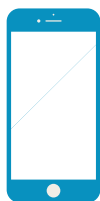


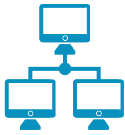





LISTE DES ETAPES A SUIVRE POUR DES MESURES PRATIQUES DE SÉCURITÉ NUMÉRIQUE POUR LES ORGANISATIONS DE LA SOCIÉTÉ CIVILE

Les informations suivantes sont un extrait de la boîte à outils Lifeline pour les OSC dans l'espace restrictif (www.csolifeline.org/advocacy-toolkit). Cela donne un bref aperçu de la façon dont les organisations de la société civile peuvent penser la sécurité numérique dans le contexte de la participation à des campagnes de plaidoyer.

Problématique	Recommandations	Conseil/ressource
Sécurité du matériel 	<ul style="list-style-type: none"> Protégez votre appareil avec un mot de passe Mettez à jour votre système d'exploitation lorsque vous y êtes invité Exécutez un logiciel antivirus Sauvegardez le contenu de vos appareils régulièrement Supprimez régulièrement les informations sensibles (envisagez un logiciel de suppression sécurisée pour effacer le contenu de l'appareil, le cas échéant) Ne branchez pas d'appareils sur des ports USB publics et ne branchez pas de clés USB inconnues sur votre appareil N'utilisez pas de réseaux Wi-Fi publics non fiables Ne laissez pas les appareils sans surveillance en public/à l'hôtel/lors de conférence 	<ul style="list-style-type: none"> Utilisez un logiciel de gestion de mots de passe pour stocker vos mots de passe : Keepass, LastPass, Dashlane Antivirus gratuits : Avira, AVG, Avast, antivirus intégré Windows Defender Supprimer vos données en toute sécurité : Bleachbit Sauvegarde sur le Cloud : <ul style="list-style-type: none"> Stockage sur le cloud chiffré de bout en bout : Tresorit Chiffrement par le client Client-side encryption https://cryptomator.org/ pour vos fichiers cloud
Chiffrement des fichiers/du disque 	<ul style="list-style-type: none"> Activer le chiffrement complet du disque sur votre appareil Utilisez Bitlocker pour Windows, Filevault pour Mac ou un logiciel de cryptage de disque open source gratuit – VeraCrypt La plupart des smartphones sont livrés avec le cryptage activé, vérifiez les paramètres pour confirmer Le cas échéant, assurez-vous de crypter les clés USB pour protéger les données qu'elles contiennent 	<ul style="list-style-type: none"> Avec le cryptage activé, votre appareil et votre mot de passe seront nécessaires pour déchiffrer les données cryptées Ressources utiles : « Keeping your Data Safe » https://ssd.eff.org/en/module/keeping-your-data-safe
Sécurité des e-mails et des réseaux sociaux 	<ul style="list-style-type: none"> Utilisez des mots de passe fort : https://xkcd.com/936/ Utilisez le même mot de passe pour un seul service uniquement Lorsque cela est possible, mettez en place l'authentification à deux facteurs Faites très attention en cliquant sur des liens ou en ouvrant des pièces jointes 	<ul style="list-style-type: none"> L'authentification à deux facteurs (2 FA) renforce la sécurité de connexion en exigeant une méthode d'authentification supplémentaire Liste des sites Web indiquant s'ils prennent en charge ou non l'authentification à deux facteurs : https://twofactorauth.org/

Problématique	Recommandations	Conseil/ressource
Services de messagerie chiffrée de bout en bout sur le Web 	Le courrier électronique chiffré de bout en bout signifie que seuls l'expéditeur et le destinataire peuvent lire les messages échangés et les données partagées entre eux.	Options gratuites sur le web : <ul style="list-style-type: none"> • Protonmail • Tutanota • Hushmail
Communication par e-mail crypté 	Si vous êtes préoccupé par la confidentialité en ligne et la sécurité de vos communications, l'une des méthodes courantes de chiffrement est la PGP. Basée sur la cryptographie à clé publique, la PGP peut s'assurer que vos données sont à l'abri des regards indiscrets et que seul le public visé peut lire le contenu de vos communications.	<ul style="list-style-type: none"> • Pretty Good Privacy (PGP encryption) (chiffrement PGP expliqué, Guide Thunderbird : https://guides.accessnow.org/tag_pgp.html) • Mailvelope (plug-in de navigateur) • Liste des applications d'e-mail qui support OpenPGP standard: https://www.openpgp.org/software/
Applications de messagerie chiffrée 	<ul style="list-style-type: none"> • Il est recommandé de savoir quelles applications sont les plus sécurisées pour votre pays/région : https://securityinabox.org/en/guide/secure-communication/ : données utilisateur et confidentialité, métadonnées, actualités récentes en matière de sécurité. (En date d'octobre 2019, l'application Signal a les normes les plus élevées) • Vérifiez les paramètres de confidentialité et de sécurité de chaque application. • Même si vous utilisez les applications les plus sécurisées, il est possible que quelqu'un puisse obtenir vos conversations sensibles ou vos fichiers personnels, car ils ont été stockés quelque part sur votre appareil. Il est essentiel de créer un processus pour réviser le contenu de l'application et supprimer régulièrement les messages sensibles (par exemple, en utilisant si possible la fonction disparition de message) 	<ul style="list-style-type: none"> • Sécurisez votre appareil mobile https://securityinabox.org/en/guide/smartphones/ • Pensez à ce dont vous avez besoin dans une messagerie sécurisée https://www.eff.org/deeplinks/2018/03/thinking-about-what-you-need-secure-messenger • Signal, l'application de messagerie sécurisée https://freedom.press/training/locking-down-signal/ • Conseils de sécurité Whatsapp (présente des problèmes de sécurité) https://www.whatsapp.com/safety • Comment sécuriser les applications de messagerie https://guides.accessnow.org/IM_Tips.html
Naviguez en toute sécurité 	<ul style="list-style-type: none"> • Mettez régulièrement à jour la version de votre navigateur. • Vérifiez l'authenticité du site Web (regardez le lien, l'icône HTTPS au début). • Sécurisez votre navigateur : https://www.eff.org/https-everywhere • Utilisez un VPN pour protéger vos informations de navigation des regards indiscrets (surtout si vous utilisez un Wi-Fi public/partagé). 	Le VPN est un tunnel crypté entre deux appareils qui vous permet d'accéder à tous les sites Web et services en ligne de manière privée et sécurisée. <ul style="list-style-type: none"> • Guide comparateur des VPN https://thatoneprivacysite.net/ • Activez votre VPN https://getoutline.org/en/home