Leitfaden Digitale Hygiene

Erhöhung des digitalen Selbstschutzes

TECH_AGAINST VIOLENCE

Herausgeberin: Tech against Violence

Kontakt: info@techagainstviolence.ch I http://techagainstviolence.ch

Datum: 30. Juni 2026

Inhaltsverzeichnis

1. Digitale Hygiene

Erhöhter Schutz vor Missbrauch

Smartphones, Online-Konten und Apps enthalten viele persönliche Informationen. Wer Zugriff darauf hat, kann einiges über eine Person erfahren oder sie überwachen, kontrollieren und ausspionieren, die Identität stehlen und missbrauchen und unerwünschte Änderungen an Benutzerprofilen vornehmen.

Es ist jedoch möglich, selbst **Massnahmen** zu ergreifen, um den Schutz zu verbessern. Sichere Accounts und Passwörter sind der erste Schritt, die eigene digitale Sicherheit deutlich zu erhöhen.

- Passwörter von Geräten, Cloud-Diensten und Benutzerkonten prüfen, Kontoeinstellungen anpassen oder Zugriffsrechte kontrollieren. All das gehört zur **digitalen Hygiene** und hilft, Risiken zu minimieren.
- Technologie kann kompliziert wirken und einschüchternd sein, doch viele Schritte sind relativ einfach umzusetzen und erfordern **kein spezielles technisches Wissen**.
- Ein vollständiger Schutz lässt sich selten garantieren, doch digitale Hygiene **veringerrt Angriffsflächen**.

Eigene Passwörter und **eigene Konten** sind der effektivste Schutz. In der Praxis ist das jedoch nicht immer leicht umzusetzen, besonders in Beziehungen oder gemeinsamen Haushalten, wo Zugänge oft geteilt werden.

In den meisten Fällen von digitaler Gewalt in (Ex-)Beziehungen sind es gemeinsam genutzte Konten oder geteilte Passwörter, die Fremdzugriffe und Kontrolle ermöglichen.

2. Passwort-Sicherheit

Mit starken Passwörtern, einem Passwortmanager und Zwei-Faktor-Authentifizierung ist es für andere deutlich schwieriger, auf persönliche Konten zuzugreifen.

Starke, einzigartige Passwörter

Passwörter schützen den Zugang zu vielen persönlichen Konten. Wenn für verschiedene Konten dasselbe Passwort verwendet wird, kann ein bekannt gewordenes Passwort den Zugriff auf mehrere Konten gleichzeitig ermöglichen. Daher sollte **jedes Konto ein eigenes Passwort** haben.

Ein **starkes Passwort** hat:

- mindestens 12 Zeichen
- Gross- und Kleinbuchstaben
- Zahlen und Sonderzeichen
- keinen persönlichen Bezug (z.B. Namen, Geburtsdaten, Lieblingsorte)

Da sich viele und starke Passwörter kaum merken lassen, kann ein **Passwortmanager** helfen.

PASSWORT-SICHERHEIT

Passwortmanager

Ein Passwortmanager hilft dabei, unterschiedliche Passwörter **sicher an einem Ort** zu verwalten. Ein einziges **Hauptpasswort** reicht, um auf die gespeicherten Passwörter zuzugreifen. Die meisten Passwortmanager können auch automatisch sichere Passwörter erstellen (Password-Generator).

Empfohlene **Passwortmanager** sind:

- Proton Pass (Schweiz)
- Secure Safe (Schweiz)
- Bitwarden
- NordPass

⚠ Wichtig: Das **Hauptpasswort** schützt alle anderen Passwörter. Es sollte stark sein, nicht weitergegeben und sicher aufbewahrt werden – am besten handgeschrieben an einem sicheren Ort, nicht digital auf dem genutzen Gerät. Wird es vergessen, geht der Zugriff verloren. Trotzdem ist ein Passwortmanager deutlich sicherer als keine Verwaltung.

PASSWORT-SICHERHEIT

Zwei-Faktor-Authentifizierung (2FA)

Die Zwei-Faktor-Authentifizierung (2FA) ist eine **zusätzliche Sicherheitsebene** für Online-Konten. Das heisst, selbst wenn ein Passwort bekannt wird, verhindert 2FA, dass unbefugte Personen Zugriff auf das Konto bekommen.

Wie **funktioniert** 2FA?

- **2FA aktivieren:** In den Sicherheitseinstellungen eines Online-Kontos (z.B. E-Mail, Banking, Social Media) kann 2FA eingeschaltet werden. Dabei lässt sich wählen, ob die Codes per SMS aufs Handy geschickt oder über eine Authentifizierungs-App generiert werden.
- **Code erhalten:** Beim Einloggen wird zusätzlich zum Passwort ein einmaliger Code abgefragt. Falls die Option SMS gewählt wurde, kommt der Code aufs Handy. Bei der Authentifizierungs-App (z.B. Microsoft Authenticator) wird der Code direkt in der App generiert.
- **Code eingeben:** Nur wer das Passwort und den aktuellen Code hat, kommt ins Online-Konto.
- **Achtung**: Beim Wechseln der Geräte und Telefonnummern an die Zwei-Faktor-Authentifizierung denken, denn diese muss mit dem neuen Gerät und der neuen Telefonnummer konfiguriert werden, sonst verliert man den Zugang.

Authentifizierungs-Apps sind in der Regel sicherer, da die Codes nicht direkt per SMS gesendet werden und der Zugang zusätzlich durch einen App-PIN geschützt ist. Gerade im Kontext von Beziehungsgewalt, wo Tatpersonen oft auch direkten Zugang auf das Handy haben, bietet die App einen besseren Schutz.

PASSWORT-SICHERHEIT

Passkeys: Die Zukunft der Anmeldung

Passkeys ersetzen Passwörter und machen das Anmelden einfacher und sicherer. Sie schützen besser vor Phishing und Missbrauch. Viele Konten unterstützen Passkeys bereits direkt beim Login oder in den Kontoeinstellungen. **Hier findet sich auf SRF** eine gute Erklärung, worum es geht.

Wie funktionieren Passkeys?

- Beim Einrichten wird ein Schlüsselpaar erstellt: ein öffentlicher und ein privater Schlüssel.
- Zur Anmeldung erfolgt die Bestätigung mit Fingerabdruck, Gesichtserkennung oder PIN.
- Der private Schlüssel bleibt auf dem Gerät und wird nicht an den Dienst gesendet.

Die Vorteile von Passkeys

Erhöhte Sicherheit

Besserer Schutz vor Phishing und Fremdzugriff.

Einfache Nutzung

Anmelden mit Fingerabdruck, Gesicht oder PIN.

Geräteüber-greifend

Mit Cloud-Sync auf mehreren Geräten nutzbar.

3. Gerätesicherheit

Ein gut geschütztes Gerät gehört zum digitalen Selbstschutz. Regelmässige Updates, ein bewusster Umgang mit Apps und Gerätesperren helfen, persönliche Daten vor Fremdzugriffen zu schützen.

Regelmässige Updates

Updates sind eine der einfachsten und effektivsten Schutzmassnahmen für Geräte, da sie bekannte **Sicherheitslücken schliessen** und so mehr Schutz vor Missbrauch oder unerwünschtem Zugriff bieten. Betriebssysteme und Apps geben in der Regel automatisch Hinweise, sobald eine neue Version verfügbar ist. Ansonsten können Updates auch manuell gestartert werden:

- **iPhone / iPad:** Einstellungen → Allgemein → Software Update
- **Android-Geräte:** Einstellungen → oft eigener Punkt "Software-Update"
- **Mac:** Systemeinstellungen → Allgemein → Software Update
- **Windows:** Einstellungen → oft eigener Punkt "Windows Update"

ⓘ Wo möglich, **automatische Updates** aktivieren, so bleiben Geräte ohne grossen Aufwand geschützt und aktuell.

GERÄTESICHERHEIT

Umgang mit Apps

Apps können ein Sicherheitsrisiko darstellen, besonders wenn sie von unbekannten Anbietern stammen, nicht selbst installiert wurden oder nicht mehr benötigt werden. Daher gilt:

- **Unbekannte** oder nicht benötigte **Apps löschen.** Gut zu wissen: Echte System-Apps lassen sich nicht löschen. Wenn eine App entfernt werden kann, ist sie nicht essential für das Gerät.
- Nur Apps aus **offiziellen App-Stores** installieren (z.B. Google Play Store, Apple App Store)
- Viele Apps fragen nach **Zugriff** auf Kamera, Mikrofon oder Standort – gut überlegen, ob das wirklich nötig ist.

Bildschirmsperre

Ein PIN, ein Passwort, Muster oder biometrische Sperre (Fingerabdruck oder Gesichtserkennung) schützt das Gerät. In vielen Fällen kennt die Tatperson die PIN zum Gerät, diese muss deshalb umgehend geändert werden.

- **PIN / Passwort:** Sollte mindestens 6 Stellen haben
- **Automatische Sperre:** Das Gerät soll nach kurzer Inaktivität automatisch gesperrt werden
- Eine **Kombination** aus starker PIN/Passwort und biometrischer Sperre erhöht den Schutz

⚠ Die **biometrische Sperre** ist komfortabel, sollte aber nicht als einziger Schutz verwendet werden. Besonders im Kontext von Beziehungsgewalt kann die Tatperson versuchen, das Gerät mit einem Foto zu entsperren oder heimlich ein Bild (z.B. wenn die betroffene Person schläft) aufnehmen, um die Gesichtserkennung zu umgehen.

4. Standort- und Ortungsfunktionen

Standort- und Ortungsfunktionen geben **Informationen über den Aufenthaltsort**. Das kann nützlich sein (z.B. für die Navigation), birgt aber auch Risiken für die Privatsphäre.

Empfohlene **Massnahmen** sind:

- **Apps:** Berechtigungen kontrollieren und Zugriff nur bei Bedarf erlauben, ansonsten deaktivieren.
  - **iPhones:** Einstellungen → Datenschutz & Sicherheit → Ortungsdienste
  - **Android:** Einstellungen → Standort → App-Berechtigungen
- **Geräteortung und Live-Standort:** Ortungsfunktionen können auch der Geräteortung dienen (z.B. bei Verlust oder Diebstahl) oder um den Live-Standort mit anderen Personen zu teilen. Freigaben für Live-Standort laufen im Hintergrund weiter und müssen manuell beendet werden.
  - **iPhones:** Über "Find My" läuft die Geräteortung. In derselben Funktion kann auch der Live-Standorts mit anderen Personen geteilt werden. Standortfreigaben prüfen: Einstellungen → [Name oben] → Find My
  - **Android:** "Mein Gerät finden" dient nur der Geräteortung. Der Live-Standort kann über die Google Maps App mit anderen Personen geteilt werden. Standortfreigaben prüfen: Google Maps → Menü → Standortfreigabe

Damit **alte oder ungewollte Standortfreigaben** nicht unbemerkt weiterlaufen, sollten diese Einstellungen regelmässig geprüft werden.

GERÄTESICHERHEIT

5. Safety Check: iPhone & Android

Der Safety Check ist ein eingebautes Sicherheitstool, das Betroffenen hilft, schnell und unkompliziert zu überprüfen, welche Apps und Personen Zugriff auf persönliche Daten haben – und diesen Zugriff sofort zu entziehen.

IPHONE (IOS 16+)

Safety Check

1. Einstellungen → Datenschutz & Sicherheit → Safety Check
2. "Notfall-Reset": Setzt sofort alle Freigaben zurück und meldet alle anderen Geräte ab
3. "Freigaben verwalten": Zeigt, welche Personen und Apps Zugriff haben – gezielt entziehbar

ANDROID

Sicherheitscheck

1. Einstellungen → Sicherheit & Datenschutz → Sicherheitscheck (je nach Hersteller variiert der Pfad)
2. Überprüft App-Berechtigungen, Kontozugriffe und Geräteadministratoren
3. Google-Konto: myaccount.google.com → Sicherheit → Zugriff Dritter prüfen

Empfehlung: Der Safety-Check sollte regelmässig gemacht werden. Wenn ein verbundenes Konto entdeckt wird, das nicht verbunden sein sollte, nicht überstürzt reagieren und gut überlegen, ob und zu welchem Zeitpunkt es getrennt werden soll. Auch nicht vergessen, Screenshots der Verbindung als Beweismittel zu machen.

6. Sicheres Surfen

Jedes Gerät hinterlässt beim Surfen und bei der Nutzung von Online-Diensten Spuren und Daten. Ein paar bewusste Einstellungen können dabei helfen, online sicherer unterwegs zu sein.

Such- und Browserverlauf

Der Verlauf zeigt, welche Seiten besucht wurden. Es lohnt sich daher, den Browserverlauf auf allen genutzten Geräten regelmässig zu löschen:

- **Laptop / Desktop:** Den Browser wählen → Menü (oft drei Punkte) → Verlauf → Verlauf löschen
- **iPhone:** Einstellungen → Browser Safari wählen (auch via Suchfunktion) → Verlauf und Websitedaten löschen
- **Android:** Auf den meisten Android-Geräten ist der Browser Chrome vorinstalliert: Chrome App öffen → Menü (drei Punkte) → Verlauf → Browserdaten löschen

SICHERES SURFEN

Privater Modus beim Surfen

Im privaten Modus (z.B. Inkognito bei Chrome, privates Fenster bei Safari) speichert der Browser weder Verlauf, Cookies noch Formulareingaben und Suchanfragen. Trotzdem: Der Modus macht nicht anonym im Internet, kann aber für **mehr Privatsphäre** auf dem jeweiligen Gerät sorgen. Es gibt auch Suchmaschinen wie DuckDuckGo oder Startpage, die weniger Daten sammeln.

Aktive Sitzungen

Eine aktive Sitzung bedeutet, dass ein Konto auf einem Gerät **angemeldet** ist und jemand darauf zugreifen kann, ohne sich neu einloggen zu müssen. Viele Online-Konten (z.B. E-Mail-Konten, Instagram, Facebook, WhatsApp) zeigen, auf welchen Geräten das Konto gerade aktiv ist.

Das lässt sich meist via Einstellungen und Sicherheit (Verknüpfte Geräte, Anmelde-Aktivität) prüfen. **Unbekannte Geräte** unbedingt abmelden und falls nötig das Passwort ändern.

Sicher surfen heisst auch: Passwörter nicht automatisch im Browser speichern (**Autofill**), sondern einen **Passwortmanager** benutzen.

7. Social-Media-Sicherheitseinstellungen

Social-Media-Konten enthalten viele persönliche Informationen und sind häufig ein Ziel für Missbrauch. Mit den richtigen Einstellungen lässt sich die Privatsphäre deutlich verbessern und das Risiko von unbefugtem Zugriff reduzieren.

Datenschutz- und Privatsphäre-Einstellungen

Wer kann Beiträge, Fotos und persönliche Informationen sehen? Diese Einstellungen sollten regelmässig geprüft werden:

- Profil auf "Privat" stellen, damit nur bestätigte Kontakte Inhalte sehen können.
- Überprüfen, wer Beiträge, Stories und Fotos sehen darf (z.B. "Nur Freunde" statt "Öffentlich").
- Kontrollieren, wer das Profil in Suchergebnissen finden kann.
- Verknüpfte Apps und Drittanbieter-Zugriffe regelmässig prüfen und entfernen.

SOCIAL-MEDIA-SICHERHEIT

Kontozugriff und Accountsicherheit

Neben den Privatsphäre-Einstellungen ist es wichtig, den Zugriff auf Social-Media-Konten aktiv zu kontrollieren.

Aktive Sitzungen prüfen

Viele Plattformen zeigen, auf welchen Geräten das Konto aktiv ist. Unbekannte Geräte sollten sofort abgemeldet werden:

- **Instagram:** Einstellungen → Sicherheit → Anmeldeaktivität
- **Facebook:** Einstellungen → Sicherheit und Login → Wo du angemeldet bist
- **TikTok:** Profil → Einstellungen → Sicherheit → Geräteverwaltung

Zwei-Faktor-Authentifizierung aktivieren

Für alle Social-Media-Konten empfiehlt sich die Aktivierung der Zwei-Faktor-Authentifizierung (2FA), um unbefugten Zugriff zu verhindern, auch wenn das Passwort bekannt ist.

SOCIAL MEDIA

Standortverfolgung auf Social Media

Social-Media-Plattformen bieten zahlreiche Möglichkeiten zur Standortverfolgung. Zum Schutz der Privatsphäre ist es wichtig, sich dieser Funktionen bewusst zu sein und die entsprechenden Einstellungen zu überprüfen.

Standort-Tags und Check-ins

Viele Plattformen ermöglichen es, Beiträge mit Standorten zu versehen. Diese Informationen sind je nach Einstellungen oft öffentlich sichtbar oder für Freunde zugänglich. Vor dem Posten sollte stets überprüft werden, welche Standortdaten geteilt werden.

Geotagging in Fotos

Fotos enthalten häufig GPS-Koordinaten in den Metadaten, die den genauen Aufnahmeort verraten können. Diese Funktion kann in der Kamera-App deaktiviert oder die Metadaten vor dem Upload entfernt werden.

Stories und Hintergründe

Auch ohne explizite Standortangaben können Hintergründe, Wahrzeichen oder lokale Details in Fotos und Videos den Aufenthaltsort verraten. Vorsicht bei der Wahl der Kulissen ist sinnvoll, da Dienste wie Google Image Search oder Geoguesser Informationen daraus ableiten können.

Live-Standort in Messenger

Apps wie WhatsApp, Telegram, Facebook Messenger oder Snapchat Snap Map bieten Live-Standort-Sharing. Regelmässig sollte geprüft werden, ob diese Funktion aktiv ist und mit wem der Standort geteilt wird; unnötige Freigaben sollten sofort beendet werden.

Aktivitätenmuster

Regelmässige Posts zu bestimmten Zeiten oder von bestimmten Orten können Routinen und Aufenthaltsorte offenlegen. Es lohnt sich, nicht zu viele Muster preiszugeben, die Rückschlüsse auf Bewegungsprofile zulassen.