Geräte- und Accountsicherheit

Für diese Themen war im Workshop kein Platz:

Sichere Passwörter

- Benutze niemals dasselbe Passwort für verschiedene Accounts
- Installier dir einen Passwort-Manager wie z.B. KeePassXC (https://keepassxc.org) Damit kannst du starke und zufällige Passwörter generieren und musst du dir nur ein einziges Masterpasswort merken.
- Mit Diceware können leicht erinnerbare aber zufällige Passwörter erstellt werden. Weiterlesen: https://helmschrott.de/blog/diceware-passwort-sicher-einfach

Account-Sicherheit

Schütze deine Online-Accounts mit Zwei-Faktor-Authentifizierung. Lies im Systemli-Wiki was das ist und wie du es aktivierst: https://wiki.systemli.org/howto/android/2fa

Nicht auf Phishing reinfallen

Phishing bezeichnet z.B. betrügerische Mails, die dich auf Fake-Webseiten locken um dein Passwort abzugreifen. Gezieltes Phishing wird auch als Spearfishing bezeichnet und ist oft schwer zu erkennen. Dieser englisch-sprachige Comic liefert eine tolle Einführung: https://thenib.com/how-to-protect-yourself-against-spearphishing/

Tipp: Insbesondere PDFs und Office-Dokumente werden oft manipuliert werden um Schadcode zu enthalten. Wer nicht vermeiden kann unbekannte Mail-Anhänge zu öffnen (z.B. als Journalistin), sollte sich mit Tools wie Dangerzone vertraut machen: https://dangerzone.rocks

Gerätesicherheit

Schütze deine Geräte vor fremdem Zugriff:

- MacOS: FileVault2 (vorinstalliert)
- Windows: Veracrypt
- Linux: Bei der Installation ”Gesamte Festplatte verschlüsseln” auswählen
- Android: Systemeinstellungen
- iOS: Systemeinstellungen

Tipp: Bei neueren Smartphones ist Verschlüsselung oft standardmäßig aktiviert und kann nicht in den Einstellungen gefunden werden. Im Zweifel online informieren.

Anonymität

Tor

- Die meisten Webanwendungen lassen sich auch mit dem Tor Browser benutzen. Für Ende-zu-Ende-Verschlüsselung mit Web-Jabber oder Riot-Web ist es allerdings nötig, kryptografische Schlüssel im Browser zwischenzuspeichern. Da der Tor Browser nach jedem Schließen seinen Speicher leert, müsste man die Fingerprints mit jeder Sitzung neu verifizieren.

Weiterlesen

- https://de.hackblossom.org/cybersecurity
- https://riseup.net/de/security
- https://wiki.systemli.org
- https://ssd.eff.org/