Stand: 19.02.2021

Checkliste für mehr Sicherheit in einer digitalen Welt

Wie sicher ich bin ich unterwegs?

Passwort-Überprüfer	https://checkdeinpasswort.de
Identitäts-Überprüfer	https://sec.hpi.de/ilc/search?lang=de
Smartphone-Umkreis-Prüfer	https://www.apkmirror.com/apk/armis-security/blueborne-vulnerability-scanner-by-armis/
Tracking-Überprüfer	http://www.dnstools.ch/visual-traceroute.html https://www.heise.de/newsticker/meldung/Track-This-Mozilla-Tool-trickst-Werbe-Tracker-aus-4458597.html

Regeln bei Kennwörtern:

- min. 12 Zeichen lang
- enthält Buchstaben, Ziffern und Sonderzeichen
- keine erkennbaren Wörter
- Buchstaben durch Zahlen oder Sonderzeichen ersetzen (z.B. mail → m@!l)
- keine Infos über sich selbst preisgeben (z.B. Geburtsdatum als Kennwort ist tabu)
- Eselsbrücke bauen (z.B. „Der Ball ist rund und das Runde muss ins Eckige“ → „DBir&dRmiE“)

- biometrische Authentifizierungen (z.B. Fingerabdrücke) vermeiden
- bei Verwendung eines Passwort-Managers (z.B. keePass):
    - niemals alle Kennwörter damit speichern
    - tendenziell eher für unwichtige Kennwörter verwenden

- PIN´s sollten min. 6 Stellen haben

To-Do´s am PC (auch Apple-Produkte):

	Maßnahme	Erläuterung
☐	Benutzerrechte trennen: einrichten eines separaten User- und Administratoren-kontos	https://www.pcwelt.de/ratgeber/Benutzerrechte-trennen-PC-Sicherheit-373573.html
☐	kostenpflichtige (!) AntiViren-Software verwenden	https://www.digitalwelt.org/antivirus/artikel/kostenloser-virenschutz
☐	Anti-Adware- und Anti-Spyware-Software verwenden	Anti-Adware: https://www.heise.de/download/product/adwcleaner-91313 Anti-Spyware: https://www.chip.de/download/39009_Anti-Spyware/
☐	AdBlocker verwenden	https://netzpolitik.org/2017/stiftung-warentest-testet-tracking-blocker-ein-muss-fuer-jeden-browser/ Beispiel: https://www.heise.de/download/product/ublock-origin-97011

☐	Anti-Tracking einrichten & aktivieren	https://www.heise.de/newsticker/meldung/Privacy-Badger-Browser-Plugin-sperrt-Werbenetzwerke-2775115.html
☐	Datensammeln der Suchmaschinen umgehen	https://www.startpage.com/de/
☐	Dateien und Speichermedien verschlüsseln	https://www.heise.de/download/product/veracrypt-95747
☐	VPN verwenden	https://www.vpnvergleich.net/warum-vpn/ kostenloste VPN (z.B. von Opera) gelten i.d.R. als nicht vertrauenswürdig

To-Do´s auf dem Smartphone und Tablet (auch Apple-Produkte):

	Maßnahme	**Erläuterung**
☐	Sperrbildschirm bzw. Lockscreen einrichten	
☐	drahtlose Schnittstellen (z.B. Bluetooth) deaktivieren	https://www.gq-magazin.de/auto-technik/article/bluetooth-sicherheit-blueborne-angriff https://www.chip.de/downloads/BlueBorne-Vulnerability-Scanner-Android-App_122986759.html
☐	WLAN-Passwörter verwalten: alle öffentlichen Netzwerke löschen und nie beitreten	https://de.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html
☐	VPN verwenden	https://www.vpnvergleich.net/warum-vpn/ kostenloste VPN (z.B. von Opera) gelten i.d.R. als nicht vertrauenswürdig
☐	AntiViren-Software verwenden	https://www.heise.de/tipps-tricks/Brauche-ich-auf-dem-iPhone-einen-Virenscanner-3853961.html https://www.heise.de/tipps-tricks/Virenscanner-fuer-Android-brauche-ich-das-3872867.html
☐	Spionagesoftware entlarven	https://www.futurezone.de/digital-life/article210983803/futurezone-hilft-So-erkennst-und-entfernst-du-Spionage-Apps-wie-FlexiSpy-von-deinem-Smartphone.html
☐	(dienstlich) kein Whatsapp nutzen	https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/whatsappalternativen-die-datenschutzregeln-im-ueberblick-13055 Alternativen: https://www.chip.de/news/Die-besten-WhatsApp-Alternativen-Top-Messenger-fuer-Android-und-iOS_102197994.html

To-Do´s im (Heim-) Netzwerk:

	Maßnahme	Erläuterung
☐	Firewall aktivieren	https://www.pc-magazin.de/ratgeber/router-firewall-richtig-konfigurieren-einstellen-schutz-hacker-viren-2483746.html
☐	Trennung von Heimnetz und Gastnetz	https://www.dasheimnetzwerk.de/03-2018/Netzwerk-sicher-durch-Bereiche.html
☐	VPN einrichten	https://www.vpnvergleich.net/warum-vpn/ z.B. bei FritzBox: https://avm.de/service/vpn/praxis-tipps/vpn-verbindung-zur-fritzbox-unter-windows-einrichten-fritzfernzugang/

To-Do´s in der Geldbörse:

	Maßnahme	Erläuterung
☐	Giro- bzw. Kreditkarte mit NFC deaktivieren oder wenigstens eine RFID-Schutzhülle mit in das Portomaine legen	https://www.bezahlen.de/schutz-vor-nfc-betrug.php

allgemein gilt:

- technische Maßnahmen zur Informationssicherheit einführen
    - Sicherheitsstandards definieren (z.B. jeden Tag eine Sicherungskopie erstellen, nach drei Jahren Festplatten austauschen, „sichere“ Passwörter wählen, etc.)
    - **Updates durchführen**
    - Regeln einhalten
    - **Backups erstellen**
- „auf Bauchgefühl hören“ & **misstrauisch sein** → technische Vorgänge hinterfragen
- Datensparsamkeit und -vermeidung (gegen Erstellung von Persönlichkeitsprofilen)
- Nicknames bzw. Pseudonyme im Internet verwenden
- Browsereinstellungen dem Sicherheitsbedürfnis anpassen
- Blockierung aktiver Inhalte
- Löschung von Cookies
- Vorsicht bei E-Mails (!):
    - möglichst nicht aus Mail heraus handeln → Links durch Mouse-Over erst überprüfen
    - noch besser: **Links nicht anklicken**; Webseite besuchen und dann erst einloggen
    - Anhänge möglichst nicht öffnen → vorher: Rücksprache mit dem Versender
- **Makros möglichst nie öffnen** (oder wenn dann nur bei sicheren Quellen)
- wenn möglich **Zwei-Faktor-Authentifizierung** verwenden (Online-Banking, Amazon, Netflix & Co.)

Was tun, wenn es mich dennoch mal erwischt?

- Datenschutzbeauftragten informieren („Datenpanne“ melden)
- ggf. IT-Abteilung der Firma etc. informieren
- ggf. Polizei einschalten
- eigenes System neu aufsetzen und alle Kennwörter neu belegen