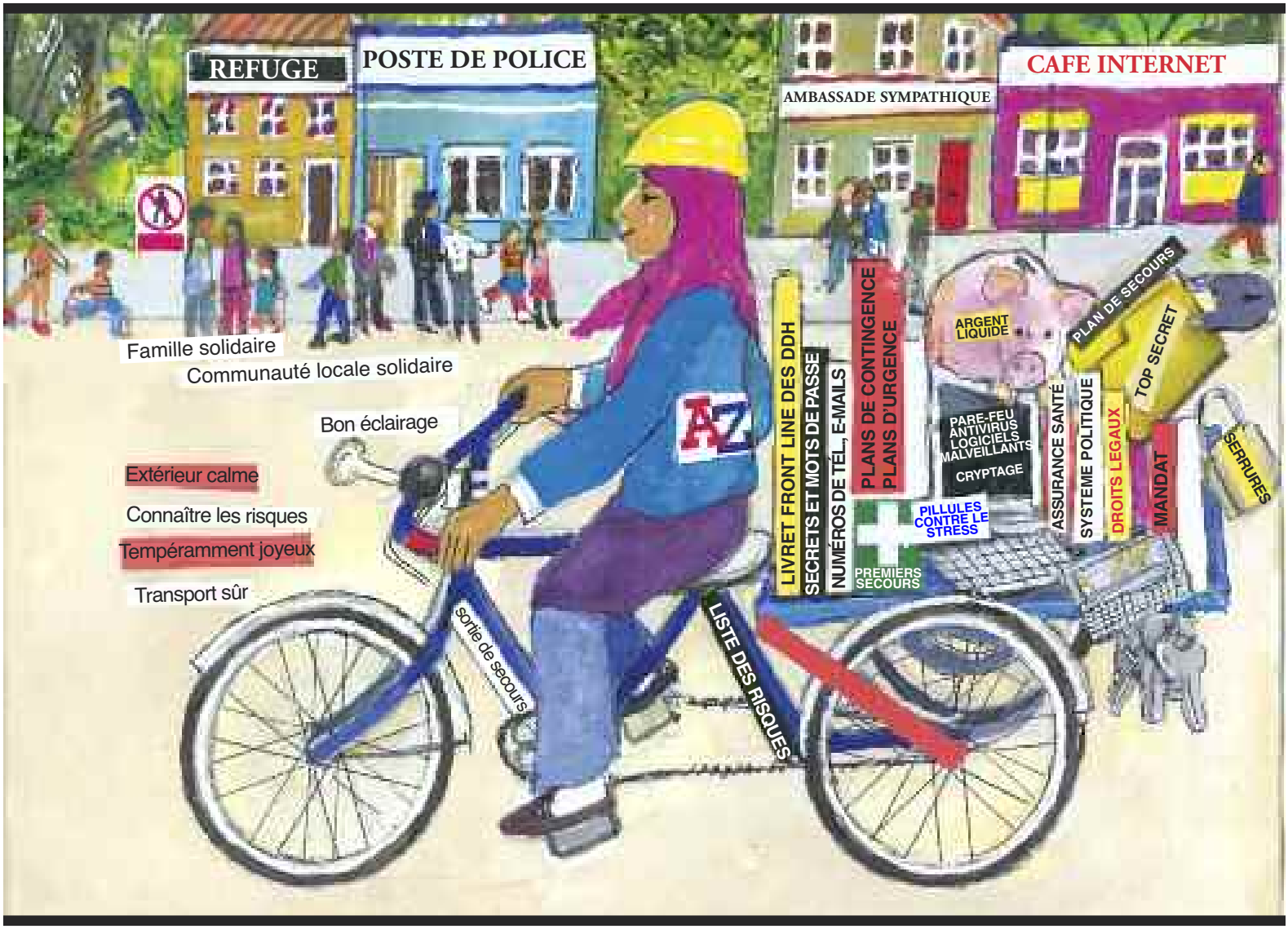
MANUEL DE SÉCURITÉ :

MESURES PRATIQUES POUR LES DÉFENSEURS DES DROITS HUMAINS EN DANGER



FRONT LINE DEFENDERS

ANNEXE 14

Sécurité des ordinateurs et des téléphones

Cette liste de contrôle n'est pas un plan de sécurité. Votre propre contexte est le facteur clé déterminant. Considérez les risques et les menaces auxquels vous êtes exposé, ainsi que toutes vos vulnérabilités. C'est simplement une liste de points importants. Pour plus d'informations, voir « Security-in-a-box » **https ://security.ngoinabox.org/fr** (Sécurité en boite).

Cette liste inclut un certain nombre de conseils qui peuvent aussi être trouvés dans la « Awareness Cards » du projet Security-in-a-box – voir le lien ci-dessus.

1. Protéger votre ordinateur contre les logiciels malveillants et les pirates

- Installez un logiciel antivirus, anti-mouchard (spyware) et un pare-feu
- N'utilisez pas de logiciels piratés – cela vous laisse vulnérable car ils ne sont pas mis à jour et vous pouvez être accusé de possession de logiciel illégal
- Songez à utiliser des logiciels libres, gratuits et de source ouverte (FLOSS), tels que Avast anti-virus, Spybot anti-spyware et Comodo firewall
- Songez à utiliser un navigateur plus sécurisé tel que Firefox, qui a une sécurité interne (pour plus d'informations, voir chapitre 1 https ://security.ngoinabox.org/fr/chapter-1, Comment protéger votre ordinateur)

2. Créer et sauvegarder des mots de passe sûrs

- Plus votre mot de passe est long, plus il sera sûr. Votre mot de passe doit dépasser 12 caractères, contenir des majuscules et des minuscules, des chiffres, des caractères spéciaux et un espace si possible.
- Il est préférable que votre mot de passe ne contienne pas de mot du dictionnaire et/ou d'informations personnelles publiques, telles qu'un anniversaire ou le nom d'un ami – mélangez les mots ou remplacez les mots avec des caractères spéciaux ou des nombres, ou mélangez des langues
- Vous pouvez utiliser une phrase – cela peut-être le titre d'un livre ou l'extrait d'une chanson (avec des caractères ou des nombres qui remplacent des lettres)
- Changez souvent votre mot de passe
- Utilisez des mots de passe forts pour différents services, mettez-les à jour régulièrement et ne partagez pas vos mots de passe (vous pouvez utiliser KeePass pour stocker tous vos mots de passe, voir chapitre 3 https ://security.ngoinabox.org/fr/chapter-3)
- Ne partagez JAMAIS vos mots de passe
- Ne laissez JAMAIS de sites web ou programmes enregistrer vos mots de passe

(Pour plus d'informations voir chapitre 3 https ://security.ngoinabox.org/fr/chapter-3)

3. Comment protéger les données sensibles stockées sur votre ordinateur

- Sauvegardez régulièrement vos fichiers et stockez la sauvegarde dans un lieu sûr
- Cachez les fichiers sensibles dans des fichiers avec des noms anodins
- Songez à chiffrer vos fichiers (bien que dans certains pays chiffrer un fichier soit illégal et risque d'attirer l'attention sur vous)
- Un programme FLOSS, appelé TrueCryp chiffre et dissimule vos fichiers
- Les fichiers supprimés peuvent toujours être récupérés par un expert – songez à utiliser des outils de suppression appelés CCleaner (pour effacer vos fichiers temporaires) et Eraser
- Si possible, vérifiez la réputation de votre fournisseur de service internet (FSI ou FAI), ou l'endroit où vous prévoyez de vous connecter, tel qu'un cybercafé
- Assurez-vous que les personnes avec qui vous communiquez sont aussi au courant de la confidentialité et de la sécurité.
- (Pour plus d'informations, voir chapitre 4 https ://security.ngoinabox.org/fr/chapter-4 et chapitre 6 https ://security.ngoinabox.org/fr/chapter-6)

4. Préserver la confidentialité de vos communications sur internet

- De nombreux comptes de courriers électroniques ne sont pas sûrs (y compris Yahoo et Hotmail) et indiquent votre adresse IP dans les messages que vous envoyez. Gmail et Riseup sont des

comptes plus sûrs, (bien que Google ait par le passé, cédé aux demandes de certains gouvernements de restreindre la liberté numérique).
- Utiliser un cybercafé peut vous exposer à la surveillance – soyez vraiment conscient des risques, qui vous contactez et quelles informations vous transmettez. Effacez votre mot de passe et l'historique de vos recherches après avoir utilisé un ordinateur.
- Utilisez "https" au lieu de "http" lorsque vous vous connectez à des services en ligne, dès que possible, afin que votre nom, mot de passe et autres informations soient transmis en toute sécurité
- N'ouvrez pas les pièces jointes transmises par quelqu'un que vous ne connaissez pas ou qui vous paraissent suspectes
- Faîtes particulièrement attention lorsque vous envoyez, recevez et consultez des informations sensibles sur internet
- Songez à utiliser un service ou programme proxy pour vous rendre anonyme sur internet. Ceci vous permet d'accéder et de communiquer sur internet en utilisant l'adresse IP d'un autre ordinateur
- Les messageries instantanées (chat) ne sont généralement pas sécurisées, mais Skype est probablement plus sûre que les autres (Pour plus d'informations, voir le chapitre 7 https ://security.ngoinabox.org/fr/chapter-7 et le chapitre 8 https ://security.ngoinabox.org/fr/node/337)

5. Réseaux sociaux
- Réfléchissez attentivement aux informations que vous partagez sur vous-même, l'endroit où vous vous trouvez, vos amis etc.
- Obtenez le consentement des autres avant de partager des informations, des documents, des photos qui les concernent et le lieu où ils se trouvent
- Assurez-vous que vos mots de passe sont sécurisés et changez-en régulièrement
- Faites attention lorsque vous accédez à votre réseau social dans un espace internet public – utilisez-les seulement si vous pouvez leur faire confiance. Effacez vos mots de passe et votre historique d'internet après avoir utilisé internet dans un lieu public
- Lisez et comprenez les documents Contrat de Licence Utilisateur Final (CLUF)- EULA en anglais, les conditions d'utilisation et/ou les lignes directrices concernant confidentialité. Ces documents peuvent changer dans le futur, il est donc important de les revoir régulièrement
- Assurez-vous que vous connaissez bien les paramètres de confidentialité de votre compte de réseau social. Ne vous fiez pas aux paramètres par défaut – personnalisez vos paramètres et revoyez-les régulièrement car le service peut effectuer des changements
- Soyez vigilants lorsque vous installez des applications suggérées par les services du réseau social. Utilisez ces applications uniquement si vous faites confiances aux sources, informez-vous des informations qu'elles vont exposer et assurez-vous de garder le contrôle des informations sortantes vous concernant (Pour plus d'informations, https ://security.ngoinabox.org/fr/node/1945)

6. Sécurité des téléphones portables
- La configuration et les technologies actuelles qui entourent les téléphones portables (y compris les SMS et les appels vocaux) ne sont pas sûrs – votre emplacement peut être déterminé et vos communications interceptées, réfléchissez donc toujours à la façon la plus sûre de communiquer des informations importantes
- Le téléphone le plus sûr est bon marché, non enregistré, sans abonnement dont vous pouvez vous débarrasser après utilisation
- Activez le blocage de votre téléphone par mot de passe ou code
- Ne sauvegardez pas d'informations sensibles sur votre téléphone, ou si c'est déjà fait, codez-les
- Soyez toujours conscient de votre environnement lorsque vous utilisez votre téléphone portable, et abstenez-vous de l'utiliser dans des lieux ou des situations risqués
- Assurez-vous que toutes les informations du téléphone soient effacées avant de le vendre ou de le faire réparer
- Détruisez les téléphones inutilisables ou les anciennes cartes SIM avant de vous en débarrasser
- Lorsque vous travaillez avec d'autres personnes ou des organisations, et que vous devez transmettre des informations sensibles, songez à avoir un téléphone ou une carte SIM différents pour votre usage personnel ou professionnel (pour plus d'informations, voir https ://security.ngoinabox.org/en/chapter-9)