Sicherheitscheck (siehe auch sicherheit.digidaktik.de) Version: 10.2019

Vorsicht! Jede Veränderung gründlich notieren und vorher (besonders beim „löschen“) jemand fragen der sich damit auskennt!

1. WLAN / WiFi kein WEP, WPA,WPS => mind. WPA2, ungewöhnlicher Name, SEHR gutes Passwort (s.u.)

2. Handy / Smartphone

a) **„Security patches mindestens bis...“** Schon beim Kauf darauf achten, bis zu welchem Zeitpunkt der Hersteller Sicherheitsupdates verspricht - i.d.R. ab Erst-Erscheinung. (*Gibt es evtl. eine LineageOS-Unterstützung?*)

b) **Bluetooth, NFC und WLAN** generell ausschalten (nur gezielt einschalten), automatisches Verbinden deaktivieren!
- auf verschlüsselte Verbindung achten (https / am besten VPN ...), (WLAN siehe oben)
- öffentliche / fremde Hotspots / Zugangspunkte (z.B. Starbucks, Telekom, ICE) nach Benutzung entfernen,
- **Update** Aufforderungen zuerst ignorieren, erst an einem sicheren Netz / WLAN über die entsprechende Funktion des Betriebssystems/Programms (nicht über SMS-Link o.ä.) **prüfen und durchführen (Verschlechterung?)**

c) GPS aus? (Bedenke: auch ohne GPS ist immer wenn das Handy Netz hat, sein - ungefährer - Ort bekannt)

d) Im Telefonica Netz (z.B. Aldi Talk, Tchibo, blau): Opt-Out: https://www.telefonica.de/dap/selbst-entscheiden.html

e) Alle Einstellungen überprüfen (z.B. iCloud, Apple-/Google-Konto, (Hintergrund-)Datennutzung, Synchronisierungen, Backup, ...), evtl. **lokales Konto per App anlegen und erst dann die Kontakte anlegen**.

f) **Apps** nur an vertrauenswürdigen Netzen aus vertrauenswürdiger Quelle (Software kann alles!) und
- wenn unbedingt benötigt installieren (evtl. einfach die WWW-Seite nutzen?) und
- auf die **Rechte** dieser App achten (z.B. eine Tastatur sollte keinen Internetzugriff haben!
  Ein Spiel mit Internetzugriff sollte keinen kompletten Zugriff auf die SD-Karte und das Adressbuch haben,
  => das **Adressbuch** darf nur weitergegeben werden, wenn alle Personen darin zugestimmt haben, …)
- auf Updates achten (und evtl. vor diesen, die Rechte erneut überprüfen)
- mit AddonsDetector von denper prüfen? Jailbreak / Rooten? Evtl. gezielt um Rechte zu entziehen?
=> https://medienwunder.wordpress.com/2015/01/20/kostenlose-android-apps-und-ein-paar-sicherheits-erwagungen/

g) Nachrichten jeder Art (SMS, e-mail, Sprachbox-Nachrichten, …) können gefälscht, kopiert, verändert, verloren gehen und nicht ankommen.

h) Auswirkungen auf die reale Welt (und befreundete Menschen!) bedenken (auch lokale Gesetze in einem anderen Land, einfache Vervielfältigung, Diebstahl, Rache, Troll-„Spaß“, Erpressung, Identitätenklau, ...)
und **im realen direkten persönlichen Kontakt (im geschützten Rahmen!) überprüfen.**

i) Internet generell eher mit (aktuellem!) Firefox **mit aktiviertem und restriktiv genutztem** NoScript-AddOn (oder zumindest uBlock Origin) und andere Browser-(Chrome/Safari)-Einstellungen durchgehen.

j) Ein kurzer unbemerkter Zugriff auf ein ungeschütztes Gerät genügt evtl. um z.B.
- auch in Zukunft einfach mit dieser Handynummer unbemerkt SMS zu verschicken
- die volle Kontrolle über das Gerät zu erlangen (inkl. Datenauslesen, als Wanze benutzen, …)

k) Eher Signal / Threema (/ Wire?) als WhatsApp (Wenn WhatsApp nicht vermeidbar, bei diesem zumindest: Einstellungen > Sicherheitswarnungen aktivieren und unbedingt Adressbuch einschränken und anonymisieren.)

l) ???: Google, iCloud, Snapchat, Instagram, Werbung, Datentarif, VoIP, Diebstahl, viele Stationen im Netz ???

m) Sicher vor Überwachung: Akku entfernen und in schalldichten Behälter geben ...

n) ...

Konkretes Beispiel für Android:

http://www.spiegel.de/netzwelt/web/android-und-die-sicherheit-tipps-zu-datenschutz-einstellungen-a-1138251.html

Lieber Menschen im realen(!) Kontakt vertrauen / glauben, als technisch / digital / „smart“ vermittelt.

http://www.digidaktik.de/medien-links.shtml - **http://www.digidaktik.de/research/**

Siehe auch:
https://ct.de/check2020 (**Diese Liste mit ihren Links digital: http://checks.digidaktik.de/**)

https://www.jugendschutz.net/ - **https://www.schau-hin.info/**smartphone-tablet/

https://sicher-im-netz.de/familie-und-kinder-kompetent-begleiten

https://mobilsicher.de/apps-kurz-vorgestellt/serie-kindersicherungs-apps-im-check

https://mobilsicher.de/ratgeber/android-fuer-mehrere-nutzer-einrichten und
https://www.futurezone.de/digital-life/article215102981

Beispiel mit Tipps für den Umgang in den Netzwerken / mit den digitalen Medien:
https://www.medien-sicher.de/2015/01/dating-apps-und-live-streaming-aus-dem-kinderzimmer/