Digitale Sicherheit für deine Geräte

1. Zugriff auf deine Geräte schützen

Sperre den Zugang zu deinen Geräten mit einem Pin-Code oder einer biometrischen Verschlüsselung wie Fingerabdruck oder Gesichtserkennung. So bleiben deine Daten und Anwendungen unangetastet.

2. Aktualisiere deine Geräte regelmässig

Softwareupdates schliessen Sicherheitslücken. Führe Updates darum zeitnah durch. Manche Betriebssysteme aktualisieren sich mit der richtigen Einstellung auch automatisch selbst über Nacht.

3. Sicher Surfen

Nutze beim Surfen im Netz deinen gesunden Menschenverstand und schau, ob die aufgerufene Webseite sicher ist. Ein **https** in der URL ist ein erster Hinweis darauf, dass sie es ist. Bei fragwürdigen Pop-ups oder Werbung ist hingegen Vorsicht geboten.

4. Nutze offizielle Stores für Downloads

Kaufe Programme und Apps nur auf vertrauenswürdigen Seiten oder bei offiziellen Anbietern. Auf welche Funktionen darf die Anwendung nach dem Download zugreifen? Bleibe achtsam und überlege, welche Zugriffe tatsächlich notwendig sind.

5. Check deine Verbindung

Sei dir bewusst, mit welchem Netz du verbunden sind. In unbekannten Netzwerken sind Online-Transaktionen nicht zu empfehlen. Verwende stattdessen lieber das eigene WLAN oder den mobilen Hotspot deines Smartphones. Ich würde öffentliche WLan (in Läden od. SBB etc.) nicht Zugriff auf mein Gerät erlauben. In Hotels ist ebenfalls WLan Vorsicht geboten!

6. Speichere deine Daten

Back-ups verhindern, dass deine Daten verloren gehen. Ob das Smartphone ins Wasser fällt oder gestohlen wird – mit einem Back-up auf einer Cloud stellst du deine Daten jederzeit ganz einfach wieder her. Achte auch hier auf einen vertrauenswürdigen Anbieter. Wir empfehlen Swisscom myCloud oder besser Proton-Services https://proton.me/de

7. Erstelle sichere Passwörter

Erstelle pro Dienstleister ein eigenes Passwort und nutze bei Bedarf einen Passwortmanager als Erinnerungshilfe. Übrigens: Passphrasen sind häufig deutlich sicherer als Passwörter. Wir empfehlen https://1password.com/de

8. Nimm dich vor Phishing in Acht

Bleibe aufmerksam und achte auf mögliche Phishing-Attacken. Phishing-Mails wirken heute oft täuschend echt, zeichnen sich aber durch Drohungen, Dringlichkeiten, Bitten oder Exklusivität aus. Prüfe den Absender genau und unterlasse es im Zweifelsfall, einen Link anzuklicken oder einen Anhang zu öffnen.

9. Nutze die 2-Faktoren-Authentisierung

Mit der 2-Faktoren-Authentisierung muss ein Login-Prozess auf einem zusätzlichen Gerät via SMS-Code oder in einer App bestätigt werden. Nutze diese doppelte Authentisierung, um deine Sicherheit zu erhöhen. Doppelt genäht hält besser.

10. Melde Angriffe

Wurdest du ein Opfer einer Phishing Attacke, Beleidigungen oder Hassrede im Netz? Melde den Angriff beim Nationalen Zentrum für Cybersicherheit NCSC und hilf mit, das Internet für uns alle sicherer zu machen.

11. Sicheren Mailserver benutzen

Google, Gmail, gmx od ähnliche Anbieter sind nicht sicher. Aber auch bluewin oder der Service bei Cyon (@grauepantherbern Adressen) sind es nicht unbedingt.

Protonmail ist m.E. der sicherste Mail Anbieter. Proton bedeutet Privatsphäre, der du vertrauen kannst. Proton bietet benutzerfreundliche verschlüsselte E-Mails, Kalender, Dateispeicher und *VPNs – alle auf der Basis eines Prinzips: deine Daten, deine Regeln. Deine Privatsphäre wird geschützt durch starke Verschlüsselung, quelloffenen Code und die Schweizer Datenschutzgesetze.

Es ist einen Versuch wert, ein einfaches Abo ist kostenlos!
Hier geht's zur Webseite: https://proton.me/de
*
VPN steht für **"Virtual Private Network"** und beschreibt die Möglichkeit eine geschützte Netzwerkverbindung unter Nutzung öffentlicher Netzwerke aufzubauen. VPNs verschlüsseln deinen Internetverkehr und verschleiern deine Online-Identität. Damit erschweren wir es Dritten, unsere Spuren im Internet zu verfolgen und Daten zu stehlen. Die Verschlüsselung findet dabei in **Echtzeit** statt. Gibt's gratis auch bei Proton.

12. Chat Programme

Whatsapp, Facebook, Instagram und ähnliche Chat Programme sind sehr unsicher, auch wenn die Werbung etwas anderes verspricht. Die haben Zugriff auf alle deine Kontakte im Händi gespeichert sind. So ist es ein Leichtes herauszufinden mit wem du kontakt hast, wer deine Familie ist, usw.
Nutze indessen zum Chatten sichere Anbieter wie:
1. Signal https://signal.org/de/download/
2. Threema. https://threema.ch/de

Wie schütze ich meine Privatsphäre auf dem Smartphone?

Beim Kauf sind die Datenschutz-Einstellungen bei Smartphones und Tablets tief bzw. offen eingestellt, womit die Privatsphäre von Nutzerinnen und Nutzern verletzt wird. Mit anderen Worten: Wenn du die Berechtigungen nicht einschränkst, werden permanent Daten über die Gerätenutzung an den Hersteller geschickt.

So schütze ich meine Privatsphäre auf dem Smartphone:

Ortungsdienste deaktivieren

Wenn das GPS-Modul ausgeschaltet ist, werden keine Informationen über deinen Standort an Dritte geschickt. Alternativ können auch nur bestimmte Apps daran gehindert werden, auf deinen Standort zuzugreifen. So geht es:

Android

Einstellungen > Sicherheit & Standort > Standort > Deaktivieren

Aufgepasst! Auch wenn in den allgemeinen Einstellungen der Ortungsdienst ausgeschaltet ist, sendet das Smartphone weiterhin Standortdaten an die Betreiberin des Betriebssystems: Google. Um auch diese auszuschalten, gehe wiederum in die *Einstellungen > Google > Standort > Google Standortverlauf > Standortverlauf pausieren (Schieberegler) > Pausieren.*

In deinem Google-Konto kannst du zudem unter *Standortverlauf > Zeitachse* checken, welche Standorte Google über dich gespeichert hat, und diese löschen.

iPhone

Einstellungen > Datenschutz > Ortungsdienste > Ortungsdienste deaktivieren

WLAN unterwegs deaktivieren

Das Smartphone registriert automatisch die vorhandenen WLAN-Netze. Derart sensible Daten ritzen klar an der Privatsphäre der Smartphone-Besitzenden, denn dadurch können die Bewegungen des Inhabers auch bei ausgeschaltetem GPS-Modul nachvollzogen werden. So geht’s:

Android

Einstellungen > Netzwerk & Internet > Wi-Fi > deaktivieren

iPhone

Einstellungen > WLAN > deaktivieren

Bluetooth deaktivieren

Bluetooth macht ein Smartphone bzw. die drauf gespeicherten Daten zusätzlich angreifbar, insbesondere an öffentlichen Plätzen wie Flughäfen oder Fussgängerzonen. Möglich ist aber auch die missbräuchliche Nutzung des Geräts (z.B. unerlaubte Telefonate auf Kosten anderer). So geht's:

Android

Einstellungen > Verbundene Geräte > Bluetooth > deaktivieren

iPhone

Einstellungen > Bluetooth > deaktivieren

Temporäre Browserdateien regelmässig löschen

Der Inhalt des temporären Zwischenspeichers (Caches) des Internetbrowsers macht ein Gerät nicht nur langsamer, sondern gibt auch ein genaues Bild über dein Nutzungs- und Surfverhalten wieder. So geht's:

Android

Einstellungen > Speicher > Browserapp (Chrome, Firefox) auswählen > Cache leeren

iPhone

Safari: Einstellungen > Safari > Verlauf und Websitedaten löschen > Verlauf und Daten löschen

Chrome: Chrome > Einstellungen > Verlauf > Browserdaten löschen > Browserdaten löschen

Geräteanalyse deaktivieren

Standardmässig sind die Geräte so eingestellt, dass permanent Analyse-, Diagnose- und Nutzungsdaten direkt an die Server des Herstellers gesendet werden. Die so gewonnenen Informationen geben auch Einblick in die Privatsphäre von Smartphone-Usern. So deaktivierst du die Übermittlung von Analysedaten:

Android

Einstellungen > Google > Google-Konto > Daten & Personalisierung > Aktivitätseinstellungen verwalten > Geräteinformationen pausieren

Einstellungen > Bedienungshilfen > Text-in-Sprache-Ausgabe > bei «Bevorzugtes Modul» auf Zahnradsymbol tippen > Anonyme Nutzungsberichte > deaktivieren

iPhone

Einstellungen > Datenschutz > Analyse > iPhone-Analyse teilen > deaktivieren

Zugriffsrechte von Apps minimieren

Standardmässig fordern Apps bei ihrer Installation viele unnötige Zugriffsrechte, die für das Funktionieren der App gar nicht nötig wären. Falls eine App den Zugriff auf die Kontakte fordert, solltest du kurz überlegen: Ist der Zugriff auf die Kontakte tatsächlich nötig? Meistens wird dieser Zugriff verwendet, um Personen in Ihren Kontakten zu finden oder einzuladen. Wenn du diese Funktionen nicht benötigst, solltest du den Zugriff verweigern.

Es ist zu empfehlen, die Berechtigungen aller Apps, die auf einem Gerät installiert sind, regelmässig zu überprüfen und Einschränkungen vorzunehmen. Falls eine Einschränkung nicht möglich ist, entferne nötigenfalls die App bzw. verzichte auf die Installation – in den meisten Fällen lassen sich Alternativen finden, die weniger datenhungrig sind.

Verwende auch einen sicheren Webbrowser daheim für dein PC

Verwende Firefox oder Brave und aktiviere auch eine alternative Suchmaschinen die deine Daten nicht speichern wie:

- Suchmaschine: Swisscows. https://swisscows.com/de
- Brave Webbrowser: https://brave.com/de/download/

Oder

- Firefox: https://www.mozilla.org/de/firefox/new/

Alternative Mail Programm für den PC:

* Thunderbird: https://www.thunderbird.net/de/

26.8.23. Daniel Megert