10. GESTION DE L'INFORMATION ET SÉCURITÉ INFORMATIQUE

> **CHAPITRE 1.11** NMP
LA SÉCURITÉ, LA COMMUNICATION ET LES TECHNOLOGIES DE L'INFORMATION

> **CHAPITRE 3.3** NMP
LA SÉCURITÉ DE LA GESTION DE L'INFORMATION

Ce chapitre sera utile aux facilitateurs si des risques pour la sécurité des données informatiques conservées par les défenseurs ont été décelés pendant l'évaluation préalable à la formation ou pendant la formation en elle-même. Mais plus généralement, cette session est principalement destinée à sensibiliser les participants à un aspect spécifique de la sécurité des technologies de l'information (TI) (voir les objectifs ci-dessous). En fonction du profil de risque informatique de l'organisation, de ses besoins de formation et de la configuration du processus de développement de capacités, ce thème peut être traité soit comme une partie d'une session de formation consacrée à la fois aux dimensions physique et informatique de la sécurité (qui sont liées), soit comme une introduction à un module de formation séparé et plus détaillé consacré à la sécurité informatique. **Les facilitateurs doivent toutefois s'assurer que l'analyse de risques réalisée par les DDH couvre bien les deux dimensions et que les plans de développement de capacités tiennent compte des liens qui les unissent. Dans le cas contraire, les sessions ne seront pas pertinentes ou ne répondront pas aux risques encourus par les DDH.**

OBJECTIFS D'APPRENTISSAGE

> Sensibiliser les participants à l'importance de la sécurité des technologies de l'information, en mettant en évidence les risques associés à la perte ou au vol de données informatiques.

> Indiquer des ressources qui aideront les DDH à améliorer la sécurité de leurs données.

MESSAGES CLÉS

> Les risques pour la sécurité des informations détenues par les DDH ne proviennent pas seulement de défaillances techniques et d'attaques ciblées commises pour avoir accès ou pour détruire ces informations, ils proviennent aussi de pratiques de communication négligentes.

> En protégeant l'accès aux informations et en faisant régulièrement des sauvegardes (back-ups) des informations, il est possible de réduire le risque de perte ou de vol de ces données.

LA SESSION

DIFFICULTÉS POUVANT SURVENIR DURANT LA SESSION :

→ Les facilitateurs doivent avoir une connaissance de base des outils de sécurité informatique (au niveau de l'utilisateur), et en particulier de ceux qui peuvent aider à minimiser les risques de perte de données et d'accès non-autorisé aux données.

→ Même s'ils utilisent des ordinateurs et d'autres appareils informatiques régulièrement, certains défenseurs n'ont qu'une compréhension très basique de leur fonctionnement. Faites en sorte que les discussions soient les plus simples possibles et évitez les termes techniques qui peuvent être déroutants ou être mal compris. Si ces termes ne peuvent pas être évités, expliquez-les avec un vocabulaire simple, non-technique, et pensez à utiliser des illustrations. Faites en sorte que ces explications restent visibles pendant toute la session, pour pouvoir y faire référence ultérieurement.

LA SESSION ÉTAPE PAR ÉTAPE :

Durée	Durée totale	Activité	Outil / méthode / matériel
05´	5´	**Introduction:** • Objectifs et structure de la session.	Préparez les points à l'avance sur un paper-board ou dans une présentation PowerPoint.
10´	15´	**Risques pour la sécurité des communications**	Paper-board
45´	60´	**Activité** : back-up de données et protection face à un accès non-autorisé	Paper-board Post-it autocollants
		Montrer aux participants comment utiliser les outils de sécurité informatique (activité facultative)	Ordinateur portable Clé USB avec la dernière version d'installation des outils « Security in a Box »
		DURÉE : COMPTER 60 MINUTES (1 HEURE) PLUS UNE PAUSE DE 20 MINUTES.	

ACTIVITÉS D'APPRENTISSAGE

Cette session s'intéresse principalement au risque de perte de données (due à l'absence de sauvegardes et au vol d'informations), et aide les participants à identifier leurs vulnérabilités existantes liées à leur façon de gérer les informations stockées sur des outils informatiques. Ces informations sont appelées « données entreposées ». La session parlera de procédures simples mais fondamentales et présentera des outils et des mesures informatiques et non-informatiques pouvant améliorer la capacité des DDH à gérer le risque.

Les facilitateurs trouveront dans les **chapitres 1.11 et 3.3 du NMP** du matériel d'enseignement pouvant les aider à préparer cette session. Comme les menaces et les technologies de protection des données informatiques évoluent très rapidement, nous encourageons les facilitateurs à se familiariser également avec d'autres sources d'informations sur ce thème. Une liste non-exhaustive de ressources complémentaires pour vous documenter plus en profondeur est indiquée à la fin de cette section.

RISQUES POUR LA SÉCURITÉ DES COMMUNICATIONS

Pour introduire ce thème, le facilitateur peut commencer par demander aux participants quels moyens ils utilisent pour communiquer avec leurs collègues et avec d'autres personnes extérieures à l'organisation ou à la communauté. Ecrivez la liste des moyens de communication cités sur votre paper-board. S'ils ne l'ont pas mentionné, rappelez aux participants que le fait de parler face-à-face est peut-être la manière la plus fréquente de communiquer (parfois par inadvertance) des informations sensibles sur leur travail. La sécurité et la protection des informations n'est donc pas qu'une question de technologies de communication sophistiquées.

Ensuite, lancez une réflexion collective avec les participants sur les différentes façons d'accéder légalement à des informations ou à des communications, mais aussi de les manipuler. Par exemple : dans une conversation face-à-face, par téléphone, ou en tirant profit du cadre de sécurité physique du bureau. Inspirez-vous des informations figurant dans le **chapitre 1.11 du NMP**.

Si les participants considèrent que leurs conversations face-à-face ou par téléphone portable risquent d'être écoutées, recommandez-leur d'inclure dans leurs plans de sécurité des protocoles pour la transmission d'informations sensibles par des communications de ce type. Vous pouvez renseigner le chapitre 1.11 du NMP comme aide-guidance.

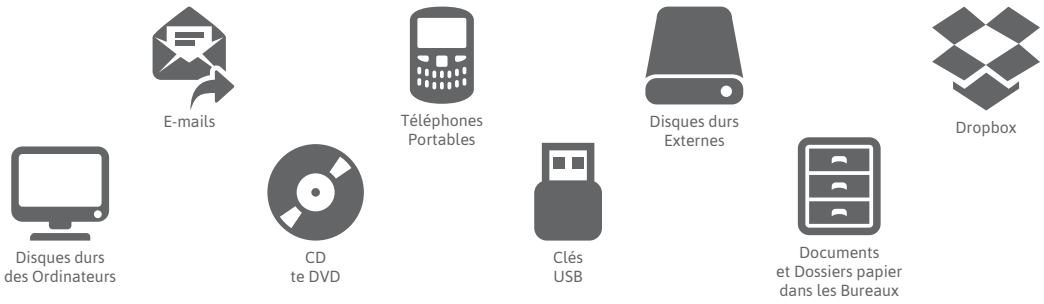
Passez ensuite à un aspect différent de la sécurité des informations en demandant aux participants le degré d'importance des informations qu'ils conservent sous format numérique (e-mails, rapports, coordonnées de partenaires et de bénéficiaires de services, etc.) Si les participants attribuent une grande importance à ces informations, demandez-leur de citer (ou indiquez-leur, s'ils n'y parviennent pas seuls) plusieurs façons dont ils risquent de perdre ces informations (p.e. suite à une erreur technique, suite à une perte ou un vol de matériel, ou suite à un accès non-autorisé).

ACTIVITÉ : BACK-UP DE DONNÉES ET PROTECTION FACE À UN ACCÈS NON-AUTORISÉ [1]

En fonction de ce qui a été vu lors des sessions précédentes réalisées avec les participants et des discussions sur les risques liés à la sécurité des informations, faites un lien avec le risque de perte de données et ce qu'il peut signifier pour les DDH et les personnes avec et pour qui elles travaillent. Demandez aux participants quelles mesures stratégiques ad hoc ils appliquent actuellement pour éviter la perte de leurs données.

Dessinez une matrice (voir ci-dessous) sur deux feuilles de paper-board collées ensemble, et affichez-la de manière bien visible sur un mur. Expliquez aux participants qu'il s'agit d'un exercice de localisation des informations dont le but est de visualiser le type d'informations qu'ils possèdent et l'endroit où elles sont stockées. Cet exercice constituera une base pour élaborer une stratégie de réduction des risques de perte de données.

Commencez par demander aux participants de faire la liste des différents endroits où sont stockées leurs informations. Si aucune suggestion n'est avancée, vous pouvez citer les éléments suivants :



Ajoutez les endroits cités par les participants dans la ligne supérieure de la matrice. Demandez ensuite aux participants quel type d'informations ou de données ils stockent dans chacun de ces endroits.

Exemple :

Écrivez un exemple sur un carton ou un post-it et placez-le dans la bonne partie de la matrice (p.e. des rapports stockés sur les disques durs des ordinateurs).

Demandez-leur s'il existe d'autres copies de ces données quelque part. Si oui, utilisez un post-it de couleur différente et placez-le à l'endroit où est stockée la copie. Profitez-en pour faire la différence entre le document original et les copies sauvegardées (ou back-ups). (Dans l'exemple ci-dessous, le orange indique le document original et le gris clair indique la sauvegarde.)

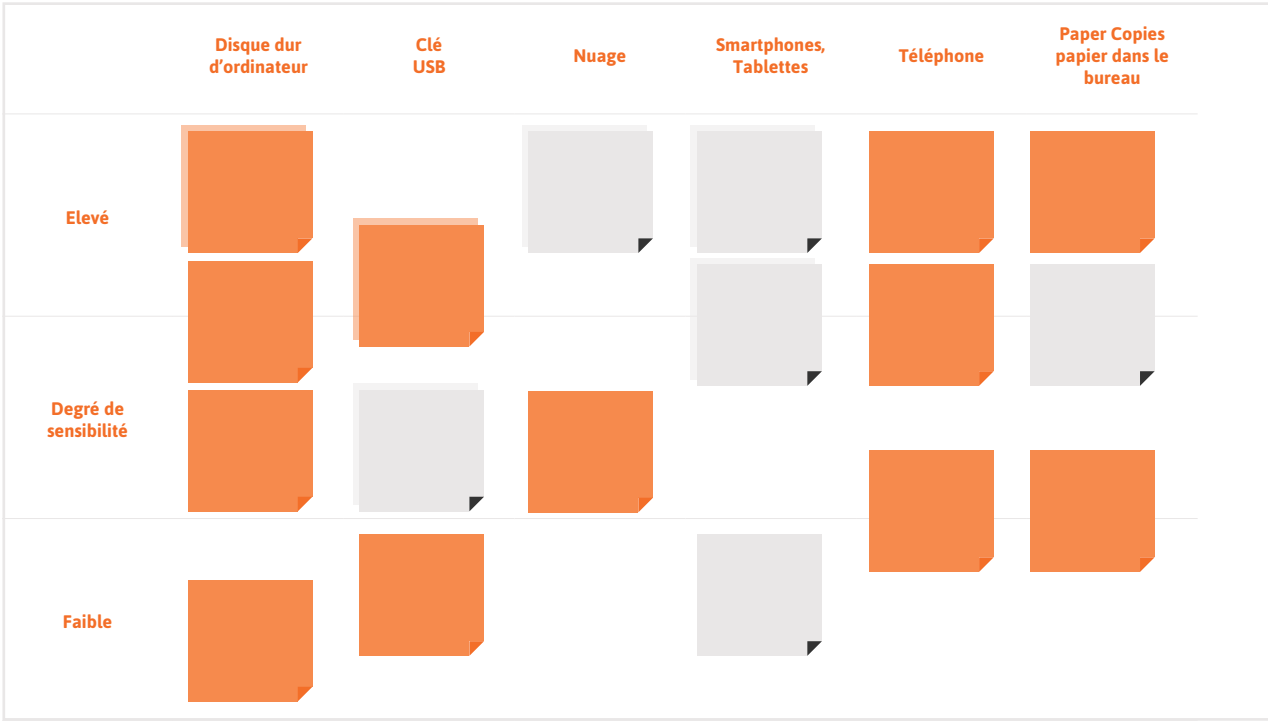
1 Cette activité est adaptée des travaux de Samir Nassar, Daniel Ó Clunaigh et Ali Ravi, du Collectif Tactical Technology, pour le projet LevelUp. Nous conseillons également aux facilitateurs de lire le **chapitre 3.3 du NMP** pour plus d'informations.

Répétez ce processus en y ajoutant une dimension supplémentaire : la sensibilité des données (c'est-à-dire les données qui en cas de perte ou d'utilisation abusive risquent de causer des dommages considérables soit aux DDH soit aux personnes avec qui ils travaillent, comme par exemple des victimes de violences de genre). Ajoutez donc un second axe (vertical) représentant la sensibilité. Plus haut un carton sera placé sur le tableau, plus les données représentées seront sensibles. Placez les deux cartons ou post-it sur l'axe représentant leur degré de sensibilité. Si le temps disponible est limité, vous pouvez réduire cette partie de l'exercice à un ou deux exemples.

Prévoyez 5 à 10 minutes pour cet exercice. Il est conseillé au facilitateur d'observer chaque groupe et de repérer les caractéristiques intéressantes (p.e. quand il y a une très grande dépendance à un seul appareil, quand il y a très peu de copies, etc.) A la fin de l'exercice, chaque équipe doit avoir complété la matrice.

Allow 5-10 minutes for this exercise. It is advisable for the facilitator to observe each group and identify interesting characteristics (e.g. where there is a particularly large dependence on one device or copies/back-ups are few, etc.). By the end of the exercise each team should have completed a matrix.

Voilà à quoi pourrait ressembler le résultat :



Expliquez que cette matrice donne une idée d'où sont situées les données. Demandez aux participants si ce sont là toutes les données que leur organisation ou communauté produit. La réponse est non, bien entendu, ce n'est qu'un faible pourcentage.

Expliquez que cette matrice donne une idée d'où sont situées les données. Demandez aux participants si ce sont là toutes les données que leur organisation ou communauté produit. La réponse est non, bien entendu, ce n'est qu'un faible pourcentage.

Pour montrer la vulnérabilité qu'entraîne cette situation, demandez aux participants ce qui peut faire en sorte qu'un ordinateur cesse de fonctionner.

- → Les virus et les programmes malveillants peuvent détruire les données stockées sur un ordinateur.
- → Les ordinateurs peuvent être volés ou confisqués.
- → Les problèmes d'infrastructures comme les pannes de courant peuvent endommager les ordinateurs.

Vous pouvez demander aux participants qui ont déjà été affectés par un de ces problèmes de lever la main.

Demandez-leur ensuite ce qui arriverait aux données si un des événements cités ci-dessus devait arriver. Pour rendre les choses plus marquantes, vous pouvez arracher brutalement chacun des post-it figurant dans cette colonne et les jeter au sol. Les post-it restants représentent alors toutes les informations qui leur restent.

Demandez aux participants de réfléchir à ce qui pourrait être fait pour éviter une telle situation. Ils répondront probablement qu'ils doivent conserver plus de copies dans des endroits différents. Expliquez que c'est ce qu'on appelle faire une sauvegarde, ou un back-up.

Si vous avez assez de temps, penchez vous maintenant sur le thème de la sensibilité des données. Si possible, prenez la matrice d'un autre groupe comme exemple. Si tous les participants ont réalisé l'exercice ensemble, choisissez une autre colonne de la matrice. Demandez aux participants quel serait l'impact si leur téléphone, leur disque dur ou leur clé USB était volé(e). Prenez les post-it collés dans la colonne concernée, mais gardez-les en main et lisez-les à voix haute. Ceci illustre le fait que quelqu'un d'autre est désormais en possession des informations contenues sur l'appareil. Demandez aux participants ce que cette personne pourrait faire avec les données et dans quelle situation les DDH se retrouveraient dans ce cas.

Sur base de l'activité précédente consacrée à la sauvegarde des données, demandez aux participants de citer au moins trois des cinq actions qu'ils doivent entreprendre pour réduire les vulnérabilités qu'ils ont identifiées. Ces actions peuvent être informatiques (citez le programme Cobian Backup) ou non-informatiques (collecter des fonds pour acheter des supports de sauvegarde, créer des protocoles de sauvegarde, etc.). En fonction de la composition du groupe, demandez aux participants d'entreprendre ces actions au niveau organisationnel (pour les groupes homogènes) ou au niveau individuel (pour les groupes hétérogènes).

- → Cette activité est essentiellement une analyse de risques concernant les données que les DDH possèdent et sont susceptibles de perdre. Elle aide à identifier les vulnérabilités existantes.
- → Pour faire cet exercice, il faudra idéalement un niveau élevé de confiance au sein du groupe de participants, ou un groupe pouvant aisément être divisé en plus petits groupes relativement homogènes. Pour les groupes où le niveau de confiance est faible et pour les groupes hétérogènes dont les participants ne se connaissent pas bien et ne souhaitent peut-être pas dévoiler aux autres quelles informations ils possèdent et comment elles sont stockées, il faudra modifier l'exercice pour le rendre plus général, tout en maintenant les mêmes enseignements.

MONTRER AUX PARTICIPANTS COMMENT UTILISER LES OUTILS DE SÉCURITÉ NUMÉRIQUE ACTIVITÉ FACULTATIVE)

Si elle est réalisée, cette partie de la session a pour but de remédier aux vulnérabilités qui ont été identifiées et de renforcer les capacités des participants à faire face au risque de perte ou d'accès non-autorisé aux « **"données entreposées "** (c'est-à-dire les données stockées sur des appareils, voir plus haut) et aux **"données en mouvement "**.

On qualifie de **"données en mouvement "** les échanges d'informations via internet, e-mail, téléphone portable ou médias sociaux qui ont fréquemment lieu entre les DDH dans le cadre de leur travail et de leur communication avec des parties prenantes. Un des principaux risques est que des adversaires parviennent à accéder à des informations sensibles sans autorisation, que ce soit en piratant des comptes d'utilisateurs, en épiant les DDH ou en interceptant les informations par d'autres moyens techniques. En aidant les DDH à identifier les vulnérabilités existantes dans ce domaine, vous les encouragerez à établir des procédures pour créer et conserver des mots de passe forts, utiliser des canaux de communication plus sûrs (cryptés), et s'assurer que les informations échangées soient elles-mêmes sécurisées (en les cryptant).

Pour remédier aux vulnérabilités identifiées pendant ces exercices, les facilitateurs devront se familiariser avec les concepts suivants :

- La création de mots de passe forts (pour les comptes de courrier électronique, les ordinateurs, les fichiers, etc.)
- Le cryptage des données entreposées et des données en mouvement
- La protection de la vie privée dans la communication via internet
- La sauvegarde d'informations
  Nous encourageons les facilitateurs à présenter ces outils de sécurité informatique aux participants en utilisant les ressources proposées sur le site Security in a Box **https://securityinabox.org** Voyez également la section Conseils aux facilitateurs, ci-dessous.

Pour travailler avec les ressources proposées par le site Security in a Box, les facilitateurs doivent prendre note des conseils suivants : **https://securityinabox.org**, les facilitateurs doivent prendre note des conseils suivants

Be conversant with the use of the tools yourself by making it a part of your own security strategy: strong password practices, encrypting information stored on devices or sent via the internet or mobile networks, and regular data back up.[2]

- Maîtrisez vous-mêmes l'utilisation des outils en les incluant dans votre propre stratégie de sécurité : choisissez des mots de passe forts, cryptez vos informations stockées sur des appareils ou envoyées par internet ou par réseau de téléphonie mobile, faites des back-ups réguliers
- Lisez attentivement la section correspondante du « Livret pratique » que vous trouverez sur la page **https://securityinabox.org/fr/howtobooklet.** Ce livret indique à quelles vulnérabilités s'adresse chaque outil et illustre ces explications par des études de cas que vous pourrez à votre tour adapter au contexte de travail de vos participants.
- Soyez conscient que les outils offrent différentes fonctions, et ne présentez que celles qui correspondent aux risques identifiés par les participants, afin de ne pas surcharger ceux-ci d'informations qu'ils n'auront peut-être jamais l'occasion d'utiliser.

2 Etant donné la rapidité de l'évolution dans ce domaine, tenez-vous au courant des derniers développements en termes de sécurité numérique et de protection des données privées en visitant régulièrement les sites Security in a Box, AccessNow (**www.accessnow.org**), Ono (**https://onorobot.org**) a), et d'autres sites de référence. Si vous en avez l'occasion, suivez une formation consacrée à la sécurité numérique. Cela vous permettra d'améliorer vos capacités d'utilisation des outils, d'en découvrir d'autres, et d'améliorer vos compétences de facilitateur dans ce domaine.

- → Lors du choix du local de la formation, vérifiez qu'il y ait bien un accès constant à l'électricité et des solutions de dépannage (comme des générateurs) pour vous assurer que la formation ne sera pas interrompue par des pannes de courant.
- → Téléchargez la dernière version des outils que vous voulez présenter sur le site Security in a Box avant la session de formation, et enregistrez-les sur votre ordinateur ou sur un espace de stockage portable pour les utiliser au cours de vos présentations et pour que les participants puissent les copier. Cette précaution permettra d'éviter les retards si la connexion internet ne permet pas aux participants de télécharger le logiciel rapidement pendant la session de formation.
- → Avant la session, testez les installations et tous les éléments que vous prévoyez de présenter, pour être certain qu'ils fonctionnent correctement sur votre ordinateur. Ceci est essentiel pour que vous soyez en mesure d'expliquer le processus d'installation et les différentes fonctions aux participants avec l'aide d'un projecteur.
- → Pour éviter la propagation de virus informatiques, demandez aux participants s'ils ont un programme antivirus et demandez-leur de vérifier qu'il est bien à jour. Vous pouvez également prévoir une copie de l'antivirus gratuit Avast pour les participants qui n'ont pas d'antivirus ou dont le programme n'est pas à jour.
- → Si les participants utilisent leur ordinateur personnel ou professionnel pendant la session de formation (plutôt que de louer des ordinateurs qui ont fait l'objet d'un entretien et d'un nettoyage pour éliminer les éventuels logiciels malveillants ou superflus), il sera probablement plus compliqué pour eux d'installer les outils ou d'effectuer certaines tâches, en raison des paramètres différents de leurs ordinateurs. Comme vous n'êtes pas technicien et que le temps disponible est limité, n'essayez pas de résoudre ces problèmes pendant la session. Demandez plutôt aux participants qui rencontrent un problème de travailler avec un de leurs collègues, de manière à faire en sorte que les objectifs de la session puissent être atteints pour l'ensemble du groupe.
- → Il est souhaitable d'avoir au moins un ordinateur pour deux participants, pour que ceux-ci puissent suivre vos instructions et s'essayer eux-mêmes aux outils.
- → Utilisez la section correspondante des « Guides pratiques » pour vous préparer à faire la démonstration des outils (**https://securityinabox.org/fr/handsonguides**). Entraînez-vous à l'avance et anticipez les questions. Utilisez un vocabulaire simple et illustrez la pertinence des outils pour répondre aux risques identifiés par les défenseurs .[3]
- → Quand vous présenterez les outils, demandez aux participants de fermer toutes les autres applications et de suivre votre première démonstration sur l'écran de projecteur. Demandez-leur ensuite de faire la même chose sur leur ordinateur en suivant la manœuvre que vous montrez à l'écran. Enfin, demandez leur de répéter la même procédure sans guidance. Plus ils auront d'opportunités de s'exercer à l'utilisation des outils, plus l'expérience d'apprentissage sera fructueuse.
- → L'utilisation d'outils de sécurité numérique peut se révéler compliquée pour de nombreux DDH. Expliquez-leur les bénéfices qu'ils tireront de l'utilisation de ces outils en réponse aux risques auxquels ils sont confrontés. Dites-leur que plus ils utiliseront les applications, plus ils se sentiront à l'aise avec elles.
- → Renvoyez les participants aux ressources proposées sur le site Security in a Box **https://securityinabox.org** pour découvrir d'autres outils et obtenir d'autres conseils. Tous ces outils sont gratuits, et la boîte à outils est mise à jour régulièrement..
- → Le Kit d'aide d'urgence en sécurité numérique pour les défenseurs des droits humains présente des scénarios de risque spécifiques et propose des conseils de mesures immédiates pour remédier à la situation. Il propose également des liens vers des ressources complémentaires comme Security in a Box et d'autres initiatives (**https://www.apc.org/en/irhr/digital-security-first-aid-kit**).

3 Level Up! est une ressource en cours d'élaboration pour les formateurs en sécurité numérique. Elle proposera des informations aidant à préparer et à donner des sessions de formation à la sécurité numérique. Consultez le site **http://level-up.cc** pour obtenir des idées et des conseils.

CONCLUSION

> Rappelez aux participants que l'activité consacrée à la sauvegarde et à la perte ou au vol de données a pour but de les éclairer quant aux endroits où sont stockées leurs données, et à la partie de ces données qui sont sensibles et qui doivent donc être protégées d'un éventuel accès non-autorisé et sauvegardées en back-up pour éviter qu'elles n'existent qu'en un seul endroit. Demandez-leur de rappeler les enseignements-clés et les lectures complémentaires nécessaires, qu'ils doivent inclure dans leurs plans d'action.

> Si vous avez parlé d'outils spécifiques de sécurité informatique, demandez aux participants de rappeler à quels risques ces outils répondent et pourquoi ils pensent qu'il y a lieu de les utiliser. Pour vous assurer de la bonne application des outils, pensez à donner aux participants des travaux pratiques, pour qu'ils puissent s'entraîner et se familiariser à leur usage.

RESSOURCES COMPLÉMENTAIRES

> Association for Progressive Communication (2013), « Digital Security First-Aid Kit for Human Rights Defenders. Voir : **https://www.apc.org/en/irhr/digital-security-first-aid-kit**

> Front Line Defenders (2009), « Digital Security and Privacy for Human Rights Defenders. Voir: **http://www.frontlinedefenders.org/files/en/esecman.en_.pdf**

> Tactical Tech Collective, «Me and My Shadow»Voir: **https://myshadow.org/**. Ressources et outils destinés à limiter les informations laissées derrière soi en utilisant internet.

> Level Up! Une boîte à outils pour les formateurs en sécurité informatique. Voir : **http://www.level-up.cc**.

> Le collectif Technical Tech et Front Line ont développé la boîte à outils de référence Security in a Box **http://securityinabox.org** disponible en ligne et sous forme de livre ou de DVD. Nous vous recommandons d'utiliser la version en ligne du logiciel, qui est la plus à jour. Securityinabox.org traite les questions suivantes:

- **Protéger votre ordinateur contre les logiciels malveillants et les pirates**
- **Assurer la sécurité physique de vos données**
- **Créer et sauvegarder des mots de passe sûrs**
- **Protéger les données sensibles stockées sur votre ordinateur**
- **Récupérer des données perdues**
- **Détruire définitivement des données sensibles**
- **Préserver la confidentialité de vos communications sur Internet**
- **Préserver votre anonymat et contourner la censure sur Internet**
- **Préserver votre anonymat et contourner la censure sur Internet**
- **Utiliser votre téléphone mobile en sécurité (autant que possible…)**
- **Utiliser votre smartphone en sécurité (autant que possible…)**

Protection International AISBL
11 Rue de la Linière
1060 Bruxelles – Belgique
+32 2 609 44 05
http://protectioninternational.org