Bundesamt
für Sicherheit in der
Informationstechnik

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

Soziale Netzwerke

Basisschutz leicht gemacht

Tipps zur sicheren Nutzung von
Facebook, Xing & Co

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

Sichere Nutzung sozialer Netzwerke

Über soziale Netzwerke können Sie mit Familie, Freunden, Kollegen und Bekannten kommunizieren, Ihre Fotos und Videos teilen und vieles mehr. Die Gefahren sozialer Netzwerke – beispielsweise Identitätsdiebstahl oder das Ausspähen privater Informationen – sollten Sie aber nicht unterschätzen. 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 Webseite *www.bsi-fuer-buerger/SozialeNetzwerke* an.

Verwenden Sie unterschiedliche E-Mail-Adressen und sichere Passwörter

Nutzen Sie nach Möglichkeit unterschiedliche E-Mail-Adressen für die Accounts der verschiedenen sozialen Netzwerke. So können Sie zumindest erschweren, dass die Informationen, die Sie auf den jeweiligen Seiten über sich preisgeben, zu einem umfassenden Profil über Sie zusammengestellt werden. Wenn Sie hierfür Freemail-Accounts nutzen, denken Sie daran, diese gelegentlich aufzurufen, damit sie aktiviert bleiben. Achten Sie bereits bei der Wahl eines Anbieters darauf, dass dieser die E-Mail-Adresse nicht verfallen lassen und an einen neuen Nutzer wieder vergeben kann. Ansonsten besteht das Risiko, dass ein anderer Nutzer diese E-Mail-Adresse übernimmt und damit Zugriff auf das zugeordnete soziale Netzwerk erhält.

Verwenden Sie zudem unterschiedliche und sichere Passwörter für die einzelnen Dienste wie Facebook oder Twitter. Für das Passwort gilt: Je länger, desto besser. Es sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Ein Passwortmanager, wie z. B. keepass, kann die Handhabung unterschiedlicher Passwörter erleichtern. Unter keinen Umständen sollten Sie Ihr Passwort an Dritte weitergeben.

Nutzen Sie eine Zwei-Faktor-Authentisierung

Nutzen Sie für den Zugriff auf Ihre Social Media Accounts eine Zwei-Faktor-Authentisierung. Das bedeutet: Als erster Faktor kommt ein starkes Passwort (Kategorie Wissen) zum Einsatz. Als zweiter Faktor kommt für die zusätzliche Authentisierung z. B. ein Sicherheitstoken, also eine Hardware-Komponente wie ein Schlüssel, eine Chipkarte oder ein spezieller USB-Stick, zum Einsatz (Kategorie Besitz). Auch eine vom Anbieter versendete SMS 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.

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. Damit können Sie Ihr Profil um nützliche Funktionen erweitern oder an Ihre persönlichen Bedürfnisse anpassen.

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

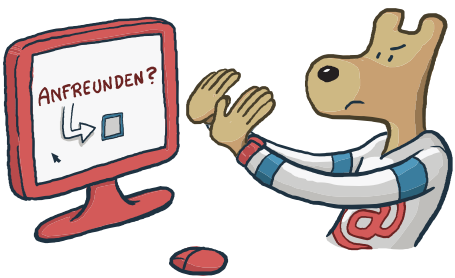
Tauschen Sie sich beispielsweise vor der Installation mit Freunden darüber aus oder informieren Sie sich im Internet, welche Apps, Add-Ons oder Plug-Ins empfehlenswert sind oder nicht.

Seien Sie bei mobiler Nutzung besonders vorsichtig

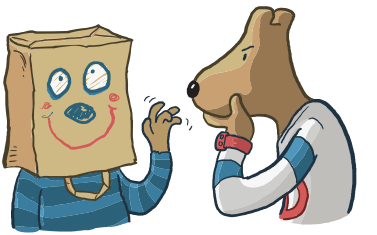
Soziale Netzwerke werden oft über mobile Geräte wie Smartphones oder Tablets genutzt. Dafür stellen die Betreiber oder Drittanbieter Apps zur Verfügung. Diese nutzen häufig auf dem Mobilgerät vorhandene sensible Daten, die Sie womöglich nicht preisgeben wollen. Dazu zählen unter anderem das Adressbuch, Fotos, Videos oder Standortangaben. Außerdem sind Sie in der Regel anschließend stets automatisch in dem sozialen Netzwerk angemeldet. Bei Verlust Ihres Gerätes kann dies ausgenutzt werden, indem sich der Finder oder Dieb als Sie ausgibt. Daher sollten Sie möglichst keine Passwörter auf Ihren mobilen Geräten speichern und sich anstatt über die App direkt über die Webseite des sozialen Netzwerkes an- und abmelden.

Seien Sie wählerisch bei Kontaktanfragen

Identitätsdiebstahl gehört zu den Risiken des digitalen Zeitalters. Wenn Sie zweifelhafte Anfragen von Bekannten erhalten, erkundigen Sie sich außerhalb sozialer Netzwerke nach der Vertrauenswürdigkeit dieser Nachrichten. Nehmen Sie grundsätzlich nur Personen in Ihre Freundes- oder Kontaktliste auf, die Sie aus der realen Welt kennen. Unbekannte könnten böswillige Absichten haben. „Falsche Freunde“ können mithilfe übernommener oder gefälschter Accounts eine fremde Identität annehmen und diese möglicherweise für Straftaten oder illegale Onlinegeschäfte missbrauchen.



Klicken Sie nicht unüberlegt auf Links oder Buttons



Online-Kriminelle nutzen soziale Netzwerke, um Nutzer mit Postings 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. Die Schadsoftware 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.

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

Jedes soziale Netzwerk bietet zahlreiche Einstellungen zum Schutz Ihrer Privatsphäre. Nutzen Sie diese, insbesondere wenn nur Ihre Freunde Ihr Profil und Ihre Postings sehen sollen. Sie können dort auch einstellen, dass Suchmaschinen Ihr Profil ignorieren. Machen Sie sich mit den möglichen Einstellungen vertraut und nutzen Sie diese zum Schutz Ihrer Privatsphäre.

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 Ihre Kinder im Netz auffindbar sind.

Prüfen Sie zudem in regelmäßigen Abständen die Sicherheitseinstellungen Ihrer Social Media Accounts. Achten Sie dabei insbesondere auf die Verknüpfung zu anderen Konten. Anbieter sozialer Netzwerke könnten diese Einstellungen von sich aus ändern.

Sehr persönliche Informationen gehören einfach nicht ins Netz. Einmal im Internet veröffentlichte Informationen entwickeln schnell ein Eigenleben und lassen sich nur sehr schwer oder nie wieder löschen. Prüfen Sie kritisch, welche persönlichen Informationen Sie 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.

Melden Sie Cyberstalker und Hasskommentare

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

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.

Informieren Sie sich über Ihre Rechte und Pflichten

Soziale Netzwerke werden von gewinnorientierten Unternehmen betrieben, die sich zumeist durch Werbung finanzieren. Die Allgemeinen Geschäftsbedingungen (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 und Texten teilen möchten. Achten Sie auch darauf, dass Sie Rechte Dritter nicht durch das Posten von Bildern, Texten oder Videos verletzen.

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

Fazit

» Das Netz vergisst nichts: Informationen, die Sie über soziale Netzwerke verbreiten, bleiben oft für immer im Netz.

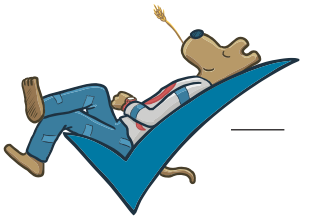
» IT-Sicherheit ist Datensicherheit: Der Schutz Ihres Smartphones, PC und Co vor Schadsoftware ist ein wichtiger Bestandteil der Datensicherheit.

» Schützen Sie Ihre Kinder: Sprechen Sie mit ihnen über deren Aktivitäten und Freunde. Klären Sie sie über die Gefahren sozialer Netzwerke auf und informieren Sie sich über die sozialen Netzwerke, in denen Ihre Kinder Mitglied sind.

Weitere Informationen zu den Themen „Soziale Netzwerke“ und „Sicheres Surfen“ finden Sie unter

www.bsi-fuer-buerger.de/SozialeNetzwerke
www.bsi-fuer-buerger.de/SicherSurfen

Soziale Netzwerke



Basisschutz leicht gemacht

- Nutzen Sie nach Möglichkeit verschiedene E-Mail-Adressen für verschiedene soziale Netzwerke. Verwenden Sie zudem unterschiedliche und sichere Passwörter.
- Nutzen Sie eine Zwei-Faktor-Authentisierung.
- Seien Sie vorsichtig bei der Installation von Apps, Add-Ons oder Plug-Ins.
- Seien Sie bei mobiler Nutzung besonders vorsichtig und speichern Sie möglichst keine Passwörter auf Ihren mobilen Geräten. Melden Sie sich lieber über die Webseite des sozialen Netzwerkes an und ab.
- Seien Sie wählerisch bei Kontaktanfragen und nehmen Sie grundsätzlich nur Personen in Ihre Freundesliste auf, die Sie aus der realen Welt kennen.

- Klicken Sie nicht unüberlegt auf Links oder Buttons in Ihrem sozialen Netzwerk, auch wenn diese von Freunden stammen.
- 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.
- Melden Sie Cyberstalker und Hasskommentare dem Betreiber des sozialen Netzwerkes, der Polizei und den Betroffenen.
- Löschen Sie Ihren Account, wenn Sie ihn nicht mehr benötigen.
- 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.

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. Mit dem Informationsangebot „BSI für Bürger“ bietet es eine unabhängige und neutrale Anlaufstelle zu Fragen der Informations- und Cyber-Sicherheit.

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: mail@bsi-fuer-buerger.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger
Service-Center: +49 (0) 800 274 1000

Stand
Juli 2019

Illustrationen
Leo Leowald · www.leowald.de

Artikelnummer
BSI-IFB 19/252