

Sicherheit im Internet



Dabei sein!
Online im Alter.

Wie nutze ich das Internet sicher?



Sicheres Gerät

- Apps aus sicheren Quellen laden
- Betriebssystem und Apps aktualisieren
- Virenschutz installieren



Sichere Internetverbindung

- WLAN mit einem sicheren Passwort schützen
- WLAN ausschalten, wenn nicht in Benutzung
- Im öffentlichen Hotspot keine persönlichen Daten eingeben



Sichere Internetseiten

- Auf SSL Verschlüsselung achten
- Datenschutzerklärung und Impressum müssen vorhanden sein



Drei Tipps für noch mehr Sicherheit
 1. Verwenden Sie sichere Passwörter
 2. Gehen Sie sparsam mit persönlichen Daten im Internet um
 3. Aktivieren Sie die Drittanbietersperre bei Ihrem Mobilfunkanbieter

Ein Projekt von  **Deutschland sicher im Netz**

Gefördert vom  **Bundesministerium für Familie, Senioren, Frauen und Jugend**

Sicheres Herunterladen (Downloaden von Apps)

Unter diesen Symbolen / Bezugsquellen können sicher Apps heruntergeladen werden, da sie strenge Sicherheitskriterien erfüllen.

		
Google Play Store (Android-Geräte)	App Store (iPhone/ iPad)	AppGallery (Huawei-Geräte)

Sichere Passwörter

Ein sicheres Passwort ist

- Einmalig: Unterschiedliche Passwörter für unterschiedliche Konten
- Kreativ: Fantasiewörter oder Dialekte, die kein Wörterbuch kennt
- Lang: Mindestens 8 Zeichen lang
- Komplex: Klein- und Großbuchstaben, Sonderzeichen und Zahlen

Passwörter merken anhand der Merksatzmethode

- Einen Satz auswählen, den Sie sich gut merken können und den 1. Buchstaben auswählen + App (Beispiel Kleinanzeigen)
- Ich trinke jeden Morgen eine Tasse Kaffee plus einem Spritzer Milch: ItjM1TK+1SMK.
- Alternative zur Merksatzmethode: Passwortmanager verwenden

Cookies

Cookies sind kleine Textdateien, die über eine Webseite im Internetbrowser eines Nutzers / einer Nutzerin gespeichert werden können.

Empfehlungen zum Umgang

- Nur technisch notwendige Cookies akzeptieren
- Cookies regelmäßig löschen
- Drittanbieter-Cookies verbieten

Phishing

Daten von Internetnutzenden werden beispielsweise über gefälschte Internetadressen, E-Mails, SMS (Smishing) oder QR-Codes (Quishing) abgefangen

Phishing-Mails erkennen

- Wer ist Absender?
- Ist eine persönliche Anrede vorhanden?
- Gibt es sprachliche Auffälligkeiten?
- Enthält die E-Mail eine Dringlichkeit?
- Wohin führt der Link?

Google-Phishingtest



Phishing-Radar



Umgang

- Folgen Sie Aufforderungen nur, wenn Sie die absendende Person oder Organisation zweifelsfrei identifizieren
- Im Zweifel: Fragen Sie telefonisch nach.

Weitere Tipps

Sichere Internetseiten verwenden

- Erkennbar an https in der Adresszeile und einem Schloss
- Datenschutzerklärung und Impressum



Smartphone sicher sperren durch

- Fingerabdruck (Touch ID)
- Gesichtserkennung (Face ID)
- PIN
- Passwort
- Iris-Scan



Fakeshops erkennen

- Nur eine Bezahlmöglichkeit? www.verbraucherzentrale.de/fakeshopfinder
- Sprachliche Mängel?
- Ungewöhnlich viel Werbung?
- Gütesiegel vorhanden?



Weitere Informationen

- Erklärvideos des Digitalen Engels und weitere Materialien
www.digitaler-engel.org/materialien
- Digitalführerschein (DiFü) www.difu.de
- Stiftung Digitale Chancen www.digitale-chancen.de
- Servicestelle „Digitalisierung und Bildung für ältere Menschen“
www.wissensdurstig.de
- Digital-Kompass: Kostenfreies Angebot zum Erlernen digitaler Kompetenzen für Menschen mit Seh-, Hör- oder Mobilitätsbeeinträchtigung www.digital-kompass.de
- Nie zu alt fürs Internet! – Broschüre zum Einstieg in das Internet
www.bmfsfj.de/publikationen
- DigitalPakt Alter: www.digitalpakt-alter.de
- Verbraucherzentrale www.verbraucherzentrale.de
- SiBa-App: www.sicher-im-netz.de/sicherheitsbarometer

Platz für Ihre Notizen: