IDENTIFIZIEREN SIE IHR RISIKOPROFIL

VIER NIVEAUS

A GRUNDRISIKO

Politische Berichterstattung auf Basis offizieller Informationen

SELBSTSCHUTZ

B ERHÖHTES RISIKO

Recherche-Journalismus, Berichterstattung auf Basis frei zugänglicher Informationen

+ DATENSCHUTZ

C STARK ERHÖHTES RISIKO

Berichterstattung zu Korruption, Waffen-, Menschen-, Drogenhandel, Migration, Extremismus, Betrug, religiöse Gruppierungen, Randgruppen, autoritäre Regime, Geheimdienste

+ QUELLENSCHUTZ

D SEHR HOHES RISIKO

Berichterstattung wie auf Stufe C, aber zugleich auf Basis vertraulicher / geheimer Informationen

+ GESICHERTE ARBEIT OFFLINE

A BASISMASSNAHMEN

01 Betriebssysteme und Programme wöchentlich aktualisieren und regelmässige Backups machen.

02 Passwörter verwenden, die lange & zufällig sind. Passwort-Manager verwenden, der mit zweitem Faktor (Passkey o. App für Einmalcodes) gesichert ist. Passwörter nie im Browser speichern!

03 Alle Konten über einen zweiten Faktor sichern (Fido2, Passkey, App mit Einmalcode OTP oder SMS/E-Mail).

04 Kommunikation über sichere Kanäle wie Signal, Threema oder Element. Apps mit Registrierungssperre sichern.

05 Zugeschickte Links, QR-Codes & Dokumente prüfen: Was spricht für deren Legitimität? Warnsignale? Wo immer möglich die Herkunft durch Anruf, Rückfrage auf einem anderen Kommunikationskanal prüfen.

06 PC-Harddisk verschlüsseln. (Bitlocker bei Windows, FileVault bei Mac, Luks bei Linux.) Externe Speicherplatten ebenfalls verschlüsseln.

07 Öff. WLAN meiden. Nutzung nur mit VPN (WireGuard) zum Heim-/Geschäftsnetzwerk o. mit VPN wie MullvadVPN, IVPN, ProtonVPN. Nie einem gratis VPN vertrauen.

08 Keine öffentlichen USB-Ladestationen verwenden.

09 Private Daten (Adresse, Geburtsdatum, Passnummer, etc.) nur wenn wirklich nötig preisgeben. Falsche Daten anzugeben ist eine Form des Selbstschutzes.

10 Keine physischen Notizen & Dokumente herumliegen lassen.

B ANONYMITÄT IM NETZ

Alle Massnahmen von Niveau A, plus:

01 Dienste anonym nutzen, Wegwerf-Mail-Adressen o. Mail-Weiterleitungen verwenden. Social-Media-Recherchen mit anonymen Profilen («Sock Puppets») durchführen.

02 Keine persönlichen Daten in KI-Modelle eingeben; das sind keine Suchmaschinen. Google nur für spezifische Zwecke nutzen, ansonsten DuckDuckGo oder StartPage.

03 Logout von Google oder Social Media, wenn nicht genutzt. Browser-Tabs schliessen, wenn nicht genutzt.

04 Tracking limitieren mit PrivacyBadger / uBlockOrigin. Browser-Sicherheit auf «strikt». Cookies löschen. Achtung bei Erweiterungen: Risiko, Gerät zu infizieren.

05 Keine Bemerkungen zu laufenden Recherchen auf Social Media oder im Small Talk. Vorsicht bei Gesprächen an öffentlichen Orten. Regelmässige offline-Backups machen.

C QUELLENSCHUTZ

Alle Massnahmen von Niveau A und B, plus:

01 Privatadresse bei Gemeinde, Post, Teledata sperren; Autonummer beim STVA sperren. Sicherstellen, dass Umfeld, Familie o. Arbeitgeber Privatadresse nicht herausgeben.

02 Sensible Kommunikation verschlüsseln. Signal, Threema oder Element verwenden. Apps mit PIN / Biometrie verriegeln. Bei Signal: Selbst-löschende Nachrichten.

03 WhatsApp nur mit Wegwerf-Nummer verwenden, Zugriff auf Kontakte blockieren. Telegram nur auf Wegwerf-Handy.

04 Erhaltene Dateien zur Sicherheit vor dem Öffnen mit https://dangerzone.rocks in sichere PDFs umwandeln.

05 Erhaltene Links nur in einer Virtual Machine / einem Live System anklicken. Bei nicht-sensitiven Daten vorher über virustotal.com oder joesandbox.com testen,

06 E-Mails vom Server nehmen und offline speichern.

07 In journalistischer Zusammenarbeit: Cloud-Daten verschlüsseln mit Cryptomator. Falls möglich für Recherche eigenen Server verwenden (Nextcloud oder Cryptpad).

08 Sensitive Daten offline speichern auf zwei verschlüsselten Harddisks. Für Projekte jeweils verschlüsselte Container anlegen mit VeraCrypt. Backup nicht vergessen!

09 Namen & Kontaktdaten von Quellen nie online speichern (weder im Telefonbuch noch in der Mail-App). Code-Namen sind eine einfache, sinnvolle Massnahme.

10 Handy wöchentlich neu starten (gegen nicht-persistente Viren). iPhone: Lockdown-Mode aktivieren. Android: Verstärkte Sicherheit aktivieren.

11 Beim Treffen mit einer Quelle Handy zuhause lassen oder frühzeitig in Faraday-Bag versorgen. Bei Sitzungen Handy ausser Hörweite oder im Faraday-Bag lassen.

12 Keine sensitiven Daten oder vertrauliche Treffen in der Online-Agenda am PC oder auf dem Handy abspeichern.

13 Handy, mit dem man mit Quellen in Kontakt steht, mit komplexerem Passwort statt 6-stelligem PIN sichern.

14 Bei absehbarem Behördenkontakt oder drohender Kontrolle: Handy und PC ausschalten. Behörden dürfen mit Fingerabdrücken / Fotos biometrische Sicherung umgehen, aber nicht Passwort-Herausgabe erzwingen.

15 Bei behördlicher Beschlagnahmung der Geräte: Redaktionsgeheimnis geltend machen. Bei richterlicher Anordnung auf Beschlagnahmung: Siegelung verlangen.

D GESICHERTE UMGEBUNG

Zwingend alle Massnahmen von A, B und C, plus:

01 Kameras an PC und Handy abdecken.

02 Wenn möglich an gesichertem und gesondertem Ort arbeiten.

03 Arbeit mit sensitiven Daten nur offline! Datenimport/-export über verschlüsselte ext. Festplatten. Ideales OS: Tails, auf extra eingerichtetem PC. PC nach Recherche löschen/ verschenken/ in anderem Kontext verwenden.

04 Passwörter für Recherche nie online speichern.

05 Im Kontakt mit Quellen ein Wegwerf-Handy verwenden. Dieses nach der Recherche löschen und entsorgen.

06 Keine unverschlüsselte Telefonate oder SMS.

07 Falls möglich auch Quelle mit Wegwerf-Handy ausstatten.

08 Auf Anzeichen von Kompromittierung achten: ungewöhnliche Neustarts oder «Updates», plötzlicher Abfall der Batterie- o. Geräteleistung, ungewöhnliche Verbindungsaufnahmen oder Apps.

09 Gefühl von Überwachung oder Beobachtung ernst nehmen! Mit Vorgesetzten, Kolleg:innen reden. Arbeitszeiten und Arbeitswege variieren.

10 Bei Terminen, wo eigenes Erscheinen bekannt ist, besonders wachsam sein: Gerichtstermine, öff. Auftritte, etc. Gleiches gilt bei vertraulichen Treffen mit Quellen.

RESSOURCEN

Für weitere Informationen und Ressourcen den QR-Code scannen:

REPORTER OHNE GRENZEN SCHWEIZ

DIGITALE SORGFALT FÜR MEDIENSCHAF-FENDE

Ein vierstufiges Konzept zum Schutz journalistischer Arbeit und zum Quellenschutz.

A Grundrisiko

B Erhöhtes Risiko

C Stark erhöhtes Risiko

D Sehr hohes Risiko

rsf-ch.ch

Juni 2026

REPORTER OHNE GRENZEN SCHWEIZ

LEITFADEN FÜR DIGITALE SICHERHEIT FÜR MEDIEN-SCHAFFENDE

Die Bedrohungen und nötigen Vorsichtsmassnahmen sind je nach Arbeitsweise sehr unterschiedlich. Diese Faltbroschüre schlägt deshalb ein modulares System mit vier Stufen vor, die aufbauend anzuwenden sind.

Digitale Sicherheit kann nie garantiert werden, letztlich ist jedes System angreifbar. Aber Journalist:innen können ihren Selbst- und Quellenschutz so stark verbessern, dass ein Angriff mit grösster Wahrscheinlichkeit ins Leere läuft und der Quellenschutz gewährleistet bleibt.

RSF REPORTER OHNE GRENZEN SCHWEIZ