Plan de sécurité

Le plan de sécurité est un document propre à chaque organisation qui regroupe les pratiques que celle-ci veut adopter dans le but de protéger ses membres, ses partenaires et ses contacts d'intérêt. Le plan doit être opérationnel et être facile à utiliser en cas d'urgence.

Contacts

Contacts en cas d'urgence	
Technicien en informatique	
Front Line Defenders – ligne d'urgence	+353-1-210-0489 https://www.frontlinedefenders.org/fr/emergency-contact
Access now – contact d'urgence	help@accessnow.org https://www.accessnow.org/help/#contact-us

Références de base

Quelques ressources particulièrement utiles pour établir les priorité et être des *guides pratiques.* Ces guides ont de l'information fiable, à jour et adaptée pour les défenseurs de droits humains à l'international.

a. Surveillance Self-Defense de l'Electronic Frontier Foundation
b. Security planner du Citizen Lab
c. Security in a box de Tactical Technology collective

Réunions

- Ne pas garder vos cellulaires avec vous lorsque vous êtes en réunion.
- Prendre les notes de vos réunions sur un ordinateur qui n'est pas connecté à l'internet.
- Toujours faire des réunions de travail dans un lieu sûr, pas dans un lieu public.

Sécurité opérationnelle

- Ne pas mentionner l'endroit où vous vous trouvez ou l'endroit où vous allez au téléphone.
- Ne pas partager d'information sensible au téléphone, par message texte ou encore par courriel si le courriel n'est pas chiffré. Si vous ne pouvez pas éviter cette situation, tentez de donner le moins de détails possibles et de parler en code. Sinon, se rencontrer physiquement est toujours un meilleur gage de sécurité lorsque cela est possible.Faire attention de ne pas parler de votre travail lorsque vous êtes dans un lieu public (autobus, restaurant, parc, etc.).
- Utiliser des alternatives sécuritaires à Skype comme Pidgin ou Jitsi.

Téléphonie mobile et information en transit

- Sécurisez l'accès à votre téléphone mobile : verrouillage de la carte SIM, chiffrement du disque dur et verrouillage de l'écran d'accueil
- Utiliser des applications telles qu'ObscuraCam pour prendre des photos.
- Considerez ajouter quelques applications « sécuritaires » sur vos appareils
- Pour toute information sensible, prioriser la communication via canaux sécurisés (signal en priorité, mais whatsapp est églement une option) ou une messagerie instantannée chiffrée (Jistsi ou Pidgin)
    - https://ssd.eff.org/fr/module/guide-pratique-utiliser-signal-pour-android
    - https://ssd.eff.org/fr/module/guide-pratique-utiliser-whatsapp-pour-android

- Utiliser des alternatives sécuritaires à Skype comme Pidgin ou Jitsi.
- Tout dépendant de votre contexte national, considérez utiliser un fureteur comme TOR pour naviguer. Cela rend votre pistage plus difficile et est un outils efficace pour détourner la censure.

Fichiers stockés

- Pour les doubles / backups, assurez-vous que tout appareil contenant des informations le moindrement confidentielles soient chiffrés ou qu'ils soient dans un endroit physique de confiance. Pour plus d'information sur les méthodes de protection de fichiers, visitez le site de tactical tech.
- Ayez un protocole pour la destruction de données de manière définitive
- Ayez un protocole pour récupérer des données

Mots de passe

- Ne jamais utiliser le même mot de passe pour vos appareils et vos comptes.
- Changer vos mots de passe après avoir été victime d'une cyber-attaque.
- Utiliser des phrases de passe plutôt que des mots de passe.
- Si vous êtes en mesure de le faire, utiliser des logiciels comme Keepass pour générer des mots de passe.
- Utilisez un gestionnaire de mot de passe tel que Keepass
- Lorsque c'est possible, utilisez un second facteur d'authentification