Handout

Reflexionsfragen zur eigenen technischen & digitalen Nutzung

Allgemein

+Wie nutze ich & beschäftige ich mich mit meinen alltäglichen Geräten und Anwendungen (z.B. Updates, Berechtigungen...)?
+Wie wichtig sind mir Privatsphäre und Datenschutz im digitalen Bereich?
+Wer kümmert sich um meine Technik? Wer richtet mir Geräte ein oder macht Updates?
+Woher habe ich Geräte, die ich benutze? Über wen laufen Verträge?

Geräte in unmittelbarer Umgebung/zuhause

+ Welche Geräte verwende ich? Welche Geräte haben Internetzugang (smart home)?
+ Für welche Geräte gibt es/nutze ich geteilte Konten mit Anderen (z.B. auch Family-Plan)?
+ Wer hat physischen Zugriff auf meine Geräte oder kennt meine Passwörter/PINs (zum Entsperren)?

Konten, Anwendungen und Passwörter

+ Benutze ich sichere und individuelle Passwörter? Speichere ich die PW sicher?
+ Bei welchen Accounts bin ich registriert? Welche Apps nutze ich?
+ Kenne ich die Privatsphäre-Einstellungen von Apps & Accounts, die ich nutze?
+ In welchen Geräten/Anwendungen bin ich standardmäßig eingeloggt? Wer nutzt diese mit?
+ Wer könnte meine Zugangsdaten kennen?

Browser/ Internet

+ Wer hat Zugriff auf meinen Browser? Kenne ich die Einstellungen meines Browsers?
+Habe ich Passwörter/ Log-in Daten oder Zahlungsmittel im Browser gespeichert?

Bilder

+ Kenne ich meine Rechte am eigenen Bild?
+Wie und wo speichere ich meine Bilder ab? Über welche Dienste verschicke ich Bilder oder lade sie hoch?
+ Welche Informationen von mir & Umgebung befinden sich auf Bildern, die ich ins Netz stelle?

ein paar Maßnahmen & Handlungsoptionen

...eigene Medienkompetenz und digitale Selbstbestimmung stärken

...Browser/Internetsurfing:
...Passwörter speichern **deaktivieren** keine Zahlungsinformationen hinterlegen
... **privates Fenster** benutzen. Verlauf und Downloads ggf. löschen (Privatsphäre-Einstellungen des Browsers überprüfen)
...in öffentlichen WLANs am besten **VPN** nutzen

...E-Mail: **BCC** statt CC verwenden (außer eine CC E-Mail Liste wird benötigt)

sichere Passwörter/PIN

…KEINE Wischmuster, FaceID, persönliche Daten, mind. 12 Zeichen, Zeichenmix

…nicht auf Zettel schreiben + drankleben

Empfehlung: Passwortmanager verwenden, *z.B. KeePass*

….2-Faktor Authentifizierung aktivieren

…immer **ausloggen** (Social-Media Konten, E-Mail, Apps…)

….Passwort im Browser **nicht** speichern & „eingeloggt bleiben" **deaktivieren**

…Zugangsdaten nicht leichtfertig weitergeben!

→ Passwort teilen ist kein Liebesbeweis

Festplatten/USB-Sticks:

Zugang **sichern** durch Verschlüsselung (Empfehlung: *Cloud – cryptomator; Festplatte/ USB – veracrypt*)

Backups machen/ Daten sichern

Kamera abkleben

Mikrofon nur bei Bedarf aktivieren

GPS/Ortungsdienste über Einstellungen + App-Berechtigung einschränken, nur bei Bedarf aktivieren

Verschicken von Bildern:

Ist dein Standort im Bild erkennbar? Ggf. zusätzliche App benutzen, um Metadaten (EXIF-Datei) zu löschen

Insbesondere bei **sensiblen** Bildern: Ende-Zu-Ende-Verschlüsselte Messenger (z.B. signal – hat View-Once-Funktion), GPS deaktivieren, Cloud-Synchronisierung deaktivieren, ggf. Körperstellen bedecken

…smartphone:

…Lockscreen so privat wie möglich halten → keine Nachrichten anzeigen lassen

…nur vertrauenswürdige Apps herunterladen, Berechtigungen überprüfen und ggf. Alternativen verwenden (→ F-Droid) (z.B. eine Taschenlampenapp braucht keine Anrufberechtigung), App-Liste überprüfen, nicht verwendete Apps löschen

…möglichst keine sensiblen Daten auf dem Smartphone speichern

…**Privatsphäre-Einstellungen** beim Smartphone und bei allen Konten überprüfen (Facebook, eBay…) & so wenig Daten wie möglich/nötig rein stellen.

…auf Social Media/öffentliche Präsenz:

…Privatsphäre-Einstellungen überprüfen → wer darf meinen Account sehen, wer darf mich kontaktieren?

…**Anonyme/geheime Konten** erstellen ohne persönliche Information, wenn möglich

…Kontaktbuch nicht synchronisieren

…..im Zweifel Gerät über Einstellungen auf Werkseinstellungen zurück setzen

weitere App-Empfehlungen & Tipps aus der Präsentation auf:
https://ag-link.xyz

Quellen: https://www.anti-stalking-projekt.de/checkliste-zur-digitalen-trennung/ CETA (https://www.ceta.tech.cornell.edu/resources), A DIY Guide to Feminist Cybersecurity (https://hackblossom.org/cybersecurity), https://www.aktiv-gegen-digitale-gewalt.de/de