IDENTIFIEZ VOTRE PROFIL

LES 4 NIVEAUX

A DANGER DE BASE

Couverture politique sur la base de sources officielles.

AUTOPROTECTION

B RISQUE ACCRU

Journalisme d'investigation sur la base de sources accessibles librement.

+ PROTECTION DES DONNEES

C RISQUE FORTEMENT ACCRU

Couverture de corruption, trafic d'armes, d'êtres humains ou de drogues, migration, extrêmismes, fraude, groupes religieux, régimes autoritaires, services de renseignement...

+ PROTECTION DES SOURCES

D RISQUE TRÈS ÉLEVÉ

Couverture des thèmes du niveau C et fondée sur des informations secrètes ou confidentielles.

+ HORS LIGNE

A MESURES DE BASE

01 Mises à jour hebdomadaires du système et sauvegardes régulières.

02 Gestionnaire de mots de passe pour générer des mots de passe longs et aléatoires. Protégé par un second facteur (passkey ou OTP). Jamais de mots de passe enregistrés dans le navigateur.

03 Second facteur sur tous les comptes (FIDO2, passkey, OTP ou, à défaut, SMS).

04 Communications via Signal, Threema ou Element et sécuriser l'application par code ou biométrie.

05 Vérifier systématiquement liens, QR codes et documents reçus. Confirmer la provenance par un appel ou un autre canal.

06 Chiffrer le disque dur de l'ordinateur et tous les supports de stockage externes.

07 Éviter les Wi-Fi publics. Si impossible VPN obligatoire. Jamais de VPN gratuit.

08 Ne jamais utiliser de bornes de recharge publiques.

09 Ne communiquer ses données personnelles que si indispensable. Donner de fausses données est une forme d'autoprotection.

10 Ne laisser traîner aucune note ni document papier.

B ANONYMAT EN LIGNE

Tout ce qui est préconisé au niveau A et :

01 Utiliser des adresses e-mail jetables ou des redirections. Recherches sur réseaux sociaux via des profils anonymes (sock puppets), jamais son compte personnel.

02 Ne jamais saisir de données personnelles dans des IA en ligne. Préférer DuckDuckGo, Startpage, Tor, Mullvad, Brave, LibreWolf ou Firefox à Google.

03 Se déconnecter des comptes Google et réseaux sociaux après usage. Fermer les onglets inutilisés.

04 Limiter le pistage avec Privacy Badger et uBlock Origin. Prudence lors de l'installation d'extensions, elles peuvent infecter l'appareil.

05 Ne jamais évoquer ses recherches en cours. Vigilance dans les espaces publics. Sauvegardes régulières hors ligne sur disques durs externes.

C PROTECTION DES SOURCES

Tout ce qui est préconisé aux niveaux A + B et :

01 Bloquer son adresse privée auprès de la commune, la poste et Teledata, et son numéro de plaque auprès du service des automobiles. S'assurer que proches et employeur ne la divulguent pas.

02 Toute communication sensible doit être chiffrée : utiliser Signal, Threema ou Element, avec messages éphémères activés.

03 N'utiliser Whatsapp et Telegram qu'avec un numéro jetable, sans donner accès aux contacts.

04 Convertir tout fichier reçu en PDF sécurisé via dangerzone.rocks avant ouverture.

05 N'ouvrir les liens reçus que dans une machine virtuelle ou un système live. Pour les données non sensibles : tester via virustotal.com ou joesandbox.com.

06 Rapatrier ses e-mails depuis le serveur et les stocker hors ligne.

07 Si stockage cloud nécessaire : chiffrer avec Cryptomator. Préférer un serveur personnel : Nextcloud ou Cryptpad.

08 Données sensibles stockées hors ligne sur deux disques chiffrés. Conteneurs VeraCrypt par projet. Sauvegarder.

09 Jamais de noms ni de coordonnées de sources sur le téléphone ou en ligne : utiliser des noms de code.

10 iPhone : Activer le mode de protection maximale. Android : Activer la protection renforcée. Redémarrer le téléphone chaque semaine.

11 Rendez-vous avec une source : laisser le téléphone à la maison ou dans un sac Faraday. En réunion, le garder hors de portée auditive.

12 Aucune donnée sensible ni rendez-vous confidentiel dans l'agenda numérique.

13 Protéger le téléphone dédié aux sources par mot de passe plutôt que par code PIN.

14 En cas de contact imminent avec les autorités : éteindre téléphone et ordinateur.

15 En cas de saisie par les autorités : invoquer le secret de rédaction. Si ordonnance judiciaire : exiger la mise sous scellés.

D ENVIRONNEMENT SÉCURISÉ

Tout ce qui est préconisé aux niveaux A + B + C et :

01 Couvrir les caméras de l'ordinateur et du téléphone

02 Si possible, travailler dans un lieu séparé et sécurisé.

03 Travail sur données sensibles exclusivement hors ligne. Import/export via disques chiffrés. OS recommandé : Tails, sur un ordinateur dédié. Réinitialiser complètement l'appareil après la recherche.

04 Ne jamais stocker ses mots de passe en ligne.

05 Téléphone jetable dédié aux sources. Réinitialiser ou détruire après la recherche.

06 Aucun appel ni SMS non chiffré.

07 Équiper la source d'un téléphone jetable si possible.

08 Surveiller les signes de compromission : redémarrages ou mises à jour inhabituels, chute soudaine de la batterie ou des performances, applications inconnues, connexions anormales.

09 Vous vous sentez surveillé, observé ? Prenez-le au sérieux. Contactez vos supérieurs ou collègues, variez vos horaires et trajets.

10 Vigilance accrue lors de tout rendez-vous où votre présence est connue à l'avance.

RESSOURCES

Pour aller plus loin, retrouvez des sources d'aide utiles en scannant ce QR code :

REPORTERS SANS FRONTIÈRES SUISSE

PRUDENCE NUMÉRIQUE POUR LES JOURNALISTES

Un système à 4 niveaux pour protéger votre travail et vos sources.

A Danger de base

B Risque accru

C Risque fort

D Risque très élevé

rsf-ch.ch

REPORTERS SANS FRONTIÈRES SUISSE

GUIDE DE SURVIE NUMÉRIQUE POUR LES JOURNALISTES

Les menaces et les mesures de précaution nécessaires varient fortement selon la manière de travailler. Ce guide propose un système modulaire en quatre niveaux à appliquer de manière progressive.

La sécurité numérique ne peut jamais être garantie. Mais les journalistes peuvent renforcer considérablement leur propre protection et celle de leurs sources, au point qu'une attaque ait peu de chances d'aboutir et que la protection de leurs sources soit assurée.

RSF REPORTERS SANS FRONTIÈRES SUISSE