

# CHECKLISTE ONLINE-SICHERHEIT

Erarbeitet von Lena Knepper

## 1. ERSTELLE SICHERE PASSWÖRTER – DAS MACHT ES SCHWERER GEHACKT ZU WERDEN

- Verwende ein PW niemals doppelt
- Verwende mindestens 15-20 Zeichen + Kombination aus Zahlen, Buchstaben, Zeichen sowie Groß- und Kleinschreibung
- Verwende ganze Passphrasen oder Eselsbrücken (Anfangsbuchstaben eines Satzes)
- Verwende einen Passwort-Manager (*LastPass*, *KeePassX*): PWs für deinen PC und dein Smartphone generieren lassen
- Aufbewahrung der PWs schriftlich (und verklausuliert) an einem sicheren Ort wie deinem Zimmer
- Diese Passwörter/-phrasen sind besonders wichtig und solltest du dir merken: PWs deines Gerätezugangs, Mailaccounts, Passwort-Managers (s.u.) und deiner Festplattenverschlüsselung
- Nutze die Zwei-Faktor-Authentifizierung für deine Online-Dienste

## 2. SOCIAL MEDIA SICHERHEITSPRAKTIKEN

– DAMIT DEINE PERSÖNLICHEN INFO'S NICHT FÜR JEDE PERSON SICHTBAR SIND

- Überprüfe deine Facebook-Einstellungen im Privatsphäre-Check
- Schränke für deine Facebook-Chronik und für Posts Zielgruppen ein und/oder lösche Beiträge
- Passe den Facebook-Gruppentyp in den Gruppeneinstellungen unter Privatsphäre an
- Passe Werbung sowie die Berechtigungen für Apps an
- Installiere einen Facebook-Container
- Verschlüssele deine Facebook-Chats im Messenger
- Passe auf Instagram deine Privatsphäre-Einstellungen an und schaue nach, wie du andere Posts und Profile blocken kannst
- Stelle für Youtube unter Datenschutz den Zugriff auf dein Profil auf ‚niemand‘, gebe persönliche Videos als ‚privat‘ oder ‚nicht gelistet‘ an, schaue nach, wie du Nutzer\_innen sperren melden kannst und wie das Melden für Videos geht

## 3. VERSCHLÜSSELTE KOMMUNIKATION

– DAMIT SIE NICHT WIE EINE POSTKARTE MITGELESEN WERDEN KANN

- Lade das Mailprogramm *Thunderbird* herunter (Outlook und Applemail sind nicht mehr sicher)
- Installiere die entsprechende Verschlüsselungs-Software *Enigmail 2.0*
- Achte immer auf die neuste Version des Mailprogramms und der Verschlüsselungs-Software
- Wichtig: Sendende und empfangende Person müssen die Verschlüsselungs-Software herunter laden
- Schütze deinen geheimen Schlüssel (private key) mit einer Passphrase von mindestens 20 Zeichen (Sonderzeichen, Groß- und Kleinschreibung und Zahlen)
- Tauscht euren öffentlichen Schlüssel aus. Du kannst deinen öffentlichen Schlüssel auch auf einen keyserver laden und den anderer Personen von keyservern downloaden
- Verschlüssele zusätzlich einzelne Textdateien, wie Word-Dateien oder PDF-Dokumente (z.B. mit *PDF24*)
- Nutze pgp-Verschlüsselung auch auf deinem Handy, damit Du auch unterwegs verschlüsselt per Mail kommunizieren kannst
- Verwende sichere Apps wie *Signal* und *Wire* (nicht Telegram)

#### 4. SELF DOXING – DAMIT KEINE\*R UNLIEBSAME DOKUMENTE VON DIR FINDEN KANN

---

- Suche nach Bildern, nach deinem Namen, deinen Nicknames und deiner IP-Adresse, deiner Wohnadresse, deiner Mailadresse
- Benutze einen anderen Browser als gewöhnlich
- Gehe sicher, dass Du parallel nicht in deine Online-Accounts eingeloggt bist
- Installiere vor dem Self-Doxing Anonymisierungsmaßnahmen wie den Tor-Browser (siehe Punkt 3) und gehe über <https://> als sicherere Verbindung
- Verwende verschiedene Suchmaschinen
- Verfeinere deine Suche, indem du mehrere Wörter in Anführungszeichen setzt
- Suche deinen Namen und deine Adresse in den Gelben Seiten, unter *Das Örtliche* oder unter *Das Telefonbuch*
- Suche nach möglicherweise geklauten Bildern (z.B. mit der google-Rückwärtssuche) oder mit *TinEye*
- Falls deine Posts auf deine IP-Adresse oder deinen Standort Rückschlüsse erlauben, lösche sie
- Lösche dir unliebsame Suchergebnisse auf google
- Prüfe ob dein Name, deine E-Mail-Adresse und Passwörter auf Datenbanken veröffentlicht wurden, indem du deine E-Mail-Adresse auf *;-have i been pwned?* eingibst
- Falls dein Account betroffen ist und du dieses Passwort auch für andere Accounts nutzt, ändere es unmittelbar

#### 5. SEI ANONYM(ER) IM INTERNET

– VERMEIDE, DASS PERSÖNLICHE DATEN GGF. MISSBRAUCHT WERDEN

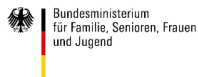
---

- Verwende Browser, der automatisch <https://> einstellt (z.B. Firefox), surfe immer unter dem <https://>-Protokoll und stelle sicher, dass du die neuste Browser-Version benutzt
- Deaktiviere Cookies, die von Werbenetzwerken benutzt werden, um dich beim Surfen auszuspähen
- Stelle deinen Browser so ein, dass er Cookies beim Beenden löscht
- Deaktiviere Plug-ins, JavaScript und Flash
- Nutze sicherere Suchmaschinen als Google (wie z.B. *duckduck.go* oder *Startpage*)
- Verwende Browser-Erweiterungen damit du beim Surfen nicht verfolgt wirst (z.B. *uBlock origin*, *https everywhere* und *privacy badger*)
- Verschlüssele vertrauliche Informationen vor dem Verschicken zusätzlich

---

Erarbeitet im Projekt "Social Media Interventions! - rechtsextremen Geschlechterpolitiken im Netz begegnen", gefördert von:

Gefördert vom



im Rahmen des Bundesprogramms

Demokratie *leben!*

