

Digitale Selbstverteidigung

Checkliste: 8 Schritte für mehr Sicherheit im Netz

Koordinierungsstelle Medienbildung Sachsen | www.ksm-sachsen.de

01 Grundlagen der digitalen Sicherheit

- Starke Passwörter nutzen und Passwortmanager einsetzen.
- Zwei-Faktor-Authentifizierung (2FA) aktivieren.
- Software immer aktuell halten.

02 Datenschutz & Privatsphäre

- Persönliche Daten minimieren und nur wenn nötig teilen.
- Privatsphäre-Einstellungen in Sozialen Netzwerken anpassen.
- Tracker blockieren.

03 Verschlüsselung nutzen

- E-Mails verschlüsseln (z.B. mit Pretty Good Privacy)
- Sichere Messenger wie Signal oder Threema verwenden.
- VPN nutzen, besonders in öffentlichen WLANs.

04 Bedrohungen erkennen & vermeiden

- Vorsicht bei Phishing-E-Mails und unbekanntem Links
- Antivirensoftware installieren
- Vorsicht bei verdächtigen Anfragen (Social Engineering).



05 Datensicherung

- Regelmäßige Backups nach der 3-2-1-Regel.
- Daten sicher löschen – Tools wie DBAN oder integrierte Funktionen nutzen.

06 Gerätesicherheit gewährleisten

- Smartphone und PC verschlüsseln.
- Nur vertrauenswürdige Apps installieren.

07 Sicherer Browsergebrauch

- Sichere Browser wie Firefox oder Brave verwenden.
- HTTPS und Cookie-Blocker aktivieren.

08 Im Notfall reagieren & regelmäßig prüfen

- Passwörter ändern, 2FA aktivieren und Konten sperren.
- Beweise sichern und Anzeige erstatten.
- Sicherheitsmaßnahmen regelmäßig überprüfen und auf dem neuesten Stand bleiben.

