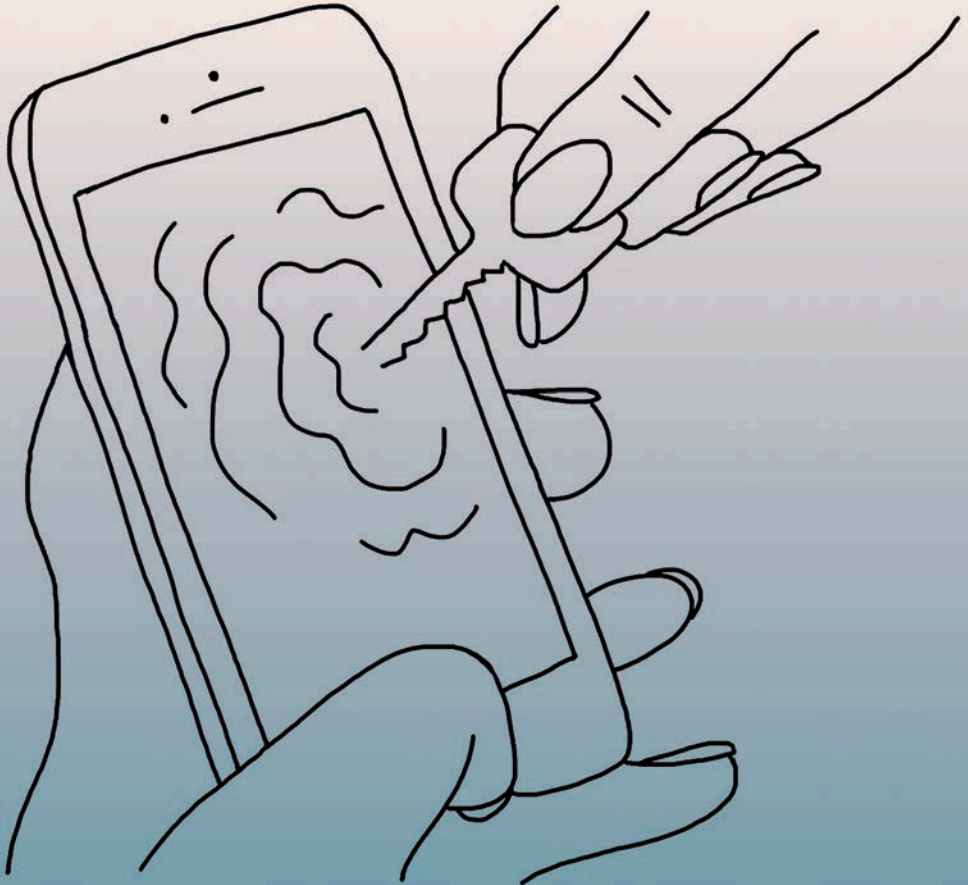


Tools zur Verschlüsselung



Who's watching you?



Viele Daten, die du online verschickst, können mitgelesen werden - von Dienst-Anbietern, Hackern oder Geheimdiensten.

Auch die digitalen Spuren, die du bei der Internetnutzung automatisch hinterlässt, sind nachvollziehbar.

Zudem kann es passieren, dass du dein Smartphone oder dein Laptop verlierst oder es dir geklaut wird. Sollen die neuen Besitzer dann alles sehen dürfen?

Um dich und deine Geräte abzusichern, haben wir ein paar Tipps und hilfreiche Tools zusammengestellt.

Links:

Eine Linksammlung mit allen Tools, die in diesem Flyer vorgestellt werden, findest du unter

www.studioimnetz.de/projekte/watchingyou

Die Linksammlung ist auch über diesen QR-Code erreichbar:



Für dein Smartphone:

Datenschutz-Einstellungen:

Welche Einstellungsmöglichkeiten solltest du anpassen? Die Seite mobilsicher.de liefert umfangreiche Checklisten zur Sicherung mobiler Geräte.

App-Berechtigungen überprüfen:

Einige Apps räumen sich unnötig viele Zugriffsrechte ein. Um einen Überblick darüber zu erhalten, ist z.B. die kostenlose App „My Permissions“ hilfreich. Sie ist für Android und iOS sowie als Browser-Erweiterung unter mypermissions.de erhältlich.

(Ähnlich funktioniert die kostenlose App Clueful, die jedoch nur für Android angeboten wird.)

Zugriffssperre: Die grundlegende Sicherung deines Smartphones ist eine Zugriffssperre, damit nicht alle, die das Gerät in die Hand nehmen, die Inhalte öffnen können.

Eine Sperre mit PIN oder Passwort ist der beste Schutz, die Muster-sperre ist weniger sicher.

Ein Gesichts- oder Fingerabdruck-Scan ist nicht empfehlenswert, da du damit wichtige biometrische Daten weitergibst

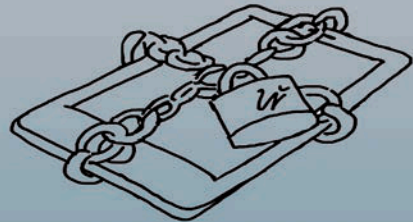
Verschlüsselung von Smartphones: Android-Phones lassen sich über die Systemeinstellungen verschlüsseln, eine Anleitung dazu findet sich z.B. bei androidpit.de.

Auch für iOS-Geräte ist eine Hardware-Verschlüsselung möglich, die bei apple.com im Support-Bereich erklärt wird.

Smartphone-Sicherheit: Zahlreiche Apps werben damit, die Sicherheit mobiler Geräte zu erhöhen. Eine unabhängige Quelle mit aktuellen Informationen zur Online-Sicherheit ist das Bundesamt für Sicherheit in der Informationstechnik: bsi-fuer-buerger.de

Messenger: Datenschutzkonforme Messenger mit Verschlüsselung der Nachrichten sind z.B. die freien Apps **Signal** und **Wire** sowie die proprietären Apps **Threema** und **Telegram**.

Einen guten Überblick liefert die „Secure-Messaging-Scorecard“ von eff.org.



Für deine E-Mail:

GnuPG: Ein Open-Source-Programm zur Verschlüsselung von E-Mails, das auf dem standardisierten Datenformat Open PGP basiert. Die verschlüsselten Daten können mit einem Schlüssel geöffnet werden, der vom Sender an den Empfänger übergeben wird. Zudem sind die User über eine digitale Signatur authentifiziert.

GPG4Win: Kostenlose GnuPG-Implementierung für Windows mit öffentlichem Quellcode. Das Programm unterstützt bei der Einrichtung eines privaten Schlüssels und bietet Tools zum Ver- und Entschlüsseln von Daten an.

Enigmail: Ein Plugin für Mozillas E-Mail-Client Thunderbird. Mit Enigmail lassen sich verschlüsselte E-Mails versenden. Der Schlüssel lässt sich in Enigmail direkt oder über Drittsoftware wie GPG4Win erzeugen.

K-9 Mail: Kostenlose und quelloffene App für Android, die die Einrichtung mehrerer E-Mail-Konten ermöglicht. Eine Mail-Verschlüsselung ist mithilfe von weiterer Software wie OpenKeychain möglich.

ProtonMail: Ein quelloffener und kostenfreier E-Mail-Dienst der Forschungseinrichtung CERN, der einen verschlüsselten E-Mail-Verkehr ermöglicht. ProtonMail ist als App für Android und iOS sowie als Web-Anwendung benutzbar.

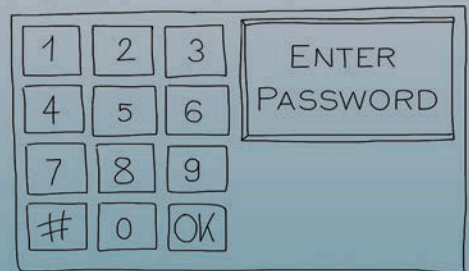
Für deinen Browser:

HTTPS Everywhere wandelt die unverschlüsselte Datenübertragung auf Webseiten in eine verschlüsselte Übertragung um. Die freie Software ist für Mozilla Firefox und Google Chrome kostenlos erhältlich.

Privacy Badger blockiert Tracking-Versuche und weitere Angriffe auf die Privatsphäre. Die Erweiterung ist frei lizenziert und für Firefox-, Chrome- und Opera-Browser erhältlich.

uBlock Origin ist ein quelloffenes, kostenfreies Browser-Plug-In, das Tracking-Anfragen, Werbung uvm. blockiert.

noScript blockiert JavaScripts, Java-Applets, Flash- und Silverlight-Animationen. Das Tool steht unter freier GNU-Lizenz und ist gratis erhältlich, jedoch nur für Mozilla Firefox. (Ein ähnliches Tool für Chrome ist ScriptSafe.)



Für deine Festplatte:

VeraCrypt: Ermöglicht die Verschlüsselung von Ordnern, Festplatten, Wechseldatenträgern oder auch des gesamten Systems. VeraCrypt ist kostenlos und als Open-Source-Programm verfügbar.

TrueCrypt: Die „Mutter“ der Verschlüsselungstools für diverse Plattformen. Obwohl TrueCrypt nicht mehr weiterentwickelt wird, ist es noch der De-facto-Standard.

BitLocker: Ein Microsoft-Programm zur Festplattenverschlüsselung. Es schützt mit Hilfe von TPM (Trusted Platform Module) das Windows-Betriebssystem und alle Benutzerdateien. BitLocker ist proprietär und nur für Windows verfügbar.

Für deinen Cloud-Speicher:

BoxCryptor: Eine Verschlüsselungssoftware für Dateien, die in Cloud-Speicherdiensten wie Dropbox, Google Drive uvm. abgelegt werden. Die proprietäre Software ist für Privatanwender kostenlos.

Whisply: Neues Online-Tool von BoxCryptor, das ebenfalls Dateien vor dem Cloud-Upload verschlüsselt. Das Tool ist mit Dropbox, Google Drive und Microsoft One Drive kompatibel und benötigt keine zusätzliche Anmeldung.

Weitere Links:



Jugendportal der unabhängigen
Datenschutzbehörden:

www.youngdata.de

Bundesbeauftragte für Daten-
schutz und Informationsfreiheit:

www.bfdi.bund.de

Informationsangebot deutscher
Datenschutzinstanzen:

www.datenschutz.de

TOR-Projekt (Programme und
Apps für Online-Anonymität):

www.torproject.org

Alle Links und Informationen sind
auch online abrufbar:

[www.studioimnetz.de/projekte/
watchingyou](http://www.studioimnetz.de/projekte/watchingyou)



Eine Zusammenstellung von
SIN – Studio im Netz e.V.
Heiglhofstr. 1, 81377 München

Stand: November 2016

Mit freundlicher Unterstützung durch:
Bundeszentrale für politische Bildung
www.bpb.de