MANUEL
LEVONS NOUS!

DEFENDDEFENDERS

East and Horn of Africa Human Rights Defenders Project

CONTENU

ACRONYMES

UA	Union Africaine
CADHP	Commission Africaine des Droits de l'Homme et des Peuples
UE	Union Européenne
DDH	Défenseur des Droits Humains
FDDH	Femme Défenseure des Droits Humains
ONG	Organisation Non Gouvernementale
OSIG	Orientation Sexuelle et Identité de Genre
ONU	Organisation des Nations Unies
DUDH	Déclaration universelle des Droits de l'Homme

REMERCIEMENTS

Le 5 mai 2017, DefendDefenders a lancé le manuel LEVONS-NOUS! pour les défenseurs africains des droits humains. Ce manuel vise à renforcer la sécurité physique et numérique des défenseurs des droits humains et des organisations en contextualisant les connaissances existantes dans le nouveau manuel de protection de Protection International ainsi que dans le manuel de Front Line Defenders sur la sécurité.

En décembre 2019, DefendDefenders a lancé le manuel LEVONS-NOUS! dans cinq langues locales ougandaises, à savoir : Acholi, Ateso, Luganda, Luo, Runyakitara.

En 2020, DefendDefenders a décidé de réviser le manuel pour tenir compte des commentaires des défenseurs des droits humains et des nouveaux concepts émergents en matière de sûreté, de sécurité et de bien-être des défenseurs des droits humains en Afrique.

L'édition actuelle est le résultat de l'expérience de DefendDefenders et du feedback des défenseurs lors des formations, de missions de recherche et de divers engagements avec les parties prenantes, ainsi que des aspects émergents en matières de sûreté et de sécurité.

L'équipe de gestion de la protection et de la sécurité composée de Janvier Hakizimana, Majid Maali, Karis Moses Oteba, Anne Nakiyingi, feue Mariam Nakibuuka , Brian Bamutaze, Leon Nsiku et Denise Kwizera a révisé le premier manuel sur la sûreté et la sécurité physique . Le deuxième manuel sur la sûreté et la sécurité numérique a été révisé par l'équipe du département de l'information et de la technologie au sein de DefendDefenders composée de Mark Kigundu, Daniel Byekwaso, Samuel Eibu, Joshua Ssengonzi, Donatien Niyongendako, Immaculate Nabwire et Abdikani Hassan. Le processus de révision n'aurait pas été couronné de succès sans les conseils et la supervision de l'équipe de la direction de DefendDefenders. Le manuel a été traduit en français par Arsene Arakaza.

Il a été révisé et édité par Victor Lisere, Janvier Hakizimana et Prisca Lika.

Le Directeur exécutif de DefendDefenders - Hassan Shire, la Directrice des programmes et de l'administration - Memory Bandera et la superviseuse du département de gestion de sécurité et protection - Tabitha Netuwa, ont apporté des contributions inestimables, de l'orientation stratégique à la révision et à la publication de cette édition.

AVANT-PROPOS

La nécessité d'une gestion de la sûreté et de la sécurité des défenseurs des droits humains (DDH) a émergé lorsque les violences subies par les défenseurs des droits humains dans le cadre de leur travail ont dépassé les capacités de protection des détenteurs d'obligations. Ainsi, dès la chute du mur de Berlin, il était évident qu'il y avait nécessité pour les défenseurs des droits humains de mettre en place des outils et stratégies de gestion de la sécurité et de la sûreté.

Ce besoin a été comblé par le Manuel Levons-Nous! : Gestion de la sécurité et de la sûreté pour les défenseurs des droits humains en Afrique. Il élargit et renforce les connaissances en matière de protection préventive des défenseurs des droits humains en Afrique.

Le manuel met l'accent sur les menaces portées à la sécurité et à la sûreté et les mesures d'atténuation des risques. Il se penche également sur des exemples tirés de l'expérience de la formation et des interactions avec les défenseurs des droits humains basés dans les communautés en Afrique et impliqués dans le travail quotidien pour la défense des droits humains dans des zones difficilement accessibles, en particulier dans l'Est et la Corne de l'Afrique.

Ces expériences précieuses ont éclairé le choix du style, des thèmes et de l'organisation du manuel, ce qui rend son contenu facilement compréhensible et pratique pour les DDH et leurs réseaux à travers l'Afrique. La particularité de ce manuel est son approche holistique de la gestion de la sécurité, qui englobe la gestion de la sécurité physique, la prise en charge de soi , le renforcement de la résilience et la sécurité numérique.

Les défenseurs des droits humains oublient ou négligent parfois leur propre sécurité dans l'exercice de leur travail. Cela ne devrait pas être le cas. Une bonne gestion de la sécurité est malheureusement devenue un élément clé du travail en faveur des droits humains dans l'Est et dans la Corne de l'Afrique étant donné que nous, les DDH, avons la responsabilité, à la fois envers nous-mêmes et ceux pour qui nous travaillons de prendre cela en considération.

Bien que l'utilisation de l'internet et des technologies de l'information dans le processus de promotion ou de la protection des droits humains ait changé la donne à bien des égards, elle expose certains DDH à des risques plus élevés necessitant des solutions adaptées qui sont indiquées dans ce manuel.

DefendDefenders a été fondé pour protéger les défenseurs des droits humains confrontés à des risques immédiats. Cependant, plus d'une décennie d'expérience nous a appris que beaucoup de choses peuvent être faites pour faire en sorte que les défenseurs des droits humains n'atteignent pas ce point critique. En prenant soigneusement en compte leur sécurité, en élaborant des plans de sécurité solides et en les respectant scrupuleusement, même les défenseurs des droits humains qui travaillent dans des conditions extrêmes peuvent limiter le risque auquel ils sont confrontés en tant qu' individus ou organisations.

Ce manuel contient des stratégies clés et des mesures concrètes que tous les défenseurs des droits humains travaillant dans l'Est et dans la Corne de l'Afrique peuvent et doivent mettre en œuvre immédiatement afin d'améliorer leur propre sécurité ainsi que celle de leurs organisations et partenaires. J'encourage tous mes collègues défenseurs des droits humains à prendre ces leçons à cœur.

Hassan Shire
Directeur Général
DefendDefenders

INTRODUCTION

L'adoption de la déclaration des Nations Unies sur les défenseurs des droits humains en 1998 et la mise en place du mandat du rapporteur spécial des Nations unies sur la situation des défenseurs des droits humains en 2000 sont des étapes majeures dans la protection des défenseurs des droits humains. Cependant, les défenseurs continuent de faire face à des menaces et à des risques malgré l'existence de ces mécanismes.

A travers l'Afrique, les défenseurs qui travaillent pour la promotion et la protection des droits humains dans des contextes politiques instables sont confrontés à des risques majeurs, tels que les meurtres, les attaques physiques, les agressions, les arrestations, l'intimidation et le rétrécissement de l'espace civique. Les Etats ont constamment échoué dans leurs enquêtes sur les violations commises à l'encontre des défenseurs des droits humains.

Pour assurer leur sécurité et la continuité de leur travail, les défenseurs des droits humains ont pris des mesures pour gérer leur sécurité individuelle et organisationnelle en évaluant les risques et en mettant en place des stratégies efficaces pour atténuer les menaces potentielles. Le fait de consacrer du temps et des ressources à la gestion de la sécurité aide les défenseurs à poursuivre leurs activités dans le domaine des droits humains et à assurer leur sûreté et sécurité.

Le manuel contextualisé de DefendDefenders sur la sûreté, la sécurité et le renforcement de la résilience est destiné à servir d'outils aux défenseurs des droits humains en Afrique pour les équiper des stratégies et des réponses nécessaires à l'environnement souvent instable dans lequel ils opèrent. Malgré les mécanismes de protection disponibles, des DDH continuent de faire face aux menaces et risques qui ont un effet indéniable à long terme sur leur santé mentale. Des défenseurs des droits humains doivent prendre des mesures pour gérer leur sûreté et sécurité.

Ce manuel reflète les expériences de DefendDefenders au cours des 17 dernières années, axées sur la promotion de la sécurité , la protection et la prise en charge de soi des défenseurs par le biais de formations, de plaidoyers et de recherches, d'un soutien technique et d'un soutien organisationnel.

La deuxième édition est basée sur les recommandations, le feedback et les interactions avec les défenseurs des droits humains, les partenaires de protection, les mécanismes nationaux, régionaux et internationaux de protection des DDH.

Ce manuel complète les ressources existantes sur la sûreté, la sécurité et la prise en charge de soi des défenseurs des droits humains. Il contextualise les connaissances et les outils pour les défenseurs en Afrique.

Ce chapitre définit les concepts de base qui sont utilisés tout au long du manuel. Comprendre ces concepts, leurs similitudes, leurs différences et leurs complémentarités est utile pour les défenseurs des droits humains lorsqu'ils procèdent à des évaluations des risques et au développement des stratégies et des mesures efficaces de sécurité.

1

CHAPITRE

DEFINITION DES CONCEPTS

Défenseur des droits humains

Les défenseurs des droits humains (DDH) sont des personnes qui, individuellement ou avec d'autres, agissent, de manière pacifique, pour promouvoir ou protéger les droits humains inscrits dans la Déclaration universelle des droits de l'Homme (1948). La Déclaration des Nations Unies de 1998 sur les défenseurs des droits de l'Homme[1] fait référence aux individus, groupes et associations contribuant à l'élimination effective de toutes les violations des droits humains et des libertés fondamentales des personnes.

N'importe qui peut être un(e) défenseur(e) des droits humains, quels que soient son niveau d'éducation, ses qualifications professionnelles, son sexe, son âge, son origine, son groupe social et sa nationalité. Par exemple, si un/une vendeur/vendeuse ambulant (e) ou un/une vendeur/vendeuse de bananes dénonce les mauvais traitements infligés à ses collègues vendeurs par les autorités fiscales locales, il/elle peut être considéré(e) comme un(e) DDH. Les défenseurs des droits humains peuvent se trouver dans le secteur privé comme dans le secteur public.

La sécurité est définie par l'état de liberté d'une personne face aux événements nuisibles intentionnellement dirigés contre lui.

La sûreté et la sécurité contiennent toutes deux l'élément de danger.

La sûreté est définie par l'état de liberté d'une personne face aux événements nuisibles imprévus/non intentionnels. La sûreté et la sécurité contiennent toutes deux l'élément de danger.

La protection est définie comme les mesures prises par les défenseurs des droits humains ou d'autres acteurs pour renforcer la sûreté et la sécurité[2].

Les incidents de sûreté et de sécurité sont des événements qui peuvent exposer les DDH et/ou leurs organisations à un danger.

La menace peut être définie comme une déclaration ou une indication d'une intention d'infliger des dommages, de punir ou de faire du mal.

Le risque peut être défini comme la possibilité d'un événement qui entraîne un préjudice.

Le bien-être peut être défini comme l'équilibre entre la santé physique, mentale et émotionnelle de quelqu'un.

1 Le nom complet de la Déclaration est la "Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits de l'homme et les libertés fondamentales universellement reconnus et " communément appelée " Déclaration sur les défenseurs des droits de l'homme" http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Translation.aspx

2 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, https://www.frontlinedefenders.org/ en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk, consulté le 23 juin 2016.

2

CHAPITRE

ANALYSE DU CONTEXTE

Le contexte de travail des défenseurs des droits humains, également appelé environnement de travail, est à la base de toute décision en matière de sûreté et de sécurité. Les risques pour la sûreté et la sécurité auxquels les DDH sont confrontés varient selon le contexte. Les défenseurs évoluent dans un environnement dynamique qui a un impact sur leur sécurité. Le contexte des DDH est constitué de facteurs et d'acteurs. Les facteurs comprennent la politique, l'économie, la culture, le genre, la religion, l'environnement géographique écologique et d'autres aspects tels que la santé, tandis que les acteurs sont les personnes soutenant ou s'opposant au travail des défenseurs des droits humains. L'analyse du contexte vise à aider les défenseurs des droits humains à prendre des décisions éclairées concernant leur sûreté et sécurité.

Méthode d'Analyse des Facteurs (MAF)

1. **Facteurs politiques :** La politique peut avoir des impacts positifs et négatifs sur les DDH et leur travail. Les DDH ne sont pas nécessairement des politiciens, mais la connaissance des fondements politiques dans chaque contexte est cruciale dans l'adoption des mécanismes de sûreté et de sécurité pour un travail efficace de défense des droits humains . Les DDH doivent se poser des questions sur les principaux facteurs politiques dans leur contexte et sur la façon dont ils affectent leur sûreté et sécurité. Par exemple, dans certains pays, les élections entrainent des attaques accrues contre les DDH. Dans les zones de conflit armé, les défenseures des droits humains sont particulièrement exposées aux violences sexuelles et aux assassinats. L'instabilité politique oblige les DDH à ajuster régulièrement les mécanismes de sûreté et de sécurité. Les DDH doivent surveiller activement l'évolution du contexte politique et son impact sur leur sûreté et sécurité.

2. **Facteurs économiques :** Les réglementations économiques, les nécessités, les facilitations et les opportunités sont essentielles au travail des défenseurs des droits humains. Les défenseurs doivent connaître les lois économiques, les réglementations et les pratiques existantes qui affectent leur travail. Il y a souvent un besoin de ressources économiques pour mettre en œuvre certaines mesures de sûreté et de sécurité. Les DDH doivent analyser les tendances économiques mondiales associées à la géopolitique pour une programmation stratégique et une planification de la sécurité appropriées.

3. **Facteurs socio-culturels :** Les défenseurs des droits humains (DDH) doivent prendre en compte les normes socioculturelles lorsqu'ils mènent leur travail en gardant à l'esprit que certaines de ces normes contredisent l'universalité, l'inaliénabilité et l'indivisibilité des droits humains. Il est important d'étudier les questions relatives aux normes traditionnelles, à la religion et aux perceptions sociales de la communauté dans laquelle les DDH opèrent. En particulier en ce qui concerne des questions telles que les droits des femmes et l'orientation sexuelle, ainsi que l'identité et l'expression de genre (OSIEG). Les DDH doivent surveiller les facteurs socio-culturels et leur impact sur leur sécurité.

4. **Facteurs technologiques :** L'utilisation de la technologie a connu une croissance rapide au cours des dernières décennies. Les défenseurs des droits humains (DDH) utilisent diverses technologies dans leur travail en faveur des droits humains , y compris le plaidoyer, le réseautage et le suivi, la surveillance, la documentation et le rapportage (SDR) des droits humains. Les facteurs technologiques examinent l'utilisation des outils numériques et soutiennent les instruments dans le processus d'atteinte des objectifs en matière de droits humains. Même si la technologie fait progresser le travail des DDH, elle est devenue l'une des principales sources de menaces et de risques. La plupart des menaces et des risques actuels se trouvent dans le domaine numérique. Par conséquent, les DDH doivent gérer les risques liés aux plateformes numériques.

- Referez -vous au livre II de ce manuel pour plus d'informations sur la sûreté et la sécurité numérique.

5. **Facteurs écologiques et géographiques :** Les conditions météorologiques et la structure du paysage déterminent l'approche des défenseurs des droits humains (DDH) sur les risques pour leur sûreté et leur sécurité découlant du travail dans des zones spécifiques. En outre, ils déterminent également de la période et du calendrier pour mener certaines activités. Par exemple, le terrain et les conditions météorologiques dictent les moyens de transport, les vêtements et l'équipement de protection à utiliser. Selon la topographie et les infrastructures disponibles, les DDH peuvent être tenus d'utiliser toute sorte de véhicules tout-terrain et des bateaux pour atteindre des zones éloignées. Le vélo, la marche ou le canotage sont quelques-unes des options qui peuvent être utilisées pour accéder à des endroits difficilement accessibles.

6. **Cadres juridiques :** En principe, les lois et les constitutions nationales assurent la protection juridique des défenseurs des droits humains (DDH). Mais certaines dispositions légales ont été détournées pour permettre la violation des droits des DDH. Les DDH sont de plus en plus confrontés à un espace civique restreint en raison de l'adoption des lois répressives. Après les attaques terroristes du 11 septembre 2001, la plupart des pays africains ont depuis adopté et utilisé des lois antiterroristes pour limiter le travail des DDH.

   En outre, certaines lois régissant les libertés de réunion et d'association ont été détournées pour justifier la violation des droits des DDH. Lorsque les DDH se familiarisent avec les législations et les ordonnances de certains domaines, ils mettent en place des mesures pour travailler en toute sécurité et, en outre, par le biais du plaidoyer, ils appellent à l'abrogation ou à la modification de certaines lois. Les violations passées des droits des DDH sont utiles pour prédire ce qui pourrait leur arriver à eux et leurs organisations.

7. **Autres facteurs :** Les problèmes de santé publique et les catastrophes naturelles mettent la vie des défenseurs des droits humains (DDH) en danger. Les DDH ont besoin d'envisager des mesures préventives et réactives en cas d'éventuel besoin médical. Les DDH travaillant sur la pollution de l'environnement et les violations des droits humains dans les établissements médicaux sont susceptibles de contracter certaines infections et maladies. Par exemple, les DDH travaillant dans des zones exposées aux maladies infectieuses comme Ebola ont de fortes chances de contracter la maladie. Pour mettre en place les meilleures pratiques, il est conseillé aux DDH de recevoir une prophylaxie, d'utiliser des équipements de protection individuelle (EPI) et de souscrire à une assurance médicale.

Méthode d'analyse des acteurs (MAA)

Les acteurs sont toutes les personnes ou institutions qui ont des intérêts dans le travail des défenseurs des droits humains (DDH). Les DDH doivent cartographier les acteurs de soutien, les acteurs d'opposition et les acteurs aux intentions inconnues. Le contexte des défenseurs des droits humains est dynamique parce que les acteurs changent leurs positions en fonction de leurs intérêts et des environnements dominants. Par conséquent, les DDH doivent surveiller les changements dans leur contexte de travail pour réévaluer si la position des acteurs a changé ou non.

Types des acteurs

Ce tableau peut être utilisé par les DDH pour catégoriser les acteurs en fonction de leurs intérêts et de leur position.

Acteurs de soutien	Acteurs d'opposition	Acteurs aux intentions inconnues
Donateurs	Auteurs de violations des droits de l'homme	Politiciens
Camarades défenseurs des droits humains	Les organismes d'application de la loi dans certains contextes	Les chefs religieux dans certains contextes
ONG internationales	Les entreprises multinationales dans certains contextes	Les universitaires dans certains contextes

- Faites attention aux amalgames dans l'analyse des acteurs!
- Dans la mesure du possible, les défenseurs des droits humains doivent mentionner des noms individuels au sein d'une unité ou d'une institution. Par exemple, alors que certains DDH peuvent supposer que les services de sécurité sont contre eux, il peut y avoir des agents au sein des services de sécurité qui soutiennent leur cause.

3

CHAPITRE

INCIDENTS DE SURETE ET DE SECURITE

Un incident de sûreté et de sécurité peut être tout événement qui expose les défenseurs des droits humains (DDH) et/ou leur organisation à un danger. Il fournit des signaux aux DDH et à leur organisation sur l'impact de leur travail en leur donnant l'occasion de réévaluer leurs mécanismes de programmation et de protection.

Exemples d'incidents de sûreté

1. Incendie ou électrocution.
2. Inondation de bureaux;
3. Épidémies.

Exemples d'incidents de sécurité

1. Personnes surveillant le travail des DDH.
2. Fuite d'informations confidentielles des DDH;
3. Fouille et perquisition des domiciles et des bureaux des DDH.

ÉTAPE 1:

Enregistrer un incident

Les défenseurs des droits humains utilisent diverses méthodes pour saisir les détails des incidents, comme les tirets ou les paragraphes. Quel que soit le format choisi, ils sont guidés par les six questions majeures comme illustrées dans le tableau ci-dessous :

La méthode de QQOQCP		
Qui?	Quoi?	Où?
Quand?	Comment?	Pourquoi?

Les enregistreurs d'incidents s'efforcent de poser autant de questions pertinentes que possibles sous chaque question majeure pour enregistrer les incidents. Ils doivent éviter les mots compliqués, les jargons et les mots à la mode pendant l'enregistrement. Ils doivent également s'assurer que les noms, adresses, chiffres et faits sont exacts pour donner une orientation appropriée dans les prochaines étapes de l'évaluation des incidents de sûreté et de sécurité.

ÉTAPE 2:

Rapporter un incident

Quand on subit ou observe un incident, on doit réaliser un rapport sur l'incident. Le rapport d'incident peut être écrit ou verbal. Toutefois le rapport d'incident doit être conservé sous forme écrite pour éviter la perte des faits enregistrés. Pour les défenseurs des droits humains (DDH) travaillant dans une organisation, le rapport d'incident doit être envoyé à la direction. Pour les DDH indépendants, le rapport d'incident peut être partagé avec leurs collègues et partenaires de confiance. Faisant référence aux six questions fondamentales, les informations contenues dans ce rapport doivent inclure[3]:

- Qui fait le rapport? Qu'est- ce qui est arrivé? Où est-ce arrivé? Quand cela est arrivé, avec le plus de précisions possibles?
- Qui était impliqué? (Avec détails de la victime de l'incident);
- Quel est l'impact sur les victimes ? (Avec détails de leur état actuel) ; Qui a perpétré l'incident ? (avec de bref détails sur le nombre, les armes, l'affiliation apparente)
- Que s'est-il passé après l'incident)
- Pourquoi l'incident a-t-il eu lieu à ce moment-là? Comment l'incident s'est produit? (moyens utilisés par les auteurs);
- Résumé de la siuation actuelle, s'il y a des problèmes ou non; s'il y en a, quelles décisions et mesures que le rapporteur d'incident propose de prendre/a déjà prises et quelles sont les actions qui sont requises?

Les DDH peuvent utiliser différents moyens de communication sécurisés pour signaler les incidents. Ils peuvent également convoquer les réunions où le rapporteur fournit des comptes rendus oraux sur les incidents.

ÉTAPE 3:

Analyser des faits sur l'incident

Lors de l'analyse des faits, certaines questions doivent être prises en considération, telles que : qui pourrait être impliqué, où l'incident s'est-il produit, y a-t-il eu une blessure physique ou tout dommage matériel, et quel était l'objectif probable des auteurs? Cela dictera la prochaine étape pour savoir si il faut réagir et quand. À ce stade, il faut déterminer la gravité de l'incident afin de savoir s'il est mineur ou grave.

ÉTAPE 4:

Réagir ou ne pas réagir

Lorsque l'analyse montre que l'incident est grave, les défenseurs des droits humains (DDH) doivent mettre en place des actions nécessaires. Les actions dépendent de la nature de l'incident. En cas d'effraction dans un bureau, de nouvelles serrures et système de sécurité doivent être mis en place. Si un DDH est arrêté, la réaction immédiate serait d'obtenir sa libération. Si un défenseur des droits humains est blessé, il est nécessaire de lui apporter les premiers soins et de chercher un traitement médical.

Si un incident est considéré comme mineur, les DDH peuvent ne pas réagir, mais ils sont tenus de documenter l'incident pour une référence ultérieure. Un incident est considéré comme grave lorsqu'il est lié au travail des DDH et à leur santé physique et mentale en général. Par conséquent, si l'incident devient une menace, une analyse approfondie est nécessaire.

3 Koenraad van Brabant 'Operational Security Management in Violent Environments' Juin 2000, page 240, https://sites.google.com/site/ngosecurity/GPR8.pdf?attredirects=0

4

CHAPITRE

COMPREHENSION DES MENACES

Qu'est-ce qu'une menace?

Une menace peut être définie comme une déclaration ou une indication d'une intention d'infliger des dommages, de punir ou de faire du mal[4]. Les menaces sont des déclencheurs qui annoncent les dangers à venir. Ils peuvent être verbaux ou non verbaux.

Exemples de menaces pour les DDH

Parmi les menaces les plus courantes contre les défenseurs des droits humains, on peut citer les suivantes :

1. Nous fermerons votre organisation si vous n'arrêtez pas votre travail.
2. Vous êtes le suivant.
3. Vous ne verrez pas vos enfants grandir; et
4. Je vais te tuer.

Les menaces sont les stratégies les plus couramment utilisées contre les DDH par les parties prenantes dont les intérêts sont affectés négativement par le travail des défenseurs des droits humains. Les menaces sont préférées aux attaques/agressions parce que ce sont les tactiques les moins coûteuses pour arrêter le travail des DDH.

Les menaces sont des signes que des préjudices pourraient arriver à l'encontre des DDH. Les agresseurs recueillent des informations sur les DDH et leur travail, ce qu'ils utilisent pour les menacer. Si les DDH continuent d'ignorer les menaces, les agresseurs peuvent transformer les menaces en sérieuse attaque physique. Par conséquent, les DDH doivent analyser les menaces pour identifier les dangers et mettre en place des mécanismes d'attenuation des risques.

4 Front Line Defenders, 'Workbook on security: Practical Steps for Human Rights Defenders at Risk' 2011, https://www.frontlinedefenders.org/en/resource-publication/workbook-security-practical-steps-human-rights-defenders-risk, consulté le 23 juin 2016.

Proférer des menaces ou constituer des menaces

Les DDH doivent savoir si ceux qui profèrent ces menaces sont assez sérieux pour commettre un acte d'agression ou d'attaque. Certaines personnes peuvent menacer, mais elles n'exécutent pas réellement leurs menaces tandis que d'autres mettent en œuvre des avertissements contre les défenseurs des droits humains (DDH). Mais tout dépend de l'environnement sociopolitique dans lequel les DDH opèrent. Il est également nécessaire de se référer à l'exécution et à la non-exécution des menaces par le passé et à la crédibilité[5] de la source des menaces.

La plupart des personnes qui profèrent des menaces constituent en fin de compte une menace : ces personnes menaceront les DDH et utiliseront tous les moyens pour exécuter leurs plans.

Certaines personnes qui profèrent des menaces ne constituent pas une menace.

Dans de nombreux cas, les menaces ne sont pas mises en œuvre parce que les auteurs veulent atteindre leurs objectifs à moindre coût. Bien que les menaces puissent ne pas être mises à exécution, les DDH sont invités à continuer de surveiller ces menaces et incidents de sécurité. similaires

Certaines personnes font rarement des menaces, elles constituent une menace. Contrairement aux deux premiers exemples, cette catégorie de personnes ne déclare pas leurs intentions de nuire. Au lieu de cela, ils se cachent en silence. Ils représentent un danger sans avertissement. Les DDH doivent interpréter comment et quand le silence peut mordre.

Manuel Adapté de Front Line Defenders : Manuel sur la sécurité

5 Idem

Des auteurs de menace et exécutants des menaces

Dans l'analyse des menaces, **les défenseurs des droits humains** (DDH) ont tendance à se concentrer davantage sur la personne qui émet des menaces. Pour diverses raisons, le véritable auteur de menace embauche d'autres personnes pour délivrer les avertissements. Les DDH doivent redoubler d'efforts pour identifier les véritables sources des menaces. Le cas ci-dessous montre que les auteurs des menaces peuvent embaucher des personnes pour exécuter ces menaces :

Le cas d'un activiste nigérian des droits fonciers, feu Ken-Saro Wiwa, montre que les personnes qui communiquent et exécutent des menaces ne sont pas les véritables auteurs – initiateurs. Cet activiste a été pendu sous les ordres du président. Cependant, une analyse approfondie montre que l'ordonnance présidentielle a été motivée et facilitée par une société multinationale (MNC) dénommée Shell .

Comment analyser les menaces

Une évaluation appropriée des menaces est nécessaire pour identifier les sources et les objectifs des menaces et examiner la probabilité de leur exécution . L'analyse des menaces peut être effectuée individuellement ou au niveau organisationnel. Les DDH indépendants peuvent impliquer leurs collègues pour tirer une conclusion impartiale sur les menaces.

Lorsque les DDH analysent des menaces, ils doivent tenir compte des faits, des reproductions symboliques, des sources et des objectifs des menaces. Cela aide à tirer une conclusion sur la question de savoir si les menaces peuvent être exécutées ou non[6]. Voici cinq étapes pour l'analyse des menaces :

1. **Établir les faits entourant les menaces:** Les DDH examinent la nature des menaces, le type de menaces, qui les a proférées et comment les menaces ont été communiquées. Il peut s'agir de messages, d'appels téléphoniques d'intimidations, de conseils sur les activités en jeu en faveur des droits humains , de convocations, de déclarations du gouvernement sur les activités des DDH, de visites de représentants du gouvernement et d'entreprises multinationales ou de visites de service de sécurité etc.

2. **Déterminer les caractéristiques des menaces au fil du temps:** Les défenseurs des droits humains (DDH) signalent une série d'actes qui ont eu lieu au cours d'une certaine période. Les DDH examinent le moment, la fréquence et la gravité des menaces. Les messages menaçants peuvent être envoyés par des moyens anormaux tels que des images d'encre rouge, de sang, de crâne et d'os, etc. Des outils de menace extrême tels que des cercueils vides ou des cercueils contenant des animaux morts peuvent également être utilisés.

3. **Examiner l'objectif des menaces:** Les défenseurs des droits humains (DDH) doivent examiner l'intention des auteurs de menaces. Il n'est peut-être pas facile de connaître l'intention exacte des agresseurs, mais les DDH doivent s'efforcer de mener une analyse approfondie de leurs intentions probables. Il est important d'examiner l'impact négatif des activités des défenseurs des droits humains sur les intérêts des parties prenantes et les types de menaces qu'ils reçoivent;

4. **Examiner la source des menaces:** Il est difficile de connaître la source exacte des menaces, car les vrais auteurs peuvent utiliser des mandataires pour mener des activités et proférer des menaces. Les DDH doivent approfondir leur analyse pour savoir d'où vient la menace. Connaître la source des menaces permet aux défenseurs des droits humains (DDH) de connaître la capacité d'exécution des menaces posées.

5. **Tirer des conclusions sur l'exécution des menaces:** Cette dernière étape aide les défenseurs des droits humains(DDH) à décider si les menaces se matérialiseront en danger ou non.

Remarque: Les faits et les tendances des menaces sont fondés sur des événements tangibles, tandis que la source et l'objectif des menaces sont fondés sur des hypothèses et des conjectures éclairées. La conclusion est basée sur la probabilité et tient compte des résultats des quatre premières étapes.

6 https://www.protectioninternational.org/wp-content/uploads/2012/04/Protection-Manual-3rd-Edition.pdf

5
CHAPITRE

EVALUATION DES RISQUES

Les défenseurs des droits humains (DDH) œuvrent en faveur du plein respect, de la protection et de la réalisation des droits humains inscrits dans la déclaration universelle des Droits de l'Homme et d'autres instruments relatifs aux droits humains. Les défenseurs qui travaillent à l'incorporation de ces instruments dans les lois nationales de divers pays dotés de systèmes de gouvernance différents se mettent en grand danger vis à vis des différentes parties prenantes y compris les autorités de l'État, le secteur privé et les communautés locales. Ces dangers sont hérités du travail des DDH et ne peuvent être éliminés. Ce chapitre examine comment les DDH gèrent et atténuent efficacement les dangers qui se produisent.

Qu'est-ce qu'un risque?

Le risque peut être défini comme la possibilité qu'un événement entraîne un préjudice. Les risques sont les dangers auxquels les DDH sont confrontés dans leur travail quotidien.

Exemples de risques

Les défenseurs des droits humains (DDH) sont confrontés à des risques tels que l'arrestation, la détention, l'emprisonnement, le meurtre, les agressions verbales et non verbales, l'enlèvement/disparitions forcées, la diffamation, le rejet par la société et les collègues professionnels, les convocations, le chantage, fermeture du bureau, raids policiers, cambriolages dans les bureaux, interception et écoute des communications des DDH et la filature . En d'autres termes, les risques sont des dangers incertains auxquels les DDH font face en raison de leurs activités en faveur des droits humains.

Composantes du risque

Le risque est composé de trois variables, à savoir la vulnérabilité, les capacités et les menaces. Les trois composantes sont interdépendantes et déterminent la probabilité et l'impact d'un risque.

1. **Vulnérabilités:** Les vulnérabilités peuvent être décrites comme des faiblesses internes des DDH qui augmentent la probabilité qu'un dommage/dégât se produise et la gravité de son impact.

2. **Capacités:** Les capacités sont des ressources, des aptitudes et des forces internes qui peuvent être utilisées pour réduire des dommages et leur impact.

3. **Menaces:** Les menaces sont des facteurs externes signalant les risques qui peuvent éventuellement affecter le travail des DDH.

Nature des risques

Les risques diffèrent selon le contexte des défenseurs des droits humains (DDH), y compris le profil, le lieu , les ressources, les approches et les activités entreprises / les problèmes subis par les DDH.

Comment évaluer les risques?

Les DDH doivent analyser correctement les risques afin de mettre en place des mesures appropriées de limitation des risques. Ils doivent identifier les risques et leurs sources et mesurer la probabilité et l'impact. Ils doivent déterminer s'ils peuvent résister aux risques identifiés.

Les risques peuvent être évalués à l'aide des étapes suivantes :

1. Identification des risques

L'identification des risques est une étape initiale mais importante de l'évaluation des risques. Il s'agit d'énumérer les dangers auxquels les DDH peuvent être confrontés. Un DDH doit dresser une liste des risques afin que chaque risque soit analysé en profondeur. Les risques peuvent être identifiés par le biais de groupe de discussion ou des échanges. Lors de l'analyse des risques, les DDH doivent examiner les incidents et les menaces en matière de sécurité, la réaction des parties prenantes et les risques encourus par les autres DDH.

2. Sources de risque

Les DDH doivent signaler les causes évidentes et sous-jacentes d'un risque. Les sources du risque peuvent être des institutions ou des individus dont les intérêts sont affectés par le travail des DDH. Les DDH doivent également examiner le lien entre deux ou plusieurs sources du risque et les interactions possibles des sources pour mettre en œuvre les risques

3. Probabilité de risque

Divers facteurs influencent l'exécution des risques. Les DDH examinent la possibilité qu'un risque se produise en examinant les capacités des sources du risque à exécuter les menaces, la nature du travail en termes de sensibilité et le contexte en termes de facteurs et d'acteurs influençant le travail des DDH. Il est important d'étudier le taux de probabilité des risques auxquels les DDH ont été confrontés dans le passé afin d'évaluer la probabilité que les risques actuels soient exécutés. La probabilité de risque est évaluée en fonction du seuil élevé, moyen ou faible ;

4. Impact d'un risque

L'impact du risque est estimé en termes de dommages associés aux risques identifiés. Les vulnérabilités et les capacités des DDH peuvent rendre les dommages élevés, moyens ou faibles

5. Tolérance au risque

La tolérance au risque est mesurée par les capacités et les vulnérabilités des défenseurs des droits humains à résister aux risques identifiés. Les DDH sont tenus d'accroître leurs capacités pour surmonter les risques identifiés et réduire leurs impacts ; et

6. Conclusion

Les DDH doivent déterminer si les risques identifiés peuvent se produire ou non. La conclusion porte sur les capacités des DDH à résister à un risque. Si les DDH peuvent supporter le risque, ils doivent mettre en place des mesures pour réduire son impact. Cette étape permet aux DDH de réfléchir également à des scénarios possibles en cas d'effectivité des risques et adopter des stratégies efficaces.

Les conceptions erronées sur la gestion des risques

1. Mettre l'accent sur les stratégies réactives: La plupart des DDH ne mettent en place des mesures de gestion de la sécurité qu'après avoir fait face à des risques ou à des menaces. Cependant, il est important de considérer tous les risques probables qui peuvent avoir un impact sur les DDH et de mettre en place des stratégies préventives ;

2. Syndrome du "copier-coller": Certains DDH appliquent des mesures de gestion de la sécurité qui fonctionnent bien pour d'autres défenseurs. Les DDH travaillent sur différents thèmes et opèrent dans des contextes différents, d'où la contextualisation des mesures de sécurité. Par exemple, l'installation de caméras de vidéosurveillance peut attirer l'attention et la suspicion sur les DDH travaillant dans les zones rurales

3. Syndrome d'héroïsme: Un courage extrême expose parfois les DDH à des risques inutiles. Il est conseillé aux DDH de mesurer leurs vulnérabilités par rapport à l'ampleur des menaces ou des risques auxquels ils sont confrontés, car ils sont plus utiles vivants que morts ;

4. Mauvaise compréhension du travail des DDH: Dans certains cas, les DDH confondent activisme politique et travail en faveur des droits humains, ce qui peut entraver le dialogue entre les autorités et la société civile. Des dialogues constructifs limités créent une suspicion mutuelle, mais les gouvernements et les défenseurs des droits humains doivent travailler en complémentarité ;

5. Tendance à ignorer leur propre sûreté et sécurité: Les DDH ont tendance à accorder plus d'importance à leur travail et aux victimes de violations de droits humains plutôt qu'à leur propre sûreté et sécurité. Le fondement du travail des défenseurs des droits humains repose sur leur sûreté et leur sécurité et, sans cela, le travail en faveur des droits humains ne peut être maintenu.

6

CHAPITRE

PLANIFICATION DE LA SURETE ET DE LA SECURITE

Les risques sont inhérents au travail des défenseurs des droits humains (DDH) et ils ne peuvent être éliminés. Cependant, ils peuvent être limités, transformés et / ou transférés. Par conséquent, les DDH doivent procéder régulièrement à une évaluation des risques afin d'élaborer des plans de sûreté et de sécurité efficaces.

La planification de la sûreté et de la sécurité est le processus de mise en œuvre de mesures préventives et réactives visant à renforcer les capacités des défenseurs des droits humains à réduire l'impact des risques. Elle s'applique aux DDH ainsi qu'aux groupes et organisations. La planification de la sûreté et de la sécurité comprend l'élaboration de politiques, de plans et de protocoles.

Une politique se compose de règles, de principes et de lignes directrices générales, tandis qu'un plan se concentre sur la mise en œuvre de la politique. Un protocole consiste aux procédures opérationnelles standardisées pour faire face à un événement spécifique.

Composantes de la politique de sûreté et sécurité

Une politique décrit la gestion globale de la sûreté et de la sécurité organisationnelle. Elle doit être adaptée aux besoins de sûreté et de sécurité d'une organisation.

Vous trouverez ci-dessous les éléments standards d'une politique de sûreté et sécurité:

- Principes: primauté de la vie sur les biens, responsabilités individuelles et collectives, l'innocuité, etc.;
- Approche et cadre de gestion de la sûreté et de la sécurité;
- Attitude à l'égard des risques: A quel point le risque est-il acceptable?

Évaluation des menaces contre l'organisation, à un niveau général

- Qui doit évaluer cela, à quelle fréquence?
- Comment cela doit-il être communiqué?

Rôles et responsabilités en matière de sûreté et de sécurité: Une politique doit énoncer clairement les rôles et les responsabilités à tous les niveaux;

- Exigences relatives au contrôle de l'efficacité de la gestion de la sécurité : par exemple, à quelle fréquence la politique doit-elle être révisée?
- Pour d'autres suggestions sur la création d'une politique de sécurité, voir People in Aids Policy Pot on Safety and Security, mai 2003[8].

Composantes d'un plan de sûreté et de sécurité

Les plans de sûreté et de sécurité visent à faire face aux risques et aux menaces liés aux défenseurs des droits humains (DDH) dans des situations ou des événements particuliers. Pour élaborer un plan, les DDH doivent réfléchir aux risques/menaces potentiels, aux vulnérabilités et capacités. Un bon plan doit identifier les risques et avoir des mesures préventives et réactives pour limiter les risques. Par exemple, les DDH travaillant sur les mutilations génitales féminines (MGF) peuvent élaborer un plan spécifique pour faire face aux risques liés à leur travail.

Que faut-il prendre en compte lors de l'élaboration d'un plan?

- Un plan doit être concis, précis et disponible en tant que document de référence, simple d'utilisation et contenant des informations à jour;
- Il doit aborder les risques et les menaces potentiels au moyen d'une évaluation appropriée; et
- Pour chaque vulnérabilité, une action doit être formulée pour répondre à la capacité requise et donc atténuer le risque.

Mise en œuvre d'un plan de sûreté et de sécurité

Pour une mise en œuvre efficace, un plan détaillé doit être communiqué à toutes les parties concernées dans un langage clair. Il doit énoncer les rôles et responsabilités précis de chaque partie et inclure des mesures disciplinaires pour assurer le respect du plan. En outre, la mise en œuvre du plan nécessite des ressources, du temps, des connaissances et de la sensibilisation. Le plan doit être revu régulièrement pour tenir compte des nouveaux risques et menaces.

Stratégies de sécurité

Il existe trois stratégies/approches principales en matière de sécurité que les DDH et leurs organisations appliquent dans leur travail quotidien en faveur des droits humains.

1. **Stratégie d'accord:** une approche qui implique de négocier avec tous les acteurs – la communauté locale, les autorités, etc., pour obtenir l'accord et, en fin de compte, le soutien de la présence et le travail de l'organisation. Bien que cela nécessite une planification minutieuse et puisse exiger beaucoup de travail, il peut s'agir de la stratégie la plus efficace à long terme pour réduire les menaces. Cette approche implique généralement une grande visibilité, de sorte qu'en période de grande menace, il est parfois plus difficile de s'adapter en étant plus discret;

2. **Stratégie de protection:** une approche qui met l'accent sur les procédures de sécurité et les éléments de protection. L'impact est principalement sur la réduction des vulnérabilités et peut être utilisé conjointement avec les deux autres stratégies pour renforcer la protection ;

3. **Stratégie de dissuasion:** une approche qui repose sur les contre-menaces pour la protection. Par exemple, si elle est menacée, une organisation peut réagir en engageant une action en justice contre la personne qui profère la menace, ou en publiant la menace, ou en répondant au responsable de la menace en expliquant les conséquences de celle ci – comme la condamnation internationale. Cette approche ne doit être utilisée que si vous avez des informations précises et des alliés puissants. Lorsque vous élaborez vos plans de sécurité, réfléchissez à la façon dont les éléments d'accord, de protection et de dissuasion peuvent élargir le champs des options dont vous disposez [9].

8 Frontline Defenders Workbook on Security, page 48
9 Frontline Defenders Workbook on Security, page 48

7
CHAPITRE

MECANISMES DE PROTECTION EXISTANTS POUR LES DDH

La reconnaissance du rôle vital des DDH et des violations auxquelles nombre d'entre eux sont confrontés a convaincu l'Organisation des Nations Unies (ONU) que des efforts particuliers étaient nécessaires pour protéger à la fois les défenseurs des droits humains et leurs activités. La première étape importante a été de définir officiellement la défense des droits humains comme un droit en soi et de reconnaître les personnes qui entreprennent un travail en faveur des droits humains en tant que DDH.

Rapporteur spécial des Nations Unies sur les défenseurs des droits humains

Le 9 décembre 1998, par sa résolution 53/144, l'Assemblée générale des Nations Unies a adopté la Déclaration sur le droit et la responsabilité des individus, groupes et organes de société pour la promotion et la protection des droits de l'homme et des libertés fondamentales universellement reconnus (communément appelée Déclaration sur les défenseurs des droits de l'homme).

La deuxième étape a été franchie en avril 2000, lorsque la Commission des droits de l'homme des Nations Unies (aujourd'hui le Conseil des droits de l'homme des Nations Unies) a demandé au Secrétaire général de nommer un représentant spécial pour les défenseurs des droits humains chargé de suivre et d'appuyer la mise en œuvre de la Déclaration[10].

En 2000, la Commission des droits de l'Homme a créé le mandat de Représentant Spécial pour la question des défenseurs des droits de l'homme (en tant que procédure spéciale) pour appuyer la mise en œuvre de la Déclaration des droits de l'homme de 1998[11].

Le mandat stipule que les principaux rôles du Rapporteur Spécial sont les suivants:

- Rechercher, recevoir, examiner et répondre aux informations sur la situation des défenseurs des droits humains;
- Établir une coopération et mener un dialogue avec les gouvernements et les autres acteurs intéressés sur la promotion et la mise en œuvre effective de la déclaration;
- Recommander des stratégies efficaces pour mieux protéger les défenseurs des droits humains et assurer le suivi de ces recommandations;
- Intégrer une perspective de genre tout au long de son travail.

10 Fiche d'information 29 - Défenseurs des droits de l'homme : protéger le droit de défendre l'être humain Rightshttps://www.ohchr.org/Documents/Publications/Fact- Sheet29en.pdf

11 HCDH, 'resolution 2000/61 establishing the mandate' http://ohchr.org/EN/Issues/SRHRDefenders/ Pages/Mandate.aspx, consulté le 1er août 2016.

Plusieurs mécanismes régionaux ont été créés à la suite de la création du Rapporteur Spécial des Nations Unies sur les défenseurs des droits de l'homme dans le but d'accroître la protection des défenseurs des droits humains. Les principaux mécanismes régionaux sont les suivants :

i. Le Rapporteur Spécial sur les défenseurs des droits de l'Homme de la Commission africaine des droits de l'Homme et des peuples (2005)[12];

ii. Le Rapporteur Spécial sur les défenseurs des droits de l'Homme de la Commission interaméricaine des droits de l'Homme[13];

iii. Les directives de l'Union Européenne sur les défenseurs des droits de l'humains adoptées par les ministres des affaires étrangères de l'UE en 2004[14]; et

L'Union Européenne a également nommé un représentant spécial pour les droits humains, qui a pour mandat de renforcer l'efficacité et la visibilité de la politique de l'UE en matière de droits humains[15].

En 2004, la Commission africaine des droits de l'Homme et des peuples (CADHP) a établi le mandat du Rapporteur Spécial sur les DDH en Afrique pour traiter de la situation des DDH en Afrique[16]avec le mandat suivant[17]:

1. Rechercher, recevoir, examiner et agir sur la base d'informations sur la situation des DDH en Afrique ;

2. Soumettre des rapports à chaque Session ordinaire de la Commission africaine ;

3. Coopérer et engager un dialogue avec les États Membres, les institutions nationales des droits humains, les organes intergouvernementaux compétents, les mécanismes internationaux et régionaux de protection des défenseurs des droits humains et les autres parties prenantes;

4. Élaborer et recommander des stratégies efficaces pour mieux protéger les défenseurs des droits humains et donner suite à ses recommandations ;

5. Sensibiliser et promouvoir la mise en œuvre de la Déclaration des Nations Unies sur les DDH en Afrique.

Depuis l'établissement de leur mandat, les Rapporteurs spéciaux ont maintenu des contacts réguliers avec les défenseurs des droits humains grâce à leur participation à des forums régionaux et ont effectué un certain nombre de visites dans les pays, y compris des visites conjointes et des communiqués de presse avec le Rapporteur Spécial des Nations Unies[18].

Le Rapporteur spécial a également encouragé les individus et les organisations non gouvernementales à soumettre des cas concernant les DDH à la CADHP. En vertu de la Charte africaine des droits de l'Homme et des peuples, la CADHP est habilitée à recevoir et à examiner des communications émanant des individus et des organisations[19].

Directives de l'Union européenne sur les défenseurs des droits humains

L'Union Européenne (UE) s'est engagée à promouvoir la mise en œuvre de la Déclaration des Nations Unies sur les défenseurs des droits humains par le biais de ses politiques étrangères. En 2004, l'UE a adopté des lignes directrices sur la manière dont ses membres contribuent à promouvoir, soutenir et protéger les défenseurs des droits humains. Bien que ces directives ne soient pas juridiquement contraignantes, elles représentent des engagements politiques de la part de l'UE et des gouvernements concernés.

La mise en œuvre de ces directives a été identifiée comme une priorité dans le cadre de la politique étrangère de l'UE en matière de droits humains.

12 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, http://www.achpr.org/sessions/35th/resolutions/69/ accessed 1 August 2016.
13 Inter-American Commission on Human Rights, AG/RES. 1842 (XXXII-O/02), 'Human Rights Defenders: Support for Individuals, Groups, and Organizations of Civil Society Working to Promote and Protect Human Rights in the Americas' http://www.oas.org/juridico/english/ga02/agres_1842.htm, accessed 1 August , 2016.
14 EUR-Lex, Access to European Union Law, 'EU guidelines on human rights defenders' 8 December 2008, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33601, accessed 1 August 2016.
15 European Union, "EU Special Representatives," https://eeas.europa.eu/headquarters/headquarters-homepage_en/3606/EU%20Special%20Representatives (accessed 11 May 2020).
16 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, http://www.achpr.org/sessions/35th/resolutions/69/ accessed 1 August 2016.
17 The African Commission on Human and Peoples' Rights, '69: Resolution on the Protection of Human Rights Defenders in Africa' 4 June 2004, http://www.achpr.org/sessions/35th/resolutions/69/ accessed 1 August 2016
18 DefendDefenders, 'Defending Human Rights, A Resource Book for Human Rights Defenders, East and Horn of Africa Human Rights Defenders Project, 2nd edition, page 8
19 Article 55 of the African Charter on Human and People' Rights

Le mandat de l'ONU collabore avec les mécanismes régionaux pour assurer la protection des défenseurs des droits humains . La collaboration comprend le partage d'expériences et d'informations, la comparaison et le renforcement mutuel des méthodes de travail et l'identification d'objectifs communs.

Les États du monde entier ont créé des mécanismes au niveau national pour la protection des DDH notamment l'inclusion des droits des DDH dans les constitutions et législations nationales, et l'inclusion de la protection des DDH dans les institutions nationales de défense des droits humains.

Dans certains cas, les États ont promulgué une législation spécifique pour la protection des DDH.

Le Rapporteur Spécial sur les défenseurs des droits humains de la Commission Africaine des Droits de l'Homme et des Peuples

Directives diplomatiques

Outre l'UE, certains pays ont adopté des lignes directrices sur la protection des DDH[20]:

- Canada : Voix en péril ;
- Pays-Bas : Plan d'action pour les DDH;
- Finlande : Directives finlandaises sur les DDH;
- Norvège : Guide du service extérieur;
- Suisse : Lignes directrices suisses révisées de 2019 sur les DDH (remplaçant la version 2014 des Directives suisses sur les DDH);
- Royaume-Uni : Soutien du Royaume-Uni aux DDH;
- États-Unis : Fiche d'information archivée sur les DDH.

Mécanismes nationaux de protection des DDH

La Déclaration sur les défenseurs des droits humains souligne que la responsabilité et le devoir primordiaux de promouvoir et de protéger les droits humains et les libertés fondamentales incombent à l'État. Par conséquent, les États sont tenus d'assurer la sécurité et la protection des DDH en mettant en œuvre la Déclaration sur les DDH.

En juin 2016, la Côte d'Ivoire a adopté la Loi sur la promotion et la protection des défenseurs des droits humains. C'est la première fois qu'un État africain a promulgué une loi dans le but spécifique de protéger les[21].

1. **Mécanismes administratifs**- Institutions nationales des droits humains, institutions juridiques telles que le pouvoir judiciaire, organismes étatiques d'application de la loi, la police, la sécurité nationale, les organes législatifs et les gouvernements locaux;

2. **Législations**- Constitutions et lois spécifiques telles que la loi sur la promotion et la protection des défenseurs des droits humains en Côte d'Ivoire;

3. **Institutions de la société civile**- Mise en réseau entre les organisations de la société civile (OSC) et les coalitions nationales pour les défenseurs des droits humains.

Le travail des défenseurs des droits humains est intrinsèquement stressant. Les risques et les menaces auxquels les DDH font face ne sont pas seulement physiques et numériques, mais le plus souvent aussi psychologiques. Les DDH sont rejetés, discriminés et font souvent trop de sacrifices en raison de leur travail.

Les interventions de sécurité se concentrent sur les composantes physiques et numériques. Cependant, la sûreté et la sécurité des DDH doivent être holistiques et inclure la santé mentale. L'état d'esprit détermine le type de décisions et de choix en matière de sécurité que les DDH prennent.

20 ISHR « Renforcer les initiatives diplomatiques pour la protection des droits de l'homme » https://www.ishr.ch/diplomatic-support
21 Téléchargez la loi ivoirienne sur les défenseurs des droits de l'homme ici, http://www.ishr.ch/sites/default/files/documents/jo_loi_defenseurs.pdf

8

CHAPITRE

PRISE EN CHARGE DE SOI ET RENFORCEMENT DE LA RESILIENCE

Comprendre le stress dans le contexte des DDH

Qu'est-ce que le stress?

Le stress peut être défini comme une réaction à un stimulus qui perturbe notre équilibre physique ou mental. C'est la réaction physique et émotionnelle d'une personne au changement. Le stress est frustrant et épuisant en raison du déséquilibre entre les capacités des DDH et les défis que présente la situation. Le stress n'est pas le même pour tout le monde - ce qui peut être stressant pour un DDH peut ne pas l'être pour un autre. De même, le stress a des niveaux différents allant de faible à l'élevé.

Types de stress.

Il existe différentes façons de décrire le stress. Selon Healthline: Informations médicales et conseils de santé auxquels vous pouvez faire confiance, le stress peut être classé comme suit en fonction de sa nature sur une période.

i) Stress aigu

C'est la forme de stress la plus courante. Elle provient des demandes et des pressions du passé récent et des demandes et pressions anticipées de l'avenir proche. Le stress aigu frappe immédiatement et provoque une augmentation rapide du niveau d'anxiété. Par exemple, être appelé pour un entretien d'embauche, manquer un vol et recevoir de mauvaises nouvelles peut provoquer la panique.

ii) Stress aigu épisodique

Lorsque le stress aigu se produit régulièrement, on parle de stress aigu épisodique. Ce type de stress est répétitif et prend généralement un schéma régulier. Il est comparable à une vague avec ses hauts et ses bas. Des exemples de stress épisodique aigu pourraient inclure le stress du paiement du loyer, le stress des frais de scolarité et le stress du remboursement des prêts.

iii) Stress chronique

C'est un type permanent de stress avec lequel les gens vivent. C'est le stress qui affecte les gens jour après jour, année après année. Le stress chronique détruit les corps, les esprits et les vies. Il provoque des ravages par un épuisement à long terme. C'est le type de stress associé à des situations permanentes telles que le disfonctionnement familial, des maladies incurables, le fait d'être pris au piège d'un mariage malheureux, d'un emploi ou d'une carrière méprisée.

Causes courantes de stress dans le contexte des DDH

- Guerres et Conflits
- Rétrécissement de l'espace politique pour l'engagement de la société civile
- Corruption et malversations économiques
- Fraudes électorales
- Harcèlement
- Arrestation et détention arbitraires
- Diffamation et Stigmatisation
- Discrimination
- Torture
- Extrême pauvreté

Symptômes de stress

Le stress a des symptômes comportementaux, physiologiques et psychologiques. Il peut être observé par un changement dans les modes de comportement et dans les fonctions biologiques de l'organisme. Il peut également se manifester par un changement dans les émotions et les processus mentaux.

La négligence de soi, le changement dans les habitudes alimentaires, vestimentaires, de sommeil, les tendances au retrait, l'agressivité, l'irritabilité, etc. sont quelques-uns des symptômes comportementaux du stress.

Les symptômes physiologiques comprennent la fatigue corporelle, la transpiration excessive, les ulcères, les maux de tête, la diarrhée et le changement du cycle menstruel.

Les symptômes mentaux et psychologiques incluent les troubles de la mémoire , les troubles de la parole, la tristesse, la colère, le faible rendement au travail.

Gestion de stress

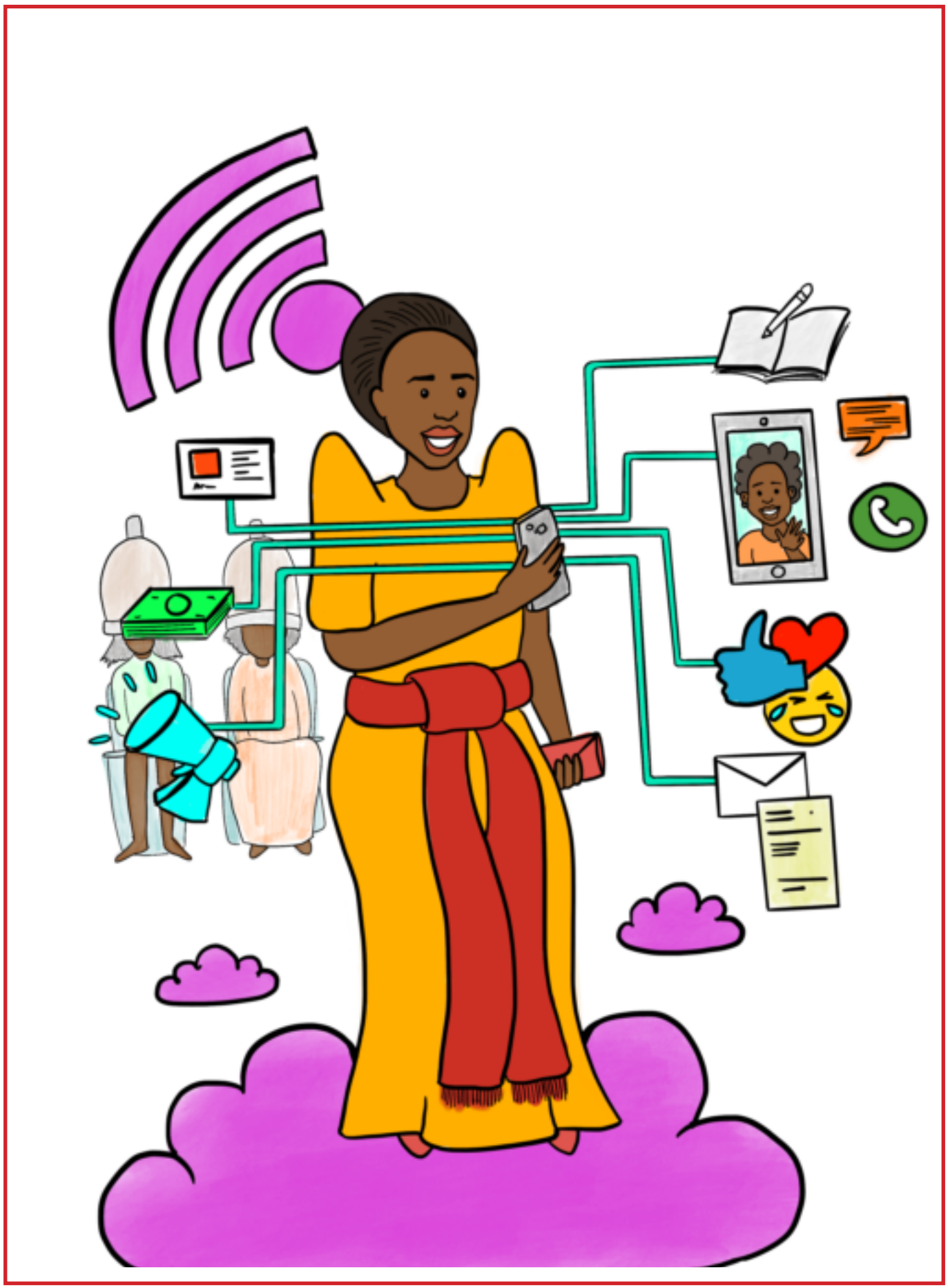
Le stress par nature ne peut pas être complètement éliminé. Dans la gestion du stress, l'objectif est de souligner quels en sont les facteurs– les principaux problèmes et exigences qui causent le stress. En faisant ça, on peut explorer des options qui aideront à surmonter l'impact négatif apporté par ces facteurs de stress. Il existe de nombreuses méthodes pour gérer le stress telles que la thérapie par la parole, la thérapie environnementale, les travaux corporels et la massothérapie, la thérapie artistique et bien d'autres. Les DDH sont encouragés à utiliser des pratiques simples de bien être qui ne nécessitent aucune expertise scientifique. Certaines des pratiques sont énumérées dans l'image ci-dessous.

D'autres moyens recommandés pour faire face au stress sont énumérés ci-dessous[22]:

- ✓ Prenez soin de vous, en mangeant sainement, en faisant de l'exercice et en dormant suffisamment
- ✓ Trouvez du soutien en parlant à d'autres personnes pour vous débarrasser de vos problèmes
- ✓ Connectez-vous socialement, car il est facile de vous isoler après un événement stressant;
- ✓ Faites une pause de ce qui vous cause du stress;
- ✓ Évitez les drogues et l'alcool, qui peuvent sembler aider à soulager le stress à court terme, mais peuvent causer plus de problèmes à long terme ;
- ✓ Apprenez à dire NON et acceptez que non est une réponse.
- ✓ Prenez le temps de vous détendre;
- ✓ Faites les choses que vous aimez, par exemple, chanter, danser, jouer à un jeu;
- ✓ Gérer votre agenda (travail, maison, loisirs);

En fin de compte, abandonnez l'activité si elle fait mal plus qu'elle motive et si d'autres solutions au stress n'ont pas fonctionné. Il est important de noter que ce n'est pas le malheur qui vous brise, c'est la façon dont vous le portez. Le stress lui-même peut entraîner des résultats positifs. Par exemple, le stress peut pousser quelqu'un à travailler plus dur / mieux. Cependant, si le stress n'est pas bien géré, il peut être très nocif.

22 Centres de contrôle et de prévention des maladies



SÉCURITÉ NUMERIQUE

UN MANUEL POUR LES DEFENSEURS AFRICAINS DES DROITS HUMAINS

CONTENU

COMMENT UTILISER CE MANUEL

Introduction: Manuel de la sécurité numérique

Etes-vous un DDH africain du vingt-et-unième siècle? . Vous êtes armé d'un esprit vif, d'un sens aigu de la justice sociale, de liens avec les communautés locales, d'un téléphone portable et d'un ordinateur portable. Il y a 20 ans, vous auriez certainement eu les trois premiers, mais le téléphone dans votre poche et l'ordinateur portable dans votre sac sont uniques au 21ème siècle.

La technologie numérique complique notre capacité à évaluer nos risques personnels et professionnels car ils sont presque toujours peu intuitifs. Sans connaissances spécialisées et techniques, il est difficile d'analyser où les appareils manquent de fiabilité pour stocker des fichiers sensibles et communiquer des informations confidentielles.

On dit souvent que l'Afrique a dépassé les anciennes technologies dans le cas des téléphones fixes filaires, car le marché des téléphones mobiles a explosé à travers le continent à un rythme beaucoup plus rapide que partout ailleurs dans le monde. Inversement, les normes technologiques, juridiques et de droits humains mondiales liées à la vie privée et à la sécurité ont un impact énorme sur l'environnement des DDH africains et de la société dans son ensemble sans nécessairement avoir une chance égale d'influer autant sur le développement.

La guerre mondiale contre le terrorisme s'est développée parallèlement à l'utilisation généralisée des technologies de télécommunications individuelles telles que l'e-mail, Skype, Facebook Messenger et WhatsApp et a mis en place une épreuve de force entre les droits individuels à la vie privée et les arguments en faveur de la sécurité collective. Dans le même temps, les entreprises de sécurité privées développent des logiciels et du matériel de piratage offensifs vendus aux gouvernements du monde entier, cela signifie que la surveillance numérique sophistiquée est à la portée des organismes d'application de la loi à des coûts nettement inférieurs.

La pandémie mondiale (COVID-19) a contraint les organisations à adopter des méthodes de travail en ligne. Cela a augmenté le risque associé au travail effectué par les DDH, car cette nouvelle normalité s'est installée très rapidement sans tenir dûment compte des risques sous-jacents pour la sécurité. Cette brochure vous permettra d'acquérir des connaissances technologiques pour mieux évaluer vos risques numériques dans la mesure où ils affectent votre travail en faveur des droits humains, et pour prendre des mesures pour atténuer ces risques. Tout au long de cette brochure, nous ferons référence à des scénarios et des histoires de DDH africains qui font face à des défis et des questions numériques dans leur travail. Cette brochure est organisée selon la structure suivante:

i) Évaluation des risques

Chaque utilisateur est confronté à des menaces (ou risques) de cybersécurité, des paysans aux présidents. Cependant, par rapport aux utilisateurs ordinaires, les enjeux sont plus élevés pour les DDH en raison de la nature de leurs activités numériques.

Dans cette section, nous allons décomposer le concept de risque et examiner les catégories de risques technologiques et leurs influences dans le monde réel. Vous apprendrez à identifier vos activités les plus à risque et à hiérarchiser les mesures visant à réduire les vulnérabilités.

ii) Cinq objectifs de sécurité

La suite de ce manuel explorera cinq catégories de sécurité numérique qui, ensemble, contribuent à la sécurité globale de vos pratiques numériques. Ces chapitres ne sont pas exhaustifs, et il n'est pas possible d'enseigner toutes les compétences à travers ces pages car les logiciels changent souvent, mais nous vous renverrons vers des ressources qui restent à jour avec les références les plus récentes. Nos cinq objectifs de sécurité sont les suivants :

a) Sécurité de base de l'appareil

Nous sommes responsables de nos appareils (et non l'inverse !), mais savons-nous comment les utiliser correctement ? Faisons-nous de notre mieux pour les maintenir en bon état de fonctionnement, résistants aux virus et autres risques qui peuvent les attaquer ? Dans cette section, nous discuterons des meilleures pratiques pour l'utilisation du système d'exploitation et des logiciels.

b) Sécurité des données sur les ordinateurs, les disques flash, les disques externes et les téléphones mobiles

Les données sont stockées sur votre ordinateur portable, votre ordinateur de bureau, votre téléphone portable, vos disques durs externes et vos clés USB. Si quelqu'un devait obtenir ces appareils ou copier des fichiers physiquement ou via un réseau, serait-il capable de lire (et de modifier) ces données? Dans cette section, nous discuterons du concept et des pratiques du cryptage, qui protège les données telles qu'elles se présentent sur vos appareils, votre stockage ou dans un cloud.

En outre, la sécurité des données est compromise si vous n'avez qu'une seule copie de vos documents importants et que cette copie est perdue en raison d'un vol, d'endommagement du matériel ou d'autres incidents informatiques. Nous examinerons les solutions de sauvegarde et la sécurité de ces pratiques.

c) Sécurité des données circulant sur les réseaux

Le prix de nos ordinateurs et téléphones vient du fait qu'ils communiquent avec d'autres appareils via Internet et les réseaux mobiles. La communication s'effectue par de nombreux moyens tels que le l'e-mail, la navigation sur le Web, la messagerie instantanée, la voix sur Protocole d'internet IP) et les messages téléphoniques et SMS (voir Sécurité mobile). Nous examinerons la nature de ces flux de communication et en comprendrons les influences sur la sécurité, en particulier dans le contexte d'une surveillance accrue.

d) Sécurité des comptes

Comment pouvons-nous nous assurer que nos comptes en ligne et hors ligne ne sont pas piratés? Ce qui entraînerait une perte de données, d'identité et "l'usurpation d'identité? Les bonnes pratiques telles que les mots de passe uniques, l'authentification à deux facteurs et les gestionnaires de mots de passe sont couvertes ici.

e) Sécurité des téléphones mobiles

Les téléphones mobiles traditionnels (appels et SMS) n'ont pas été construits de façon sécurisée . Les smartphones introduisent de nouvelles capacités et de nouveaux risques et nous en apprenons davantage sur tous les domaines de sécurité ci-dessous en ce qui concerne les téléphones mobiles.

Évaluation des risques

Il n'y a pas de solution unique pour assurer votre sécurité en ligne. La sécurité numérique ne concerne pas le type d'outils que vous utilisez. Il s'agit plutôt de comprendre les menaces auxquelles vous faites face et comment vous pouvez les contrer. Il faudrait effectuer une évaluation des menaces pour s'adapter à leurs besoins.

Lors d'une évaluation, vous devez vous poser cinq questions principales:

1. Que voulez-vous protéger?
2. De qui voulez-vous le protéger?
3. Quelle est la probabilité que vous deviez le protéger?
4. Quelle est la gravité des conséquences si vous échouez?
5. Quels risques êtes-vous prêt à encourir pour essayer de prévenir ces conséquences?

Lorsque nous parlons de la première question, nous faisons souvent référence aux biens. Un bien est quelque chose que vous appréciez et que vous voulez protéger. Lorsque nous parlons de sécurité numérique, les biens en question sont généralement des données . Par exemple, vos courriels, listes de contacts, messages instantanés et fichiers sont tous des biens. Vos appareils sont également des biens.

Notez une liste des données que vous souhaitez conserver, où elles sont conservées, qui peut y accéder et ce qui empêche les autres d'y accéder.

Pour répondre à la deuxième question : De qui voulez-vous le protéger ? Il est important de comprendre qui pourrait vouloir vous cibler ou cibler vos informations, ou qui est votre ennemi . Un ennemi est une personne ou une entité qui constitue une menace contre un ou plusieurs de vos biens. Par exemple, ces ennemis potentiels sont des entreprises, des mafias- acteurs gouvernementaux ou pirates informatiques sur un réseau public.

Dressez une liste de ceux qui pourraient vouloir voler vos données ou le contenu de vos communications. Il peut s'agir d'un individu, d'un organisme gouvernemental ou d'une société.

Une menace est quelque chose de mauvais qui peut arriver à un bien. Il existe de nombreuses façons dont un ennemi peut menacer vos données. Par exemple, un ennemi peut lire vos communications privées lorsqu'elles transitent par le réseau, ou il peut supprimer ou endommager vos données. Il pourrait également désactiver votre accès à vos propres données.

Les motivations des ennemis diffèrent considérablement, tout comme leurs attaques. Un gouvernement qui tente d'empêcher la diffusion d'une vidéo montrant des violences policières peut se contenter de simplement supprimer ou réduire la disponibilité de cette vidéo, alors qu'un opposant politique peut souhaiter avoir accès à un contenu secret et le publier à votre insu.

Notez ce que votre adversaire pourrait vouloir faire avec vos données privées.

La puissance de votre agresseur est également une chose importante.. Par exemple, votre opérateur de téléphonie mobile a accès à tous vos enregistrements téléphoniques et a donc la possibilité d'utiliser ces données contre vous. Un pirate informatique sur un réseau Wi-Fi ouvert peut accéder à vos communications non cryptées. Votre gouvernement pourrait avoir un pouvoir plus grand.

Pour répondre à la troisième question, vous devez tenir compte du risque. Le risque est la probabilité qu'une menace particulière contre un bien particulier s'exécute et va de pair avec la capacité. Bien que votre opérateur de téléphonie mobile ait la capacité d'accéder à toutes vos données, le risque qu'il publie vos données privées en ligne pour nuire à votre réputation est faible.

Il est important de faire la distinction entre les menaces et les risques. Une menace est une mauvaise chose qui peut arriver, le risque est la probabilité que la menace se produise. Par exemple, il y a une menace que votre bureau soit cambriolé, mais le risque que cela se produise est beaucoup moins élevé dans un endroit où vous avez des gardes ou des voisins amicaux contrairement à un endroit hostile.

L'analyse des risques est un processus à la fois personnel et subjectif ; tout le monde n'a pas les mêmes priorités ou les mêmes points de vue sur les menaces, ni de la même manière. Beaucoup de gens trouvent certaines menaces inacceptables, quel que soit le risque, car la simple présence de la menace ne peut être acceptée. Dans d'autres cas, les gens ne tiennent pas compte des risques élevés parce qu'ils ne considèrent pas la menace comme un problème.

Maintenant, pratiquons l'évaluation des menaces

Si votre bureau stocke des rapports pointant la corruption dans la fonction publique, vous vous demanderez peut-être :

- Le bureau devrait-il avoir des gardes 24 heures sur 24, des caméras de vidéosurveillance?
- Dans quel type de serrure devrions-nous investir?
- Avons-nous besoin d'une sécurité plus avancée en plus d'une serrure de porte solide?

- Quelle est l'importance de ce que nous essayons de protéger?
  - Des preuves qui peuvent mettre fin à la corruption dans la fonction publique

- Quelle est la menace?
  - Les auteurs présumés tenteront d'entrer par effraction et d'accéder à ces dossiers.

- Quel risque réel si l'accusé entre par effraction? Est-ce probable?
  - Si les auteurs de la corruption obtiennent ces témoignages, ils peuvent attaquer physiquement les lanceurs d'alerte.
  - Ils peuvent voler les fichiers et détruire les preuves qui peuvent être utilisées contre eux

Une fois que vous vous êtes posé ces questions, vous êtes en mesure d'évaluer les mesures à prendre. Si vos biens sont précieux, mais que le risque d'effraction est faible, vous ne voudrez probablement pas investir trop d'argent pour une serrure. Cependant, si le risque est élevé, vous voudrez vous procurer les meilleures serrures du marché, et peut-être même ajouter un système de sécurité.

La sécurité numérique en cinq parties

IMPORTANT

Les actions décrites dans les sections suivantes sont souvent techniques et peuvent comporter différent degrés de risque. Apporter des modifications à vos appareils peut provoquer des erreurs inattendues ou, si elles ne sont pas correctement mises en œuvre, peuvent entraîner une perte de données. Il est conseillé de rechercher toutes les étapes nécessaires pour apporter des modifications techniques en fonction de votre appareil et de votre contexte, de sauvegarder les données importantes, de stocker correctement les nouveaux mots de passe (voir Sécurité du compte pour des conseils spécifiques) et de faire appel à une assistance technique si nécessaire.

Comment puis-je me protéger contre les logiciels malveillants ?

Nansubuga est une défenseur ougandais des droits fonciers. Elle a acheté un nouvel ordinateur, il y a 6 mois. Mais l'ordinateur tourne lentement, elle voit des fenêtres sur son écran qu'elle ne comprend pas, et ses données mobiles (4G) semblent s'épuiser trop rapidement. Elle conservait des documents de projet sur une clé USB, mais ils disparaissent constamment de sa clef.. Elle ne comprend pas ce qui se passe, c'est un nouvel ordinateur et elle a installé tous ses logiciels à partir de sites de téléchargement en ligne et via de bons amis.

Nansubuga est très probablement confrontée à des infections de logiciels malveillants sur son ordinateur. Les logiciels malveillants sont une menace qui affecte tous les utilisateurs d'ordinateurs. *Les logiciels malveillants peuvent entraîner une perte d'informations, une réduction des performances, le vol de documents et l'espionnage.*

SÉCURITÉ DE BASE DE L'APPAREIL

De plus, les juridictions et les perspectives en matière de sécurité numérique varient et chaque individu devrait chercher à en comprendre les risques encourus en fonction de son contexte. Tous les aspects de la vie tournent maintenant autour de la technologie et d'internet , incluant votre téléphone, votre voiture, votre montre et votre réfrigérateur tous connectés à Internet avec la capacité d'envoyer et de recevoir des informations.

Nous confions à nos appareils de nombreuses informations qui montrent qui nous sommes, où nous sommes, ce que nous faisons, ce que nous planifions et avec qui.. Ces dispositifs sont des cibles évidentes pour les attaques, les compromissions et les infiltrations.

Dans ce contexte, il est très important que tous les utilisateurs de nouvelles technologie et d'Internet aient un niveau de connaissances et de compétences de base pour protéger leurs appareils contre les pirates, les logiciels malveillants et toute autre menace pouvant mettre leur vie en danger en raison de la compromission ou de l'attaque de l'appareil.

La sécurité de base des appareils implique les pratiques et les étapes qui mettent vos appareils dans une configuration optimale pour éviter toute compromission.

Logiciel malveillant: programme ou fichier utilisé pour nuire aux utilisateurs d'ordinateurs. Il agit de différentes manières, notamment en perturbant le fonctionnement de l'ordinateur, en recueillant des informations sensibles, en usurpant l'identité d'un utilisateur pour envoyer des spam ou de faux messages, ou en accédant à des systèmes informatiques privés. La majorité des logiciels malveillants sont criminels et sont le plus souvent utilisés pour obtenir des informations bancaires ou des identifiants de connexion pour des comptes de messagerie ou de réseaux sociaux.

Les logiciels malveillants sont également utilisés par des acteurs étatiques et non étatiques pour contourner le cryptage et pour espionner les utilisateurs. Par exemple1, les logiciels malveillants ont un large éventail de capacités. Ils peuvent permettre à un pirate d'enregistrer à partir d'une webcam et d'un microphone et de désactiver le paramètre de notification.

Logiciel antivirus

Vous devez utiliser un logiciel antivirus sur votre ordinateur et votre smartphone. Les logiciels antivirus peuvent être très efficaces pour lutter contre les logiciels malveillants génériques non ciblés qui pourraient être utilisés par des criminels contre la population en général. Cependant, les logiciels antivirus sont généralement inefficaces contre les attaques ciblées et autres attaques sophistiquées, telles que celles vendues par la société de sécurité israélienne NSO Group.

Indicateurs de compromission

Lorsqu'il n'est pas possible de détecter des logiciels malveillants à l'aide d'un logiciel antivirus, il est encore parfois possible de trouver des indicateurs de compromission. Par exemple, Google donne parfois un avertissement aux utilisateurs de Gmail indiquant qu'il pense que votre compte a été ciblé par des pirates soutenus par l'État. De plus, vous remarquerez peut-être une notification indiquant que votre webcam est allumée lorsque vous ne l'avez pas activée vous-même (bien que les logiciels malveillants avancés puissent les désactiver). Cela pourrait être un indicateur de compromission.

---

23 http://pastebin.com/MP8zpQ26

D'autres indicateurs sont moins évidents. Vous remarquerez peut-être que votre adresse e-mail est accessible à partir d'une adresse IP inconnue ou que vos paramètres ont été modifiés pour envoyer des copies de tous vos e-mails à une adresse e-mail inconnue. Votre ordinateur devrait déjà avoir un pare-feu activé tel que le pare-feu Windows ou OS X intégré, mais il est utile d'activer également les pares-feux commerciaux faisant partie de l'ensemble du programme de sécurité Internet.

Comment les agresseurs peuvent-ils utiliser des logiciels malveillants pour me cibler?

Le moyen le plus simple d'être ciblé par des logiciels malveillants est la réception d'e-mails d'hameçonnage. Un agresseur se fait passer pour quelqu'un que vous connaissez et vous envoie un e-mail avec une pièce jointe contenant des logiciels malveillants. Une fois que vous avez téléchargé la pièce jointe et l'avez ouverte, le logiciel malveillant infecte votre ordinateur ou votre appareil.

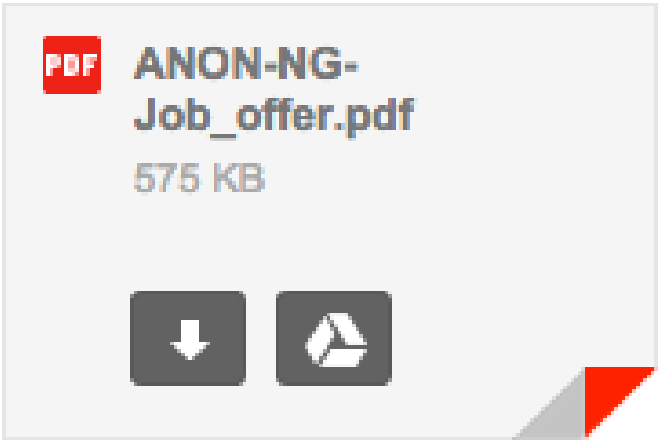
Les attaques "zero-day" sont une autre méthode plus sophistiquée d'infection des appareils avec des logiciels malveillants particulièrement utilisés par les gouvernements et les criminels. Les attaques du type "zero-day" exploitent une vulnérabilité jusque-là inconnue dans un appareil ou une application. Considérez votre ordinateur comme une forteresse; "zero day" serait une entrée secrète cachée que vous ne connaissez pas, mais qu'un agresseur a découverte. Vous ne pouvez pas vous protéger contre une entrée secrète dont vous ignorez même l'existence. Les gouvernements et les organismes chargés de l'application de la loi stockent des exploits "zero-day" pour les utiliser dans des attaques ciblées de logiciels malveillants. Les criminels et autres acteurs peuvent également avoir accès à des attaques de type "zero-day" qu'ils peuvent utiliser pour installer secrètement des logiciels malveillants sur votre ordinateur. Les attaques "zero-day" sont utilisées pour cibler des grandes figures parce qu'ils sont chers à l'achat.

Il existe de nombreuses façons dont un agresseur pourrait essayer de vous inciter à installer des logiciels malveillants sur votre ordinateur. Ils peuvent déguiser la charge utile en un lien vers un site Web, un document, un PDF ou même un programme conçu pour aider à sécuriser votre ordinateur. Vous pouvez être ciblé par un e-mail (qui peut sembler provenir de quelqu'un que vous connaissez), via un message sur Skype ou Twitter, ou même via un lien publié sur votre page Facebook. Plus l'attaque est ciblée, plus l'agresseur prendra soin de vous tenter de télécharger le logiciel malveillant.

Par exemple, en décembre 2014, Neamin Zeleke, directeur général de la Ethiopia Satellite Televisiom (ESAT), a été pris pour cible dans son bureau aux États-Unis avec un logiciel de surveillance à distance de "Hacking Team" qui a été envoyé par l'e-mail prétendant avoir des informations sur les élections éthiopiennes.

En 2013, l'un des collègues de Zeleke a été infecté par un logiciel malveillant après avoir ouvert ce qui semblait être un fichier Microsoft Word. Ils ont appris plus tard qu'il s'agissait du système de contrôle à distance "Hacking Team".

La meilleure façon d'éviter d'être infecté par ce type de logiciels malveillants ciblé est d'éviter d'ouvrir les documents et d'installer un anti-virus en premier lieu. Les personnes ayant plus d'expertise informatique et technique auront un meilleur instinct sur ce qui pourrait être un logiciel malveillant et ce qui pourrait ne pas l'être, mais des attaques bien ciblées peuvent être très convaincantes. Si vous utilisez Gmail, ouvrez des pièces jointes suspectes dans Google Drive plutôt que de les télécharger (les images par exemple) ce qui protégerait votre ordinateur si elles sont effectivement infectées. L'utilisation d'une plate-forme informatique plus sécurisée, comme Ubuntu, Chrome OS ou Mac OS X, améliore considérablement vos chances contre de nombreuses astuces de diffusion de logiciels malveillants, mais ne vous protégera pas contre les adversaires les plus sophistiqués.



Si vous utilisez Gmail, vous pouvez afficher le document joint en cliquant sur cette icône triangulaire à l'intérieur du deuxième carré (et non sur la flèche de téléchargement) du premier carré. Il apparaîtra sur votre navigateur via les filtres de Google plutôt que de télécharger et de s'exécuter sur votre ordinateur, vous épargnant tout risque de virus à l'intérieur du fichier.

Une autre chose que vous pouvez faire pour protéger votre ordinateur contre les logiciels malveillants est de toujours vous assurer que vous exécutez la dernière version de votre logiciel et téléchargez les dernières mises à jour de sécurité. Au fur et à mesure que de nouvelles vulnérabilités sont découvertes dans les logiciels, les entreprises peuvent résoudre ces problèmes et proposer une correction en tant que mise à jour logicielle, mais vous ne récolterez pas les avantages de leur travail si vous installez la mise à jour sur votre ordinateur. Il est communément admis que si vous exécutez une Copie non enregistrée de Windows, vous ne pouvez pas ou ne devez pas accepter les mises à jour de sécurité. Ce n'est pas vrai. Voir ci-dessous plus d'informations sur la mise à jour de vos systèmes.

Que dois-je faire si je trouve des logiciels malveillants sur mon ordinateur?

Si vous trouvez des logiciels malveillants sur votre ordinateur, déconnectez votre ordinateur d'Internet et cessez immédiatement de l'utiliser. Chaque action sur l'ordinateur que vous effectuez peut-être envoyée à un pirate . Vous pourrez peut-être apporter votre ordinateur à un expert en sécurité, qui pourra peut-être découvrir plus de détails sur le logiciel malveillant Si vous avez trouvé le logiciel malveillant, sa suppression ne garantit pas la sécurité de votre ordinateur.

Si vous pensez que votre ordinateur principal contient des logiciels malveillants, connectez-vous à un ordinateur que vous croyez sûr et modifiez vos mots de passe ; chaque mot de passe que vous avez tapé sur votre ordinateur pendant qu'il était infecté pourrait maintenant être compromis.

Vous pourrez aussi réinstaller le système d'exploitation sur votre ordinateur pour supprimer le logiciel malveillant. Cela supprimera la plupart des logiciels malveillants, mais certains logiciels malveillants sophistiqués peuvent persister.

Realiser les mises à jour

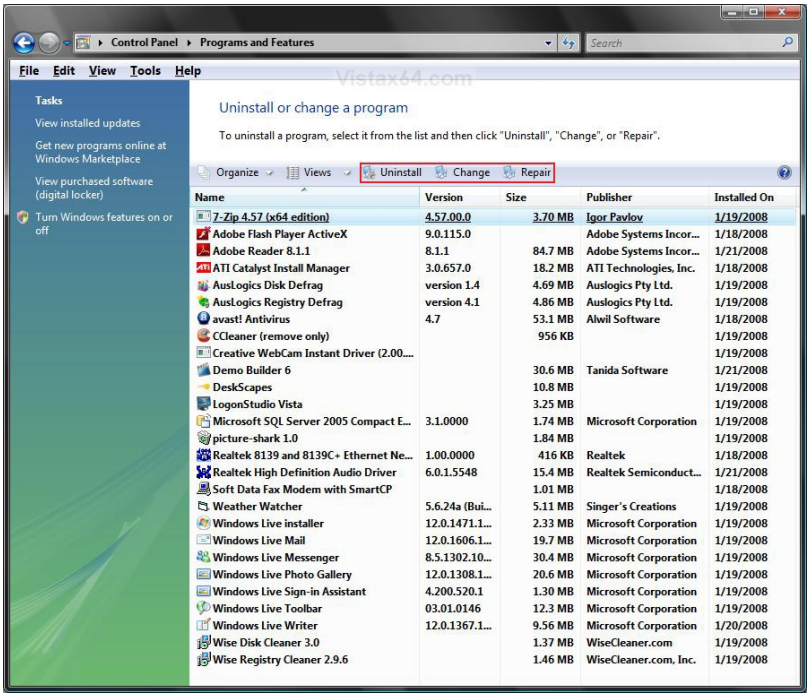
Le matériel informatique et les logiciels ne sont jamais parfaits. Il y aura toujours des problèmes de performance, de stabilité et de sécurité qui apparaîtront sur n'importe quel logiciel : cela inclut votre système d'exploitation (Windows, OS X, Linux), votre téléphone mobile (Android, iOS, Windows Phone), votre logiciel (Adobe, Java, Office, Chrome, Firefox, etc.). Il existe un marché florissant de chercheurs constamment à la recherche de vulnérabilités dans nos systèmes. Ces chercheurs peuvent être des "White Hats" qui divulguent publiquement les vulnérabilités et encouragent les développeurs à corriger les logiciels, défauts, ou il peut s'agir de "Black Hats" qui vendent des vulnérabilités à des acheteurs criminels et gouvernementaux qui prévoient d'utiliser ces vulnérabilités contre des utilisateurs de logiciels.

Si vous voulez voir à quel point les vulnérabilités sont courantes, rendez-vous sur

Https://www.eXploit-db.com/ et parcourez le nombre de vulnérabilités existantes pour les logiciels que nous utilisons. Cela explique pourquoi on nous demande de mettre à jour notre système et nos logiciels.

[Boîte à faire]

Chaque fois que vous avez la possibilité de mettre à jour un logiciel, vous devriez le faire. Si on vous demande de mettre à jour maintenant ou plus tard, mettez toujours à jour dès que possible, ne le remettez pas à plus tard ! Si vous avez la possibilité d'activer les mises à jour automatiques, activez-les. Si vous utilisez le haut débit mobile et payez pour l'utilisation d'Internet par/MB ou par/GB, trouvez une heure pour vous connecter à Internet à partir d'une source illimitée telle qu'une université, une bibliothèque, un bureau ou un café, et commencez les mises à jour. Activez les mises à jour automatiques de votre système d'exploitation, mettez à jour votre navigateur et tous les logiciels que vous utilisez régulièrement. Les gestionnaires d'application mis à jour peuvent également vous aider à gérer les mises à jour et à vous assurer que vous pouvez installer les mises à jour disponibles pour vos applications.



24 Google Chrome includes a secured version of Ado be Flash inside of all of its updates.

Pratiques de logiciels sécurisés

Étant donné que les logiciels deviennent malheureusement vulnérables et doivent être mis à jour tout le temps, l'un des moyens les plus simples de rester en sécurité est d'éviter d'installer des programmes inutiles. Adobe Flash et Oracle Java sont deux programmes qui ont souvent des défauts critiques. Vous n'aurez probablement peut-être pas besoin de l'un ou l'autre de ces programmes sur votre ordinateur2. Accédez à votre liste de programmes installés (Dans Windows: Ajout/Suppression de programmes ou Désinstaller ou modifier un programme) et vérifiez ce qui est installé. Y a-t-il des programmes dont vous ne reconnaissez pas le nom ? Certains d'entre eux peuvent être importants pour le fonctionnement de votre ordinateur, mais si quelque chose vous semble suspect, recherchez ce que c'est et décidez si vous le supprimez. Méfiez-vous particulièrement des logiciels installés qui n'ont pas d'éditeur répertorié dans la colonne Éditeur. Recherchez également les barres d'outils du navigateur d'assistance qui ont été installées à votre insu.

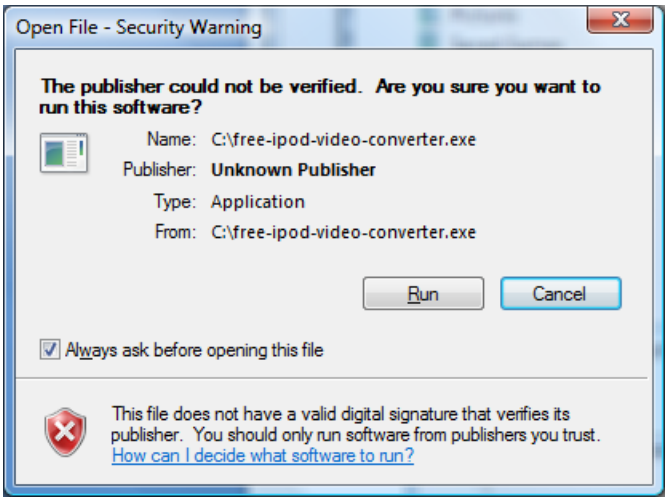
Sources fiables

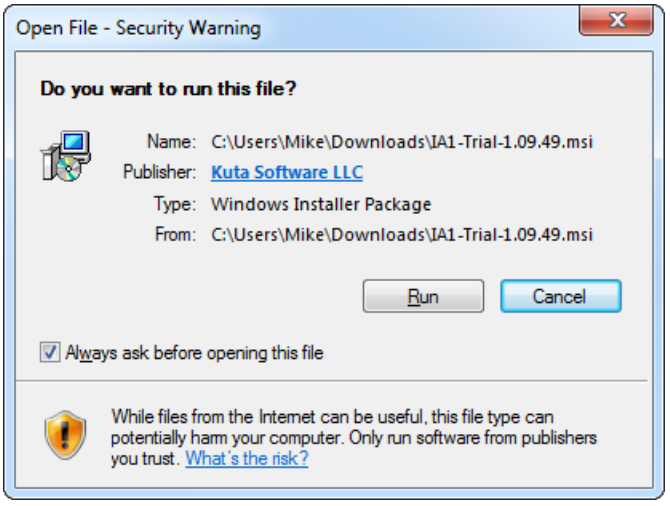
Le logiciel doit être obtenu directement auprès de l'éditeur du logiciel autant que possible. Par exemple,

Il est préférable de télécharger Adobe Reader à partir de https://get.adobe.com/reader/ plutôt que de www.download.com ou de toute autre source. De même, vous devez éviter d'installer des logiciels à partir des disques durs d'amis ou des fichiers EXE qui vous sont envoyés par e-mail ou messagerie instantanée. Le logiciel peut être modifié ou peut être complètement faux et infecter votre ordinateur.

Les sites de téléchargement gratuit regroupent souvent des téléchargements de logiciels avec d'autres téléchargements supplémentaires indésirables qui promettent des fonctionnalités supplémentaires, mais ne sont pas initialement désirés ou nécessaires et peuvent même être nocifs pour votre ordinateur. Voir une histoire en ligne3 sur un test pour installer les 10 meilleurs téléchargements qui ont conduit un ordinateur à être gravement endommagé !

Chaque fois que vous installez un logiciel, vérifiez l'éditeur du logiciel. La plupart des éditeurs réputés signent leur logiciel, ce qui indique qu'il provient d'eux et n'a pas été modifié. Comparez les deux écrans d'avertissement Windows suivants pour voir la différence entre les logiciels signés et non signés :





N'oubliez pas que la plupart des logiciels dont vous avez besoin peuvent être obtenus gratuitement directement sur les sites Web des éditeurs. Si vous voyez une offre pour obtenir quelque chose gratuitement que vous auriez autrement dû payer, c'est probablement trop beau pour être vrai ! Prenez quelques précautions de base et vous préserverez la vitesse, la stabilité et la sécurité de votre ordinateur à long terme

2 Google Chrome includes a secure version of Adobe Flash inside all updates.
3 http://www.howtogeek.com/198622/her - es-what-happens-when-you-install-the-top-10-download.com-apps/

SECURITE DES DONNEES SUR LES APPAREILS

Daud travaille pour une ONG. Il y a quelques semaines, ils ont été victimes d'un cambriolage dans leurs bureaux, où des ordinateurs de bureau, des ordinateurs portables, des appareils photo et des téléphones portables ont été volés. Les contrats, les documents financiers, les contacts, les dossiers de recherche et les publications de l'organisation ont tous été volés. Aucun ordinateur n'avait fait de sauvegarde des données. La direction de Daud s'inquiète des motivations des voleurs et craint que les informations confidentielles qu'ils détenaient ne tombent entre de mauvaises mains.

La perte de données est douloureuse pour tout individu ou organisation car elle vous nuit à deux égards: d'une part, vous perdez vous-même des informations vitales nécessaires à votre travail, et d'autre part, quelqu'un d'autre a maintenant vos informations en sa possession sans autorisation.

Daud devrait lutter contre ce risque à plusieurs niveaux. Il peut utiliser le cryptage pour brouiller des données afin que seule la personne avec le mot de passe correct puisse lire les données d'origine. Il peut également sauvegarder régulièrement des données sur des appareilsphysiques et en ligne.

Qu'est-ce que le cryptage?

Le cryptage est un moyen de brouiller les données afin que seules les parties autorisées puissent avoir accès aux informations.

Aujourd'hui, nous avons des ordinateurs qui peuvent effectuer le cryptage pour nous. La technologie de cryptage numérique s'est étendue au-delà des simples messages secrets ; par exemple, le cryptage peut être utilisé à des fins plus élaborées, telles que la protection de documents, la vérification de l'auteur de messages ou la navigation anonyme sur le Web.

Protéger vos données grâce au cryptage

Beaucoup d'entre nous transportons nos matériels de communications, des informations sur nos contacts et des documents sensibles de travail sur des ordinateurs portables, des disques durs et même des téléphones mobiles. Ces données peuvent inclure des informations confidentielles sur votre travail, votre communauté, vos réseaux et le suivi des droits de l'homme. Un appareil physique peut être volé ou copié en quelques secondes.

Les ordinateurs et les téléphones mobiles peuvent être verrouillés par des mots de passe, des codes PIN ou des symboles, mais ces verrous ne permettent pas de protéger les données si l'appareil lui-même est saisi. Il est relativement simple de contourner ces verrous car vos données sont stockées sous une forme facilement lisible dans l'appareil.

En utilisant le cryptage, vous pouvez rendre plus difficile pour ceux qui volent des données de déverrouiller leurs secrets. Si vous utilisez le cryptage, votre adversaire a besoin non seulement de votre appareil, mais aussi de votre mot de passe pour déchiffrer/déverrouiller les données cryptées - il n'y a pas de raccourci. Il existe différentes applications du cryptage : cryptage complet de l'appareil, cryptage de fichiers ou de dossiers et cryptage des communications (qui seront expliqués dans le chapitre suivant)

Il est plus sûr et plus facile de crypter toutes vos données, pas seulement quelques dossiers. La plupart des ordinateurs et des smartphones offrent un cryptage complet de l'appareil (ou du disque complet) en option. Le cryptage complet de l'appareil garantit que le contenu d'un ordinateur ou d'un téléphone ne peut pas être consulté par des personnes non autorisées. Le cryptage complet de l'appareil brouillera toutes les informations écrites sur l'appareil et aura besoin d'un mot de passe pour déchiffrer les informations avant que l'appareil puisse être utilisable.

Les téléphones Android l'offrent dans les paramètres de sécurité, et les appareils mobiles Apple tels que l'iPhone et l'iPad le décrivent comme la protection des données et l'activent automatiquement si vous définissez un mot de passe. Sur un ordinateur utilisant Windows Professionnel l'application de cryptage est connu sous le nom de BitLocker. Sur Mac, il s'appelle FileVault. Sur les appareils Linux, le cryptage complet du disque est généralement offert lorsque vous configurez votre système pour la première fois via un système appelé LUKS. Des logiciels indépendants comme VeraCrypt et Disk Cryptor peuvent également vous aider à atteindre les mêmes objectifs.

Les systèmes de cryptage complet du disque peuvent également être utilisés pour crypter des appareils portables tels que des disques durs externes et des disques flash à l'aide de BitLocker to Go (Windows), Filevault (Mac) ou VeraCrypt (Windows, Mac et Linux).

Une faiblesse potentielle du cryptage complet de l'appareil est qu'il s'agit d'un point de vulnérabilité unique : si vous êtes obligé de déverrouiller un appareil, tous vos fichiers seront vulnérables. Une solution plus robuste consiste à combiner le cryptage complet de l'appareil avec le cryptage des fichiers et des dossiers pour protéger vos documents les plus vulnérables de toute personne ayant accès à vos comptes d'appareils principaux.

Le cryptage des fichiers et dossiers vous permettent de crypter des fichiers ou des parties uniques de votre ordinateur. Une option excellente multiplateforme (fonctionnant sur les ordinateurs Windows, Mac et Linux) est VeraCrypt.

VeraCrypt vous permet de créer un volume secret pour vos fichiers qui fonctionne comme un disque flash USB virtuel mais qui existe en fait à l'intérieur d'un fichier unique crypté sur votre ordinateur. Une autre option, très facile à utiliser, est AxCrypt , un logiciel Windows uniquement, qui ajoute le cryptage des fichiers au menu "clic droit " de votre ordinateur, vous permettant de crypter des fichiers individuels facilement et à volonté.

Consultez la partie suivante du manuel pour obtenir des liens pour en savoir plus sur ces options.

Rappelez-vous cependant que le cryptage n'est efficace que si votre mot de passe l'est aussi. N[écrivez pas votre mot de passe sur un post-It attaché à votre ordinateur et ne conservez pas une liste de mots de passe dans votre bloc-notes. Si votre agresseur obtient votre appareil, il peut essayer de nombreux mots de passe jusqu'à ce qu'il devine le bon. Les logiciels de craquage peuvent essayer des millions de mots de passe par seconde. Cela signifie qu'il est peu probable qu'un code PIN à quatre chiffres protège vos données très longtemps, et même un mot de passe long ne pourra que ralentir votre hacker. Dans ces conditions, un mot de passe suffisamment fort devrait comporter plus de quinze caractères. Consultez le chapitre de la sécurité du compte pour plus d'informations sur la création de mots de passe forts.

Logiciels et guides de cryptage

Cryptage de l'ordinateur

BitLocker (Windows) - Disponible sur les versions professionnelles de Windows 7 et 8, et sur la plupart des versions de Windows 8 [26]. et posterieures. En savoir plus sur Microsoft avec un guide étape par étape sur son utilisation. Un guide plus facile à utiliser est disponible sur HowToGeek-1plus, un autre sur Windows Central spécifiquement pour Windows 10[27]. Notez que BitLocker nécessite par défaut un appareil appelé module de plateforme sécurisée (MPS) qui n'est souvent disponible que sur les ordinateurs professionnels haut de gamme. Les deux guides liés ici incluent des instructions sur la façon d'activer BitLocker sur les ordinateurs sans MPS.

FileVault (Mac) - Le cryptage complet de l'appareil est facile à configurer sur la plupart des ordinateurs Mac. Suivez les instructions d'Apple pour activer FileVault à partir de vos Préférences Système[28].

Disk Cryptor29 (Windows) - Lisez le guide de "Electronic Frontier Foundation" sur le logiciel de cryptage complet de disque pour Windows[30].

26 http://www.howtogeek.com/192894/how-to-set-up-bitlocker-encryption-on-windows/
27 http://www.windowscentral.com/how-use-bitlocker-encryption-windows-10
28 https://support.apple.com/en-us/HT204837
29 https://diskcryptor.net/
30 https://ssd.eff.org/en/module/how-encrypt-your-windows-device

VeraCrypt[31] (Windows, Mac, Linux) - Logiciel qui peut crypter des parties de votre disque dur ou le disque entièrement et des disques amovibles. "Security in a Box"est un excellent guide[32].

Cryptage du téléphone

Cryptage de téléphone Android - Lisez le guide de HowToGeek[33].

Cryptage iPhone et iPad - Il suffit d'activer un verrouillage par mot de passe sur votre appareil pour activer le cryptage de l'appareil. Pour en savoir plus, consultez le guide de 'Electronic Frontier Foundation [34]

Disques externes

BitLocker To Go **(Windows)** – Cryptez les disques durs externes et les disques flash avec BitLocker to Go[35].

File Vault (Mac) – Cryptez les disques durs externes et les disques flash en faisant clic droit sur le périphérique amovible dans la barre de recherche et en choisissant Crypter ... Puis choisir un mot de passe. Voir le guide d'Apple[36].

Notez que les solutions des disques externes ci-dessus limiteront l'usage des disques cryptés uniquement aux ordinateurs Mac ou Windows. VeraCrypt propose également une solution de cryptage de disque externe multiplateforme.

SAUVEGARDE DE VOS DONNÉES

La sécurité de l'information, c'est aussi avoir accès à vos données quand vous en avez besoin. Quelles sont les menaces à la disponibilité de vos informations? Le vol de vos ordinateurs dans des lieux publics et privés est un risque courant, mais des choses comme les virus, plantage d'ordinateur, les incendiess, les dégâts des eaux ou les pannes de disque dur peuvent entraîner la perte de données aussi. Pour faire face à ce risque, vous devez régulièrement conserver des sauvegardes de vos fichiers.

Les sauvegardes sont traditionnellement effectuées sur des disques durs externes, des clés USB et des disques amovibles tels que des CD et des DVD. Ces supports de stockage sont vulnérables au vol et aux accès indésirables, vous devez donc également crypter vos sauvegardes. Consultez la liste des ressources de la section précédente pour savoir comment chiffrer des disques de stockage externes.

Faire des sauvegardes peut être aussi simple que de copier et coller vos dossiers de travail sur un disque externe. Cependant, de nombreuses applications sont disponibles pour aider à effectuer des sauvegardes. Windows dispose de deux options de sauvegarde intégrées (non disponibles dans toutes les versions) : Sauvegarder & Restaurer [37] préservera tout le système à partir duquel vous pourrez récupérer vos données en cas de perte , en outre, vous pouvez planifier les mises à jour de cette sauvegarde complète; et l'historique des fichiers[38], qui conservera les versions des documents au fur et à mesure qu'elles changent au fil du temps. Vous pouvez utiliser l'un ou l'autre de ces systèmes ou les deux en même temps. Mac OS X dispose également d'un système de sauvegarde intégré appelé "Time Machine"[39] qui fournit des sauvegardes incrémentielles sur un disque dur externe, qui peut éventuellement être crypté en activant l'option de cryptage lors de l'installation.

Il est utile d'avoir une sauvegarde numérique en nuage "Cloud" locale et à distance de vos fichiers. Vous pouvez utiliser des programmes de sauvegarde cloud gratuits populaires tels que **Dropbox, Google Drive, Copy et OneDrive**. Si vous êtes certain de la confidentialité de vos sauvegardes contre l'accès par le fournisseur de cloud (tel que Google, Microsoft et Dropbox), vous devriez regarder les programmes de sauvegarde qui cryptent vos fichiers sur votre ordinateur avant qu'ils ne soient téléchargés vers le fournisseur de cloud : voir Mega, Sync.com, SpiderOak et Wuala. Il existe même un logiciel qui crypte votre fichier localement, puis transmet les fichiers cryptés à Dropbox et à d'autres fournisseurs de sauvegarde Cloud : voir BoxCryptor,[40] Duplicati,[41] et Vivo[42]

31 https://veracrypt.fr/en/Home.html
32 https://securityinabox.org/en/guide/veracrypt/windows
33 http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/
34 https://ssd.eff.org/en/module/how-encrypt-your-iphone
35 https://technet.microsoft.com/en-us/magazine/ff404223.aspx
36 https://www.uvm.edu/it/kb/article/encrypt-external-drive/
37 https://support.microsoft.com/en-us/help/17127/windows-back-up-restore
38 https://support.microsoft.com/en-us/help/17128/windows-8-file-history
39 Time Machine https://support.apple.com/en-us/HT201250
40 https://www.boxcryptor.com/
41 www.duplicati.com

SECURITE DES DONNEES CIRCULANT SUR LES RESEAUX INFORMATIQUES

... Geraldine est une défenseure des droits qui milite pour la protection de l'environnement. Elle planifiait une réunion de sensibilisation avec toutes les personnes de sa région pour les informer d'une initiative gouvernementale prévue pour donner une forêt aux investisseurs étrangers. Elle a écrit un e-mail à tous les dirigeants locaux, leur disant d'informer tout le monde de la date et du lieu de la réunion. Quelques jours après la réunion, elle a été choquée d'apprendre qu'aucun des dirigeants locaux n'avait reçu son e-mail.
Quelques jours plus tard, elle a reçu la visite de la police qui l'a mise en garde contre l'incitation au public et le sabotage des programmes gouvernementaux. Elle s'est demandé ce qu'il était advenu de son courriel et comment la police avait obtenu sa communication au lieu des destinataires prévus.

Ce qui est arrivé à Géraldine s'appelle la surveillance. C'est quand quelqu'un peut surveiller vos communications parce qu'elles sont communiquées en texte brut sur Internet.

Géraldine peut utiliser des cryptages tels que Protocole de Transfer hypertexte sécurisé (HTTPS), L'application "GPG" et Réseau Privé Virtuel (VPN) pour garder ses communications secrètes et confidentielles afin qu'elles ne puissent pas être utilisées pour l'intimider alors qu'elle fait son travail.

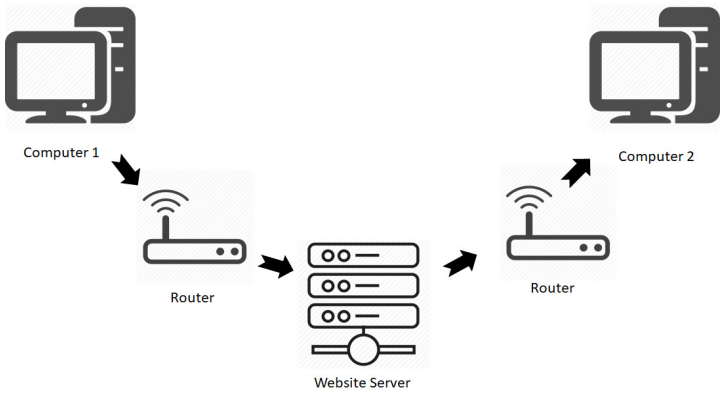
Comment fonctionne l'internet

Internet est un réseau de réseaux qui permet l'échange d'informations entre l'ordinateur client et les serveurs. Les ordinateurs clients sont les appareils que vous utilisez, tels que votre ordinateur portable, votre ordinateur de bureau, votre téléphone mobile. Ils demandent des informations ou des services hébergés ou stockés sur des ordinateurs serveurs. L'ordinateur client et l'ordinateur serveur utilisent une variété de protocoles (comme un langage partagé que toutes les parties comprennent) tels que HTTP (Protocole de Transfert Hypertexte) pour les requêtes et réponses entre eux. Toutes les informations communiquées via le protocole HTTP circulent sur Internet sous forme de texte brut : toute personne ayant une position privilégiée dans le réseau comme un service Internet, Le fournisseur, l'administrateur d'un cybercafé ou l'un des centaines de milliers de points d'échange internet pourrait enregistrer vos communications.

Une illustration simple du fonctionnement d'Internet serait quelqu'un qui accède à un site Web pour lire des informations.

Comme vous pouvez le voir, il existe de nombreux autres ordinateurs impliqués dans la connexion de l'utilisateur au serveur dont il a besoin. Sur des protocoles non sécurisés, ces autres ordinateurs pourraient également lire et même modifier le contenu de la communication de l'utilisateur.

Heureusement, il existe des protocoles plus sécurisés pour aider à sécuriser nos données et nos communications qui se déplacent sur Internet. Cependant, nous devons comprendre ce qu'ils sont et quels sont les outils qui les utilisent.

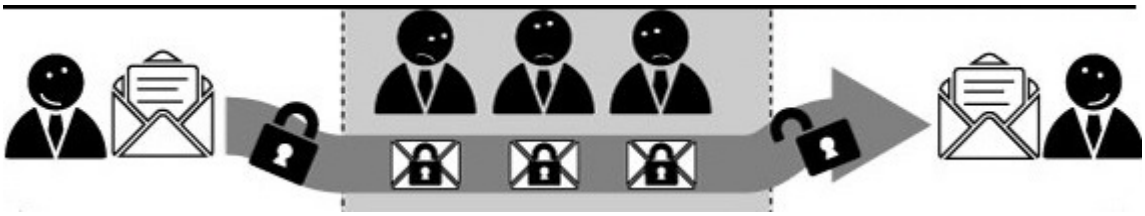


Communiquer avec les autres

Les réseaux de télécommunications et Internet ont rendu la communication avec les gens plus facile que jamais, mais ont également rendu la surveillance plus répandue qu'elle ne l'a jamais été dans l'histoire de l'humanité. Sans prendre de mesures supplémentaires pour protéger votre vie privée, chaque appel téléphonique, message texte, courriel, message instantané, appel vocal sur protocole internet, discussion vidéo et message sur les réseaux sociaux peut être vulnérable aux oreilles indiscrètes.

Souvent, le moyen le plus sûr de communiquer avec les autres est en personne physique, sans que des ordinateurs ou des téléphones soient impliqués. Puisque ce n'est pas toujours possible, la meilleure chose à faire est d'utiliser le cryptage de bout en bout lors de la communication sur un réseau si vous avez besoin de protéger le contenu de vos communications.

Comment fonctionne le cryptage de bout en bout ?



Lorsque deux personnes veulent communiquer en toute sécurité (par exemple, Kamau et Abuya), elles doivent chacune générer des clés cryptographiques. Avant que Kamau n'envoie un message à Abuya, il le crypte dans la clé d'Abuya afin que seul Abuya puisse le décrypter. Ensuite, elle envoie le message déjà crypté sur Internet. Quelqu'un peut écouter Kamau et Abuya, si 'il a accès au service que Kamau utilise pour envoyer ce message (comme son compte de messagerie). Alors, il peut voir seulement les données cryptées et ne pourra pas lire le message. Quand Abuya le reçoit, il doit utiliser sa clé pour le décrypter en un message lisible. C'est ainsi que fonctionne le cryptage de bout en bout.

Le cryptage de bout en bout implique un certain effort, mais c'est le seul moyen pour les utilisateurs de vérifier la sécurité de leurs communications sans avoir à faire confiance à la plate-forme qu'ils utilisent tous les deux. Certains services, tels que Skype, ont revendiqué[43] offrir un cryptage de bout en bout alors qu'ils semblent ne pas le faire . Pour que le cryptage de bout en bout soit sécurisé, les utilisateurs doivent être en mesure de vérifier que la clé de cryptage qu'ils utilisent appartient aux bonnes personnes . Si un logiciel de communication n'a pas cette capacité interne, alors tout cryptage qu'il pourrait utiliser peut-être intercepté par le fournisseur de services lui-même par exemple si un gouvernement l'y oblige.

Appels vocaux

Lorsque vous passez un appel à partir d'un téléphone fixe ou mobile, votre appel n'est pas crypté de bout en bout. Si vous utilisez un téléphone mobile, votre appel peut être (faiblement) crypté entre votre combiné et les antennes de téléphonie cellulaire. Cependant, lorsque votre conversation circule sur le réseau téléphonique, elle est vulnérable à l'interception par votre compagnie de téléphone et, par extension, par tout gouvernement ou organisation qui a du pouvoir sur votre compagnie de téléphone. Le moyen le plus simple de vous assurer d'avoir un cryptage de bout en bout sur les conversations vocales est d'utiliser la communication vocale de protocole d'internet instantanée.

Faites attention ! La plupart des fournisseurs populaires de communication vocale du protocole internet, tels que Skype et Google pour Google Meet, offrent un cryptage de transport afin que les espions ne puissent pas écouter, mais les fournisseurs eux-mêmes sont toujours potentiellement en mesure d'écouter. Selon votre type de menace, cela peut ou non poser un problème.

Certains services /outils qui offrent une communication vocale cryptée de bout en bout incluent :

- Wire[44]
- Silent Phone[45]
- Signal[46]

Afin d'avoir des conversations vocales sur internet cryptées de bout en bout, les deux parties doivent utiliser le même logiciel (ou deux logiciels compatibles).

Messages texte et Messagerie instantanée

Les messages texte standard n'offrent pas de cryptage de bout en bout. Si vous souhaitez envoyer des messages cryptés sur votre téléphone, envisagez d'utiliser un logiciel de messagerie instantanée crypté au lieu de messages texte. Actuellement, la seule façon d'envoyer des messages cryptés est d'utiliser l'application Silence[47] pour Android, anciennement msg Sécurisé

D'autres options de messagerie sécurisée fonctionnent sur Internet. Ainsi, par exemple, les utilisateurs de[48] Android et iOS peuvent discuter en toute sécurité en utilisant Signal. [49]

43 https://support.skype.com/en/faq/fa10983/what-are-p2p-communications
44 https://wire.coma/en/
45 https://www.silentcircle.com/services#mobile
46 https://ssd.eff.org/en/module/how-use-signal-ioshttps://ssd.eff.org/en/module/how-use-signal-android
47 https://silence.im/
48 https://whispersystems.org/#privacy
49 https://ssd.eff.org/en/module/how-use-signal-ioshttps://ssd.eff.org/en/module/how-use-signal-android

"Off-the-Record (OTR)" est un protocole de cryptage de bout en bout pour les conversations textuelles en temps réel qui peut être utilisé en plus d'une variété de services.

Certains outils qui intègrent "OTR" avec la messagerie instantanée incluent:
Pidgin[50] (Linux)

- Adium[51] (For OS X)
- ChatSecure[52] (Android)
- Jitsi[53] (For Windows, Linux, and OS X)
- Jitsi Meet[54] (pour une vidéoconférence sécurisée dans votre navigateur Web)

L'e-mail(Courrier électronique)

La plupart des fournisseurs de messagerie vous donnent un moyen d'accéder à votre l'e-mail à l'aide d'un navigateur Web, tel que Firefox, Microsoft Edge, Chrome, etc. Parmi ces fournisseurs, la plupart d'entre eux utilisent le Protocole de Transfert Hypertexte Sécurisé (HTTPS), ou le cryptage de la couche transport. Vous pouvez verifier que votre fournisseur de messagerie électroniques utilise HTTPS, en vous connectant à votre courriel web. Si l'adresse URL (Localisateur des ressourcés Uniformes) commence avec les lettres HTTPS et non pas Protocole de Transfert Hypertexte (HTTP), cela est bien le cas.

Si votre fournisseur de l'e-mail utilise HTTPS, mais ne le fait pas par défaut, essayez de remplacer HTTP par HTTPS dans l'URL et actualisez la page. Si vous souhaitez vous assurer que vous utilisez toujours HTTPS sur les sites où il est disponible, téléchargez le module complémentaire de navigateur HTTPS Everywhere[55] pour Firefox ou Chrome.

Certains fournisseurs de courriel Web qui utilisent HTTPS par défaut incluent:

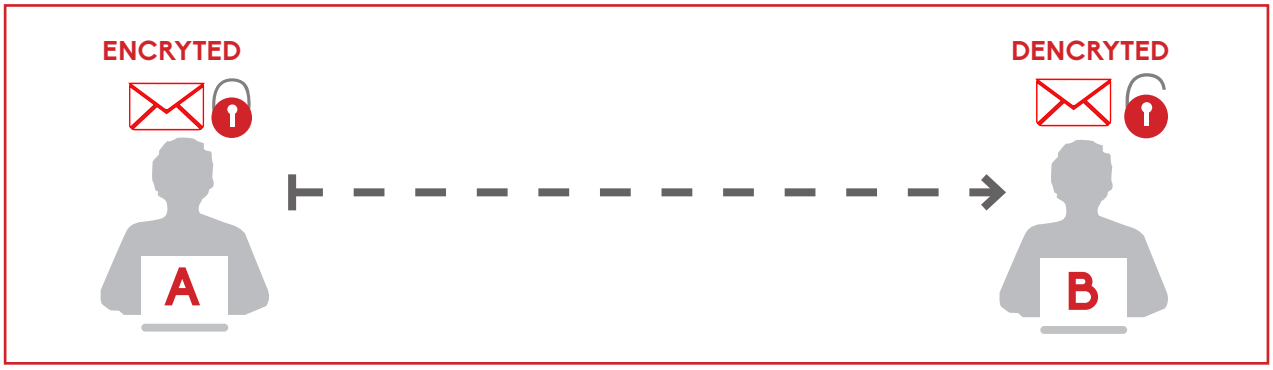
- Gmail
- Riseup
- Yahoo

Certaines messageries en ligne vous donnent la possibilité de choisir d'utiliser HTTPS par défaut en le sélectionnant dans vos paramètres. Le service le plus populaire qui le fait encore est "Hotmail"

Que fait le cryptage de la couche de transport et pourquoi en avez-vous besoin?

HTTPS, également appelé Couche de sockets sécurisée (SSL) ou Sécurité de la Couche de Transport, (TLS), crypte vos communications afin qu'elles ne puissent pas être lues par d'autres personnes sur votre réseau. Cela peut inclure d'autres personnes utilisant le même Wi-Fi dans un aéroport ou un café, les autres personnes de votre bureau ou de votre école, les administrateurs de votre fournisseur d'internet., des pirates informatiques malveillants, des gouvernements ou des responsables de l'application de la loi. Les communications envoyées via votre navigateur Web, y compris les pages Web que vous visitez et le contenu de vos e-mails, articles de blog et messages, en utilisant HTTP plutôt que HTTPS sont susceptibles d'être interceptées et lu par un pirate informatique.

Les acteurs étatiques et non-étatiques malveillants sont de plus en plus habiles pour détourner des sessions HTTPS entre l'ordinateur et le serveur. De cette façon, ils peuvent présenter au navigateur un faux certificat SSL de votre serveur prévu et si vous ignorez les avertissements du navigateur, toute la session et les échanges d'informations entre votre ordinateur et le serveur seront compromis.



50 https://ssd.eff.org/en/module/how-use-otr-linux
51 https://ssd.eff.org/en/module/how-use-otr-mac
52 https://guardianproject.info/howto/chatsecurely/
53 https://jitsi.org/
54
55 https://www.eff.org/https-everywhere

Dans de telles circonstances, il est très important de ne pas procéder à la connexion à moins qu'il ne s'agisse d'un certificat local auto-signé. Il est généralement conseillé d'attendre un moment et d'essayer d'accéder à nouveau au site plus tard si l'avertissement affiché dans l'image ci-dessus vous est présenté.

Sécurité avancée de la messagerie utilisant des logiciels clés de cryptographie (GPG/PGP)

Mais il y a certaines choses que le protocole HTTPS ne peut pas faire. Lorsque vous envoyez des messages à l'aide de HTTPS, votre fournisseur de messagerie reçoit toujours une copie non cryptée de votre communication. Les gouvernements et les organismes d'application de la loi peuvent être en mesure d'accéder à ces données avec un mandat. Aux États-Unis, par exemple, la plupart des fournisseurs de messagerie ont des directives qui précisent qu'ils vous informeront lorsqu'ils auront reçu une demande gouvernementale d'accès à vos données étant donné qu'ils sont légalement autorisés à le faire, mais ces directives sont strictement volontaires et, dans de nombreux cas, les fournisseurs sont légalement empêchés d'informer leurs clients sur des demandes de leurs données. Certains fournisseurs de messagerie, tels que Google[56], Yahoo[57] et Microsoft[58], publient des rapports de transparence, détaillant le nombre de gouvernements qui font des demandes de données des utilisateurs, quels pays font les demandes et la fréquence à laquelle l'entreprise s'y est conformée en transmettant des données.
Si vous êtes menacé par un gouvernement ou des forces de l'ordre, ou si vous avez une autre raison de vouloir vous assurer que votre fournisseur de messagerie n'est pas en mesure de remettre le contenu de vos communications via un e-mail à un tiers, vous pouvez envisager d'utiliser le cryptage de bout en bout pour vos communications par e-mail.

"PGP (ou Pretty Good Privacy)" est la norme pour le cryptage de bout en bout de vos e-mails. Utilisé correctement, il offre des protections très fortes pour vos communications. PGP est également appelé GPG (Gnu Privacy Guard). Dans PGP, chaque partie crée une clé en deux parties : une partie privée et une partie publique. Vous protégez la partie privée en toute sécurité sur vos propres appareils, mais vous distribuez la partie publique à toute personne avec qui vous souhaitez communiquer en utilisant PGP. Pour aider à illustrer les concepts de PGP, Tactical Technology Collective a une série de vidéos explicatives appelées Decrypting Encryption[59].

[Boîte de ressources]

Pour obtenir des instructions détaillées sur l'installation et l'utilisation du cryptage PGP/GPG pour votre messagerie à l'aide des clients de messagerie sur votre ordinateur, consultez ces guides pour MacOSX, Windows,[60] et Linux[61].

Pour utiliser PGP/GPG dans votre navigateur Web à l'aide du webmail, envisagez d'utiliser le navigateur branché Mailvelope[62] ou faites attention aux clients de courriel Web complets comme ProtonMail[63].

Assurez-vous que le cryptage est activé sur votre client de messagerie avant de communiquer une information ou une pièce jointe à votre destinataire. Pour ce faire, suivez comment activer le cryptage PGP sur vos clients de messagerie à partir du lien: https://ssd.eff.org/en/module-categories/tool-guides

Ce que le cryptage de bout en bout ne fait pas !!!

Le cryptage de bout en bout protège le contenu de votre communication, non pas le principe même de la communication. Il ne protège pas vos métadonnées, c'est-à-dire tout le reste, y compris la ligne "objet" de votre e-mail, ou avec qui et quand vous communiquez.
Les métadonnées peuvent fournir des informations extrêmement révélatrices sur vous même lorsque le contenu de votre communication reste secret.
Les métadonnées de vos appels téléphoniques peuvent révéler des informations très intimes et sensibles. Par exemple:
Ils savent que vous avez appelé au service de soutien sur la dépression à 14h24 et que vous avez utilisés 18 minutes mais ils ne savent pas de quoi vous avez parlé.

- Ils savent que vous appelé la radio locale pendant une heure de discussion sur des sujets politiques mais le contenu exact de l'appel reste secret.
- Ils savent que vous avez appelé un centre d'information gratuite sur le VIH, puis votre médecin , puis votre entreprise d'assurance maladie dans la même heure Mais ils ne peuvent pas savoir de quoi vous avez parlé.

56 https://www.google.com/transparencyreport/
57 https://transparency.yahoo.com/
58 https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
59 https://tacticaltech.org/projects/decrypting-encryption
60 https://ssd.eff.org/en/module/how-use-pgp-mac-os-x
61 https://ssd.eff.org/en/module/how-use-pgp-linux
62 https://www.mailvelope.com/
63 https://protonmail.com/

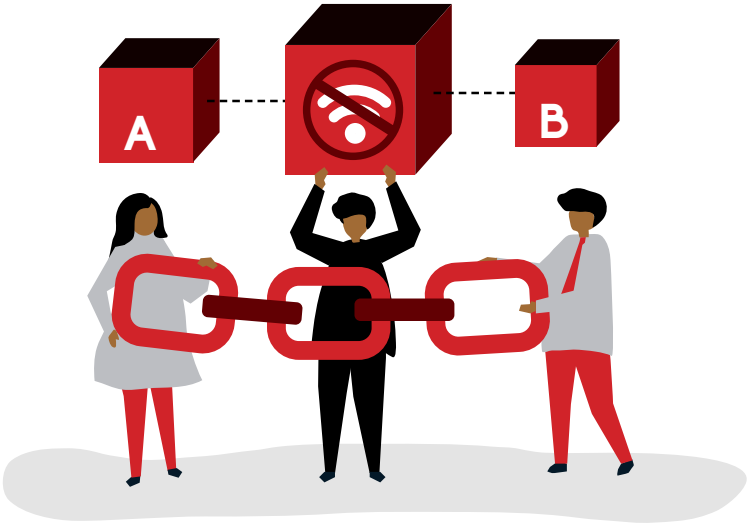
- Ils savent que vous avez reçu un appel de la part du bureau général de l'opposition politique locale alors qu'il mettait en place une campagne contre les lois régissant les médias; puis que vous ayez appelé immédiatement votre patron, mais le contenu de ces appels reste à l'abri du gouvernement.

- Ils savent que vous avez appelé un gynécologue, parlé pendant une demi-heure, puis appelé le numéro local du planning familial plus tard dans la journée, mais personne ne sait de quoi vous avez parlé.

Si vous appelez à partir d'un téléphone cellulaire, les informations sur votre emplacement sont des métadonnées. Par exemple, en 2009, le politicien allemand du Parti vert Malte Spitz a poursuivi en justice l'entreprise Deutsche Telekom pour les forcer à transmettre les six mois des données téléphoniques de Spitz, données qu'il a mises à la disposition d'un journal allemand pour démontrer l'importance des métadonnées. Le résultat [64] a montré un historique détaillé des déplacements de Spitz. Spitz a prononcé une conférence TED inspirante sur cette affaire qui est disponible en ligne[65].

64 http://www.zeit.de/datenschutz/malte-spitz-data-retention
65 http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching?language=en

Comment contourner la censure en ligne



De nombreux gouvernements, entreprises, écoles et points d'accès publics utilisent des logiciels pour empêcher les internautes d'accéder à certains sites Web et services Internet. C'est ce qu'on appelle le filtrage ou le blocage d'Internet et c'est une forme de censure. Le filtrage de contenu se présente sous différentes formes. Parfois, des sites Web entiers sont bloqués, parfois des pages Web individuelles et parfois le contenu est bloqué en fonction des mots-clés qu'ils contiennent. Un pays peut bloquer complètement Facebook, ou seulement bloquer des pages de groupe Facebook particulières, ou il peut bloquer n'importe quelle page ou recherche sur le Web qui comporte le mot homosexualité.

Quelle que soit la façon dont le contenu est filtré ou bloqué, vous pouvez presque toujours obtenir les informations dont vous avez besoin en utilisant un outil de contournement. Les outils de contournement fonctionnent généralement en détournant votre activité sur le Web ou autre via un autre ordinateur, de sorte qu'il contourne les machines menant à la censure. Un intermédiaire par lequel vous faites passer vos communications dans ce processus est appelé un "proxy".

Les outils de contournement n'offrent pas nécessairement une sécurité ou un anonymat supplémentaire, même ceux qui promettent la confidentialité ou la sécurité ou qui ont des termes comme "anonyme" dans leurs noms.

Il existe différentes façons de contourner la censure sur Internet, dont certaines fournissent des couches de sécurité supplémentaires. L'outil qui vous convient le mieux dépend de la menace qui pèse sur vous.

Techniques de base

HTTPS est la version sécurisée du protocole HTTP utilisé pour accéder aux sites Web. Parfois, un censeur bloque uniquement la version non sécurisée d'un site, vous permettant d'accéder à ce site simplement en entrant la version du domaine qui commence par le Protocole de Transfert Hypertexte Sécurisé HTTPS. Ceci est particulièrement utile si le filtrage que vous rencontrez est basé sur des mots-clés ou ne bloque que des pages Web individuelles. HTTPS empêche les censeurs de lire votre activité sur le Web, de sorte qu'ils ne peuvent pas dire quels mots-clés sont envoyés, ou quelle page Web individuelle vous visitez (les censeurs peuvent toujours voir les noms des domaines de tous les sites Web que vous visitez).

Si vous soupçonnez ce type de blocage simple, essayez de saisir https:// à la place de http://.

Essayez d'installer l'extension HTTPS Everywhere[66] pour activer automatiquement HTTPS pour les sites compatibles.

Une autre façon de contourner les techniques de censure de base est d'essayer un autre nom de domaine ou une autre URL. Par exemple, au lieu de visiter http://twitter.com[67]. Vous pouvez visiter https://mobile.twitter.com,[68] la version mobile du site. Les censeurs qui bloquent les sites Web ou les pages Web fonctionnent généralement à partir d'une liste noire de sites Web interdits, de sorte que tout ce qui ne figure pas sur cette liste noire passera. Ils peuvent ne pas connaître toutes les variantes du nom.

66 https://www.eff.org/https-everywhere
67 https://twitter.com/
68 https://mobile.twitter.com/home

"Proxy" basé sur le Web

Un proxy basé sur le Web (tel que http://proxy.org/[69]) est un bon moyen de contourner la censure. Pour utiliser un proxy Web, il vous suffit d'entrer l'adresse filtrée que vous souhaitez utiliser. Le proxy affichera alors le contenu demandé.

Les "proxy" basés sur le Web sont un bon moyen d'accéder rapidement aux sites Web bloqués, mais n'offrent souvent aucune sécurité et seront un mauvais choix si la menace inclut une surveillance de votre connexion Internet. De plus, ils ne vous aideront pas à utiliser d'autres services non liés aux pages Web bloquées, tels que votre programme de messagerie instantanée. Enfin, les "proxys" basés sur le Web eux-mêmes posent un risque pour la vie privée de nombreux utilisateurs, en fonction du type de menace, car le proxy produira un enregistrement complet de tout ce que vous faites en ligne.

Paramètres du Système DNS

Souvent, les gouvernements appliquent la censure dans leur pays en demandant aux fournisseurs de services Internet de valider des listes noires en utilisant ce qu'on appelle le système de noms de domaine (DNS). Les serveurs DNS font partie de l'infrastructure qui aide votre navigateur à identifier l'emplacement Web réel des sites Web que vous connaissez. Par exemple, lorsque vous tapez www.bbc.co.uk, un serveur DNS est ce qui informe votre navigateur que BBC est situé sur un serveur à l'adresse IP 212.58.244.20. En manipulant les serveurs DNS, votre ordinateur pourrait être trompé en pensant qu'un site Web, tel que la BBC, n'existe pas ou existe à un faux emplacement.

Pour contourner ce type de blocage, vous pouvez simplement modifier les serveurs DNS par défaut utilisés par votre ordinateur. Google propose deux serveurs publics [70]: 8.8.8.8 et 8.8.4.4. OpenDNS[71] propose des serveurs publics , 208.67.222.222 et 208.67.220.220, qui bloquent en outre les logiciels malveillants et les sites d'hameçonnage connus.

Vous pouvez même définir ces paramètres DNS sur un bureau ou un routeur communal afin que tous les utilisateurs puissent en bénéficier. Des instructions sur la façon de modifier les paramètres DNS sur différents systèmes d'exploitation et routeurs peuvent être trouvées sur https://use.opendns.com.

Réseaux privé virtuel (VPN)

Un réseau privé virtuel (VPN) crypte et fait passer toutes les données Internet de votre ordinateur par le fournisseur VPN situé dans un autre pays. Une fois qu'un service VPN est correctement configuré, vous pouvez l'utiliser pour accéder aux pages Web, au l'e-mail, à la messagerie instantanée, à la communication vocale de protocole internet et à tout autre service Internet. Un VPN protège votre activité contre l'interception locale, mais votre fournisseur VPN peut conserver des archives de votre activité (sites Web auxquels vous accédez et quand vous y accédez) ou même fournir à un tiers la possibilité d'espionner directement votre navigation Web.

Certains des VPN gratuits à considérer sont les suivants : Betternet[73], Psiphon[74], BitMask[75], et Opera[76].

Pour quelques recommandations sur les services VPN payants, cliquez ici[77]. Certains VPN avec des politiques de confidentialité exemplaires pourraient toujours être gérés par des personnes malveillantes.

"Onion Router (Tor)"

Tor est un logiciel libre et gratuit qui est destiné à vous fournir l'anonymat, mais qui vous permet également de contourner la censure. Lorsque vous utilisez Tor, les informations que vous transmettez sont plus sécurisées car votre trafic est renvoyé autour d'un réseau distribué de serveurs, appelés "Onion Router". Cela pourrait fournir l'anonymat, puisque l'ordinateur avec lequel vous communiquez ne verra jamais votre adresse Protocole Internet (IP), mais verra plutôt l'adresse I P du dernier Tor. Routeur par lequel votre activité a voyagé.

Lorsqu'il est utilisé avec quelques fonctionnalités optionnelles (bridges and ofsproxy), Tor est l'étalon-or pour contourner la censure sécurisée contre un État local, car il contournera presque toute censure nationale et, s'il est correctement configuré, protégera votre identité d'un pirate ayant accès au réseau du pays. Cependant, cela peut être lent.

Apprenez à utiliser Tor en utilisant ce guide[78] de la documentation du projet Tor.

69 http://proxy.org/
70 https://developers.google.com/speed/public-dns/?hl=en
71 https://use.opendns.com/
72 https://use.opendns.com/
73 https://www.betternet.co
74 https://www.psiphon3.com/
75 https://bitmask.net
76 https://www.opera.com/apps/vpn
77 https://torrentfreak.com/which-vpn-services-take-your-anonymity-seriously-2014-edition-140315/
78 https://2019.www.torproject.org/docs/documentation.html.en

SÉCURITÉ DU COMPTE

Seseko est la Directrice Exécutive d'une organisation de minorités sexuelles. Tôt le matin, elle a reçu un courriel sur son téléphone lui disant que son adresse e-mail expirerait dans quatre heures si elle n'agissait pas. À la fin de ce courriel, il y avait un lien qui proposait de la connecter à son e-mail pour éviter qu'il ne soit fermé. Sans trop réfléchir, elle a ouvert le lien qui l'a amenée à une page de connexion qui ressemblait exactement à la page de connexion Gmail. Elle a mis son nom d'utilisateur et son mot de passe, mais lors de la soumission, rien ne s'est vraiment passé. Elle est revenue en arrière et a continué à lire ses autres courriels.

Plus tard dans la journée, elle a reçu des informations selon lesquelles le site Web de l'organisation avait été piraté et dégradé et n'était plus accessible. C'est alors qu'elle a été informée par le chef du département de technologie de communication et d'information de l'organisation qu'elle avait reçu un e-mail de sa part demandant un accès temporaire au site Web rendu inaccessible très tôt ce matin-là.

Ce que Seseko a vécu ce matin-là, c'est une attaque par hameçonnage ciblée pour le vol de mot de passe. Une fois que les attaquants ont mis la main sur son compte de messagerie, ils peuvent facilement compromettre n'importe quelle partie de l'organisation.

Il existe une solution très simple mais puissante que Seseko peut utiliser pour éviter que ce type d'attaque ne se reproduise. C'est ce qu'on appelle l'authentification à deux facteurs. Il est également utile d'avoir des mots de passe forts et différents pour chaque compte en ligne.

Création de mots de passe forts

Puisqu'il est difficile de se souvenir de nombreux mots de passe différents, les gens ont du mal à travailler efficacement avec les mots de passe et nous sommes tentés par la stratégie qui consiste à réutiliser le même mot de passe pour plusieurs comptes, services et sites car les utilisateurs sont dépassés par la nécessité de créer un nouveau mot de passe pour chacun d'eux.

La pratique est très mauvaise car elle peut conduire à la compromission de tous les comptes sur lesquels le même mot de passe est utilisé. Cela signifie que la sécurité d'un mot de passe donné peut dépendre de la sécurité du service le moins sécurisé où il a été utilisé.

Éviter la réutilisation des mots de passe est une précaution de sécurité précieuse, mais vous ne pourrez pas vous souvenir de tous vos mots de passe si tous sont différents. Heureusement, il existe des outils logiciels pour vous aider à le faire : un gestionnaire de mots de passe (également appelé coffre-fort de mot de passe) est une application logicielle qui permet de stocker de nombreux mots de passe . Il n'est donc pas difficile d'éviter d'utiliser le même mot de passe dans plusieurs contextes. Le gestionnaire de mots de passe les protège tous avec un seul mot de passe principal (ou, idéalement, une phrase secrète - voir la partie suivante ci-dessous) de sorte que vous n'avez à vous souvenir que d'une chose. Le gestionnaire de mots de passe peut gérer l'ensemble du processus de création et de stockage des mots de passe pour l'utilisateur.

Par exemple, KeePassXC est un coffre-fort gratuit pour mot de passe, c'est un logiciel libre etgratuit que vous conservez sur votre bureau. Il est important de noter que si vous utilisez KeePassXC, il n'enregistrera pas automatiquement les modifications et les ajouts. Cela signifie que s'il plante après avoir ajouté des mots de passe, vous pouvez les perdre pour toujours. Vous pouvez modifier cela dans les paramètres.

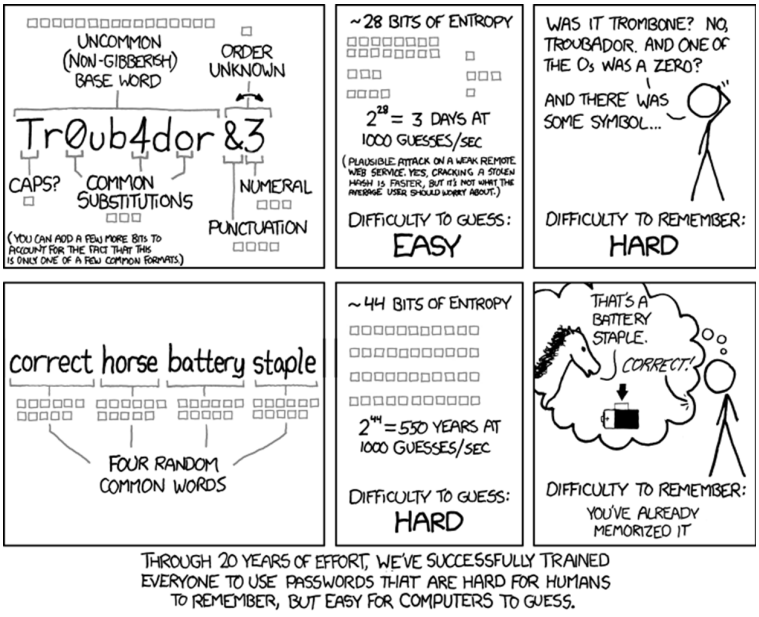
L'utilisation d'un gestionnaire de mots de passe vous aide également à choisir des mots de passe forts, difficiles à deviner pour un hackeur. Cela est également important. Trop souvent, les utilisateurs d'ordinateurs choisissent des mots de passe courts et simples qu'un pirate informatique peut facilement deviner, comme mot de passe1, 12345, une date de naissance ou le nom d'un ami, d'un conjoint ou d'un animal de compagnie. Un gestionnaire de mots de passe peut vous aider à créer et à utiliser un mot de passe aléatoire sans modèle ni structure, un mot de passe qui ne sera pas devinable. Par exemple, un gestionnaire de mots de passe est capable de choisir des mots de passe comme vAeJZ! Q3p$Kdkz/CRHzj0v7, dont un être humain aurait peu de chances de se souvenir – ou de deviner. Ne vous inquiétez pas; le gestionnaire de mots de passe peut s'en souvenir pour vous!

Choisir des mots de passe forts

Il y a quelques mots de passe qui doivent être mémorisés et qui doivent être particulièrement forts : ceux qui verrouillent finalement vos propres données avec la cryptographie. Cela inclut, au moins, les mots de passe de votre appareil, le cryptage comme le cryptage complet du disque et le mot de passe principal de votre gestionnaire de mots de passe.

Les ordinateurs sont maintenant assez rapides pour deviner rapidement des mots de passe inférieurs à une dizaine de caractères. Cela signifie que les mots de passe courts de toute nature, même totalement aléatoires comme nQ\ m=8'x ou ! s7e&nUY ou gaG5'bG, ne sont plus suffisamment forts par rapport au cryptage aujourd'hui.

Il existe plusieurs façons de créer une phrase secrète forte et mémorisable ; la méthode la plus simple et la plus sûre est celle de Diceware[79] d'Arnold Reinhold.



Source: XKCD[80]

La méthode de Reinhold consiste à lancer des dés qui fourniront des nombres variés pour choisir au hasard plusieurs mots dans une liste donnée. Ensemble, ces mots formeront votre phrase secrète. Pour le cryptage de disque (et le mot de passe sécurisé), nous vous recommandons de sélectionner un minimum de six mots. Une version simplifiée de Diceware implique simplement d'enchaîner vous-même une variété de mots aléatoires. Voir cette bande dessinée pour une illustration de la façon dont cette méthode peut être plus facile à utiliser et plus sûre pour obtenir des mots de passe complexes comme nQ\m=8'x.

Lorsque vous utilisez un gestionnaire de mots de passe, la sécurité de vos mots de passe et de votre mot de passe principal dépend de la sécurité de l'ordinateur sur lequel le gestionnaire de mots de passe est installé et utilisé. Si votre ordinateur ou votre appareil est compromis et qu'un logiciel espion est installé, le logiciel espion peut vous regarder taper votre mot de passe principal et pourrait voler le contenu du coffre-fort. Il est donc toujours très important de garder votre ordinateur et vos autres appareils vierges de logiciels malveillants lors de l'utilisation d'un gestionnaire de mots de passe.

79 http://world.std.com/~reinhold/diceware.html
80 https://xkcd.com/936/

Authentification Multifacteur et mots de passe à usage unique

De nombreux services et outils logiciels vous permettent d'utiliser l'authentification à deux facteurs, également appelée vérification en deux étapes ou connexion en deux étapes. Ici, l'idée est que pour vous connecter, vous devez être en possession d'un certain appareil : généralement un téléphone portable, mais, dans certaines versions, un appareil spécial appelé jeton de sécurité (jeton-valeur). L'utilisation de ce système garantit que même si votre mot de passe pour le service est piraté ou volé, le voleur ne pourra pas se connecter à moins qu'il n'ait également la possession ou le contrôle d'un deuxième appareil et les codes spéciaux que cet appareil est le seul à pouvoir créer.

En règle générale, cela signifie qu'un voleur ou un pirate informatique devrait contrôler à la fois votre ordinateur portable et votre téléphone avant d'avoir un accès complet à vos comptes.

Puisque cela ne peut être mis en place qu'avec la coopération de l'opérateur de service, il n'y a aucun moyen de le faire par vous-même si vous utilisez un service qui ne l'offre pas.

L'authentification à deux facteurs à l'aide d'un téléphone mobile peut être effectuée de deux manières : le service peut vous envoyer un message texte (SMS) sur votre téléphone chaque fois que vous essayez de vous connecter (en fournissant un code de sécurité supplémentaire que vous devez saisir), ou votre téléphone peut lancer une application d'authentification qui génère des codes sécurisés depuis le téléphone lui-même. Cela aidera à protéger votre compte dans la situation où un pirate obtient votre mot de passe mais n'a pas d'accès physique à votre téléphone mobile.

De nombreux services en ligne offrent désormais une authentification à deux facteurs. Une liste mise à jour de ces services est disponible sur https:// www.turnon2fa.com. Vous pouvez commencer avec vos comptes Google[81], Yahoo[82], Facebook[83] et Twitter[84]!

Certains services, tels que Google, vous permettent également de générer une liste de mots de passe à usage unique. Ceux-ci sont destinés à être imprimés ou écrits sur papier et emportés avec vous (bien que dans certains cas, il soit possible de mémoriser un petit nombre d'entre eux). Chacun de ces mots de passe ne fonctionne qu'une seule fois, donc si l'un d'entre eux est volé par un logiciel espion lorsque vous le saisissez, le voleur ne pourra plus l'utiliser pour quoi que ce soit à l'avenir.

Menaces de sévices physiques ou d'emprisonnement

Enfin, comprenez qu'il y a toujours un moyen pour les hackeurs d'obtenir votre mot de passe : ils peuvent vous menacer directement de préjudice physique ou de détention. Si vous craignez que cela puisse être une possibilité, envisagez des moyens de cacher l'existence des données ou de l'appareil que vous protégez par mot de passe, plutôt que de croire que vous ne transmettrez jamais le mot de passe. Une possibilité est de maintenir au moins un compte qui contient des informations en grande partie sans importance, dont vous pouvez divulguer le mot de passe rapidement.

Si vous avez de bonnes raisons de croire que quelqu'un peut vous menacer pour vos mots de passe, il est bon de vous assurer que vos appareils sont configurés de manière qu'il ne soit pas évident que le compte que vous révélez n'est pas le vrai. Votre compte réel est-il affiché dans l'écran de connexion de votre ordinateur ou affiché automatiquement lorsque vous ouvrez un navigateur? Si c'est le cas, vous devrez peut-être reconfigurer les choses pour rendre votre compte moins évident.

Veuillez noter que la destruction intentionnelle de preuves ou l'obstruction à une enquête peuvent être considérés comme crime distinct, entrainant souvent des conséquences désastreuses. Dans certains cas, cela peut être plus facile à prouver pour le gouvernement et permettre des peines plus importantes que le crime présumé faisant l'objet d'une enquête initiale.

81 https://www.google.com/landing/2step/
82 https://login.yahoo.com/account
83 https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920
84 https://blog.twitter.com/2013/getting-started-with-login-verification

SÉCURITÉ MOBILE

Fayed est un militant qui travaille sur la transparence, la responsabilité et la liberté d'expression. Il a beaucoup d'amis qui ont fui son pays à cause de l'oppression du gouvernement. Il appelle régulièrement et envoie des messages à ses amis militants de la diaspora pour les informer de la situation dans le pays et leur faire partager des histoires qu'il ne peut pas partager à l'intérieur du pays.

Un matin, la police l'a arrêté chez lui et l'a traîné devant les tribunaux, l'accusant de planifier de renverser le gouvernement et de communiquer avec des terroristes. Devant les tribunaux, le procureur a présenté comme preuve des enregistrements de ses appels vocaux réguliers à ses amis de la diaspora et des messages qu'il leur a écrits en ternissant l'image du gouvernement.

Fayed aurait dû savoir que les appels vocaux et les messages classiques ne peuvent pas être utilisés pour communiquer des informations sensibles car ils sont facilement enregistrés par les compagnies de téléphonie. Fayed aurait dû se renseigner sur ces risques et sur les applications de téléphonie mobile qui peuvent être utilisées pour chiffrer les appels vocaux et les messages textes.

Le problème des téléphones mobiles

Les téléphones mobiles sont devenus des outils de communication omniprésents fondamentaux, maintenant utilisés non seulement pour les appels téléphoniques, mais aussi pour accéder à Internet, envoyer des messages texte (SMS) et documenter le monde.

Malheureusement, les téléphones mobiles n'ont pas été conçus pour la confidentialité et la sécurité. Non seulement ils protègent mal vos communications, mais ils vous exposent également à de nouveaux types de risques de surveillance. La plupart des téléphones mobiles donnent à l'utilisateur beaucoup moins de contrôle qu'un ordinateur de bureau personnel ou portable. Il est plus difficile de remplacer le système d'exploitation, plus difficile d'enquêter sur les attaques commises par des logiciels malveillants, plus difficile de supprimer ou de remplacer les logiciels indésirables et plus difficile d'empêcher des parties prenantes comme l'opérateur mobile de surveiller la façon dont vous utilisez l'appareil.

Certains de ces problèmes peuvent être résolus en utilisant un logiciel de confidentialité tiers, mais certains d'entre eux ne le peuvent pas. Ici, nous allons décrire certaines des façons dont les téléphones peuvent aider à la surveillance et saper la confidentialité de leurs utilisateurs.

Suivi de la géolocalisation

L'une des menaces les plus puissantes pour la confidentialité des téléphones mobiles – mais qui est souvent complètement invisible – est la façon dont votre localisation est tracée toute la journée (et toute la nuit) via les signaux qu'ils diffusent. Il existe différentes façons de géolocaliser un téléphone portable par d'autres.

La géolocalisation de téléphones mobiles

Un opérateur de réseau peut le faire en observant la force du signal que différentes antennes de télécommunication observent à partir du téléphone mobile d'un abonné en particulier, puis en calculant où ce téléphone doit être situé afin d'en tirer les conclusions et de trouver la localisation.. Il n'y a aucun moyen de se cacher de ce type de suivi électronique si votre téléphone mobile est allumé et transmet des signaux au réseau d'un opérateur. La relation inégale entre le gouvernement et les opérateurs de télécommunications signifie que le gouvernement pourrait forcer l'opérateur à transmettre des données de localisation sur un utilisateur (en temps réel ou en tant que dossier historique). En 2010, un défenseur allemand de la confidentialité nommé Malte Spitz a utilisé les lois sur la protection de la confidentialité pour amener son opérateur mobile à lui remettre les documents qu'il avait à son sujet. Il a choisi de les publier en tant que ressource éducative afin que d'autres personnes puissent comprendre à quel point les opérateurs mobiles peuvent surveiller les utilisateurs de cette façon. (Vous pouvez [85] ici voir ce que l'opérateur savait de lui.) La possibilité pour le gouvernement d'accéder à ce type de données n'est pas théorique : elle est déjà largement utilisée par les forces de l'ordre dans le monde entier.

Vous pouvez explorer les données obtenues sur 6 mois par Malte Spitz auprès de sa compagnie de téléphone montrant ses mouvements et les données d'appel téléphonique sur Zeit Online[86].

Un autre type connexe de demande gouvernementale est appelé un déversement cellulaire. Dans ce cas, un gouvernement demande à un opérateur mobile une liste de tous les appareils mobiles qui étaient présents dans une certaine zone à un moment donné. Cela peut être utilisé pour enquêter sur un crime, ou pour savoir qui était présent à une manifestation particulière. (Le gouvernement ukrainien aurait utilisé ce système de récupération de données de géolocalisation à cette fin en 2014, pour dresser une liste de toutes les personnes dont les téléphones portables étaient présents lors d'une manifestation anti-gouvernementale.)

Il existe également des dispositifs utilisés par les forces de l'ordre ou d'autres organisations techniquement sophistiquées qui peuvent collecter des informations de localisation directement appelés capteurs IMSI (une fausse antenne de téléphonie cellulaire portable prétendant en être une vraie et attraper ainsi les téléphones mobiles de certains utilisateurs, détecter leur présence, et intercepter leurs communications. Les capteurs IMSI sont des dispositifs physiques qui doivent être amenés à un endroit particulier pour surveiller la zone. Il n'existe actuellement aucune défense fiable contre tous les capteurs IMSI, bien que certaines applications détectent leur présence dans certains cas. Parfois, la désactivation des connexions par données cellulaires et de l'itinérance peut empêcher la connexion aux capteurs IMSI.

Fuites d'informations de localisation provenant des applications et de la navigation Web

Les smartphones modernes peuvent déterminer leur propre position, souvent à l'aide du Système de Positionnement Global (GPS) et parfois d'autres services fournis par les sociétés de localisation (qui demandent généralement à l'entreprise de deviner l'emplacement du téléphone en fonction d'une liste de téléphones portables, antennes et / ou réseaux Wi-Fi que le téléphone peut voir d'où il se trouve). Les applications peuvent demander au téléphone ces informations de localisation et les utiliser pour fournir des services basés sur l'emplacement, tels que des cartes qui vous montrent votre position.

85 http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz
86 http://www.zeit.de/datenschutz/malte-spitz-data-retention

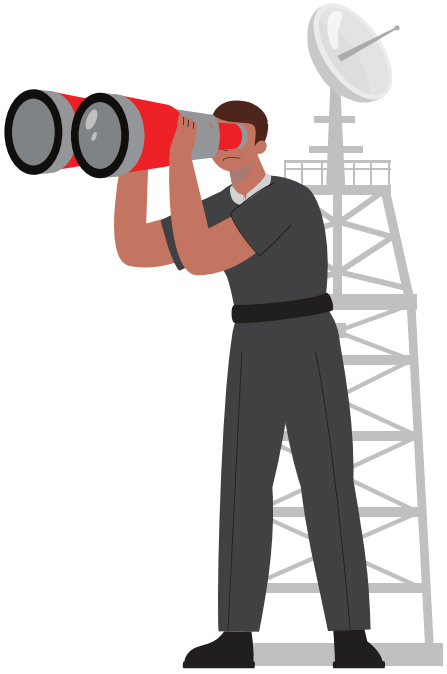
Certaines de ces applications transmettront ensuite votre position sur le réseau à un fournisseur de services, ce qui, à son tour, fournira un moyen à d'autres personnes de vous suivre. (Les développeurs d'applications n'ont peut-être pas été motivés par le désir de suivre les utilisateurs, mais ils pourraient toujours se retrouver avec la possibilité de le faire, et ils pourraient finir par révéler des informations de localisation sur leurs utilisateurs aux gouvernements ou aux pirates). Certains smartphones vous donneront le contrôle sur la question de savoir si les applications peuvent trouver votre emplacement physique. Une bonne pratique de confidentialité consiste à essayer de restreindre les applications qui peuvent voir ces informations et, au minimum, à vous assurer que votre emplacement est uniquement partagé avec des applications auxquelles vous faites confiance et qui ont une bonne raison de savoir où vous êtes.Dans chaque cas, le suivi de géolocalisation ne consiste pas seulement à trouver où se trouve quelqu'un en ce moment, comme dans une scène de film palpitante où des agents poursuivent quelqu'un dans les rues. Il peut également s'agir de répondre à des questions sur les activités historiques des gens et sur leurs croyances, leur participation à des événements et leurs relations personnelles. Par exemple, le suivi de géolocalisation pourrait être utilisé pour essayer de savoir si certaines personnes sont dans une relation amoureuse, pour savoir qui a assisté à une réunion particulière ou qui était à une manifestation particulière, ou pour essayer d'identifier la source confidentielle d'un journaliste.

Éteindre les téléphones

On craint généralement que les téléphones puissent être utilisés pour surveiller les gens, même lorsqu'ils ne sont pas activement utilisés pour passer un appel. En conséquence, les personnes ayant une conversation sensible sont parfois invitées à éteindre complètement leur téléphone, ou même à retirer les batteries de leurs téléphones.

La recommandation de retirer la batterie semble se concentrer principalement sur l'existence de logiciels malveillants qui donnent l'impression que le téléphone s'éteint sur demande (ne montrant finalement qu'un écran vide), tout en restant vraiment allumé et capable de surveiller les conversations ou de passer ou de recevoir un appel de manière invisible. Ainsi, les utilisateurs pourraient être amenés à penser qu'ils ont réussi à éteindre leur téléphone alors qu'ils ne l'avaient pas fait. De tels logiciels malveillants existent, du moins pour certains appareils, bien que nous ayons peu d'informations sur leur fonctionnement ou leur utilisation.

Éteindre les téléphones a son propre inconvénient potentiel : si beaucoup de gens à un endroit le font tous en même temps, c'est un signe pour les opérateurs mobiles qu'ils ont tous pensé qu'il y avait quelque chose qui méritait qu'ils éteignent leurs téléphones (ce peut être le début d'un film dans une salle de cinéma, ou le départ d'un avion dans un aéroport, mais cela peut aussi être une réunion ou une conversation sensible.) Une alternative qui pourrait donner moins d'informations est de laisser les téléphones de tout le monde dans une autre pièce où les microphones des téléphones ne seraient pas en mesure d'entendre les conversations.



Espionnage des communications mobiles

Les réseaux de téléphonie mobile n'ont pas été conçus à l'origine pour utiliser des moyens techniques afin de protéger les appels des abonnés contre les écoutes téléphoniques. Cela signifiait que n'importe qui avec le bon type de récepteur radio pouvait écouter les appels.

La situation est un peu meilleure aujourd'hui, mais parfois seulement légèrement. Des technologies de cryptage ont été ajoutées aux normes de communication mobile pour tenter d'empêcher l'écoute. Mais beaucoup de ces technologies ont été mal conçues[87] (parfois délibérément, en raison de la pression du gouvernement pour ne pas utiliser de cryptage trop fort !). Ils ont été déployés de manière inégale, de sorte qu'ils peuvent être disponibles sur un téléphone portable mais pas sur un autre, ou dans un pays mais pas dans un autre, et ont parfois été mis en œuvre de manière incorrecte. Par exemple, dans certains pays, les opérateurs n'activent pas du tout le cryptage ou utilisent des normes techniques obsolètes.Cela signifie qu'il est souvent encore possible pour quelqu'un avec le bon type de récepteur radio d'intercepter les appels et les messages texte lorsqu'ils sont transmis par voie hertzienne.

87 http://www.aftenposten.no/verden/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-98459b.html

Même lorsque les meilleures normes de l'industrie sont utilisées, comme c'est le cas dans certains pays et sur certains opérateurs mobiles, il y a toujours des gens qui peuvent écouter. Au minimum, les opérateurs mobiles eux-mêmes peuvent intercepter et enregistrer toutes les données sur qui a appelé ou envoyé un message à qui, quand et ce qu'ils ont dit. Ces informations peuvent être mises à la disposition des gouvernements locaux ou étrangers par le biais d'arrangements officiels ou informels. Dans certains cas, des gouvernements étrangers ont également piraté les systèmes des opérateurs mobiles afin d'obtenir un accès secret aux données des utilisateurs.

Infecter les téléphones avec des logiciels malveillants

Les téléphones peuvent être infectés par des virus et d'autres types de logiciels malveillants, soit parce que l'utilisateur a été amené à installer un logiciel malveillant, soit parce que quelqu'un a pu pirater l'appareil en utilisant une faille de sécurité dans le logiciel de l'appareil existant. Comme avec d'autres types d'appareils informatiques, le logiciel malveillant peut alors espionner l'utilisateur de l'appareil.

Par exemple, un logiciel malveillant sur un téléphone mobile pourrait lire des données privées sur l'appareil (comme des messages texte ou des photos stockées). Il pourrait également activer les capteurs de l'appareil (tels que le microphone, la caméra, le GPS) pour trouver où se trouve le téléphone ou pour surveiller l'environnement, même en transformant le téléphone en mouchard.

Cette technique a été utilisée par certains gouvernements pour espionner les gens via leurs propres téléphones et a créé de l'anxiété à l'idée d'avoir des conversations sensibles lorsque des téléphones mobiles sont présents dans la pièce. Certaines personnes réagissent à cette possibilité en déplaçant les téléphones portables dans une autre pièce lors d'une conversation sensible, ou en les éteignant (Les gouvernements eux-mêmes interdisent souvent aux gens, même aux membres du gouvernement, d'apporter des téléphones cellulaires personnels dans certaines installations sensibles, principalement parce qu'ils craignent que les téléphones ne soient infectés par un logiciel leur permettant d'enregistrer des conversations.)

Une autre préoccupation est que les logiciels malveillants pourraient théoriquement faire en sorte qu'un téléphone fasse semblant de s'éteindre, tout en restant secrètement allumé (et en affichant un écran noir, de sorte que l'utilisateur croit à tort que le téléphone est éteint). Cette préoccupation a conduit certaines personnes à retirer physiquement les batteries de leurs appareils lors de conversations très sensibles.

Meilleures pratiques de sécurité recommandées pour les smartphones

Il est impossible d'imaginer la vie sans smartphones, surtout si l'on est impliqué dans une forme quelconque de travail, d'organisation ou de collaboration. Cela rend le ciblage des individus, des organisations et des communautés très facile étant donné que les téléphones ont toujours accès aux espaces les plus protégés dans les maisons, les organisations et les communautés. Voici quelques-unes des mesures que les communautés et les individus peuvent prendre pour rester en sécurité lorsqu'ils utilisent des téléphones mobiles.

Configurer un verrouillage d'écran sur le téléphone

Il peut s'agir d'un scan, des symboles, des codes chiffrés ou d'un mot de passe. Cela garantira que le contenu de votre téléphone ne sera pas accessible à des personnes aléatoires / non autorisées qui ont accès à votre téléphone. Au moins l'un des quatre conviendra, mais un mot de passe est l'option la plus sûre pour un téléphone mobile. Plus d'informations ci-dessous pour savoir comment crypter le disque dur de votre smartphone.

Maintenez à jour le système d'exploitation et les applications de votre téléphone

Les fabricants de téléphones et les développeurs d'applications essaient toujours d'améliorer la sécurité, l'efficacité et les performances de leurs produits en créant et en envoyant régulièrement des mises à jour. Le téléchargement et l'installation de ces mises à jour garantissent que votre logiciel ou votre appareil est à l'abri des virus, mais effectue également des opérations de mise à jour. L'installation des mises à jour peut être effectuée dans votre magasin d'applications (appstore/ google store...) ou dans les paramètres de votre appareil.

Installer des applications provenant uniquement de sources fiables

La plupart des smartphones ont un magasin d'applications (store) de confiance prédéterminé où les applications sont téléchargées. Ces stores (installateurs d'applications) testent et vérifient que les applications peuvent être utilisées en toute sécurité. Les applications téléphoniques téléchargées directement à partir d'Internet sont très difficiles à vérifier et garantir qu'elles ne sont pas malveillantes est très difficile. C'est pourquoi il est recommandé de ne télécharger des applications qu'à partir d'un store (installateur d'application) de confiance comme "Google Play Store ou Apple Store" autre qu'Internet.

De plus, la désinstallation d'applications que vous n'utilisez plus libère de l'espace sur votre téléphone, ce qui le rend plus efficace.

Sur une note connexe, il est utile de toujours savoir quelles applications sont installées sur votre téléphone et de supprimer les applications que vous ne reconnaissez pas ou que vous n'utilisez plus. Cela peut aider à améliorer la vitesse du système, à réduire les risques de perte de confidentialité et à réduire le nombre de mises à jour d'applications que vous devez télécharger.

Éteignez le Wi-Fi et le Bluetooth du téléphone s'ils ne sont pas utilisés

Le Bluetooth et le Wi-Fi sur un téléphone lorsqu'il est allumé essaieront toujours de se connecter aux réseaux sans fil à proximité ou aux appareils respectifs connectés au Bluetooth. Cela se produit automatiquement lorsque des informations détaillées sur l'appareil, telles que les identifiants de l'appareil et les capacités de transfert de données, sont diffusées. Ces informations peuvent être collectées par des individus malveillants et utilisées pour cibler l'appareil. Il est recommandé d'activer uniquement le WIFI et le Bluetooth lors de leur utilisation. Assurez-vous également que la recherche de nouveaux appareils Bluetooth soit désactivée.

Communiquer en toute sécurité sur un smartphone

Les appels téléphoniques et les SMS ne sont pas sécurisés car ils peuvent être interceptés par les opérateurs téléphoniques. Les communications privées ou sensibles doivent être effectuées sur des applications et des plates-formes sécurisées. Les applications de communication sécurisées intègrent le cryptage. Le Cryptage de bout en bout est la forme de cryptage la plus fiable pour les systèmes de communication. Il garantit que les appels et les messages ne peuvent pas être interceptés ou écoutés. Le message ou l'appel est crypté à partir de l'appareil de l'expéditeur et uniquement décrypté sur l'appareil du destinataire. Des applications telles que WhatsApp, Signal, Telegram, Wire, Slack intègrent toutes cette technologie et il est conseillé de les utiliser pour les communications sensibles ou privées. Toutes les parties qui communiquent entre elles doivent avoir installé l'application pour avoir une communication sécurisée.

Les téléphones mobiles accélèrent chaque année l'accès et la connectivité à Internet, en particulier parmi les communautés à revenu faible et moyen. Cela signifie que de plus en plus de personnes comptent sur les téléphones mobiles pour communiquer, s'organiser et collaborer. Malheureusement, la communication sur Internet avec un smartphone est susceptible d'être surveillée et interceptée par les gouvernements et les entreprises de télécommunications. La surveillance signifie que quelqu'un peut surveiller et suivre ses activités en ligne. Pour protéger la confidentialité des activités en ligne, il existe des outils qui peuvent être utilisés non seulement pour crypter les activités en ligne, mais aussi pour anonymiser / masquer l'identité des utilisateurs sur Internet.

Une ressource très utile pour vous aider à savoir si votre application de messagerie vous offre une sécurité et confidentialité suffisante est sécurisée "Electronic Frontier Foundations Secure Messaging Scorecard"[88].

Les réseaux privés virtuels ou VPN cachent les activités Internet des utilisateurs en accédant à Internet via un réseau informatique situé dans un emplacement géographique différent. Les VPN contournent également la censure sur Internet en accédant indirectement aux pages censurées via un autre ordinateur utilisant des communications cryptées. "Onion Router ou Tor" est unique car il offre l'anonymat en plus de tout service VPN. Il fournit l'anonymat en décomposant chaque étape de la connexion et en l'attribuant à un ordinateur différent du réseau Tor, ce qui rend difficile de savoir quel ordinateur demande une ressource sur Internet. Les VPN peuvent être gratuits ou payants, les versions payantes ont généralement des fonctionnalités supplémentaires tandis que Tor est gratuit.

Sécurité des comptes

Les comptes en ligne comme le Webmail, Facebook et Twitter ont toujours compté sur les mots de passe pour la sécurité et le contrôle d'accès. Cela a été un désastre car les piratages des grandes entreprises ont exposé les mots de passe des utilisateurs, ce qui facilite les prises de contrôle de compte et les détournements. Cela a entraîné une refonte de la sécurité des comptes en ligne, passant d'un système basé uniquement sur un mot de passe à un système de vérification en deux étapes beaucoup plus sécurisées. L'authentification à deux facteurs nécessite un code envoyé à un téléphone ou lu à partir d'une application sur le téléphone de l'utilisateur en plus du mot de passe. Ce système garantit que même si un mot de passe d'un compte est volé, il est presque impossible d'accéder au compte sans le code du téléphone. Tous les comptes importants ont maintenant cette fonctionnalité, et c'est la meilleure option pour garantir la sécurité du compte.

Sécurité opérationnelle

En plus des problèmes de sécurité développés ci-dessus, votre téléphone peut vous aider à effectuer effectivement votre travail en toute sécurité. Vous trouverez ci-dessous un bref aperçu de certaines applications pertinentes :

Tella[89] est une application de documentation pour Android. Dans des environnements difficiles, avec une connectivité Internet limitée ou inexistante ou face à la répression. Tella rend plus facile et plus sûre la documentation des événements, qu'il s'agisse de violence, de violations des droits humains, de corruption ou de fraude électorale.

Mobile martus[90] est une application collectrice de données qui se connecte à la base de données de documentation sécurisée Martus91. Il permet à l'utilisateur d'envoyer des rapports de terrain en toute sécurité dans un projet de documentation existant, puis le rapport est effacé en toute sécurité du téléphone immédiatement après l'envoi. Il est disponible pour Android.

Umbrella[92] est une application gratuite d'apprentissage autoguidé disponible pour Android. Il couvre de nombreux sujets de sécurité numérique, organisationnelle et opérationnelle dans un format mobile agréable. Il comprend des listes de contrôle utiles lors de la planification et de la mise en œuvre de pratiques de sécurité améliorées. En savoir plus sur **Security First.**

88 https://www.eff.org/secure-messaging-scorecard
89 https://play.google.com/store/apps/details?id=org.hzontal.tella&hl=en&gl=US
90 https://play.google.com/store/apps/details?id=org.martus.android&hl=en
91 https://www.martus.org/
92 https://play.google.com/store/apps/details?id=org.secfirst.umbrella

Ressources

Ce guide n'est que le début. Apprenez-en plus et obtenez des Guides pratiques mis à jour à partir des ressources ci-dessous:

Security in box [93] - Chapitres tactiques et Guides étape par étape sur la façon d'utiliser bon nombre des logiciels abordés dans ce livret. Voir aussi leurs Guides communautaires pour les défenseurs africains des droits environnementaux [94] et les minorités sexuelles [95].

Surveillance self-défence[96] - Chapitres sur la protection contre la surveillance et Guides pratiques sur les logiciels.

Digital First Aid Kit[97] - Un guide pratique pour répondre à divers types d'attaques numériques.

SaferJourno[98] – Un manuel de formation à la sécurité numérique spécialement destiné à l'enseignement des journalistes.

Level-Up[99] - Programme de formation dans la sécurité numérique pour les formateurs

SAFETA[100] - Cadre d'audit de sécurité numérique pour les professionnels de la sécurité

The Digital First Aid Kit[102] - Partenariat pour les défenseurs numériques

Umbrella[103] - est une application d'apprentissage autoguidée gratuite disponible pour Android.

93 https://securityinabox.org/en
94 https://securityinabox.org/en/eco-rights-africa
95 https://securityinabox.org/en/lgbti-africa
96 https://ssd.eff.org/
97 https://www.digitaldefenders.org/digitalfirstaid/
98 https://saferjourno.internews.org/
99 https://www.level-up.cc/
100 https://safetag.org/
101 https://www.virustotal.com/
102 https://www.digitaldefenders.org/digitalfirstaid/
103 https://play.google.com/store/apps/details?id=org.secfirst.umbrella

Annexes

Annexe 1 : Résumé de la Déclaration des Nations Unies sur les défenseurs des droits de l'homme

L'élaboration de la Déclaration sur les défenseurs des droits humains a commencé en 1984 et s'est terminée avec l'adoption du texte par l'Assemblée générale en 1998, à l'occasion du 50e anniversaire de la Déclaration universelle des droits de l'homme. Un effort collectif de plusieurs ONG de défense des droits humains et de certaines délégations d'États a permis de faire en sorte que le texte soit fort, utile et pragmatique. Peut-être plus important encore, la Déclaration ne s'adresse pas seulement aux États et aux défenseurs des droits humains, mais à tout le monde. Il nous dit que nous avons tous un rôle de DDH à jouer et souligne qu'il existe un mouvement mondial en matière de droits humains qui nous concerne tous. Le nom complet de la Déclaration est la Déclaration sur le droit et la responsabilité des individus, groupes et organes de la société de promouvoir et protéger les droits humains et libertés fondamentales universellement reconnus. – avec ce titre plus long est souvent abrégé en La Déclaration sur les défenseurs des droits humains.

1. Caractère juridique

La Déclaration n'est pas un instrument juridiquement contraignant, mais elle contient une série de principes et de droits qui sont fondés sur les normes relatives aux droits humains inscrites dans d'autres instruments internationaux qui sont juridiquement contraignants – comme le Pacte international relatif aux droits civils et politiques.

En outre, la Déclaration a été adoptée par consensus par l'Assemblée générale et représente donc un engagement très ferme des États en faveur de sa mise en œuvre. Les États envisagent de plus en plus d'adopter la Déclaration en tant que législation nationale contraignante.

2. Les dispositions de la Déclaration

La Déclaration prévoit le soutien et la protection des défenseurs des droits de l'Homme dans le cadre de leur travail. Elle ne crée pas de nouveaux droits, mais articule plutôt les droits existants de manière à faciliter leur application au rôle pratique et à la situation des droits humains. Il accorde une attention, par exemple, à l'accès au financement par les organisations de DDH, à la collecte et à l'échange d'informations sur les normes relatives aux droits humains et leur violation.

La Déclaration décrit certains devoirs spécifiques des États et les responsabilités de chacun en matière de défense des droits humains, en plus d'expliquer son articulation avec le droit national. La plupart des dispositions de la Déclaration sont résumées au paragraphe [104] ci-après. Il est important de réaffirmer que les défenseurs des droits humains ont l'obligation, en vertu de la Déclaration, de mener des activités pacifiques.

a) Droits et protections accordés aux défenseurs des droits humains

Les articles 1, 5, 6, 7, 8, 9, 11, 12 et 13 de la Déclaration prévoient des protections spécifiques pour les défenseurs des droits humains, notamment les droits suivants :

- Rechercher la protection et la réalisation des droits humains au niveau national et international ;
- Mener des activités dans le domaine des droits humains, individuellement et en association avec d'autres;
- Former des associations et des organisations non gouvernementales ;
- Se réunir ou faire des assemblées pacifiquement ;
- Rechercher, obtenir, recevoir et détenir des informations relatives aux droits humains ;
- Développer et discuter de nouvelles idées et de nouveaux principes en matière de droits humains et plaider pour leur acceptation ;
- Soumettre aux organismes gouvernementaux, agences et organisations concernées par les affaires

104 Des commentaires détaillés sur la Déclaration ont été fournis dans le rapport du Secrétaire général à la Commission des droits de l'homme à sa cinquante-sixième session, en 2000 (E/CN.4/2000/95). Le rapport contient également des propositions pour la mise en œuvre de la Déclaration. En outre, en juillet 2011, Margaret Sekaggya a publié un commentaire de la Déclaration sur les défenseurs des droits de l'homme, un document clé cartographiant les droits prévus dans la Déclaration basé principalement sur les informations reçues et les rapports produits par le mandat.

publiques les critiques et les propositions visant à améliorer leur fonctionnement et à attirer l'attention sur tout aspect de leur travail susceptible d'entraver la réalisation des droits de l'homme ;
- Exprimer un désaccord avec les politiques officielles et des actes relatifs aux droits humains et d'avoir de telles plaintes revues
- Offrir et fournir une assistance juridique professionnellement qualifiée ou d'autres conseils et assistance en matière de défense des droits humains ;
- Assister aux audiences publiques, procédures et procès afin d'évaluer leur conformité avec la législation nationale et les obligations internationales en matière de droits humains ;
- D'avoir librement accès aux organisations non gouvernementales et intergouvernementales et de communiquer librement avec elles ;
- Recevoir des dommages et intérêts
- Exercer légalement le travail et la profession de défenseur des droits humains;
- Jouir d'une protection effective en vertu des lois nationales pour réagir ou s'opposer, par des moyens pacifiques, à des actes ou omissions imputables à l'État qui entraînent des violations des droits humains; et
- Solliciter, recevoir et utiliser des ressources aux fins de la promotion des droits humains (y compris la réception de fonds venant de l'étranger).

b) Les devoirs des États

Les États ont la responsabilité de mettre en œuvre et de respecter toutes les dispositions de la Déclaration. Toutefois, les articles 2, 9, 12, 14 et 15 font particulièrement référence au rôle des États et indiquent que chaque État a une responsabilité et un devoir:

- Protéger, promouvoir et mettre en œuvre tous les droits humains;
- Veiller à ce que toutes les personnes sous leur juridiction puissent jouir dans la pratique de tous les droits et libertés en matières sociales, économique, politique et autres;
- Adopter les mesures législatives, administratives et autres nécessaires pour assurer la mise en œuvre effective des droits et libertés;
- Offrir une réparation effective aux personnes qui affirment avoir été victimes d'une violation des droits de l'homme;
- Mener des enquêtes rapides et impartiales sur les violations présumées des droits de l'homme;
- Prendre toutes les mesures nécessaires pour assurer la protection de chacun contre toute violence, menace, représailles, discrimination, pression ou tout autre acte arbitraire résultant de l'exercice légitime des droits énoncés dans la Déclaration;
- Promouvoir la compréhension par tous des droits civils, politiques, économiques, sociaux et culturels;
- Assurer et soutenir la création et le développement d'institutions nationales indépendantes pour la promotion et la protection des droits humains, telles que des médiateurs ou des commissions des droits humains; et
- Promouvoir et faciliter l'enseignement des droits humains à tous les niveaux de l'éducation formelle et de la formation professionnelle.

c) Les responsabilités de chacun

La Déclaration souligne que chacun a des devoirs envers et au sein de la communauté et nous encourage tous à être des défenseurs des droits humains. Les articles 10, 11 et 18 énoncent la responsabilité de chacun de promouvoir les droits humains, de sauvegarder la démocratie et ses institutions et de ne pas violer les droits fondamentaux d'autrui. L'article 11 fait spécialement référence aux responsabilités des personnes exerçant des professions susceptibles d'affecter les droits fondamentaux d'autrui, et est particulièrement de rigueur pour les fonctionnaires de police, les avocats, les juges, etc.

d) Le rôle des lois nationales

Les articles 3 et 4 décrivent la relation entre la Déclaration et les lois nationales et internationales en vue d'assurer l'application des normes juridiques les plus élevées possibles en matière de droits de l'homme.

DEFENDDEFENDERS

East and Horn of Africa Human Rights Defenders Project