige.

Soziale Netzwerke haben zudem Verhaltensregeln (Netiquette), die zu beachten sind.

9

Löschen Sie Ihren Account, wenn Sie ihn nicht mehr benötigen

Sollten Sie einen Account stilllegen wollen, sichern Sie bei Bedarf Ihre Daten außerhalb des Netzwerkes und löschen diese dann im Account. Befolgen Sie im Weiteren genau das Prozedere des Anbieters zum Löschen des Nutzerkontos. Dazu gehört in manchen Fällen auch, dass Sie sich innerhalb eines bestimmten Zeitraums nicht wieder einloggen.

10

Lesen Sie die Datenschutzbestimmungen und die Allgemeinen Geschäftsbedingungen (AGB)

Soziale Netzwerke werden von gewinnorientierten Unternehmen betrieben, die sich zumeist durch Werbung finanzieren. Die AGB geben Aufschluss darüber, wie der Anbieter mit Ihren persönlichen Daten umgeht und wie diese an die Werbewirtschaft weitergegeben werden. Machen Sie sich mit den AGB und den Bestimmungen zum Datenschutz gründlich vertraut – und zwar bevor Sie ein Profil anlegen.

Einige soziale Netzwerke räumen sich an Ihren Veröffentlichungen Nutzungsrechte ein. Dadurch übertragen Sie zum Beispiel die Nutzungsrechte an Ihren Fotos und Videos an den Betreiber des sozialen Netzwerkes. Außerdem ist es durchaus üblich,

dass gewährte Nutzungsrechte auch dann bestehen bleiben, wenn Sie das Netzwerk verlassen und Ihr Profil löschen. Überlegen Sie vor Veröffentlichung, ob Sie die Rechte an Ihren Bildern, Videos und Texten teilen möchten. Achten Sie auch darauf, dass Sie Rechte Dritter nicht durch das Posten von Bildern, Texten oder Videos verletzen.

Weitere Informationen

- Ein wichtiger Hinweis für Eltern: Sprechen Sie mit Ihren Kindern über die Risiken sozialer Netzwerke und informieren Sie sich über die Plattformen, die Ihre Kinder zum Austausch mit Freundinnen und Freunden nutzen.
  bsi.bund.de/kinderschutz
- Das Netz vergisst nichts: Informationen, die Sie über soziale Netzwerke verbreiten, bleiben oft für immer im Netz. Dritte können sie nutzen, um Informationen über Sie zusammenzutragen.
  bsi.bund.de/socialengineering
- IT-Sicherheit ist Datensicherheit: Der Schutz Ihrer Geräte – PC, Smartphone & Co – vor Schadsoftware ist ein wichtiger Bestandteil der Datensicherheit.
  bsi.bund.de/internetsicherheit

Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Als unabhängige und neutrale Anlaufstelle bietet es Ihnen für einen sicheren digitalen Alltag umfangreiche Informationen.

IMPRESSUM

Herausgeber:
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

Bezugsquelle:
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: service-center@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi_bund
Service-Center: +49 (0) 800 274 1000

Stand: März 2021
Bilder: © GettyImages
Layout und Gestaltung: Faktor 3 AG

Artikelnummer: BSI-IFB 21/252