Livret pratique

Ce livret pratique est conçu pour expliquer certains enjeux que vous devez connaître afin de mieux protéger votre sécurité numérique. Nous avons voulu cerner et décrire les risques potentiels et vous aider à prendre des décisions réfléchies quant aux moyens à mettre en place pour réduire ces risques. À cette fin, le livret pratique répond à huit questions d'ordre général liées à la sécurité numérique de base, la protection des données et la confidentialité des communications.

Au début de chaque chapitre, vous trouverez des scénarios de mise en contexte animés par des personnages fictifs qui réapparaîtront lors de brèves conversations tout au long du chapitre afin d'illustrer certaines notions et répondre à quelques questions élémentaires. Vous trouverez également une courte liste de leçons particulières à retenir à la lecture du chapitre. Il est indiqué de consulter cette liste avant d'entamer la lecture du chapitre. En lisant un chapitre donné, vous trouverez un certain nombre de termes techniques qui renvoient au glossaire situé à la fin du livret. Vous trouverez également des références aux logiciels qui sont examinés dans la compilation de Guides pratiques inclus dans cette trousse à outils.

Chaque chapitre ou guide pratique inclus dans cette trousse à outil peut être lu individuellement, formaté dans votre navigateur pour impression facile ou partagé en format électronique. Cependant, vous retirerez le maximum du projet Security in-a-box si vous êtes en mesure de suivre les liens pertinents et les références qui sont éparpillées à travers le livret pratique et les guides d'utilisation des logiciels. Si vous disposez d'une copie imprimée de ce livret, vous devriez la garder à portée de main lorsque vous manipulez les guides pratiques. Vous devriez aussi vous rappeler de compléter la lecture du chapitre du livret portant sur un outil particulier avant de vous fier tout à fait à cet outil pour protéger votre sécurité numérique.

Si possible, vous devriez lire les chapitres du livret pratique selon l'ordre présenté. La sécurité est un processus dynamique, et il peut parfois s'avérer inutile de se défendre contre une grave menace à la confidentialité de ses communications, par exemple, si l'on ne s'est pas d'abord assuré de protéger son ordinateur contre les virus et autres logiciels malveillants. Cela reviendrait à verrouiller votre porte d'entrée après que le cambrioleur ait pénétré dans votre domicile. Cela ne veut pas dire que l'un ou l'autre de ces sujets est plus important que les autres. C'est simplement que les derniers chapitres tiennent pour acquis que vous avez déjà assimilé certaines notions et que vous connaissez bien l'état de l'ordinateur sur lequel vous vous apprêtez à installer de nouveaux logiciels.

Bien entendu, il y a de nombreuses raisons pour lesquelles vous pourriez vouloir lire ces chapitres dans un autre ordre que celui qui vous est présenté. Vous pourriez être à la recherche de conseils sur la façon de créer des copies de sauvegarde avant de commencer à installer les outils décrits dans les Guides pratiques. Vous pourriez vous retrouver dans une situation où, devant l'imminence d'une menace à votre vie privée, vous deviez apprendre en toute urgence à protéger les données sensibles stockées sur votre ordinateur, tel qu'abordé au chapitre 4. Ou peut-être travaillez-vous dans un café Internet, à partir d'un ordinateur dont le niveau de sécurité est indépendant de votre volonté et duquel vous n'avez pas l'intention d'accéder à des données sensibles. Si vous souhaitez utiliser cet ordinateur pour visiter un site Internet qui est bloqué dans votre pays, rien ne vous empêche de passer directement au *Chapitre 8 : préserver votre anonymat et contourner la censure sur Internet*.

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

Quels que soient vos objectifs, vous ne pourrez vraiment assurer la sécurité de votre ordinateur qu'en commençant par veiller à sa santé générale. C'est pourquoi, avant de commencer à vous préoccuper, par exemple, de créer des mots de passe sûrs, d'établir des communications confidentielles et de supprimer définitivement des données délicates, vous devriez vous assurer que votre ordinateur n'est pas vulnérable aux attaques des *pirates* [1] ou infectés par des *programmes malveillants* [2] comme des virus ou des logiciels espions (ou mouchards). Sans d'abord passer par cette étape primordiale, il est impossible de garantir l'efficacité des autres mesures de précaution que vous mettrez en place. Autrement dit, il est inutile de verrouiller votre porte d'entrée si le cambrioleur est déjà au rez-de-chaussée et il ne sert à rien de fouiller méticuleusement le rez-de-chaussée si la porte d'entrée reste toute grande ouverte.

Ce chapitre explique donc comment entretenir vos programmes et utiliser des outils comme *Avast* [3], *Spybot* [4] et *Comodo Firewall* [5] pour protéger votre ordinateur contre les infections de programmes malveillants et les attaques de *pirates*. Bien que les outils suggérés dans le présent chapitre soient conçus pour Windows (le système d'exploitation le plus vulnérable à ces attaques), les utilisateurs de systèmes *GNU / Linux* [6] et Apple OS X sont aussi menacés et devraient tenir compte des tactiques présentées ici.

Scénario de départ

Assani milite pour les droits humains dans un pays africain francophone. Ses deux adolescents, Salima et Muhindo, ont offert de l'aider avec quelques tâches informatiques élémentaires qui lui ont été confiées. Après avoir constaté l'état

général de son ordinateur, ils lui ont proposé de lui montrer comment faire en sorte que sa machine soit fonctionnelle et reste « en santé ». Assani apprécie l'idée d'utiliser des logiciels libres, gratuits et de source ouverte (FLOSS), mais il ne sait pas si ces programmes sont plus ou moins sûrs que les programmes commerciaux. Il demande donc conseil à ses enfants.

Qu'apprendrez-vous dans ce chapitre

- Certaines des menaces spécifiques que posent les programmes malveillants à la confidentialité et la sécurité de vos données, à la stabilité de votre système informatique et à la fiabilité des autres programmes de sécurité installés sur votre ordinateur ;
- Comment utiliser un ensemble d'outils recommandés pour vous protéger contre ces menaces ;
- Comment maintenir un niveau de sécurité élevé en actualisant régulièrement vos logiciels ;
- Pourquoi vous devriez utiliser des *gratuiciels* [7] (et ainsi éviter les dangers liés aux logiciels piratés ou aux licences d'utilisation limitées), et des outils à licence *FLOSS* [8] lorsque cela est possible, afin d'accroître le niveau de sécurité de votre système informatique.

Les virus

Il existe plusieurs moyens de classer les virus et chacune de ces méthodes comporte son lot de catégories aux noms plus ou moins colorés. Vers, macrovirus, Chevaux de Troie (ou *Trojan*) et portes dérobées (ou *Backdoor*), sont quelques-uns desexemples les plus connus. Plusieurs de ces virus se répandent par l'Internet, par courrier électronique, par l'intermédiaire de sites malveillants ou par d'autres moyens dans le but d'infecter des ordinateurs vulnérables et/ou mal protégés. D'autres virus se propagent par l'entremise de dispositifs et périphériques amovibles, notamment les clés USB et les disques durs externes, dont la configuration permet aux utilisateurs d'écrire des données en plus de lire celles qui s'y trouvent déjà. Les virus peuvent détruire, endommager ou infecter les données qui se trouvent sur votre ordinateur, y compris les données qui sont stockées sur vos disques durs externes. Ils peuvent aussi prendre le contrôle de votre ordinateur pour attaquer d'autres ordinateurs. Heureusement, il existe plusieurs programmes antivirus que vous pouvez utiliser pour préserver l'intégrité de votre système et protéger les personnes avec qui vous échangez des données.

Programme antivirus

Il existe un excellent *gratuiciel* antivirus pour Windows nommé *Avast* [3], qui est facile à utiliser, régulièrement actualisé et très respecté par les spécialistes. Vous devez vous enregistrer tous les 14 mois, mais l'enregistrement, les mises à jour et le programme lui-même sont gratuits.

Expérience pratique : se lancer avec le *Guide pratique Avast* *[9]*

Il existe de nombreux autres programmes antivirus commerciaux bien connus constituant une alternative à Avast. *Clam Win* est une alternative *FLOSS* à Avast. Bien qu'il manque à ce programme certaines des fonctions importantes qui devraient être incluses dans un antivirus principal, Clam Win comporte l'avantage de pouvoir être lancé à partir d'une clé USB pour balayer un ordinateur où vous n'êtes pas autorisé à installer de nouveaux logiciels.

Astuces pour utiliser efficacement un logiciel antivirus

- Ne lancez pas deux programmes antivirus en même temps. Cela pourrait entraîner un ralentissement important de votre ordinateur, ou même le faire planter. Il est important de désinstaller un programme antivirus avant d'en installer un nouveau.
- Assurez-vous que votre programme antivirus vous permette de recevoir des mises à jour. Plusieurs programmes commerciaux pré installés sur des ordinateurs neufs doivent être enregistrés (et achetés) au terme d'une certaine période, sans quoi il devient impossible d'installer les mises à jour. Tous les logiciels suggérés ici comportent la mise à jour gratuite.
- Assurez-vous que votre programme antivirus s'actualise automatiquement et régulièrement. Comme de nouveaux virus sont conçus et distribués quotidiennement, votre ordinateur risque de devenir vulnérable rapidement si votre antivirus n'est pas actualisé avec les plus récentes définitions de virus. Avast cherche automatiquement des mises à jour lorsque vous êtes connecté à Internet.
- Si votre programme antivirus présente une fonction de détection de virus « en continu », assurez-vous qu'elle soit toujours activée. Différents programmes ont différents noms pour cette fonction (« protection en temps réel » (*realtime protection*), « protection résidente » ou un autre nom similaire), mais la plupart des antivirus comportent une telle fonction. Consultez la ***section 3.2.1*** [10] du ***Guide pratique Avast*** [11] pour plus de renseignements sur le « scanner résident » de ce programme.
- Balayez (scannez) régulièrement tous les fichiers qui sont stockés sur votre ordinateur. Vous n'avez pas à le faire

quotidiennement (d'autant plus si la fonction « résidente » de votre programme est activée), mais vous devriez le faire assez souvent. La fréquence de vos balayages dépend de votre utilisation. Avez-vous récemment connecté votre ordinateur à un réseau inconnu ? Avec qui avez-vous partagé l'utilisation de clés USB ? Recevez-vous fréquemment des pièces jointes suspectes par courriel ? Quelqu'un d'autre dans votre domicile ou votre milieu de travail a-t-il eu des problèmes avec un virus dernièrement ? Pour plus de renseignements sur les meilleures habitudes à prendre pour balayer efficacement votre ordinateur, veuillez consulter le ***Guide pratique Avast*** [11].

Prévenir les infections virales

- Soyez extrêmement prudent lorsque vous ouvrez des pièces jointes dans un e-mail, ou tous fichiers reçus par messagerie instantanée comme MSN, Skype, etc. Il est conseillé de n'ouvrir aucun fichier dont vous ne connaissez pas l'origine. Si vous devez le faire, vous devriez d'abord sauvegarder la pièce jointe dans un répertoire quelque part sur votre ordinateur avant d'ouvrir le fichier en question avec le programme approprié (tel que Microsoft Word ou Adobe Acrobat). En utilisant le menu `Fichier` du programme pour ouvrir le fichier manuellement, au lieu de double-cliquer sur le fichier ou permettre à votre programme de messagerie de l'ouvrir automatiquement, vous êtes moins susceptible d'être infecté par un virus.
- Tenez compte des risques possibles lorsque vous connectez à votre ordinateur des dispositifs amovibles, comme des CD, des DVD ou des clés USB. Vous devriez tout d'abord vous assurer que votre programme antivirus est à jour et que son scanner résident est en fonction. Il est aussi suggéré de désactiver la fonction **Exécution automatique** des lecteurs connectés à votre système. Cette fonction peut être utilisée par certains virus pour infecter votre ordinateur. Dans Windows XP, vous pouvez effectuer cette opération en allant dans **Poste de travail**, en cliquant à droite sur le lecteur CD ou DVD voulu, en sélectionnant **Propriétés** et en cliquant sur l'onglet **Exécution automatique**. Pour chaque type de contenu, sélectionnez l'option **Ne rien faire** ou l'option **Me demander à chaque fois de choisir une action**, puis cliquez sur **OK**.
- Vous pouvez également empêcher certaines infections tout simplement en utilisant des logiciels libres (ces programmes sont souvent plus sûrs et les développeurs de virus sont moins enclins à les attaquer).

Assani : J'ai un programme de nettoyage de virus, que je lance assez régulièrement. Donc, mon ordinateur est en santé, non ?

Salima : Et bien, le simple fait d'avoir installé un programme antivirus ne suffit pas ! Il faut aussi protéger ton ordinateur contre les logiciels espions et les pirates. Pour cela, il te faudra installer quelques outils supplémentaires.

Les logiciels espions (ou mouchards)

Les logiciels espions, ou mouchards (*Spyware* en anglais), sont des *programmes malveillants* [2] conçus pour surveiller les tâches que vous effectuez sur votre ordinateur et sur Internet, et pour transmettre ensuite ces renseignements à un tiers qui n'y aurait pas normalement accès. Ces programmes peuvent, entre autres choses, enregistrer les mots que vous tapez sur votre clavier, les mouvements de votre souris, les programmes que vous utilisez ou les sites que vous visitez sur Internet. Par conséquent, ces logiciels peuvent mettre en danger la sécurité de votre ordinateur et révéler des renseignements confidentiels à propos de vous, de vos contacts et de vos activités. Puisque les mouchards infectent les ordinateurs par les mêmes moyens que les virus, plusieurs des suggestions énumérées ci-dessus sont aussi utiles pour se prémunir contre cette autre classe de logiciels malveillants. Comme les sites Internet malveillants constituent une source importante d'infection par mouchards, vous devriez faire particulièrement attention aux sites que vous visitez et vous assurer que les paramètres de votre navigateur soient réglés pour maximiser votre sécurité.

Assani : On dirait un scénario de film d'espionnage. Mon ordinateur est-il vraiment « infecté par des logiciels espions » ?

Muhindo : Crois-le on non, c'est très courant. Si les programmes que tu as téléchargés n'ont pas infecté ton ordinateur, il est fort probable qu'au moins un des sites que tu as visités l'ait fait. Le fait que tu utilises Windows et Internet Explorer augmente encore les chances que tu aies été infecté ! Si tu n'as jamais inspecté ton ordinateur pour y détecter des logiciels espions, je pense que tu seras surpris de constater le nombre de mouchards déjà installés.

Logiciels anti-mouchards

Vous pouvez utiliser des logiciels anti-mouchards pour protéger votre ordinateur contre ce type d'infection. *Spybot* [4] est un de ces programmes fort efficaces pour localiser et supprimer certains programmes malveillants que les antivirus ignorent tout simplement. Cependant, tout comme pour les programmes antivirus, il est très important que vous mettiez régulièrement à jour les définitions de logiciels malveillants de Spybot et que vous effectuiez fréquemment un balayage de votre ordinateur.

Expérience pratique : se lancer avec le Guide pratique Spybot [12]

Prévenir les infections de logiciels espions

- Restez sur vos gardes lorsque vous naviguez sur Internet. Soyez à l'affût des fenêtres intempestives (ou *Pop-up*, ces fenêtres de navigateur qui s'ouvrent automatiquement) et lisez leur contenu attentivement au lieu de simplement cliquer sur `OUI` ou `OK`. Lorsque vous doutez de la légitimité des demandes qui vous sont faites, vous devriez toujours fermer les fenêtres intempestives en cliquant sur le `X` dans le coin supérieur droit de la fenêtre au lieu de cliquer sur `Annuler`. Cela peut empêcher certains sites d'installer à votre insu des logiciels malveillants sur votre ordinateur.
- Augmentez le niveau de sécurité de votre navigateur en l'empêchant de lancer automatiquement les programmes potentiellement dangereux parfois inclus dans le *code source* [13] des sites que vous visitez. Si vous utilisez *Mozilla Firefox* [14], vous pouvez installer le module complémentaire *NoScript* [15], dont les fonctions sont décrites à la ***section 4*** [16] du ***Guide pratique Firefox*** [17].
- N'acceptez jamais d'installer ou de lancer ce type de contenu s'il provient de sites Internet inconnus ou suspects.

Assani : J'ai lu quelque part que les « applets Java » et les « contrôles ActiveX » peuvent être dangereux. Mais je n'ai pas la moindre idée de quoi il s'agit.

Salima : Ce sont des exemples différents d'objets pratiquement identiques : des petits programmes téléchargés par le navigateur lorsque l'on visite certains sites Internet. Les développeurs les utilisent pour créer des sites complexes, mais ces outils peuvent aussi être utilisés pour répandre des virus et des logiciels espions. Il n'est pas vraiment nécessaire de savoir comment ces programmes fonctionnent, pourvu que tu aies installé et lancé le module NoScript.

Le pare-feu

Un pare-feu est un programme conçu pour contrôler les données entrantes depuis l'Internet. C'est aussi le pare-feu qui contrôle en dernier lieu les données sortantes. Un peu comme un garde de sécurité posté en permanence à la porte d'un immeuble pour décider qui peut y entrer et en sortir, un pare-feu reçoit et examine toutes les données entrantes et sortantes et décide des mesures à prendre selon le résultat de ses inspections. Évidemment, il est essentiel que vous défendiez votre système contre les connexions suspectes provenant d'Internet ou des réseaux locaux, puisque ce sont deux points d'accès possibles à votre ordinateur pour les virus et les pirates. La surveillance des connexions sortantes (à partir de votre ordinateur) est elle aussi très importante.

Un bon pare-feu vous permet de définir des permissions d'accès pour chacun des programmes installés sur votre ordinateur. Lorsqu'un de ces programmes tente d'établir une connexion avec l'extérieur, le pare-feu bloque automatiquement la connexion et vous soumet un avertissement, à moins qu'il ne reconnaisse le programme et soit en mesure de confirmer que vous avez déjà défini une permission pour ce type de connexion. Cela sert principalement à empêcher des *logiciels malveillants* [2] existants de répandre des virus ou d'inviter des pirates [18] à envahir votre ordinateur. À cet égard, un bon pare-feu offre à la fois une seconde ligne de défense et un système d'alarme efficace pour vous signaler toute menace à l'intégrité et la sécurité de votre ordinateur.

Les logiciels pare-feu

Les dernières versions de Microsoft Windows incluent un pare-feu intégré qui est désormais activé automatiquement. Malheureusement, le pare-feu Windows comporte plusieurs limites. Par exemple, il n'inspecte pas les connexions sortantes. Cependant, il existe un excellent *gratuiciel* [7] appelé *Comodo Personal Firewall* [19], qui peut sécuriser encore plus efficacement votre ordinateur.

Expérience pratique : se lancer avec le Guide pratique Comodo Firewall [20]

Prévenir les connexions réseau suspectes

- Installez uniquement les programmes essentiels sur l'ordinateur que vous utilisez pour effectuer des tâches délicates. Assurez-vous d'obtenir ces programmes de sources fiables. Désinstallez tous les logiciels que vous n'utilisez pas.
- Déconnectez votre ordinateur d'Internet lorsque vous ne l'utilisez pas et éteignez-le complètement pendant la nuit.
- Ne révélez votre mot de passe Windows à personne.
- Si certains services Windows que vous n'utilisez plus sont toujours activés, vous devriez les désactiver. À ce propos, veuillez consulter la section ***Lecture complémentaire*** [21], à la fin de ce chapitre.
- Assurez-vous que tous les ordinateurs branchés au réseau local de votre bureau disposent d'un pare-feu actif.
- Si vous n'en avez pas déjà un, vous devriez envisager d'installer un pare-feu supplémentaire pour protéger l'ensemble du réseau local au bureau. Plusieurs *passerelles* [22] commerciales à large bande incluent un pare-feu

facile d'utilisation. L'activation de cet outil peut grandement améliorer la sécurité de votre réseau local. Si vous ne savez pas trop par où commencer, vous pouvez toujours demander de l'aide à la personne qui a mis le réseau en place initialement.

Assani : Alors, tu voudrais que j'installe un antivirus, un programme anti-mouchards et un pare-feu ? Est-ce que mon ordinateur peut supporter tout ça ?

Muhindo : Absolument. En fait, de nos jours, ces trois outils constituent le strict minimum si tu souhaites sécuriser ton ordinateur. Comme ces trois programmes sont conçus pour fonctionner ensemble, il ne devrait pas y avoir de problème. N'oublie pas cependant que tu ne dois jamais faire fonctionner simultanément deux antivirus ou deux pare-feu.

Actualiser vos logiciels

Les programmes informatiques sont souvent volumineux et complexes. Il est pratiquement inévitable que certains des logiciels que vous utilisez régulièrement comportent des erreurs et que ces erreurs menacent la sécurité de votre ordinateur. Par contre, les développeurs de logiciels continuent à cerner ces erreurs et à distribuer des mises à jour qui contribuent à les réparer. Il est donc **essentiel que vous actualisiez régulièrement tous les programmes qui sont installés sur votre ordinateur, y compris le système d'exploitation**. Si Windows ne s'actualise pas automatiquement, il est possible de configurer le système pour automatiser les mises à jour. Vous n'avez qu'à cliquer sur **Démarrer**, sélectionner **Tous les programmes** et cliquer sur **Windows Update**. Cela ouvrira une fenêtre de Windows Explorer et vous serez dirigé ver la page Microsoft Update, où vous pourrez activer l'option **Mises à jour automatiques**. À ce sujet, veuillez consulter la section ***Lecture complémentaire***, ci-dessous.

De même, il est important de veiller à ce que tous les autres logiciels installés sur votre ordinateur sont bien à jour. Pour ce faire, il vous faut d'abord savoir quels sont les programmes que vous avez sur votre ordinateur et peut-être désinstaller ceux dont vous n'avez pas besoin (sur Windows, allez dans le panneau de configuration puis *Programmes* ou *Ajout / Suppression de programmes*). Ensuite, il est bon d'examiner pour chaque programme s'il s'agit de la dernière version, comment il peut être mis à jour et se mettre à jour automatiquement par la suite.

Rester à jour avec des outils gratuiciel et FLOSS (logiciels libres et open source)

Les *logiciels propriétaires* exigent souvent que vous fournissiez une preuve d'achat avant de vous permettre d'installer des mises à jour. Si vous utilisez une copie piratée de Microsoft Windows, par exemple, vous ne serez probablement pas en mesure d'actualiser le système, ce qui rend vos données particulièrement vulnérables. En ne disposant pas d'une licence d'utilisation valide, vous vous mettez, vous et ceux avec qui vous travaillez, en danger. L'utilisation illégale de certains logiciels pose également des risques non techniques. En effet, dans un nombre croissant de pays, les autorités ont commencé à vérifier que les organismes disposent d'une licence d'utilisation valide pour chaque logiciel qu'ils utilisent. Des policiers ont confisqué des ordinateurs et procédé à la fermeture définitive d'organisme, sous prétexte que ces derniers pratiquaient la « piraterie informatique ». Il est très facile, pour certains gouvernements qui ont intérêt à interférer dans le travail de ces organismes, d'abuser de cette justification. Heureusement, vous n'êtes pas obligé d'acheter des logiciels dispendieux pour vous protéger de ce genre de tactiques.

Nous recommandons fortement le recours à des solutions de *logiciel libre* ou *FLOSS* (logiciels libres et open source), pour remplacer les *logiciels propriétaires* que vous utilisez présentement, et plus particulièrement les programmes pour lesquels vous ne disposez pas de licence d'utilisation. Les outils en *logiciel libre* et *FLOSS* sont la plupart du temps conçus par des développeurs bénévoles et des organismes à but non lucratif qui les distribuent et les actualisent gratuitement. Les outils *FLOSS*, en particulier, sont habituellement considérés comme plus sûrs que les *logiciels propriétaires&* parce qu'ils sont conçus de manière transparente. Dans le même ordre d'idée, le *code source* de ces programmes peut librement être examiné par divers groupes de spécialistes, qui en retour contribuent à cerner des problèmes et à proposer des solutions.

Plusieurs applications *FLOSS* ont la même apparence et fonctionnent de la même manière que les *logiciels propriétaires* qu'ils ont été conçus pour remplacer. Par ailleurs, il est tout à fait possible d'utiliser ces outils en même temps que des *logiciels propriétaires*, dont le système d'exploitation Windows, sans aucun problème. Même si vos collègues continuent à utiliser la version commerciale d'un type de programme particulier, vous pourrez quand même continuer à échanger des fichiers et partager des données avec la même aisance qu'auparavant. Par exemple, nous vous suggérons de remplacer Internet Explorer, Outlook ou Outlook Express et Microsoft Office par Firefox, Thunderbird et *LibreOffice* (https://www.libreoffice.org/ [23]), respectivement.

En fait vous pourriez même vous défaire complètement du système d'exploitation Microsoft Windows pour adopter une solution *FLOSS* plus sûre appelée *GNU / Linux*. La meilleure façon d'évaluer si vous êtes prêt à faire ce changement est tout simplement d'en faire l'essai. Vous pouvez télécharger une version *LiveCD* de *Ubuntu Linux* (http://www.ubuntu.com/ [24]), la graver sur un CD ou un DVD, insérer ce dernier dans le lecteur de votre ordinateur et redémarrer. Quand le démarrage sera complété, votre ordinateur fonctionnera sur *GNU / Linux* et vous pourrez alors décider si cela vous convient. Ne vous inquiétez pas, rien de tout cela n'est permanent. Quand vous aurez fini d'explorer, vous n'aurez qu'à éteindre l'ordinateur et retirer le *LiveCD* d'Ubuntu. Au prochain démarrage, l'ordinateur s'amorcera avec Windows et tous vos réglages, applications et données seront rétablies exactement comme avant. En plus d'offrir les avantages généraux

et sécuritaires d'un logiciel libre, Ubuntu comporte un outil de mise à jour gratuit et facile à utiliser, qui contribuera à faire en sorte que votre système d'exploitation et la plupart des autres logiciels installés restent actualisés et sécurisés.

Lecture complémentaire

- Voir le chapitre Malicious Software and Spam [25] et l'annexe Internet Program Settings [26] du manuel Digital Security and Privacy for Human Rights Defenders [27].
- Restez à l'affût des développements de virus en visitant régulièrement le site Internet Virus Bulletin [28].
- Apprenez à déterminer quels « services Windows » sont superflus et à désactiver ceux dont vous n'avez pas besoin [29].
- Les autres trousses à outils du Collectif Tactical Technology (TTC [30]) peuvent vous aider à passer aux outils *FLOSS* et *gratuiciels* pour tous vos besoins logiciels.
- Téléchargez des *Rescue CD* d'amorçage gratuits [31] pour balayer votre ordinateur et supprimer les virus qui pourraient s'y trouver sans démarrer Windows.
- Si vous pensez que votre ordinateur est infecté par un virus ou autre logiciel malveillant, consultez le Malware removal Guide for Windows [32].

2. Assurer la sécurité physique de vos données

Malgré tous les efforts que vous avez déployés pour construire une barrière numérique autour de votre ordinateur, il est bien possible que vous vous aperceviez un jour que la machine, ou qu'une copie des données qui se trouvaient dessus, a été perdue, volée ou endommagée par un accident ou un acte malveillant. Des événements anodins comme une saute de courant, une fenêtre laissée ouverte ou une tasse de café renversée peuvent entraîner des situations fâcheuses, comme la perte totale de vos données ou des avaries irréparables à votre ordinateur. Vous pouvez toutefois éviter ce genre de désastre en appliquant des mesures simples comme une évaluation minutieuse des risques, un entretien constant de votre système informatique et la mise en place d'une *politique de sécurité* [33].

Scénario de départ

Shingai et Rudo forment un couple d'aînés qui, depuis plusieurs années, aident les victimes du VIH-SIDA au Zimbabwe à maintenir leur accès aux médicaments essentiels. Ils ont récemment fait une demande de bourse pour être en mesure d'acheter des ordinateurs et du matériel informatique dans le but de monter un réseau local dans leur bureau. Comme ils vivent dans une région secouée par des turbulences politiques et fragilisée par une infrastructure précaire, leurs bailleurs de fonds et eux veulent s'assurer que leur matériel informatique sera à l'abri, pas seulement des pirates et des virus, mais aussi des confiscations, des tempêtes, des surtensions et autres catastrophes du même ordre. Ils ont donc demandé à Otto, un technicien en informatique de la région, de les aider à concevoir un plan d'action pour assurer la sécurité physique des ordinateurs et du réseau informatique qu'ils monteront si leur demande de bourse est acceptée.

Qu'apprendrez-vous dans ce chapitre

- Quelques exemples de *menaces physiques* [34] à l'intégrité de votre ordinateur et des données qui y sont stockées ;
- Les meilleurs moyens de protéger votre matériel informatique contre certains de ces risques ;
- Comment mettre en place un environnement de travail sain pour les ordinateurs et le matériel du réseau informatique ;
- Les éléments à considérer dans la conception d'un plan de sécurité informatique pour le bureau.

L'évaluation des risques

Plusieurs organismes sous-estiment l'importance de maintenir la sécurité physique de leur environnement de travail et de leur matériel informatique. Conséquemment, il leur manque souvent une politique claire concernant les mesures à mettre en place pour protéger les ordinateurs et dispositifs de sauvegarde contre le vol, les conditions climatiques extrêmes, les accidents et autres *menaces d'ordre physique* [35]. L'importance de telles politiques peut sembler évidente, mais il peut aussi s'avérer compliqué d'en formuler clairement les éléments. Plusieurs organismes, par exemple, installent des cadenas de bonne qualité sur la porte d'entrée de leurs locaux (et plusieurs installent également des barreaux aux fenêtres), mais s'ils ne font pas attention au nombre de copies des clés, ni à qui ces clés sont confiées, leurs données confidentielles demeurent vulnérables.

Shingai : Nous voudrions inclure un résumé de notre politique de sécurité dans la demande de bourse, mais il nous faut tout d'abord nous assurer que cette politique est complète. Que devrait-on y inclure ?

Otto : J'ai bien peur de ne pas pouvoir vous proposer une solution universelle au défi que pose la sécurité physique. Les

caractéristiques d'une bonne politique dépendent presque toujours des circonstances et conditions particulières à un organisme ou un individu. Voici tout de même un conseil utile : lorsque vous entamez la conception d'un plan de sécurité, il vous faut étudier attentivement votre environnement de travail et cerner vos points faibles pour ensuite trouver les moyens de les renforcer.

Lorsque vous évaluez les risques courus par votre organisme ainsi que ses points vulnérables, vous devez vous pencher sur les différents niveaux de danger auxquels vos données sont exposées.

- Tenez compte des moyens de communication que vous utilisez et de votre utilisation particulière de ces moyens. Par exemple, la correspondance par courrier postal, le télécopieur, la ligne téléphonique physique, le téléphone portable, le courrier électronique, la messagerie *Skype* [36], etc.
- Tenez compte des moyens que vous employez pour stocker vos données. Les disques durs, les serveurs Internet et de courriel, les clés USB, les disques durs externes, les CD et DVD, les téléphones portables, les copies imprimées et les notes rédigées à la main sont des exemples courants.
- Tenez compte des lieux où ces choses sont situées physiquement. Elles peuvent être au bureau, à la maison, dans une poubelle à l'extérieur du local ou, de plus en plus, « quelque part dans Internet »... Dans ce dernier cas, il peut s'avérer particulièrement difficile de déterminer l'emplacement physique de certaines données.

Gardez à l'esprit que la même information peut être vulnérable à plusieurs niveaux. De la même façon que vous utilisez un programme antivirus pour protéger le contenu d'une clé USB contre les *logiciels malveillants* [2], vous devez utilisez un plan de sécurité détaillé pour empêcher que les mêmes données soient volées, perdues ou détruites. Même si certaines mesures de sécurité d'ordre général, comme une politique de sauvegarde des données à l'extérieur du bureau, sont utiles contre les menaces physiques et numériques, d'autres mesures concernent spécifiquement les dangers physiques.

Quand vous décidez qu'il est plus sûr de transporter votre clé USB dans un sac de plastique scellé au fond de votre sac de voyage plutôt que dans votre poche, vous faites un choix qui concerne la sécurité physique de vos données, mêmes si celles-ci sont numériques. Comme d'habitude, le caractère particulier de la politique dépend de la situation. Devez-vous traverser la ville d'un bout à l'autre à la marche, ou plutôt traverser des frontières nationales ? Quelqu'un d'autre que vous transportera-t-il votre sac ? Est-ce qu'il pleut ? C'est le genre de questions dont vous devriez tenir compte lorsque vous prenez des décisions de cette nature.

Protéger vos données des intrus

Les individus malveillants qui souhaitent accéder à vos données représentent un type de *menace physique* [35] important. Ce serait une erreur de croire que ce type de danger est le seul qui menace physiquement vos données, mais ce serait encore plus dangereux de l'ignorer. Il y a un ensemble de mesures que vous pouvez appliquer pour réduire les risques d'intrusion physique. Les catégories et suggestions énumérées ci-dessous constituent un point de départ : vous devriez interpréter ces suggestions selon votre propre situation. La plupart de ces suggestions sont aussi bien appropriées pour la maison que pour le bureau.

Le milieu où se trouve votre bureau

- Apprenez à connaître vos voisins. Selon le climat et le degré de sécurité qui prévalent dans votre pays et votre voisinage, l'une ou l'autre des possibilités suivantes s'appliquent : soit vous pouvez faire de vos voisins des alliés qui vous aideront à surveiller et protéger votre bureau ; soit vous pouvez ajouter vos voisins à la liste des menaces possibles dont vous devez tenir compte dans votre plan de sécurité.
- Évaluez les moyens de protection des portes, fenêtres et autres points d'accès qui mènent à votre bureau.
- Envisagez la possibilité d'installer une caméra de surveillance ou une alarme reliée à un détecteur de mouvement.
- Si possible, mettez en place une aire de réception où les visiteurs seront accueillis avant d'entrer dans le bureau, ainsi qu'une salle de réunion séparée de l'espace de travail régulier.

Le bureau

- Protégez les câbles de réseau en les faisant passer à l'intérieur du bâtiment.
- Gardez le matériel réseau, tel que les *serveurs* [37], *routeurs* [22], *commutateurs* [22], *concentrateurs* [22] et modems, dans une salle ou une armoire verrouillée. Un intrus disposant d'un accès libre à ces pièces d'équipement pourrait facilement y installer des *logiciels malveillants* [2] dans le but de voler vos données ou d'attaquer vos ordinateurs ultérieurement. Dans certaines circonstances, il peut être utile de cacher serveurs, ordinateurs ou autre équipement dans un grenier, dans un faux plafond ou même chez un voisin et de les utiliser via une connexion sans fil.
- Si vous avez un accès réseau sans fil, il est essentiel que vous sécurisiez votre *point d'accès* [22] pour empêcher que des intrus parasitent votre réseau ou se mettent à surveiller vos communications. Si vous utilisez un réseau sans fil non sécurisé, quiconque habite dans votre quartier et dispose d'un ordinateur portable devient un intrus en puissance. C'est une définition inhabituelle de « physique », mais rappelez-vous qu'un individu malveillant qui a la possibilité de surveiller votre réseau sans fil dispose du même accès qu'un intrus qui aurait réussi à pénétrer dans le bureau pour connecter un câble Ethernet au réseau. Les étapes comprises dans le processus de sécurisation du réseau sans fil varient selon le matériel et les logiciels employés pour établir le point d'accès, mais elles sont habituellement faciles à suivre.

Votre environnement de travail

- Vous devriez placer votre moniteur judicieusement, autant lorsque vous êtes à votre poste que lorsque vous êtes absent du bureau, de telle sorte que les autres ne puissent pas lire ce qui y est affiché. Cela implique que vous teniez compte de la situation des fenêtres, des portes ouvertes et des postes de travail des invités, s'il y a lieu.
- Les boîtiers de la plupart des ordinateurs de bureau comportent une petite fente conçue pour recevoir un cadenas. Cette précaution sert à assurer que seules les personnes qui détiennent la clé seront en mesure d'ouvrir le boîtier. Si vous avez des boîtiers de ce genre au bureau, vous devriez les verrouiller pour empêcher que des intrus aient accès au matériel. Vous devriez aussi tenir compte de cette fonction lorsque vous achetez de nouveaux ordinateurs.
- Utilisez des *câbles de sécurité* [38], lorsque cela est possible, pour empêcher que des intrus ne partent avec vos ordinateurs sous le bras. Cela est particulièrement important pour les ordinateurs portables ou les ordinateurs de bureau miniatures qui peuvent facilement être dissimulés dans un sac ou sous un manteau.

Les logiciels et paramètres liés à la sécurité physique

- Assurez-vous que le démarrage de votre ordinateur soit protégé par un mot de passe. Si ce n'est pas le cas, vous pouvez activer cette fonction dans Windows en cliquant sur le menu *Démarrer*, en sélectionnant le *Panneau de configuration*, et en double-cliquant sur *Comptes d'utilisateurs*. Dans la fenêtre *Comptes d'utilisateurs*, sélectionnez votre propre compte et cliquez sur *Créer un mot de passe*. Choisissez un mot de passe sûr, tel qu'indiqué au chapitre ***3. Créer et sauvegarder des mots de passe sûrs*** [39], saisissez votre mot de passe, puis confirmez-le et cliquez sur *Créer un mot de passe*.
- Il existe quelques paramètres dans le *BIOS* [40] de votre ordinateur qui concernent la sécurité physique. Premièrement, vous devriez configurer votre ordinateur pour qu'il ne soit pas possible de l'amorcer à partir du périphérique USB ou des lecteurs CD-ROM ou DVD. Ensuite, vous devriez définir un mot de passe pour le BIOS lui-même, de telle sorte qu'un intrus éventuel ne soit pas en mesure de modifier les paramètres. Là encore, assurez-vous d'employer un mot de passe sûr.
- Si vous employez une base de données de mots de passe, tel que suggéré au ***chapitre 3*** [39], pour stocker les mots de passe de Windows et du BIOS d'un ordinateur donné, assurez-vous de garder une copie de la base de données ailleurs que sur cet ordinateur.
- Prenez l'habitude de fermer votre compte chaque fois que vous vous éloignez de votre ordinateur. Dans Windows, vous pouvez le faire rapidement en maintenant enfoncée la touche du clavier où figure le logo de Windows et en pressant simultanément la touche L. Cela ne fonctionnera que si vous avez créé un mot de passe pour votre compte, tel que décrit ci-dessus.
- *Chiffrez* [41] toutes les données sensibles qui sont sauvegardées sur les ordinateurs et les dispositifs de stockage amovibles du bureau. Veuillez consulter le chapitre ***4. Protéger les données sensibles stockées sur votre ordinateur*** [42] pour plus de détails et de références vers les guides pratiques appropriés.

Rudo : J'avoue que je suis un peu réticent à modifier quoi que ce soit dans le BIOS. Est-ce je risque d'endommager l'ordinateur si je me trompe ?

Otto : Tout à fait, en tous cas pendant quelque temps. En fait, les paramètres qu'il faudrait changer sont plutôt simples, mais l'affichage du BIOS lui-même peut être quelque peu intimidant et il est effectivement possible que l'ordinateur ne démarre plus normalement si tu te trompes. En règle générale, si vous n'êtes pas à l'aise de modifier des réglages du BIOS, il est préférable de demander de l'aide à une personne plus expérimentée.

Les dispositifs portables ou amovibles

- Gardez toujours près de vous votre ordinateur portable, votre téléphone portable ou tout autre dispositif portable où sont stockés des renseignements de nature délicate, surtout si vous êtes en voyage ou si vous restez à l'hôtel. Il est utile de voyager avec un câble de sécurité pour votre ordinateur portable, même s'il est parfois difficile de trouver un objet approprié pour l'y attacher. N'oubliez pas que les périodes de repas sont souvent exploitées par les voleurs, dont plusieurs ont appris à fouiller les chambres d'hôtel lorsque leurs occupants en sont absents.
- Si vous avez un ordinateur portable, une tablette tactile ou autre appareil mobile, tâchez d'éviter de les mettre en évidence. Il est inutile de montrer aux voleurs que vous transportez des items de valeurs ou de révéler à des individus qui pourraient souhaiter accéder à vos données que vous transportez dans votre sac un disque dur rempli de précieux renseignements. Évitez d'utiliser vos dispositifs portables dans des lieux publics et, si possible, ne transportez pas votre ordinateur portable dans un sac conçu à cet effet.

Maintenir un environnement sain pour votre matériel informatique

Comme plusieurs autres appareils électroniques, les ordinateurs sont très fragiles. Ils réagissent mal au courant électrique instable, aux températures extrêmes, à la poussière, à l'humidité et à la tension mécanique. Il existe plusieurs mesures de précaution que vous pouvez appliquer pour protéger vos ordinateurs et autres appareils informatiques contre des dangers physiques :

- Les problèmes électriques, comme les sautes de courant, les pannes et les coupures complètes ou partielles peuvent gravement endommager un ordinateur. Des irrégularités de ce genre peuvent faire planter votre disque dur et causer des dommages aux données qu'il contient, ou même occasionner des dégâts irréparables aux composants électroniques de l'ordinateur.
    - Si vous en avez les moyens, vous devriez installer un *dispositif d'alimentation sans interruption* [43] (*ASI, ou UPS en anglais* [43]) sur tous les ordinateurs importants de votre bureau. L'ASI stabilise l'approvisionnement en électricité et fournit un courant électrique temporaire en cas de coupure.
    - Même dans les cas où les dispositifs d'ASI ne sont pas appropriés ou sont trop chers, vous devriez utiliser des filtres de courant ou des parasurtenseurs, deux appareils qui protégeront efficacement vos ordinateurs contre les sautes de courant inattendues.
    - Testez votre réseau électrique avant d'y connecter du matériel informatique important. Essayez, autant que possible, d'utiliser des prises de courant à trois bornes, l'une d'elles étant un « fil de terre » (ou *ground*). Avant de brancher des ordinateurs au réseau électrique d'un nouveau local, prenez une journée ou deux pour observer le comportement du réseau lorsque seulement des articles électriques peu énergivores, comme une lampe ou un ventilateur de table, y sont branchés.
- Pour éviter les accidents, de façon générale, ne placez pas de matériel important dans les passages, dans l'aire de réception ou les autres lieux facilement accessibles. Les dispositifs d'alimentation sans interruption, les parasurtenseurs, les barres multiprises et les fils d'extension (et tout spécialement ceux qui sont branchés aux *serveurs* [37] et autres éléments du réseau) devraient être situés là où ils ne pourront pas être débranchés par mégarde.
- Si vous pouvez trouver des câbles d'ordinateur, des barres multiprises et des fils d'extension de qualité supérieure, vous devriez en acheter suffisamment pour brancher tous les appareils du bureau et en prendre quelques-uns de plus en extra. Les barres multiprises qui se débranchent toutes seules du mur, ne se branchent pas de façon sécuritaire ou génèrent constamment des étincelles ne sont pas seulement agaçantes, elles constituent une menace importante à la sécurité physique des ordinateurs qui y sont branchés. Elles peuvent aussi pousser des utilisateurs frustrés à attacher des fils d'ordinateur trop lâches avec du ruban adhésif, ce qui peut évidemment provoquer un incendie.
- Si vous gardez un ordinateur à l'intérieur d'une armoire, assurez-vous qu'il y ait une bonne ventilation, faute de quoi la machine pourrait surchauffer.
- Le matériel informatique ne devrait jamais être installé à proximité d'un radiateur, d'une bouche d'aération, d'un climatiseur ou de toute autre conduite ou canalisation.

Concevoir une politique de sécurité

Après avoir évalué attentivement les menaces qui vous guettent et les points vulnérables de vos systèmes, vous devez évaluer les différentes solutions à mettre en place pour améliorer votre sécurité physique. Vous devriez concevoir une *politique de sécurité* [44] détaillée et mettre l'ensemble de ces solutions par écrit. Ce document servira de directive générale pour vous, vos collègues et les nouveaux venus à votre organisme. Ce plan devrait aussi inclure une liste d'actions à entreprendre en cas d'urgences liées à un éventail de dangers différents. Chacune des personnes engagées auprès de votre organisme devrait prendre le temps de lire, mettre en vigueur et maintenir ces normes de sécurité. Vous devriez aussi les encourager à poser des questions et suggérer des améliorations à votre politique de sécurité.

Votre politique de sécurité physique peut comporter plusieurs sections, selon les circonstances :

- Une politique d'accès au local qui tient compte des éléments suivants : les systèmes d'alarmes ; le nombre de clés en circulation, ainsi que chaque personne qui en détient une copie ; les périodes où les invités sont admis dans le bureau ; à qui revient le contrat d'entretien et autres enjeux du même ordre.
- Une politique expliquant quelles parties du bureau sont d'accès restreint (seuls les employés et les visiteurs autorisés peuvent y aller).
- Un inventaire détaillé de votre matériel, y compris les numéros de série et une description physique de chaque appareil.
- Une marche à suivre pour la destruction des documents imprimés contenant des renseignements de nature délicate.
- Des procédures d'urgence concernant :
    - Les personnes à aviser si des renseignements de nature délicate sont révélés ou perdus ;
    - Les personnes à contacter en cas d'incendie, d'inondation ou autre catastrophe naturelle ;
    - La marche à suivre pour effectuer certaines réparations essentielles ;
    - Les moyens de communiquer avec les compagnies ou organismes qui fournissent les services essentiels, tel que l'électricité, l'eau courante, l'accès Internet, etc.
    - Comment récupérer les données stockées sur votre système de sauvegarde à l'extérieur du bureau. Vous trouverez plus de conseils à ce sujet au chapitre ***5. Récupérer des données perdues*** [45].

  Vous devriez réviser votre politique de sécurité périodiquement et la modifier pour intégrer tous les changements qui se sont produits depuis la dernière révision. Évidemment, il est important de faire une ou plusieurs copies de sauvegarde de votre document de politique de sécurité, comme pour tous vos renseignements importants. Veuillez consulter la section ***Lecture complémentaire*** [46], ci-dessous, pour plus de renseignements sur la rédaction d'une politique de sécurité.

Lecture complémentaire

- Pour plus de conseils sur l'évaluation des risques, veuillez consulter les sections Security Awareness [47] et Threat Assessment [48] du manuel Digital Security and Privacy for Human Rights Defenders [49].
- Pour des consignes détaillées sur le réglage d'un mot de passe pour le BIOS, veuillez consulter le chapitre Windows Security [50] du manuel Digital Security and Privacy for Human Rights Defenders [49].
- Pour des directives supplémentaires sur la rédaction d'une politique de sécurité, veuillez consulter le Case Study 1 [51] du manuel Digital Security and Privacy for Human Rights Defenders [49].
- Consultez également le Protection Manual [52] et le Protection Handbook [53] à l'intention des *Human Rights Defenders*.

3. Créer et sauvegarder des mots de passe sûrs

La plupart des services sécurisés qui nous permettent d'utiliser les technologies numériques pour accomplir des tâches importantes (comme l'authentification des séances de travail sur un ordinateur personnel, l'envoi de courrier électronique, le *chiffrement* [54] ou la dissimulation de données de nature délicate) exigent que nous gardions en mémoire un ou plusieurs mots de passe. Ces codes secrets, phrases ou séquences de caractères inintelligibles constituent souvent une première barrière (et parfois la seule et unique barrière) entre nos données et les tiers qui souhaiteraient lire, copier, modifier ou détruire ces renseignements sans notre permission. Il existe plusieurs stratagèmes par lesquels une personne malveillante pourrait intercepter vos mots de passe, mais vous pouvez aussi vous défendre efficacement contre la plupart de ces manœuvres en appliquant quelques mesures de précaution fondamentales et en ayant recours à une *base de données de mots de passe sécurisée* [55], tel que le programme *KeePass* [56].

Scénario de départ

Mansour et Magda sont frère et sœur. Ils habitent un pays arabophone. Ensemble, ils gèrent un blog où ils dénoncent anonymement plusieurs violations de droits humains et mènent une campagne en faveur de changements d'ordre politique. Récemment, Magda s'est aperçue que le mot de passe de son service webmail avait été modifié à son insu. Après avoir réinitialisé le mot de passe, elle a pu se connecter au service, mais elle a constaté en ouvrant sa corbeille d'arrivée que plusieurs de ses nouveaux messages étaient marqués comme lus. Elle soupçonne qu'un intrus malintentionné ait pu obtenir ou deviner son mot de passe. Or, elle utilise le même mot de passe pour plusieurs autres comptes de courriel et sites Internet. Elle en discute avec Mansour, qui a moins d'expérience qu'elle en la matière, pour lui expliquer la situation et lui signaler son inquiétude.

Qu'apprendrez-vous dans ce chapitre

- Les éléments essentiels d'un mot de passe sûr ;
- Quelques astuces pour mémoriser des mots de passe longs et complexes ;
- Comment utiliser une base de données de mots de passe sécurisée de KeePass pour sauvegarder des mots de passe au lieu de les mémoriser.

Choisir et conserver des mots de passe sûrs

D'habitude, pour protéger un objet de valeur, on le place sous clé. Les maisons, les voitures et les cadenas de vélo sont généralement protégés par une serrure et une clé correspondante ; les fichiers sécurisés sont quant à eux protégés par des clés de *chiffrement* [41], les cartes de débit par des numéros d'identification personnelle et les comptes de courriel par des mots de passe confidentiels. Toutes ces clés, qu'elles soient physiques ou abstraites, ont une chose en commun : elles peuvent aussi bien accomplir leur fonction lorsqu'elles aboutissent dans les mains d'une autre personne que vous. Vous pouvez bien installer des pare-feu sophistiqués, ouvrir des comptes de courriel sécurisés et utiliser des disques chiffrés, si votre mot de passe est faible et facile à deviner, ou si vous le laissez tomber entre les mains de personnes mal intentionnées, toutes ces mesures de précaution seront inutiles.

Les éléments essentiels d'un mot de passe fort

Un bon mot de passe doit être difficile, voire impossible, à deviner par un programme informatique.

- **Il doit être long :** Plus un mot de passe est long, moins il est probable qu'un programme informatique soit en mesure

de le deviner rapidement. Vous devriez essayer, autant que possible, de créer des mots de passe de dix caractères ou plus. Certaines personnes utilisent des mots de passe comportant plus d'un mot, avec ou sans espaces. On parle alors de phrases secrètes, ou « phrases de passe ». C'est une bonne idée, pourvu que le programme ou le service que vous utilisez vous permette de choisir des mots de passe assez longs.

- **Il doit être complexe :** En plus de la longueur, la complexité d'un mot de passe contribue à faire en sorte qu'un logiciel de « craquage (ou cassage) de mots de passe » soit incapable de trouver la bonne combinaison de caractères. Autant que possible, vous devriez toujours utiliser une combinaison de majuscules, de minuscules, de chiffres et de symboles (comme des signes de ponctuation) dans tous vos mots de passe.

Un bon mot de passe doit être difficile, voire impossible, à deviner par qui que ce soit.

- **Il doit être pratique :** Si vous écrivez votre mot de passe quelque part parce que vous êtes incapable de vous en rappeler, vous vous rendez vulnérable à un tout autre type de menaces : quiconque est à portée de votre écran ou accède temporairement à votre poste de travail, votre portefeuille ou même la poubelle à l'extérieur de votre bureau, est susceptible de trouver votre mot de passe. Si vous n'êtes pas capable de trouver un mot de passe qui est suffisamment long et complexe, mais tout de même facile à mémoriser, les conseils énumérés à la section ***Mémoriser des mots de passe sûrs*** [57], ci-dessous, vous seront peut-être utiles. Sinon, vous devriez tout de même choisir une combinaison sûre, mais il vous faudra peut-être l'enregistrer à l'aide d'un programme de *base de données de mots de passe sécurisée* [55], comme *KeePass* [58]. D'autres types de fichiers protégés par mot de passe, comme les documents Microsoft Word, ne sont pas fiables pour cet usage, car il est facile de les casser en quelques secondes à l'aide d'outils que l'on trouve facilement sur Internet.

- **Il ne doit comporter aucun élément personnel :** Votre mot de passe ne devrait pas faire référence à vous personnellement. Ne choisissez pas un mot de passe incluant des renseignements comme votre nom, votre numéro d'assurance sociale, votre numéro de téléphone, le nom de vos enfants, de vos conjoints ou de vos animaux domestiques, votre date d'anniversaire ou quoi que ce soit d'autre qu'une personne mal intentionnée pourrait facilement apprendre à votre sujet en effectuant une recherche rapide.

- **Gardez-le pour vous :** Ne révélez votre mot de passe à personne, à moins que cela ne soit absolument nécessaire. Si vous deviez tout de même, pour une raison ou une autre, partager votre mot de passe avec un ami, un collègue ou un membre de votre famille, vous devriez d'abord modifier le mot de passe, transmettre le mot de passe temporaire à cette personne, puis, lorsqu'elle a fini de s'en servir, rétablir votre mot de passe secret. Normalement, vous devriez recourir à une solution de rechange (comme créer un compte particulier pour chacune des personnes qui souhaitent ou doivent accéder au service dont il est question) plutôt que de partager votre mot de passe avec une autre personne. Pour garder votre mot de passe secret, vous devez aussi faire attention que personne ne vous espionne lorsque vous le saisissez sur un clavier ou le récupérez dans une base de données de mots de passe sécurisée.

Un mot de passe doit être choisi de telle sorte que vous soyez en mesure de limiter les dégâts si quelqu'un parvient à l'intercepter.

- **Assurez-vous qu'il soit tout à fait unique :** Éviter d'utiliser le même mot de passe pour plusieurs comptes. Autrement, si une personne mal intentionnée parvient à deviner ou intercepter votre mot de passe, elle aura accès à encore plus de vos données. Cela est d'autant plus important que certains services comportent des lacunes qui font qu'il est relativement facile de casser les mots de passe. Si, par exemple, vous utilisez le même mot de passe pour votre compte d'utilisateur Windows et votre compte Gmail, une personne ayant accès à votre ordinateur pourra, le cas échéant, débusquer votre mot de passe et se connecter également à votre compte de courriel. Pour les mêmes raisons, il est déconseillé de simplement échanger vos mots de passe d'un compte à l'autre.

- **Rafraîchissez-le régulièrement :** Changez vos mots de passe régulièrement, préférablement tous les trois mois. Certaines personnes s'attachent à un mot de passe en particulier et n'en change jamais. C'est une très mauvaise idée. Plus vous gardez le même mot de passe longtemps, plus il sera facile à deviner. De plus, si une personne arrive à utiliser votre mot de passe pour accéder à vos données et se connecter à vos services à votre insu, elle pourra le faire impunément jusqu'à ce que vous changiez enfin votre mot de passe.

Mansour : Mais si je te fais confiance ? Ça va si je te donne mon mot de passe, non ?

Magda : Et bien, tout d'abord, même si tu fais suffisamment confiance à une personne pour lui confier ton mot de passe, cela ne signifie pas nécessairement que cette personne en prendra soin, non ? Même si je ne ferais rien de mal avec ton mot de passe, je pourrais par exemple l'écrire sur un bout de papier et le perdre. Tu vois ? C'est peut-être même comme ça que je me suis mise dans ce pétrin ! Par ailleurs, ce n'est pas uniquement une question de confiance. Si tu es le seul à connaître ton mot de passe, tu n'auras pas à te demander un jour qui a bien pu se connecter à ton compte sans autorisation. En fait, au point où j'en suis, je suis assez certaine que quelqu'un a deviné ou « cassé » mon mot de passe, parce que je ne l'ai jamais écris nulle part ni révélé à qui que ce soit.

Mémoriser et enregistrer des mots de passe sûrs

À la lecture des recommandations énumérées ci-dessus, vous vous dites peut-être que seule une personne ayant une mémoire photographique pourrait se rappeler de plusieurs mots de passe aussi longs, complexes et inintelligibles sans les consigner par écrit. L'importance d'utiliser un mot de passe différent pour chaque compte complique encore les choses. Il existe toutefois quelques astuces qui pourront vous aider à créer des mots de passe faciles à mémoriser mais

extrêmement difficiles à deviner, même pour une personne qui se sert d'un logiciel de « craquage de mots de passe ». Vous pouvez aussi enregistrer vos mots de passe en utilisant une *base de données de mots de passe sécurisée* [55], comme *KeePass* [58].

Mémoriser des mots de passe sûrs

Il est important d'utiliser plusieurs types de caractères pour composer un nouveau mot de passe. Par exemple :

- Combinez des minuscules et des majuscules : 'My naME is Not MR. MarSter'
- Faites alterner des lettres et des chiffes : 'a11 w0Rk 4nD N0 p14Y'
- Incluez des symboles ou des signes de ponctuation : 'c@t(heR1nthery3'
- Combinez des mots empruntés à plusieurs langues : 'Let Them Eat 1e gateaU du ch()colaT'

Toutes ces méthodes contribuent à augmenter le niveau de complexité d'un mot de passe. Elles vous permettent de choisir des mots de passe sûrs sans pour autant abandonner l'idée de les mémoriser. Même si certaines des substitutions les plus courantes (comme l'utilisation du zéro au lieu du 'o', ou celle du '@' au lieu du 'a') sont depuis longtemps incorporées aux outils qu'emploient les pirates pour craquer les mots de passe, il est toujours utile d'y recourir. Ces substitutions simples augmentent considérablement le temps requis par un programme pour deviner un mot de passe et, dans la plupart des situations où il n'est tout simplement pas possible d'utiliser de tels outils, elles font en sorte qu'il est très difficile pour un humain de deviner la bonne combinaison.

Vous pouvez aussi employer des *procédés mnémoniques* [59] plus traditionnels, comme des acronymes. Cela vous permet de transformer de longues phrases en séquences de caractères complexes et, à première vue, aléatoires :

- 'To be or not to be? That is the question' devient '2Bon2B?TitQ'
- 'We hold these truths to be self-evident: that all men are created equal' devient 'WhtT2bs-e:taMac='
- 'Are you happy today?' devient 'rU:-)2d@y?'

Nous vous présentons ces quelques exemples pour vous aider à trouver votre propre méthode de combinaison de mots et de phrases à la fois complexes et facile à mémoriser.

Le petit effort à fournir pour rendre le mot de passe plus complexe revêt une très grande utilité. Le fait d'augmenter la longueur du mot de seulement quelques caractères ou d'y ajouter des chiffres ou des caractères spéciaux peut rendre celui-ci beaucoup plus difficile à cracker. En guise de démonstration, le tableau ci-dessous expose le temps nécessité par un hacker pour cracker un mot de passe selon sa complexité - en allant du mot le plus simple au plus complexe.

Exemples de mot de passe	Temps de crackage avec un ordinateur basique	Temps de crackage avec un ordinateur très performant
bananas	Moins d'une journée	Moins d'une journée
bananalemonade	2 jours	Moins d'une journée
BananaLemonade	3 mois, 14 jours	Moins d'une journée
B4n4n4L3m0n4d3	3 siècles, 4 décennies	1 mois, 26 jours
We Have No Bananas	19151466 siècles	3990 siècles
W3 H4v3 N0 B4n4n45	20210213722742 siècles	4210461192 siècles

Bien sûr, le temps nécessité pour cracker l'un des mots de passe présentés ci-dessus variera considérablement selon la nature de l'attaque et les ressources dont l'attaquant dispose. En outre, de nouvelles méthodes de crackage de mots de passe sont constamment en cours d'élaboration. Toutefois, le tableau démontre bien qu'il suffit de varier les caractères et d'utiliser deux mots, ou mieux encore une phrase courte, pour rendre la tâche du hacker d'autant plus difficile.

Le tableau ci-dessus est basé sur des calculations Passfault [60]. Passfault fait partie d'un certain nombre de sites vous permettant de tester la force de vos mots de passe. De tels sites offrent certes de précieuses informations quant à l'efficacité relative des différents types de mots de passe, il est toutefois conseillé de ne pas y entrer votre mot de passe actuel.

Enregistrer des mots de passe de façon sécurisée

Même si un minimum d'inventivité peu vous aider à mémoriser tous vos mots de passe, la nécessité de modifier vos mots de passe régulièrement peut vite venir à bout de votre créativité. Comme solution de rechange, vous pouvez utiliser un programme pour générer automatiquement des mots de passe complexes et abandonner complètement l'idée de les mémoriser. Vous pouvez sauvegarder ces mots de passe aléatoires dans une base de données de mots de passe sécurisée, chiffrée et portable. C'est ce que propose le programme KeePass.

Expérience pratique : se lancer avec le Guide pratique KeePass [61]

Évidemment, si vous privilégiez cette méthode, il est particulièrement important que vous créiez une phrase secrète sûre pour KeePass ou tout autre programme employé à cet effet. Chaque fois que vous devez saisir un mot de passe pour un compte ou un service donné, vous pouvez le récupérer à l'aide de votre phrase secrète principale, ce qui facilite le recours à toutes les suggestions mentionnées ci-dessus. KeePass est portable, ce qui signifie que vous pouvez déposer la base de données sur une clé USB au cas où vous auriez besoin de rechercher un ou plusieurs mots de passe lorsque vous êtes loin de votre ordinateur principal.

Même s'il s'agit probablement de la meilleure option pour une personne qui dispose de plusieurs comptes différents, cette méthode comporte quelques désavantages. Premièrement, si vous perdez ou supprimez malencontreusement la seule et unique copie de votre base de données de mots de passe, vous ne pourrez plus accéder aux comptes dont le mot de passe y était stocké. C'est pourquoi il est de toute première importance que vous conserviez une copie de sauvegarde de votre base de données KeePass. Consultez attentivement le chapitre ***5. Récupérer des données perdues*** [62] pour plus de conseils sur la création de copies de sauvegarde. Heureusement, le fait que votre base de données soit chiffrée signifie que vous n'avez pas à paniquer si vous perdez une clé USB ou un disque de sauvegarde où vous l'aviez stockée.

Le deuxième inconvénient majeur peut s'avérer encore plus grave. Si vous oubliez votre phrase secrète principale pour KeePass, il n'existe aucun moyen pour récupérer le contenu de la base de mots de passe. Il est donc capital que vous choisissiez une phrase secrète principale aussi sûre que facile à mémoriser !

Dans certaines situations, la force de cette méthode peut en devenir la faiblesse. Si quelqu'un vous force à donner votre phrase secrète principale pour KeePass, il aura accès à tous les mots de passe stockés dans cette base de données. S'il s'agit d'une situation à laquelle vous puissiez être confronté, considérez la base de données KeePass comme un fichier sensible et veillez à sa protection comme décrit dans le chapitre ***4. Protéger les données sensibles stockées sur votre ordinateur*** [63]. Vous pouvez également créer une base de données KeePass séparée, destinée à contenir les mots de passe protégeant des informations plus sensibles - et prenez des précautions supplémentaires pour cette base de données.

Mansour : Attends un peu. Si KeePass utilise un seul et unique mot de passe pour protéger tous les autres mots de passe, comment cela est-il plus sûr que d'utiliser le même mot de passe pour tous les comptes ? Si un type mal intentionné parvient à dénicher ton mot de passe principal, il pourra accéder à toutes tes données, non ?

Magda : C'est une bonne question, et c'est vrai qu'il est extrêmement important de protéger la phrase secrète, c.-à-d. le mot de passe principal. Mais il y a quand même quelques différences importantes entre les deux méthodes que tu compares. Premièrement, le « type mal intentionné » en question n'aurais pas seulement besoin du mot de passe principal, il faudrait aussi qu'il ait accès à la base de données KeePass correspondante. Par contre, si tu n'utilises qu'un seul mot de passe pour tous tes comptes, le type n'aurait besoin que de ce mot de passe unique pour accéder à toutes tes données. Par ailleurs, nous savons que KeePass est un programme extrêmement sûr, pas vrai ? Et bien, on ne peut pas en dire autant de plusieurs programmes et sites Internet. Certains sont beaucoup moins sûrs que d'autres et tu ne voudrais surtout pas que quelqu'un parvienne à se connecter à un site faible et utilise ensuite ce qu'il y a appris pour accéder à des comptes mieux sécurisés. Et il y a un dernier point. Il est très facile, dans KeePass, de changer ton mot de passe principal si tu juges que c'est nécessaire. Je n'ai pas eu cette chance ! J'ai dû passer la journée au complet à modifier chacun de mes mots de passe.

Lecture complémentaire

- Veuillez consulter le chapitre Password Protection [64] et l'annexe How long should my password be? [65] du manuel Digital Security and Privacy for Human rights Defenders [49].[1]
- Wikipédia présente de bons articles sur les mots de passe [66] [2], la force des mots de passe [67] [3] et le cassage de mots de passe [68].[4]

Liens

[1] www.frontlinedefenders.org/manual/en/esecman [49]
[2] www.fr.wikipedia.org/wiki/Password [69]
[3] www.en.wikipedia.org/wiki/Password_strength [70]
[4] www.fr.wikipedia.org/wiki/Password_cracking [71]

4. Protéger les données sensibles stockées sur votre ordinateur

L'accès non autorisé aux données qui se trouvent sur votre ordinateur ou vos dispositifs de stockage portatifs peut être obtenu à distance, si « l'intrus » est en mesure de lire ou de modifier ces données via Internet, ou physiquement si ce dernier trouve le moyen de mettre la main sur votre matériel. Vous pouvez vous protéger contre ces deux formes d'intrusion en améliorant aussi bien la sécurité physique que la sécurité numérique de vos données, comme nous l'avons vu au chapitre ***1. Protéger votre ordinateur contre les logiciels malveillants et les pirates*** [72] et au chapitre ***2. Assurer la sécurité physique de vos données*** [73]. Il est toutefois préférable de mettre en place plusieurs moyens de défense complémentaires. C'est pourquoi vous devriez également protéger les données elles-mêmes de telle sorte que vos renseignements de nature délicate auront de meilleures chances de rester en sécurité, même si toutes vos autres mesures de sécurité s'avèrent insuffisantes.

Il existe deux approches générales de la sécurisation des données. Vous pouvez *chiffrer* [41] vos données sensibles et les rendre ainsi illisibles pour toute autre personne que vous, où les dissimuler pour que personne d'autre que vous ne soit en mesure de les trouver. Il existe des outils informatiques pour chacune de ces approches, y compris un programme *FLOSS* [74] appelé *TrueCrypt* [75], qui peut à la fois chiffrer et dissimuler l'existence de vos données.

Scénario de départ

Claudia et Pablo travaillent ensemble au sein d'un ONG dont la mission est de défendre les droits de la personne dans un pays sud-américain. Depuis plusieurs mois, ils compilent les dépositions de nombreux témoins de violations de droits humains commises par l'armée dans leur région. Si les renseignements personnels concernant ces courageux témoins étaient rendus publics, ceux-ci seraient en grave danger, ainsi que les membres de l'ONG qui sont actifs dans cette région. Pour l'instant, ces renseignements sont conservés dans une feuille de calcul stockée sur l'ordinateur Windows XP de l'organisme, lequel est connecté à Internet. Par souci de sécurité, Claudia a créé une copie de sauvegarde de ces données sur un CD, qu'elle garde quelque part à l'extérieur du bureau.

Qu'apprendrez-vous dans ce chapitre

- Comment chiffrer les données stockées sur votre ordinateur ;
- Quels sont les risques encourus par le chiffrement de données ;
- Comment protéger des données stockées sur une clé USB, en cas de perte ou de vol ;
- Quelles sont les étapes à suivre pour cacher des données afin de les protéger des intrusions physiques ou virtuelles.

Chiffrer vos données

Pablo : Mais mon ordinateur est déjà protégé par le mot de passe de connexion à Windows ! Ça ne suffit pas ?

Claudia : En fait, les mots de passe de connexion à Windows sont réputés pour être faciles à craquer. De plus, quiconque parvient à manipuler ton ordinateur assez longtemps pour le redémarrer en glissant un LiveCD dans le lecteur de disques sera en mesure de copier l'ensemble de tes données sans se préoccuper du mot de passe. Si l'intrus a l'occasion de partir avec l'ordinateur, ne serait-ce que pour une courte période, tu cours encore plus de risques. Et ce n'est pas uniquement des mots de passe Windows dont tu devrais t'inquiéter. Les mots de passe de Microsoft Word ou d'Adobe Acrobat ne sont pas plus fiables.

Chiffrer [54] vos données, c'est un peu comme les déposer dans un coffre-fort verrouillé et sécurisé. Seules les personnes qui disposent de la combinaison (dans ce cas-ci, une clé de chiffrement ou une phrase secrète) peuvent accéder au contenu. Cette analogie est particulièrement appropriée au programme *TrueCrypt* [76] et autres logiciels semblables. Ces programmes, au lieu de protéger les fichiers individuellement, servent à créer des espaces sécurisés, nommés « volumes chiffrés », où vous pouvez stocker une quantité importante de fichiers. Ces outils, toutefois, ne protègent pas les fichiers qui se trouvent ailleurs sur votre ordinateur ou sur vos dispositifs de stockage portables.

Expérience pratique : se lancer avec le Guide pratique TrueCrypt [77]

Même si d'autres programmes offrent des fonctions de *chiffrement* [78] tout aussi efficaces, le logiciel **TrueCrypt** [78]contient plusieurs fonctions importantes vous permettant de concevoir votre stratégie de sécurité de l'information. Il offre la possibilité de **chiffrer de façon permanente la totalité du disque de votre ordinateur**, y compris tous vos fichiers, tous les fichiers temporaires créés au cours de votre travail, tous les programmes que vous avez installés et tous les fichiers du système d'exploitation Windows. TrueCrypt est compatible aux volumes *chiffrés* [78] sur des dispositifs de stockage amovibles. Il fournit des fonctions de « déni plausible » décrites dans la section ***Dissimuler vos données*** [79] ci-dessous. En outre, TrueCrypt repose sur une licence *FLOSS* [8].

Pablo : Bon, maintenant je suis inquiet. Qu'en est-il des autres utilisateurs sur un même ordinateur ? Est-ce que cela signifie qu'ils peuvent lire les fichiers qui se trouvent dans le répertoire Mes documents ?

Claudia : J'aime ta façon de t'inquiéter ! Si ton mot de passe Windows ne te protège pas des intrus, comment pourrait-il te protéger des autres utilisateurs sur le même ordinateur ? En fait, normalement, tout le monde peut voir ton dossier Mes documents. Les autres utilisateurs n'ont même pas besoin de recourir à des manœuvres sophistiquées pour accéder à tes fichiers. Même si le répertoire est défini comme « privé », il n'est toujours pas sécurisé, à moins que tu n'utilises un mécanisme de chiffrement.

Astuces concernant l'utilisation du chiffrement

Le stockage de données confidentielles comporte des risques pour vous et vos collègues. Le chiffrement des données contribue à réduire ces risques, mais ne les élimine pas complètement. La première mesure à prendre pour protéger des renseignements de nature délicate est de réduire le plus possible le nombre de ces renseignements que vous stockez sur votre ordinateur. À moins d'avoir une très bonne raison de conserver un fichier en particulier (ou une catégorie de données à l'intérieur d'un fichier) vous devriez tout simplement le supprimer. (À ce sujet, veuillez consulter le chapitre ***6. Détruire définitivement des données sensibles*** [80].) La deuxième étape est d'utiliser un bon programme de chiffrement, comme TrueCrypt.

Claudia : Nous ne sommes peut-être pas obligés de conserver des renseignements qui pourraient servir à identifier nos témoins. Qu'en penses-tu ?

Pablo : Je suis d'accord. Nous devrions consigner le strict minimum. De plus, nous devrions trouver un code simple pour protéger les noms et les lieux que nous devons absolument enregistrer.

Pour revenir à l'analogie du coffre-fort, vous devriez gardez à l'esprit un certain nombre de questions lorsque vous utilisez TrueCrypt ou d'autres programmes du même genre. Peu importe le degré de robustesse de votre coffre-fort, cela ne vous servira à rien si vous laissez la porte ouverte. Lorsque votre volume TrueCrypt est « monté » (c.-à-d. quand vous pouvez vous-même accéder aux données qui s'y trouvent), vos données sont vulnérables. C'est pourquoi vous devriez toujours le garder fermé (démonté), sauf quand vous lisez ou modifiez les fichiers qui y sont stockés.

Il y a quelques situations où il est particulièrement important que vous vous rappeliez de démonter vos volumes chiffrés :

- Démontez vos volumes chiffrés lorsque vous vous éloignez de votre ordinateur plus de quelques minutes. Même si vous avez l'habitude de laisser votre ordinateur sous tension pendant la nuit, assurez-vous de ne jamais laisser vos données sensibles à la portée des intrusions physiques ou numériques.
- Démontez vos volumes chiffrés avant d'éteindre votre ordinateur ou de le mettre en veille. Cela concerne aussi bien la fonction « veille » que la fonction « veille prolongée », qui sont habituellement utilisées sur les ordinateurs portables mais qui peuvent également se retrouver sur un ordinateur de bureau.
- Démontez toujours vos volumes chiffrés avant de permettre à qui que ce soit de manipuler votre ordinateur. Lorsque vous transportez votre ordinateur portable avec vous pour traverser un point de contrôle ou une frontière, il est très important que vous démontiez vos volumes chiffrés et éteigniez complètement votre ordinateur.
- Démontez vos volumes chiffrés avant de connecter une clé USB, ou tout autre dispositif de stockage amovible inconnu, à votre ordinateur (y compris les appareils qui appartiennent à vos amis, parents et collègues).
- Si vous conservez un volume chiffré sur une clé USB, rappelez-vous que de retirer la clé ne suffit pas nécessairement à déconnecter immédiatement le volume. Même si vous êtes dans une situation où vous êtes forcé de sécuriser vos fichiers en toute vitesse, vous devez démonter le volume comme d'habitude, arrêter le disque externe ou la clé, et ensuite déconnecter physiquement le dispositif en question. Il peut être utile de répéter cette séquence à quelques reprises pour trouver la façon la plus rapide de procéder.

Conseil : Si vous décidez de garder votre volume TrueCrypt sur une clé USB, il est utile d'y conserver également une copie du programme TrueCrypt. Cela vous permettra d'accéder à vos données à partir d'un autre ordinateur que le vôtre. Évidemment, les consignes de sécurité élémentaires s'appliquent : si vous avez un doute raisonnable que l'ordinateur est infecté par des *logiciels malveillants* [81], vous ne devriez probablement pas y saisir votre mot de passe ni accéder à vos données sensibles.

Dissimuler vos données

L'inconvénient principal de garder un coffre-fort à la maison ou au bureau (sans mentionner d'en transporter un dans sa poche !) est que ces objets ne sont habituellement pas très discrets. Plusieurs personnes craignent que l'utilisation de procédés de *chiffrement* [54] ne les incrimine. C'est une préoccupation raisonnable. Même si les raisons légitimes de chiffrer des données sont beaucoup plus nombreuses que les raisons illégitimes, cette menace n'en est pas moins très réelle. Essentiellement, il existe deux raisons pour lesquelles une personne n'aurait pas intérêt à utiliser des programmes comme TrueCrypt : l'éventuel risque d'auto incrimination; et le risque d'indiquer très précisément où se trouvent vos renseignements les plus sensibles.

Tenir compte du risque d'auto incrimination

Les procédés de chiffrement sont illégaux dans certains pays, ce qui signifie que le téléchargement, l'installation ou l'utilisation de logiciels de chiffrement, en tant que tels, constituent des infractions criminelles. Si la police, l'armée ou les services secrets font partie des groupes à qui vous souhaitez cacher des renseignements, l'infraction à ces lois pourrait être utilisée comme prétexte pour placer vos activités sous enquête ou harceler votre organisme. En fait, à dire vrai, ce type de menace n'a pas toujours de lien avec la légalité des logiciels dont il est question. Dans tous les cas où le simple fait d'être associé de près ou de loin à l'utilisation de programmes de chiffrement peut entraîner des accusations d'activités criminelles ou d'espionnage (et ce, sans égard à ce qui se trouve réellement à l'intérieur des volumes chiffrés), il est très important de réfléchir longuement avant de déterminer si l'utilisation de tels programmes est vraiment appropriée à la situation particulière de votre organisme.

Si vous êtes effectivement dans une situation épineuse, vous avez quelques options :

- Vous pouvez simplement éviter d'utiliser des programmes de sécurisation de données. Cela vous oblige à ne conserver strictement que des données non confidentielles ou à inventer un système de code personnalisé pour protéger vos renseignements sensibles.
- Vous pouvez recourir à la ***stéganographie*** [82], une technique qui consiste à dissimuler vos données confidentielles au lieu de les chiffrer. Il existe des outils qui permettent de faciliter le recours à ce procédé, mais leur utilisation exige beaucoup de préparation et, de toute façon, vous risquez quand même de vous incriminer devant les groupes ou personnes qui apprendraient que vous avez utilisé ces outils.
- Vous pouvez essayer de stocker tous vos renseignements sensibles dans un compte webmail, mais cela nécessite une bonne connexion réseau et une connaissance assez avancée de l'informatique et des services Internet. Par ailleurs, vous ne pouvez recourir à cette méthode que si le chiffrement réseau est moins incriminant que le chiffrement de fichiers. Surtout, il vous faut à tout prix éviter de copier par accident des renseignements sensibles sur votre ordinateur… et de les y oublier.
- Vous pouvez stocker vos données sensibles ailleurs que sur votre ordinateur. Sur une clé USB ou un disque dur portable, par exemple. Par contre, ces dispositifs sont habituellement plus susceptibles d'être perdus ou confisqués que les ordinateurs de bureau. C'est pourquoi il est généralement fortement déconseillé d'y stocker des renseignements sensibles non chiffrés.

Selon les circonstances, vous pouvez employer l'une ou l'autre, ou une combinaison, des tactiques énumérées ci-dessus. Néanmoins, même dans les cas où les risques d'auto incrimination sont importants, le recours à ***TrueCrypt*** [76] peut s'avérer la solution la plus sûre. Il est alors particulièrement important de déguiser le plus efficacement possible vos volumes chiffrés.

Pour faire en sorte que votre volume chiffré soit moins suspect, vous pouvez le renommer pour lui donner l'aspect d'un autre type de fichier. Par exemple, vous pouvez attribuer au fichier l'extension de format *.iso* pour lui donner l'aspect d'une image CD (cela est particulièrement approprié pour des volumes d'environ 700 Mo). D'autres types d'extension seraient plus réalistes pour des volumes plus petits. C'est un peu comme si vous dissimuliez votre coffre-fort derrière un tableau accroché au mur de votre bureau. L'astuce ne résistera peut-être pas à une inspection minutieuse, mais elle offre tout de même un minimum de protection. Vous pouvez également renommer le programme TrueCrypt lui-même si vous l'avez stocké comme n'importe quel autre fichier quelque part sur votre disque dur ou sur une clé USB, au lieu de l'installer comme vous le feriez normalement pour tout autre programme. Le ***Guide pratique TrueCrypt*** [77] vous explique comment faire cela.

Tenir compte du risque d'indiquer l'emplacement de vos données de nature délicate

Dans certaines circonstances, vous serez peut-être moins préoccupé par les conséquences éventuelles d'être « pris » avec des logiciels de chiffrement sur votre ordinateur ou votre clé USB que par le fait que votre volume chiffré risque de révéler précisément où se trouvent les renseignements que vous souhaitez protéger. Bien que, dans un tel cas, personne ne soit en mesure de lire les données, un intrus éventuel saura que lesdites données sont là et que vous avez pris des précautions extraordinaires pour les cacher. Cela vous expose aux diverses méthodes non techniques auxquelles votre intrus pourra recourir pour accéder aux données, comme l'intimidation, le chantage, les interrogatoires ou la torture. C'est dans une situation comme celle-là que la fonction de « possibilité de démenti » de TrueCrypt (abordée en détails ci-dessous) entre en jeu.

La fonction de « possibilité de démenti » de TrueCrypt est un des éléments qui confèrent à ce programme une certaine supériorité sur les autres programmes de chiffrement de données. Cette fonction peut être vue comme une forme singulière de stéganographie, qui vous permet de cacher vos renseignements les plus sensibles parmi des données dont la nature est moins délicate. C'est un peu comme si vous installiez un « double fond » invisible dans votre coffre-fort pas-vraiment-subtil. Si un intrus parvient à vous soutirer la clé, où vous force à lui donner la combinaison du coffre-fort, il y trouvera des « leurres » convaincants (des renseignements moins importants pour vous, mais qui satisferont tout de même sa curiosité), mais pas les renseignements que vous voulez vraiment protéger.

Vous et vous seul savez que votre coffre-fort contient un compartiment secret. Cela vous permet de « démentir » que vous cachez d'autres secrets que ceux que vous avez déjà révélés à l'intrus. Cela est particulièrement pratique dans les situations où vous êtes forcé, pour une raison ou une autre, de révéler votre mot de passe (par ex. parce que vous, vos associés, collègues, parents ou amis êtes la cible de menaces juridiques ou physiques). Le but de cette fonction est de vous donner la possibilité de vous soustraire à une situation potentiellement dangereuse, et ce, même lorsque vous choisissez de continuer à protéger vos données. Par contre, comme nous l'avons vu à la section ***Tenir compte du risque***

d'auto incrimination, cette fonction n'est pas vraiment utile si le simple fait d'être pris avec un coffre-fort dans votre bureau entraîne pour vous ou votre organisme des conséquences graves et/ou inacceptables.

La fonction de « possibilité de démenti » de TrueCrypt vous permet de stocker un « volume caché » à l'intérieur d'un volume chiffré standard. Vous ne pouvez ouvrir ce volume qu'avec un mot de passe différent de celui utilisé pour ouvrir le volume standard. Même si un intrus spécialiste parvient à accéder au volume standard, il lui sera tout simplement impossible de prouver l'existence d'un volume caché. Bien sûr, cette personne pourrait très bien savoir que le programme TrueCrypt offre la possibilité de dissimuler des données de cette façon, alors il n'y a aucune garantie que la menace disparaîtra lorsque vous révélerez le mot de passe de « diversion ». Par contre, plusieurs personnes utilisent TrueCrypt sans pour autant se servir de la fonction de « volume caché » et, en règle générale, il est pratiquement impossible de déterminer par analyse informatique si un volume chiffré comporte un tel « double fond ». Cela dit, il vous revient entièrement de vous assurer que l'existence de votre volume caché ne soit pas révélée par des moyens non techniques : ne laissez jamais le volume caché inutilement ouvert et ne créez pas de raccourcis vers les fichiers qu'il contient, par exemple. Les liens indiqués à la section ***Lecture complémentaire*** [83], ci-dessous, offrent des conseils supplémentaires à ce sujet.

Claudia : Bon, alors nous n'avons qu'à balancer des trucs sans importance dans le volume standard et placer tous les témoignages importants dans le volume caché. As-tu des vieux PDF ou quelque chose du genre qu'on pourrait utiliser comme diversion ?

Pablo : En fait, je pensais justement à ça. Je me disais que le principe de ce stratagème est de révéler le mot de passe du volume standard uniquement si nous n'avons aucun autre choix, pas vrai ? Mais pour que cela soit convaincant, nous devons nous assurer que les fichiers que nous livrons comme leurres aient l'air d'être importants, tu ne crois pas ? Sinon, pourquoi prendrions-nous la peine de le chiffrer ? Peut-être devrions-nous utiliser comme leurres des documents ayant trait à nos finances, par exemple, ou encore une liste de faux mots de passe.

Lecture complémentaire

- Pour plus de renseignements sur la sécurisation des fichiers, veuillez consulter les chapitres Cryptology [84] et Steganography [85], ainsi que le Case Study 3 [86], du manuel Digital Security and Privacy for Human Rights Defenders [49].
- La TrueCrypt Documentation [87] discute en détail de nombreux aspects du chiffrement d'informations, tandis que le TrueCrypt FAQ [88] offre des réponses aux questions les plus courantes à propos de TrueCrypt.

5. Récupérer des données perdues

Chaque nouvelle méthode de stockage ou de transfert de données informatisées apporte son lot de moyens inédits par lesquels ces données peuvent être perdues, volées ou détruites. Le fruit de plusieurs années de travail peut disparaître en un seul instant par suite d'un cambriolage, d'un moment d'inattention, d'une confiscation de matériel ou tout simplement parce que la technologie est trop fragile. Les professionnels de l'assistance informatique emploient une formule éloquente : « Il ne s'agit pas de savoir *si* vous perdrez vos données, mais bien *quand* vous les perdrez ». Alors *quand* cela se produira chez-vous, il est essentiel que vous ayez déjà une copie de sauvegarde fraîchement mise à jour, ainsi qu'une méthode de récupération éprouvée. Malheureusement, c'est souvent au lendemain d'une perte irrémédiable qu'on se rend compte de l'importance de mettre en place un système de sauvegarde efficace.

Bien qu'il s'agisse d'un élément fondamental de la sécurité informatique, il n'est pas simple de formuler une bonne politique de sauvegarde des données. Plusieurs facteurs entrent en ligne de compte et contribuent à faire de cette question un enjeu organisationnel particulièrement épineux. On n'a qu'à penser à la nécessité de sauvegarder les données originales et les copies de sauvegarde en plusieurs emplacements physiques différents, à l'importance de préserver la confidentialité de ces copies de sauvegarde et au défi que pose la coordination entre plusieurs personnes qui partagent des données et utilisent chacune plusieurs dispositifs de stockage, pour se rendre compte à quel point cet enjeu est complexe. En plus d'aborder certaines stratégies de sauvegarde et de récupération de fichiers, ce chapitre présente deux programmes particulièrement utiles : *Cobian Backup* [89] et *Undelete Plus* [90].

Scénario de départ

Elena est une militante environnementaliste. Elle habite un pays russophone, où elle travaille depuis un certain temps à la conception d'un site Internet dont l'objectif serait de diffuser des présentations artistiques (images, vidéos, cartes et témoignages divers) pour illustrer l'étendue du problème que pose la déforestation illégale dans sa région. Depuis plusieurs années, elle a réussi à accumuler une somme importante de documents, de fichiers média et de données géographiques concernant l'exploitation forestière. La plupart de ces données sont stockées sur un ordinateur Windows au bureau de l'ONG où elle est employée. En travaillant à la mise sur pied de son site Web, elle a réalisé le caractère délicat de son projet et a commencé à se préoccuper de la sauvegarde de ses données. Elle craint entre autre que son ordinateur subisse des dommages importants avant même que le site ne soit en ligne, car d'autres membres de son organisme utilisent parfois son ordinateur. C'est pourquoi elle voudrait aussi apprendre comment récupérer des données supprimées par accident. Elle demande à son neveu, Nikolai, de l'aider à mettre en œuvre une stratégie de sauvegarde de données.

Qu’apprendrez-vous dans ce chapitre

- Comment organiser vos données et en créer des copies de sauvegarde ;
- Où vous devriez conserver vos copies de sauvegarde ;
- Comment gérer vos copies de sauvegarde de façon sécurisée ;
- Comment récupérer des fichiers qui ont été supprimés accidentellement.

Identifier et organiser vos données

Même si, de toute évidence, il est extrêmement important de prendre des mesures appropriées pour se prémunir contre d’éventuels désastres (en assurant la sécurité physique des données, en installant de bons programmes antivirus et un bon pare-feu [91], et en se dotant de mots de passe sûrs, etc.), aucune mesure ne peut suffire à vous protéger contre toutes les menaces possibles. À vrai dire, trop d’événements imprévisibles peuvent survenir inopinément, comme une infection virale, une attaque de *pirates informatiques* [18], un court-circuit, une saute de tension électrique, un dégât d’eau, un cambriolage, une confiscation de matériel, une démagnétisation, un plantage général du système d’exploitation ou une panne de matériel, pour n’en nommer que quelques-uns. En somme, se préparer au désastre est aussi important que de s’en protéger.

Elena : Je sais qu’il est important de créer des copies de sauvegarde, Nikolai, mais ne devrais-je pas demander à quelqu’un d’autre de le faire pour moi ? Est-ce que j’ai vraiment le temps, les ressources ou même la capacité de le faire moi-même ?

Nikolai : Tu y arriveras, ne t’en fais pas. La conception d’un bon plan de sauvegarde exige un peu de concentration, mais ce n’est pas long, ni difficile, et ça ne coûte rien. Comparé à la perte totale de tes données, c’est un inconvénient plutôt mineur, non ? De toute façon, la sauvegarde de tes données est définitivement quelque chose que tu devrais gérer toi-même. À moins que les personnes qui t’aident habituellement sur les questions informatiques soient extrêmement fiables et bien informées sur les emplacements où tu conserves tes données, tu as tout avantage à mettre toi-même en place une stratégie de sauvegarde qui te convienne.

La première étape est de déterminer clairement où sont situées vos données personnelles et professionnelles. Vos courriels, par exemple, sont peut-être stockés sur le serveur de votre fournisseur de service de courriel, ils sont peut-être stockés sur votre ordinateur, ou encore répartis entre ces deux emplacements. Par ailleurs, vous avez peut-être plusieurs comptes de courriel. Vous devez aussi tenir compte des documents importants qui sont stockés sur les ordinateurs que vous utilisez régulièrement, à domicile et au travail. Pensez aux carnets d’adresses, aux historiques de messagerie instantanée et à tous vos paramètres personnalisés. Certains renseignements importants sont peut-être stockés sur des dispositifs de stockage amovibles, comme des clés USB, des disques durs externes, des CD ou DVD, ou même de vieilles disquettes. Votre téléphone portable comporte habituellement une liste de contacts et vous y avez peut-être conservé des messages texte importants. Si vous avez un site Internet, vous y avez peut-être déposé une grande quantité d’articles composés au fil des ans. Finalement, n’oubliez pas de tenir compte de toutes vos archives non informatisées, comme vos cahiers de notes, journaux personnels, correspondances, etc.

Ensuite, vous devez déterminez lesquels de ces fichiers sont vos « originaux » et lesquels sont des copies, ou duplicata. La copie originale est habituellement la version la plus récente d’un fichier ou d’un groupe de fichiers et correspond à la copie que vous modifieriez si vous deviez en actualiser le contenu. Évidemment, cette distinction n’a aucune incidence si vous ne disposez que d’une seule copie d’un fichier donné, mais elle est très importante pour certains types de données. Un scénario catastrophe assez courant se produit lorsque des copies de sauvegardes sont créées à partir des duplicata non actualisés d’un document important, alors que la copie originale est perdue ou détruite. Imaginez, par exemple, que vous êtes en voyage depuis plus d’une semaine et prenez le temps d’actualiser régulièrement la copie d’une feuille de calcul que vous conservez sur votre clé USB. Dans ce cas-ci, vous devriez considérer cette copie comme l’originale, puisque les sauvegardes automatiques périodiques de l’ancienne version qui se trouvent sur votre ordinateur de bureau ne tiennent pas compte des changements que vous avez apportés à la copie que vous transportez avec vous sur votre clé USB.

Essayez de dresser une liste complète des emplacements physiques de toutes les copies originales et de tous les duplicata des données que vous avez recensées. Cela vous aidera à bien définir vos besoins particuliers et à définir une politique de sauvegarde appropriée. Le tableau ci-dessous offre un exemple simple. Évidemment, votre liste à vous risque d’être beaucoup plus longue et de contenir plusieurs dispositifs de stockage, avec plus d’un seul type de données, ainsi que des types de données qui se retrouvent sur plus d’un dispositif de stockage.

Type de données	Original/Duplicata	Dispositif de stockage	Emplacement
Documents informatisés	Originaux	Disque dur principal de l’ordi.	Bureau
Quelques documents informatisés	Duplicata	Clé USB	Sur moi

importants	Duplicata	Clé USB	Sur moi
Bases de données des programmes (photos, carnets d'adresses, calendriers, etc.)	Originaux	Disque dur principal de l'ordi.	Bureau
Quelques documents informatisés	Duplicata	CDs	Maison
Courriels et contacts de courriel	Originaux	Compte Gmail	Internet
Contacts de messagerie texte et téléphoniques	Originaux	Téléphone portable	Sur moi
Documents imprimés (contrats, factures, etc.)	Originaux	Tiroir du bureau	Bureau

Dans le tableau ci-dessus, vous pouvez constater que :

- Les seuls documents qui survivraient à un éventuel plantage complet de votre ordinateur de travail sont les documents stockés sur votre clé USB ou les CD que vous conservez à la maison.
- Vous n'avez aucune copie autonome (hors-ligne) de vos courriels ou de vos carnets d'adresses, ce qui signifie que si vous oubliez votre mot de passe (ou si une personne mal intentionnée parvient à le changer à votre insu), vous perdrez l'accès à ces données.
- Vous n'avez aucune copie de sauvegarde des renseignements qui se trouvent sur votre téléphone portable.
- Vous n'avez aucune copie de sauvegarde, informatisée ou physique, de vos documents imprimés, comme vos contrats ou factures.

Définir une stratégie de sauvegarde

Pour créer des copies de sauvegarde de tous les types de fichiers listés ci-dessus, vous aurez besoin d'une combinaison de logiciels et de procédés particuliers. Essentiellement, vous devez vous assurer que chaque type de données est stocké dans au moins deux emplacements différents.

Les documents informatisés - Créez une copie de sauvegarde complète de tous les documents qui se trouvent sur votre ordinateur à l'aide d'un programme comme *Cobian Backup* [89], abordé en détails ci-dessous. Stockez cette copie de sauvegarde sur un support portable que vous pourrez conserver à la maison ou dans un autre lieu sûr. Les disques durs externes, CD/DVD ou clés USB sont des choix possibles. Certaines personnes utilisent des CD ou DVD car le risque d'écraser et de perdre une sauvegarde est moins grand. Le prix des CD vierges est assez abordable si bien que vous pouvez en utiliser un nouveau pour chaque copie de sauvegarde. Comme ce type de données contient habituellement les renseignements les plus sensibles, il est particulièrement important que vous protégiez vos documents informatisés en recourant à un procédé de chiffrement. Vous pouvez apprendre comment chiffrer vos données dans le chapitre ***4. Protéger les données sensibles stockées sur votre ordinateur*** [42] et en consultant le ***Guide pratique TrueCrypt*** [92].

Les bases de données des programmes - Après avoir déterminé l'emplacement des bases de données de vos programmes, vous pouvez créer des copies de sauvegarde de la même manière que pour vos documents numériques.

Les courriels - Au lieu de n'accéder à vos courriels que par l'entremise d'un navigateur Web, vous devriez installer sur votre ordinateur un client de messagerie comme *Thunderbird* [93] et le configurer pour fonctionner avec votre compte de courrier électronique. Le ***guide pratique Thunderbird*** [94] explique en détail comment procéder. De même, la plupart des services webmail fournissent des directives concernant l'utilisation d'un client de messagerie et sur la marche à suivre pour y importer votre carnet d'adresses. Vous trouverez plus d'information à ce sujet dans la section suivante, à la fin du présent chapitre. Si vous décidez de déplacer vos anciens messages e-mail vers votre ordinateur afin qu'ils ne soient pas stockés sur le serveur (par ex. pour des raisons de sécurité), assurez-vous qu'ils soient inclus dans la sauvegarde de documents électroniques, comme décrit ci-dessus.

Le contenu de votre téléphone portable - Pour créer des copies de sauvegarde des numéros de téléphone et des messages texte stockés sur votre téléphone portable, vous pouvez connecter l'appareil directement à votre ordinateur et utiliser le logiciel approprié, que l'on retrouve généralement sur le site Internet du fabricant. Vous devrez peut-être acheter un câble USB spécial pour effectuer cette opération.

Les documents imprimés - Lorsque cela est possible, vous devriez numériser tous vos documents importants et les sauvegarder de la même façon que vos documents informatisés.

En fin de compte, vous devriez avoir réarrangé vos dispositifs de stockage, vos types de données et vos copies de sauvegarde de telle manière que vos données seront mieux préparées au désastre éventuel :

Type de données	**Original/Duplicata**	**Dispositif de stockage**	**Emplacement**
Documents informatisés	Originaux	Disque dur principal de l'ordi.	Bureau

Documents informatisés	Duplicata	CD	Maison
Quelques documents informatisés importants	Duplicata	Clé USB	Sur moi

Type de données	Original/Duplicata	Dispositif de stockage	Emplacement
Bases de données des programmes	Originaux	Disque dur principal de l'ordi.	Bureau
Bases de données des programmes	Duplicata	CD	Maison

Type de données	Original/Duplicata	Dispositif de stockage	Emplacement
Courriels et contacts de courriel	Duplicata	Compte Gmail	Internet
Courriels et contacts de courriel	Original	Thunderbird sur l'ordi. de travail	Bureau

Type de données	Original/Duplicata	Dispositif de stockage	Emplacement
Messages texte et contacts de téléphone portable	Originaux	Tél. portable	Sur moi
Messages texte et contacts de téléphone portable	Duplicata	Disque dur principal de l'ordi.	Bureau
Messages texte et contacts de téléphone portable	Duplicata	Carte SIM de sauvegarde	Maison

Type de données	Original/Duplicata	Dispositif de stockage	Emplacement
Documents imprimés	Originaux	Tiroir du bureau	Bureau
Documents numérisés	Duplicata	CD	Maison

Elena : Je connais des gens qui conservent tous leurs documents importants sur Gmail en les attachant à des brouillons de messages ou en s'envoyant des courriels à eux-mêmes. Est-ce que cela compterait comme un « emplacement physique secondaire » pour mes fichiers ?

Nikolai : Cela pourrait t'aider à récupérer un ou deux documents perdus mais, honnêtement, c'est un peu malcommode. D'après toi, combien de documents serais-tu prête à sauvegarder de cette façon chaque semaine ? De plus, tu dois te demander dans quelle mesure ces pièces jointes sont vraiment sécurisées, d'autant plus si tu crains, tant soit peu, que tes courriels soient surveillés. À moins que tu ne te connectes à Gmail de façon sécurisée, cette procédure équivaut à servir tes renseignements les plus précieux sur un plateau d'argent à quiconque s'y intéresse. Il serait relativement sûr de se servir d'une connexion HTTPS à Gmail pour sauvegarder des petits volumes TrueCrypt ou des bases de données KeePass, parce que ces fichiers sont chiffrés, mais je ne conseillerais vraiment pas ce procédé comme stratégie générale de sauvegarde.

Créer une copie de sauvegarde numérique

De tous les types de fichiers mentionnés ci-dessus, ce sont des « documents informatisés », c.-à-d. les documents numériques, que la plupart des gens ont tendance à se préoccuper lorsqu'ils mettent en place une politique de sauvegarde de leurs données. Ce terme est plutôt ambigu, mais il désigne généralement les fichiers dont vous assurez vous-même la gestion, et qui s'ouvrent manuellement en double-cliquant sur le nom ou en passant par le menu Fichier d'une application appropriée. Plus précisément, il est question de fichiers texte, de documents de traitement de texte, de présentations, de PDF et de feuilles de calcul, pour ne citer que quelques exemples. Contrairement aux messages de courrier électronique, par exemple, les documents informatisés ne sont habituellement pas synchronisés avec des copies distantes sur Internet.

Lorsque vous sauvegardez vos documents informatisés, vous devriez toujours vous rappeler de sauvegarder également les bases de données de vos programmes. Si vous utilisez un calendrier électronique ou un carnet d'adresse électronique, par exemple, vous devrez trouver le répertoire où ces programmes stockent leurs données. Avec un peu de

chance, ces bases de données se trouveront au même emplacement que vos documents informatisés, puisque ceux-ci sont habituellement stockés dans le répertoire `Mes documents` d'un système Windows. Si ce n'est pas le cas, vous devriez ajouter le répertoire approprié à votre copie de sauvegarde.

Les messages de courriel stockés à l'aide d'un client de messagerie comme *Mozilla Thunderbird* [93] présentent un exemple particulier de base de données. Si vous utilisez un programme de messagerie (et tout particulièrement si vous ne souhaitez pas ou êtes incapable de stocker une copie de vos messages sur le serveur de courriels), vous devriez vous assurer d'inclure la base de données de courriel dans votre sauvegarde régulière. Il est possible que vous considériez vos fichiers graphiques et audio comme des documents informatisés ou des items associés à une base de données de programme, selon l'utilisation que vous en faites. Certaines applications, comme Windows Media Player et iTunes, par exemple, fonctionnent comme des bases de données. Si vous utilisez des programmes comme ceux-là, vous devrez peut-être effectuer une recherche sur votre disque dur pour découvrir où sont stockés les fichiers média dont ils assurent la gestion.

Les dispositifs de stockage

Avant de faire une copie de sauvegarde de vos documents informatisés, vous devez d'abord choisir un ou des dispositifs de stockage appropriés.

Les disques ou clés de mémoire USB - Les disques ou clés de mémoire USB peuvent ne coûter presque rien et offrent une grande capacité de mémoire. Il est facile d'en supprimer le contenu ou de réécrire plusieurs fois dessus. Les disques ou clés USB ont une durée de vie limitée qui dépend en grande partie de la manière et de la fréquence d'utilisation. Elle est estimée à environ dix ans.

Les disques compacts (CD) Les CD peuvent stocker jusqu'à 700 Mo de données. Vous aurez besoin d'un *graveur de CD* [95] et de disques vierges pour créer une copie de sauvegarde sur CD. Si vous souhaitez effacer le contenu d'un CD et actualiser les fichiers qui y sont stockés, vous aurez besoin d'un graveur CD-RW et de disques réinscriptibles. Tous les systèmes d'exploitations courants, dont Windows XP, comportent maintenant des logiciels intégrés qui permettent de graver des CD et CD-RW. Gardez à l'esprit que les données gravées sur ces disques risquent de se détériorer après une période de dix à quinze ans. Si vous devez conserver une copie de sauvegarde pour une longue période, vous devriez graver un nouveau CD périodiquement, acheter des disques spéciaux de « longue durée » ou utiliser une autre méthode de sauvegarde.

Les disques numériques polyvalents (DVD) - Les DVD peuvent stocker jusqu'à 4,7 Go de données. Ils fonctionnent essentiellement de la même façon que les CD, mais requièrent du matériel un peu plus cher. Vous aurez besoin d'un *graveur DVD ou DVD-RW* [95], et de disques appropriés. Comme pour les CD, les DVD normaux se dégradent avec le temps.

Les serveurs distants - Un serveur de sauvegarde bien entretenu peut offrir une capacité de mémoire quasiment illimitée, mais c'est la vitesse et la stabilité de votre connexion Internet qui déterminera si cette option est appropriée à votre situation. N'oubliez pas que la tenue d'un serveur de sauvegarde à l'intérieur même de votre bureau trahit la règle voulant qu'il est nécessaire de conserver une copie de sauvegarde de vos données dans au moins deux emplacements physiques séparés. Il existe par ailleurs des services de stockage gratuits sur Internet, mais vous devriez soigneusement considérer les risques liés au fait de mettre vos informations en ligne et vous devriez toujours chiffrer vos données avant de les téléverser sur des serveurs gérés par des individus ou organismes que vous ne connaissez pas ou en qui vous ne faites pas entièrement confiance. Veuillez consulter la section ***Lecture complémentaire*** [96], à la fin de ce chapitre, pour plus de conseils à ce sujet.

Les logiciels de sauvegarde

Cobian Backup est un logiciel facile à utiliser qui peut être programmé pour exécuter des sauvegardes automatiquement, à des intervalles prédéterminés, et actualiser uniquement les fichiers qui ont été modifiés depuis la dernière sauvegarde. Le programme peut également comprimer les copies de sauvegarde pour économiser l'espace.

Expérience pratique : se lancer avec le *Guide pratique Cobian Backup* [97]

Comme toujours, il est conseillé de chiffrer vos fichiers de sauvegarde à l'aide d'un programme comme *TrueCrypt* [75]. Vous trouverez plus de renseignements sur le chiffrement de données dans le chapitre ***4. Protéger les données sensibles stockées sur votre ordinateur*** [42].

Expérience pratique : se lancer avec le *Guide pratique TrueCrypt* [92]

Lorsque vous utilisez ces logiciels de sauvegarde, il y a un certain nombre de manœuvres que vous pouvez effectuer pour faire en sorte que votre système de sauvegarde fonctionne sans heurts :

- Organisez adéquatement vos fichiers sur votre ordinateur. Autant que possible, essayez de transférer tous les document informatisés dont vous souhaitez faire une copie de sauvegarde dans un seul emplacement, comme par exemple dans le répertoire `Mes documents`.
- Si vous utilisez des logiciels qui utilisent une base de données, vous devriez tout d'abord déterminer l'emplacement des bases de données. Si l'emplacement initial n'est pas pratique pour vous, voyez si le programme vous permet d'en choisir un nouveau pour y déplacer la base de données. Si cela s'avère possible, vous pouvez déplacer la base de données du programme vers le répertoire où vous aviez déjà stocké vos documents informatisés.
- Déterminez un intervalle régulier pour la création des sauvegardes automatiques.
- Tâchez d'établir une procédure standard pour tous les membres du personnel de votre bureau qui n'adhèrent pas déjà à une politique de sauvegarde commune. Expliquez bien à vos collègues l'importance d'une telle politique.
- N'oubliez pas de tester le processus de récupération des données depuis vos copies de sauvegarde. En fin de compte, ce n'est pas tant la procédure de sauvegarde qui vous importe, sinon la procédure de récupération !

Elena : OK, j'ai donc créé une copie de sauvegarde chiffrée quand j'étais au bureau, que j'ai ensuite gravée sur un CD. Cobian est maintenant programmé pour actualiser ma sauvegarde dans deux jours. Mon poste de travail au bureau comporte un tiroir que je peux fermer à clé, où j'ai l'intention de garder mes CD de sauvegarde pour éviter de les perdre ou de les endommager.

Nikolai : Mais que feras-tu si les locaux de l'ONG sont détruits par un incendie ? Les ordinateurs, les bureaux, les CD de sauvegarde et tout. Ou encore, imagine que ton forum serve de tremplin pour une méga manifestation environnementaliste et que le gouvernement décide alors d'intervenir, de tout fermer et de saisir le matériel ? Je doute fort que la petite serrure de ton tiroir puisse résister à la police si elle décide de confisquer tes CD. Pourquoi ne pas conserver ces copies de sauvegarde à la maison ? Ou encore demander à un ami de les garder pour toi ?

Récupérer des fichiers supprimés accidentellement

Lorsqu'on supprime un fichier dans Windows, celui-ci disparaît (c.-à-d. qu'on ne le voit plus), mais son contenu est toujours sur l'ordinateur. Même après avoir vidé la **Corbeille**, les données du fichier que vous avez supprimé peuvent habituellement être retracés sur le disque dur. À ce sujet, veuillez consulter le chapitre ***6. Détruire définitivement des données sensibles*** [98]. Dans certains cas, lorsque vous supprimez accidentellement un fichier ou un dossier important, cette faille de sécurité peut jouer à votre avantage. Il existe plusieurs programmes qui peuvent vous aider à récupérer ces données fraîchement supprimées, y compris un logiciel ***Recuva*** [99].

Expérience pratique : se lancer avec le *Guide pratique Recuva* [99]

Ces programmes ne fonctionnent pas toujours, parce que Windows peut déjà avoir écrit de nouvelles données par-dessus celles que vous avez supprimées et souhaitez maintenant récupérer. Pour cette raison, il est important que vous effectuiez le moins de tâches possible sur votre ordinateur entre le moment où les données ont été supprimées accidentellement et le moment où vous essayez de les récupérer à l'aide d'un programme comme Recuva. Plus vous utilisez votre ordinateur avant de tenter de récupérer les données, plus il est improbable que vous réussissiez. Cela signifie par ailleurs que vous devriez utiliser la version portable de *Recuva* au lieu de l'installer après avoir supprimé un fichier important. L'installation du logiciel nécessite l'écriture de nouvelles informations dans le système de fichiers, ce qui pourrait fortuitement écraser les données critiques que vous êtes en train d'essayer de récupérer.

Même s'il peut sembler ardu de mettre en place toutes les procédures et d'apprendre à utiliser tous les programmes abordés dans le présent chapitre, il est plutôt facile de maintenir une bonne stratégie de sauvegarde une fois que le système est bien instauré. C'est l'installation initiale qui demande un certain effort. Puisque le processus de sauvegarde est possiblement l'aspect le plus important d'une stratégie globale de sécurité informatique, vous pouvez être sûr que ces efforts n'auront pas été déployés en vain.

Lecture complémentaire

- Vous pourrez trouver plus de renseignements à propos des sauvegardes et de la récupération de données perdues en consultant le chapitre Information Backup, Destruction and Recovery [100] du manuel Digital Security and Privacy for Human Rights Defenders [27].
- Notez que la sauvegarde en ligne représente de nouveaux risques. Tâchez au moins de **ne pas oublier de chiffrer vous-même vos données sensibles séparément** avant de les transférer sur le serveur. En supposant que vous suivez l'étape ci-dessus, il existe des services gratuits de sauvegarde en ligne permettant de sauvegarder facilement vos données. Certaines options incluent : Wuala [101], SpiderOak [102], Google Drive [103], tahoe-lafs [104].
- Vous trouverez sur Wikipédia [105] un excellent article concernant la récupération de données.

6. Détruire définitivement des données sensibles

Dans les chapitres précédents, nous avons présenté un certain nombre de programmes et de pratiques exemplaires qui vous aideront à protéger vos données de nature délicate. Mais qu'arrive-t-il lorsque vous décidez de vous débarrasser de données dont vous n'avez plus besoin ? Si vous décidez, par exemple, que la copie de sauvegarde chiffrée d'un fichier donné constitue une garantie suffisante et que vous voulez supprimer l'original, quel est le meilleur moyen de procéder ? Malheureusement, la réponse est plus compliquée que l'on croit. Lorsqu'on supprime un fichier, même après avoir vider la `Corbeille`, le contenu de ce fichier reste intact quelque part sur le disque dur et peut être récupéré, avec les outils appropriés et un peu de chance, par n'importe qui.

Pour vous assurer que vos données supprimées n'aboutissent pas dans les mains de personnes mal intentionnées, vous devrez avoir recours à un logiciel spécial pour effacer vos données de façon sécurisée et définitive. *Eraser* [106], abordé plus en détails ci-dessous, est l'un de ces programmes. On peut comparer Eraser à une déchiqueteuse : on l'emploie pour détruire complètement un document au lieu de le jeter à la corbeille en espérant que personne ne le trouve. Évidemment, la suppression de fichiers n'est qu'un exemple de situations où vous devriez détruire des renseignements de nature délicate. En réfléchissant bien aux types de renseignements qu'une personne (à plus forte raison une personne puissante et mue par des intérêts politiques) pourraient apprendre à votre sujet ou à propos de votre organisme en lisant certains fichiers que vous croyiez avoir supprimés, d'autres exemples de situations vous viendront sûrement à l'esprit, comme : la destruction de copies de sauvegarde, le *nettoyage (wiping)* [107] de vieux disques durs, la suppression de vieux comptes d'utilisateur, la suppression de votre historique de navigation, etc. *CCleaner* [108], l'autre programme abordé dans ce chapitre, vous aidera à faire face au défi que pose la suppression des innombrables fichiers temporaires accumulés sur votre ordinateur par le système d'exploitation et les programmes que vous utilisez régulièrement.

Scénario de départ

Elena est une militante environnementaliste, résidente d'un pays russophone, qui gère un site Internet de plus en plus populaire où elle dénonce l'étendue du problème que pose la déforestation illégale dans sa région. Elle a créé des copies de sauvegarde des données utilisées pour monter le site, et elle en garde au moins une à son domicile, une au bureau et une troisième sur son nouvel ordinateur portable. Récemment, elle a également commencé à conserver une copie du journal de connexion au serveur et de la base de données contenant les contributions au forum de discussion de son site. Bientôt, Elena doit se rendre à l'étranger pour assister à une grande conférence réunissant des environnementalistes de plusieurs pays, dont plusieurs ont déjà rapporté s'être fait confisquer leur ordinateur portable pendant plusieurs heures à la frontière. Afin de protéger ses données sensibles et préserver la sécurité de certains participants à son forum de discussion, elle a transféré ses copies de sauvegarde dans un volume TrueCrypt chiffré et supprimé la copie qui se trouvait sur son ordinateur portable. Lorsqu'elle a demandé conseil à son neveu Nikolai, celui-ci lui a bien expliqué que si elle craint de se faire confisquer son ordinateur par les agents frontaliers, la simple suppression de ses vieilles copies de sauvegarde ne suffit pas.

Qu'apprendrez-vous dans ce chapitre

- Comment supprimer définitivement les données sensibles qui se trouvent sur votre ordinateur ;
- Comment supprimer définitivement les données sensibles qui se trouvent sur des dispositifs de stockage amovibles comme des CD ou des clés USB ;
- Comment empêcher que des intrus soient en mesure de récupérer les documents que vous avez déjà affichés sur votre ordinateur ;
- Comment entretenir votre ordinateur de telle sorte que les fichiers supprimés ne puissent jamais être récupérés.

Supprimer des données

D'un point de vue strictement technique, il n'existe sur votre ordinateur aucune fonction de suppression. Bien sûr, vous pouvez toujours transférer un fichier vers la `Corbeille` puis vider cette dernière. Mais, en réalité, cette opération ne sert qu'à modifier (ou « vider ») l'icône de `Corbeille`, retirer le nom de fichier d'un index caché répertoriant toutes les actions effectuées sur votre ordinateur, et indiquer à Windows que le système peut maintenant utiliser l'espace qu'occupait ce fichier pour écrire de nouvelles données. Mais tant et aussi longtemps que le système n'aura pas écrit par-dessus, cet espace sera toujours occupé par le contenu du fichier supprimé. C'est un peu comme un tiroir de classeur dont on aurait retiré l'étiquette, mais qui contiendrait toujours les dossiers qui s'y trouvaient. C'est pourquoi il est possible, avec les bons programmes et en agissant assez rapidement, de récupérer des données que vous avez supprimées accidentellement. Cette opération est expliquée en détails au chapitre ***5. Récupérer des données perdues*** [45].

Vous devriez également vous rappeler que des fichiers sont créés et supprimées à votre insu, de façon non sécurisée, chaque fois que vous utilisez votre ordinateur. Imaginez, par exemple, que vous deviez rédiger un volumineux rapport. Cela vous prendra peut-être une semaine complète à raison de plusieurs heures par jour, et chaque fois que le document sera sauvegardé automatiquement, Windows en créera une nouvelle copie et la stockera quelque part sur votre ordinateur. Après quelques jours, vous aurez peut-être sauvegardé sans le savoir de nombreuses versions du même document à divers stades de sa création.

Windows supprime habituellement les anciennes versions d'un fichier, bien entendu, mais il ne cherche pas l'emplacement exact de l'original pour réécrire par-dessus de façon sécurisée chaque fois qu'une nouvelle copie est créée. Au lieu de cela, le système place la plus récente version dans une nouvelle section du classeur mentionné ci-dessus, transfère l'étiquette de l'ancienne section à la nouvelle et laisse l'ancienne version du document là où il est jusqu'à ce qu'un autre programme réquisitionne cette espace. Manifestement, si vous avez de bonnes raisons de vouloir détruire toute trace d'un document qui se trouve actuellement dans votre classeur, il ne sera pas suffisant d'en retirer seulement la dernière copie, et encore moins de simplement en jeter l'étiquette.

D'autre part, n'oubliez pas que les disques durs de vos ordinateurs ne sont pas les seuls dispositifs où il est possible de stocker des données numériques. Les CD, les DVD, les clés USB, les disquettes, les cartes de mémoire flash et les disques durs externes présentent exactement les mêmes failles. Vous ne devriez donc pas vous en remettre à la simple opération de suppression ou de réécriture si vous voulez effacer définitivement certaines données sensibles de l'un ou l'autre de ces dispositifs et périphériques.

Le nettoyage des données à l'aide d'un programme de suppression sécurisée

Lorsque vous utilisez un programme de suppression sécurisée comme ceux que nous recommandons dans le présent chapitre, il est plus juste de dire que vous remplacez, ou « écrasez », les données sensibles, que de simplement parler de suppression. Revenons aux documents conservés dans le classeur mal étiqueté dont il était question ci-dessus, et admettons qu'ils sont rédigés au crayon de plomb. Le programme de suppression sécurisée ne se contentera pas d'effacer ce qui y est écrit, il gribouillera en plus par-dessus chaque mot. Et comme des phrases écrites au crayon de plomb, les données informatisées peuvent tout de mêmes êtres lues (quoique difficilement) après avoir été effacées. Il est même parfois possible de les lire après qu'on ait gribouillé par-dessus. C'est pourquoi les programmes recommandés ici écrasent plusieurs fois les fichiers avec des données aléatoires. Ce processus est appelé « *nettoyage* [107] » (ou *wiping* en anglais). En écrasant plusieurs fois les données à éliminer (le nombre de « passes » est important), le programme réduit exponentiellement les probabilités qu'une personne mal intentionnée parvienne à récupérer ces données. Les spécialistes s'accordent généralement pour dire que trois passes ou plus sont nécessaires (certains recommandent jusqu'à sept passes), mais les programmes de « nettoyage » le font automatiquement.

Le nettoyage des fichiers

Il existe deux moyens répandus pour nettoyer vos disques durs et autres dispositifs de stockage dans le but de supprimer définitivement les données sensibles que vous souhaitez éliminer. Vous pouvez nettoyer un fichier unique ou nettoyer tout l'espace « non alloué » du disque dur. Avant de choisir l'une ou l'autre de ces méthodes, il est utile de se rappeler notre exemple du long rapport dont plusieurs versions se retrouvent un peu partout sur votre disque dur, et ce, même si un seul fichier est visible. Si vous écrasez le fichier lui-même, vous vous assurez que la version actuelle est définitivement supprimée, mais vous laissez les autres copies intactes. En fait, il n'y a aucun moyen de cibler précisément ces copies parce qu'il n'est pas possible de les localiser sans l'aide de logiciels spéciaux. En nettoyant tout l'espace libre de votre disque dur, cependant, vous vous assurez que toutes les données préalablement supprimées seront définitivement détruites. Pour revenir à la métaphore du classeur, cette procédure est comparable à une recherche systématique de tous les documents stockés dans le classeur dont l'étiquette a été retirée, pour en effacer le contenu et écrire plusieurs fois par-dessus l'ancien contenu.

Eraser [106] est un programme de suppression sécurisée, gratuit et de code source libre, extrêmement facile à utiliser. Vous pouvez nettoyer des fichiers de trois façons différentes avec Eraser : en sélectionnant un fichier en particulier, en sélectionnant le contenu entier de votre `Corbeille`, ou en nettoyant tout l'espace libre de votre disque dur. Eraser peut aussi nettoyer le contenu du *fichier d'échange* [109] de Windows.

Expérience pratique : se lancer avec le *Guide pratique Eraser* [110]

Même si, a priori, les programmes de suppression sécurisée ne risquent pas d'endommager les fichiers visibles (à moins que vous ne les nettoyiez volontairement), la précaution est de mise. Après tout, un accident est si vite arrivé. C'est justement pourquoi les `Corbeilles` et les logiciels de récupération de données sont tellement utiles. Si vous vous habituez à nettoyer vos données chaque fois que vous supprimez quelque chose, vous pourriez vous retrouver dans une situation où il serait tout simplement impossible de réparer une erreur toute banale. Assurez-vous de toujours avoir une copie de sauvegarde avant de nettoyer de grandes quantités de données.

Elena : Je sais que les programmes de traitement de texte comme Microsoft Word ou Open Office génèrent des copies temporaires des documents que je rédige. Est-ce que d'autres programmes font la même chose, ou devrais-je surtout m'inquiéter des fichiers que je crée et supprime moi-même ?

Nikolai : En fait, les programmes que tu utilises laissent des traces de tes renseignements personnels et de tes activités à plusieurs endroits sur ton ordinateur. Les sites que tu as visités, les brouillons de courriels que tu as rédigés

récemment et autres trucs semblables en sont quelques exemples. Tous ces renseignements peuvent être plus ou moins sensibles, selon la fréquence à laquelle tu utilises cet ordinateur.

Le nettoyage des données temporaires

La fonction qui permet à Eraser de nettoyer tout l'espace non alloué d'un disque dur n'est pas aussi dangereuse qu'elle le semble, parce qu'elle n'écrase que les données préalablement supprimées. Les fichiers normaux, c.-à-d. toujours visibles, ne seront pas touchés. Cependant, cela soulève un autre enjeu : Eraser ne peut pas être utilisé pour écraser des données sensibles qui n'ont pas été supprimées, mais qui sont par contre bien cachées. Les fichiers contenant des données de ce type peuvent être dissimulés dans des répertoires peu connus, par exemple, ou sauvegardés avec des noms inintelligibles. Cette question n'est pas particulièrement importante pour vos documents informatisés, mais elle peut l'être pour les données qui sont sauvegardées automatiquement chaque fois que vous utilisez votre ordinateur. Voici quelques exemples :

- Les données temporaires enregistrées automatiquement par votre navigateur lorsqu'il affiche des pages Web, dont le texte, les images, les *cookies* [111], les détails du compte et les renseignements personnels utilisés pour remplir des formulaire en ligne, sans oublier l'historique de navigation.
- Les fichiers temporaires sauvegardés par divers programme pour vous aider à récupérer vos documents lorsque l'ordinateur plante inopinément avant que vous ayez pu sauvegarder vos modifications. Ces fichiers contiennent, par exemple, du texte, des images, des données de feuilles de calcul et les noms d'autres fichiers.
- Des fichiers et des liens sauvegardés par Windows par souci de commodité, comme les raccourcis vers les programmes que vous avez utilisés récemment, les liens flagrants vers des répertoires que vous souhaiteriez garder secrets et, évidemment, le contenu de votre `Corbeille` si vous avez oublié de la vider.
- Le fichier d'échange de Windows. Quand la mémoire vive de votre ordinateur est utilisée à pleine capacité, comme lorsque vous faites fonctionner plusieurs programmes simultanément sur un vieil ordinateur, Windows copie parfois les données que vous utilisez dans un seul grand fichier, appelé fichier d'échange (ou swap file, en anglais). En fait, selon l'utilisation que vous faites de l'ordinateur, ce fichier pourrait contenir à peu près n'importe quoi, y compris des pages Web, le contenu de certains documents, des mots de passe ou même des clés de chiffrement. Le fichier d'échange n'est pas supprimé lorsque vous éteignez votre ordinateur. C'est pourquoi vous devez le nettoyer manuellement.

Pour éliminer de votre ordinateur les fichiers temporaires les plus courants, vous pouvez utiliser un gratuiciel appelé *CCleaner* [108]. Ce logiciel a été conçu spécialement pour nettoyer les traces que génèrent des programmes comme Internet Explorer, *Mozilla Firefox* [14] et Microsoft Office (tous trois connus pour leur indiscrétion), ainsi que le système Windows lui-même. CCleaner supprime les fichiers temporaires définitivement et de façon sécurisée. Vous n'êtes donc pas obligé de nettoyer systématiquement l'espace non alloué du disque dur avec Eraser après chaque utilisation du programme.

Expérience pratique : se lancer avec le *Guide pratique CCleaner* [112]

Conseils sur l'utilisation de programmes de suppression sécurisée

Vous êtes familier avec certains des moyens par lesquels des données sensibles peuvent être exposées sur votre ordinateur ou vos dispositifs de stockage, et ce, malgré toute la vigilance déployée pour les supprimer adéquatement. Vous savez également quels outils utiliser pour *nettoyer* [107] ces données et les supprimer définitivement. Vous devriez suivre un certain nombre d'étapes simples (surtout si c'est la première fois que vous utilisez ces programmes) pour vous assurer que vos disques durs soient nettoyés de façon sûre et efficace :

- Créez une copie de sauvegarde chiffrée de tous vos fichiers importants, tel qu'indiqué au chapitre ***5. Récupérer des données perdues*** [45] ;
- Fermez tous les programmes dont vous n'avez pas actuellement besoin et déconnectez-vous d'Internet ;
- Supprimez tous les fichiers superflus de tous vos périphériques et dispositifs de stockage, puis vider votre `Corbeille` ;
- Nettoyez tous les fichiers temporaires à l'aide de *CCleaner* [108] ;
- Nettoyez le *fichier d'échange* [109] de Windows à l'aide d'*Eraser* [106] ;
- Nettoyez tout l'espace libre de vos disques durs et autres dispositifs de stockage à l'aide d'Eraser. Vous devrez peut-être laisser ce processus en marche toute une nuit, car cette opération peut être assez lente.

Vous devriez ensuite prendre l'habitude de :

- Utiliser CCleaner périodiquement pour nettoyer vos fichiers temporaires ;
- Nettoyer vos documents de nature délicate à l'aide d'Eraser, au lieu de simplement les transférer dans la `Corbeille` ou d'utiliser la fonction `Supprimer` de Windows ;
- Utiliser Eraser périodiquement pour nettoyer le fichier d'échange de Windows ;
- Utiliser Eraser périodiquement pour nettoyer tout l'espace non alloué de vos disques durs, clés USB et autres dispositifs de stockage où vous avez récemment déposé et supprimé des données de nature délicate. Cela concerne également vos disquettes, CD et DVD réinscriptibles et cartes de mémoire flash (utilisées dans votre caméra, votre téléphone portable ou votre lecteur de musique portable).

Conseils sur le nettoyage d'un dispositif de stockage

Il est possible que vous deviez éventuellement *nettoyer* [107] un dispositif de stockage au complet. Lorsque vous vendez ou donnez un vieil ordinateur, il est préférable d'en retirer le disque dur et de laisser le nouveau propriétaire s'en procurer un nouveau. Si, pour une raison ou une autre, cela n'est pas possible, vous devriez à tout le moins nettoyer le disque minutieusement avec *Eraser* [106] avant de le donner. Et même si vous conservez le disque, que vous ayez l'intention de le réutiliser ou de le jeter, il est indiqué de le nettoyer minutieusement. Dans le même ordre d'idée, si vous faites l'achat d'un nouveau disque dur, il est conseillé de nettoyer votre vieux disque après avoir copié vos données et créé une copie de sauvegarde. Si vous avez l'intention de jeter ou de recycler un vieux disque dur, vous devriez aussi envisager de le détruire physiquement. (Plusieurs spécialistes de l'assistance informatique recommandent d'asséner quelques bons coups de marteaux sur tout périphérique ayant servi à stocker des données sensibles avant de le jeter.)

Dans l'une ou l'autre des situations décrites ci-dessus, vous devrez utiliser Eraser pour nettoyer un disque dur au complet, ce qui est évidemment impossible tant et aussi longtemps que le système d'exploitation fonctionne à partir de ce même disque dur. La méthode la plus simple pour contourner ce problème est de débrancher le disque et de l'insérer dans un « boîtier pour disque dur externe » à interface USB, que vous pouvez ensuite connecter à n'importe quel ordinateur où est installé Eraser. Vous pourrez alors supprimer le contenu du disque au complet et, par la suite, utiliser Eraser pour nettoyer tout l'espace libre. Heureusement, ce n'est pas une manœuvre que vous aurez à répéter très souvent (l'opération peut s'avérer plutôt longue).

Au lieu de nettoyer les données qui ont été gravées sur un CD ou un DVD réinscriptible, il est souvent plus simple et plus sûr de détruire le disque. Si nécessaire, vous pouvez en graver un nouveau pour stocker les données que vous souhaitez préserver. Bien sûr, c'est aussi le seul moyen de « supprimer » le contenu d'un disque non réinscriptible. Il est étonnamment difficile de détruire complètement le contenu d'un CD ou d'un DVD. Vous avez peut-être même déjà entendu dire qu'on a déjà réussi à récupérer des renseignements à partir de CD qui avaient été coupés en tous petits morceaux. Même si ces histoires sont vraies, reconstruire des données de cette façon exige beaucoup de temps et d'expertise. Ce sera à vous de juger si quelqu'un est susceptible de dépenser autant d'énergie et mobiliser autant de ressources pour accéder à vos données. Normalement, une bonne paire de ciseau ou une déchiqueteuse robuste devrait faire l'affaire. Si vous voulez prendre des précautions supplémentaires, vous pouvez jeter les fragments du disque détruit dans plusieurs lieux différents, loin de votre bureau.

Elena : J'ai encore un vieux CD de sauvegarde des journaux de connexion au serveur. J'ai entendu dire qu'il est possible d'effacer le contenu d'un CD en le plaçant dans un four à micro-ondes. Ça me paraît une très mauvaise idée. Est-ce qu'il y a vraiment des gens qui font ça ? Est-ce que ça fonctionne ?

Nikolai : J'imagine que ça doit détruire les données assez efficacement, mais je n'en ai aucune idée, parce que je n'ai jamais mis un CD dans un four à micro-ondes ! Tu as raison, c'est vraiment une idée bizarre ! Même si par miracle le métal n'endommageait pas le four et ne déclenchait pas un incendie, je suis persuadé que le plastique dégagerait des émanations particulièrement toxiques en fondant. À bien y penser, je ne recommanderais pas de mettre un CD au feu non plus.

Lecture complémentaire

- Bien que Mozilla Firefox n'utilise pas de techniques de suppression sécurisée pour les éliminer définitivement, le programme offre les moyens de supprimer automatiquement la plupart des fichiers temporaires qu'il génère. Cette fonction est présentée dans le ***Guide pratique Firefox*** [17] et sur le site Internet de Firefox [113].[1]
- La section FAQ de CCleaner [114] [2] fournit des renseignements supplémentaires sur l'installation et l'utilisation de ce programme.
- Bien que la majeure partie de l'essai soit plutôt technique, l'introduction du Secure Deletion of Data from Magnetic and Solid-State Memory [115] [3], de Peter Guttmann, vaut la peine qu'on s'y attarde, puisque la méthode [116] [4] qu'il décrit a eu une influence majeure sur le développement d'Eraser et d'autres outils similaires.

Liens

[1] https://support.mozilla.com/en-US/kb/Clearing+Private+Data [117]

[2] www.ccleaner.com/help/faq [114]
[3] www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/ [115]
[4] www.en.wikipedia.org/wiki/Gutmann_method [118]

7. Préserver la confidentialité de vos communications sur Internet

L'aspect pratique, le rapport coût-efficacité et la flexibilité des services de courriel et de messagerie instantanée en font des instruments extrêmement précieux pour les individus et organismes qui disposent d'un accès, ne serait-ce que limité, à Internet. Pour ceux dont la connexion est plus rapide et plus stable, des outils comme *Jitsi* [119], *Skype* [36] ou d'autres programmes de *voix sur réseau IP* (*VoIP* [120]) présentent les mêmes caractéristiques avantageuses. Malheureusement, en ce qui a trait à la confidentialité, ces solutions numériques ne sont pas toujours fiables. Bien sûr, il n'y a là rien de nouveau. Le courrier postal, le téléphone et les messages texte sont des moyens de communication tout aussi vulnérables, particulièrement quand ils sont utilisés par des personnes que les autorités ont choisi de surveiller pour une raison ou une autre.

Une différence importante entre les moyens de communication traditionnels et les méthodes numériques propres à Internet est que ces dernières permettent à l'utilisateur de déterminer lui-même le niveau de sécurité qu'il juge approprié. Si vous envoyez des courriels et des messages instantanés ou participez à des conversations VoIP par voies non sécurisées, ces communications seront presque certainement moins confidentielles qu'une lettre écrite ou qu'un appel téléphonique traditionnel. C'est qu'il est relativement facile, à l'aide de puissants ordinateurs, d'exécuter des recherches automatiques à travers une somme colossale de données afin d'identifier des expéditeurs, des destinataires et certains mots-clé particuliers. Lorsqu'il est question de surveiller les voies de communications traditionnelles, il faut habituellement mobiliser beaucoup plus de ressources pour atteindre un degré d'efficacité similaire. Cela dit, il est possible de contourner ces mesures de contrôle en mettant en place certaines précautions élémentaires. La flexibilité des communications par Internet et la force des nouveaux procédés de *chiffrement* [41] peuvent désormais assurer un niveau de confidentialité qui était autrefois exclusivement réservé aux forces armées et services de renseignements.

En suivant attentivement les recommandations avancées dans ce chapitre et en explorant le potentiel des logiciels qui y sont présentés, vous serez en mesure d'améliorer considérablement la sécurité de vos communications numériques. Le service de courriel *Riseup* [121], le module complémentaire *OTR* [122] du programme de messagerie instantanée *Pidgin* [123], *Mozilla Firefox* [14] et le module complémentaire *Enigmail* [124] du client de messagerie *Mozilla Thunderbird* [93] sont tous d'excellents outils. Vous devriez toutefois garder à l'esprit que la confidentialité d'une conversation numérique n'est jamais garantie à cent pour cent. Il subsiste toujours une menace qui nous a échappée, que ce soit un *enregistreur de frappe* [125] installé à votre insu sur votre ordinateur, une personne qui écoute aux portes, un correspondant imprudent ou quoi que ce soit d'autre.

L'objectif de ce chapitre est de vous aider à vous protéger contre ces menaces, autant que possible. Nous n'avons pas l'intention de minimiser l'importance de ces dangers, mais nous ne voulons pas non plus faire valoir la position extrême, défendue par certains, selon laquelle aucune information ne devrait être communiquée par Internet à moins que l'on soit disposé à la rendre tout à fait publique.

Scénario de départ

Claudia et Pablo sont employés par une ONG dans un pays sud-américain. Après avoir passé plusieurs mois à compiler les dépositions de nombreux témoins de violations de droits humains commises par l'armée dans leur région, Claudia et Pablo ont entrepris des démarches pour protéger ces données importantes. Ils ont gardé uniquement les renseignements dont ils avaient vraiment besoin, qu'ils ont stockés immédiatement dans un volume TrueCrypt. Ils ont ensuite créé des copies de sauvegarde de ce volume, qu'ils gardent à plusieurs emplacements physiques. En préparant la publication d'un rapport préliminaire, où ils exposeront certains aspects des témoignages recueillis, ils se sont rendus compte qu'ils doivent discuter d'enjeux sensibles avec un collègue qui se trouve à l'étranger. Même s'ils se sont entendus pour ne révéler aucun nom de personnes ou de lieux, ils veulent s'assurer que leurs échanges par courriel et messagerie instantanée resteront tout à fait confidentiels. Claudia a organisé une rencontre pour aborder l'importance de la sécurité des communications et veut savoir si ses collègues ont des questions à ce sujet.

Qu'apprendrez vous dans ce chapitre

- Pourquoi la plupart des services de courriel et de messagerie instantanée ne sont pas sécurisés ;
- Comment créer un compte de courriel plus sûr ;
- Comment augmenter le niveau de sécurité de votre compte de courriel ;
- Comment utiliser un service sécurisé de messagerie instantanée ;
- Que faire si vous avez de bonnes raisons de croire que quelqu'un accède à votre courrier électronique ;
- Comment authentifier l'identité d'un correspondant.

Sécuriser votre courriel

Tout d'abord, vous devriez appliquer quelques mesures importantes pour améliorer la sécurité de vos communications par courrier électronique. La première chose à faire est de vous assurer que personne d'autre que votre destinataire ne soit en mesure de lire le message que vous envoyez. Cette question est abordée dans les sections ***Préserver la confidentialité de votre courrier électronique*** et ***Adopter un service de courriel sécurisé***, ci-dessous. Au delà des questions élémentaires, il est essentiel que vos correspondants soient en mesure de vérifier, hors de tout doute, qu'un message donné provient bel et bien de vous et non pas d'une tierce personne qui aurait réussi à usurper votre identité. Nous verrons cela à la sous-section ***Chiffrer et authentifier des messages individuellement*** [126] de la section ***Principes de sécurité avancée*** [127].

Vous devriez toujours savoir quoi faire lorsque vous avez l'impression que la confidentialité de vos communications par courriel a été transgressée. La section ***Que faire si vous soupçonnez que vos communications par courriel sont surveillées*** [128] aborde cette question délicate.

Gardez également à l'esprit qu'un service de courriel sécurisé ne vous servira pas à grand-chose si chaque mot que vous tapez est enregistré par un logiciel espion et retransmis périodiquement à un tiers. Le chapitre ***1. Protéger votre ordinateur contre les logiciels malveillants et les pirates*** [72] offre de bons conseils sur les moyens de se prémunir contre ce type de menaces et le chapitre ***3. Créer et sauvegarder des mots de passe sûrs*** [39] vous aidera à protéger efficacement l'accès à vos comptes de courriel et de messagerie instantanée.

Préserver la confidentialité de votre courrier électronique

L'Internet est un réseau de communication ouvert où les données circulent habituellement dans des formats lisibles. Si un message de courriel est intercepté entre un expéditeur et un destinataire, son contenu peut facilement être lu. Comme l'Internet est justement un vaste réseau global qui repose sur une multitude d'ordinateurs intermédiaires pour faire circuler les données, plusieurs personnes ont l'occasion d'intercepter un message. Votre fournisseur de services Internet (*FSI ou FAI* [129] ou *ISP*, en anglais) est le premier intermédiaire du message que vous envoyez à un destinataire donné. De même, le FSI de votre destinataire est le dernier intermédiaire par lequel le message transite avant d'aboutir dans la corbeille d'arrivée de celui-ci. À moins que vous ne mettiez en place certaines mesures de précaution, votre message pourrait très bien être intercepté et falsifié à l'une ou l'autre de ces étapes, ou à n'importe quelle étape entre les deux.

Pablo : Je parlais justement de ça avec une de nos partenaires et elle me disait que ses collègues et elles sauvegardent parfois des messages importants dans le répertoire « Brouillons » d'un compte de courriel dont ils partagent le mot de passe. Ça me paraît un peu étrange, mais est-ce que ça peut fonctionner ? Est-ce que ça n'empêche pas justement les tiers malveillants de lire ces messages, puisqu'ils ne sont jamais vraiment envoyés ?

Claudia : Chaque fois que tu lis un message sur ton ordinateur, même si ce n'est qu'un brouillon, son contenu t'a été envoyé par Internet. Sinon, tu ne pourrais pas l'afficher sur ton écran, pas vrai ? Le problème, c'est que si quelqu'un t'a placé sous surveillance, il ne se contente pas d'inspecter tes messages, il peut aussi espionner toutes les données qui circulent depuis et vers ton ordinateur. En d'autres termes, ce truc ne peut fonctionner que si tous les collègues en question se connectent au compte partagé de façon sécurisée. Et si c'est le cas, il n'est pas moins pratique de créer des comptes séparés pour chaque personne.

Il existe depuis fort longtemps un moyen de sécuriser la connexion entre votre ordinateur et les sites que vous visitez. C'est ce niveau de sécurité que l'on retrouve, par exemple, lorsqu'on saisi un mot de passe ou les détails d'une carte de crédit sur un site Internet. La technologie qui rend possible ce genre de connexion s'appelle *chiffrement* [41] par *Secure Sockets Layer (SSL)* [130]. Il est possible de distinguer une connexion SSL d'une connexion normale en jetant un coup d'œil attentif à la **barre de navigation** de votre navigateur Web.

Toutes les adresses commencent normalement par la formule **HTTP**, tel qu'illustré ci-dessous :

Lorsque vous visitez un site Internet sécurisé, l'adresse commence par la formule `HTTPS` :

Le **S** supplémentaire signifie que votre ordinateur a ouvert une connexion sécurisée à ce site. Vous pouvez aussi remarquer une icône de cadenas, soit dans la `barre de navigation`, soit dans la `barre d'état` tout au bas de la fenêtre du navigateur. Ces éléments vous indiquent qu'aucun intrus ne sera en mesure d'espionner vos communications avec ce site en particulier.

En plus de protéger vos mots de passe et transactions financières, ce type de chiffrement est idéal pour sécuriser les communications par courriel. Par contre, plusieurs fournisseurs de services de courriel n'offrent pas l'accès sécurisé, alors que d'autres exigent que vous activiez vous-même la fonction, soit en réglant une préférence à cet effet, soit en saisissant

la formule **HTTPS** manuellement. Vous devriez toujours vous assurer que votre connexion est sécurisée avant de vous enregistrer sur un site, de lire vos courriels ou d'envoyer des messages.

Vous devriez aussi être sur vos gardes lorsque le navigateur signale un *certificat de sécurité* [131] invalide au moment de se connecter à un compte de courriel. Cela pourrait signifier qu'un tiers tente de s'interposer dans la communication entre votre ordinateur et le serveur afin d'intercepter vos messages. Finalement, si vous utilisez un service webmail pour échanger des renseignements sensibles, il est essentiel que votre navigateur soit aussi fiable que possible. Nous suggérons fortement d'installer *Mozilla Firefox* [14] et ses modules de sécurité complémentaires.

Expérience pratique : se lancer avec le *Guide pratique Firefox* [17]

Pablo : Une de nos partenaires qui doit collaborer à la rédaction du rapport utilise habituellement son compte de courriel Yahoo lorsqu'elle est à l'extérieur du bureau. Je crois aussi me rappeler qu'une autre personne utilise Hotmail. Si j'envoie un message à ces personnes, est-ce que d'autres personnes peuvent les lire ?

Claudia : Probablement. Les sites Internet de Yahoo, Hotmail et plusieurs autres fournisseurs de services webmail ne sont pas sécurisés et ne protègent donc pas la confidentialité de leurs usagers. Il va falloir changer les habitudes de quelques personnes si nous voulons discuter de ces témoignages en privé.

Adopter un service de courriel sécurisé

Très peu de fournisseurs de service webmail offrent l'accès SSL aux comptes de courriel. Yahoo et Hotmail, par exemple, offrent une connexion sécurisée *seulement* lorsque vous vous connectez (pour protéger votre mot de passe) mais vos messages, eux, sont envoyés et reçus de façon non sécurisée. De plus, Yahoo, Hotmail et d'autres fournisseurs de services gratuits intègrent *l'adresse IP* [132] de l'ordinateur que vous utilisez dans tous les messages que vous envoyez.

Les comptes Gmail, par contre, utilisent une connexion sécurisée à partir du moment où vous vous connectez jusqu'à ce que vous déconnectiez. Vous pouvez vérifier ceci dans la barre d'adresse, présentant une URL commençant par 'https', le 's' indiquant une connexion sécurisée. Contrairement à Yahoo et Hotmail, Gmail ne révèle pas votre adresse IP aux destinataires du message. Cela dit, il n'est pas recommandé de dépendre uniquement de Google si la confidentialité de vos communications est un enjeu important. Google balaye et enregistre le contenu des messages de ses usagers pour une variété de raisons et a déjà acquiescé aux requêtes de gouvernements reconnus pour imposer des limites aux droits numériques. Voir la section ***Lecture complémentaire*** [133], à la fin de ce chapitre, pour plus de renseignements à propos de la Charte de confidentialité de Google.

Si possible, vous devriez créer un nouveau compte de courriel *Riseup* [121] en visitant https://mail.riseup.net [134]. Les administrateurs de Riseup offrent des services de courrier électronique à des centaines d'activistes de partout dans le monde et se font un point d'honneur de protéger rigoureusement les données qui sont stockées sur leurs serveurs. Depuis plusieurs années, les services offerts par le collectif Riseup constituent une solution fiable pour tous ceux qui souhaitent utiliser un courriel sécurisé. Contrairement à Google, ils ont des politiques très strictes concernant la confidentialité de leurs utilisateurs et n'ont aucun intérêt commercial qui pourrait éventuellement entrer en conflit avec ces politiques. Pour créer un compte Riseup, cependant, vous aurez besoin de deux « codes d'invitation ». Ces codes peuvent vous être fournis par quiconque dispose déjà d'un compte Riseup. Si vous avez une copie reliée de ce livret, vous devriez également avoir reçu vos « codes d'invitation ». Sinon, vous devrez trouver deux usagers Riseup et leur demander de vous faire parvenir des codes d'invitation.

Expérience pratique : se lancer avec le Guide pratique RiseUp [135]

Gmail et Riseup n'offrent pas seulement le service webmail. Les deux fournisseurs peuvent être utilisés avec un client de messagerie comme *Mozilla Thunderbird* [93], qui permet le recours aux techniques présentées à la section ***Principes de sécurité avancée*** [127], ci-dessous. Il est tout aussi important de s'assurer que votre client de messagerie établisse une connexion chiffrée à votre fournisseur de service que de se connecter au webmail via HTTPS. Pour plus de renseignements sur les clients de messagerie, nous vous invitons à consulter le ***Guide pratique Thunderbird*** [136]. À tout le moins, vous devriez activer la fonction de chiffrement SSL ou TLS pour vos serveurs entrant et sortant.

Pablo : Alors, devrais-je créer un nouveau compte Riseup, ou bien continuer à utiliser Gmail, mais avec une adresse sécurisée 'https' ?

Claudia : C'est ta décision, mais il y a un certain nombre d'éléments dont tu devrais tenir compte lorsque tu choisis un service de courriel régulier. Premièrement, est-ce que le fournisseur permet une connexion sécurisée à son serveur ? Gmail le fait, donc ça va. Deuxièmement, fais-tu confiance aux administrateurs quant à la confidentialité de tes communications ? Vont-ils lire tes messages ou en partager le contenu avec un tiers ? C'est à toi d'évaluer les risques. Finalement, tu dois déterminer s'il est acceptable que tu sois associé à ce fournisseur. En d'autres termes, est-il possible

que tu t'attires éventuellement des ennuis parce que tu as une adresse « riseup.net » (qui est reconnue pour être populaire auprès des activistes) ? Devrais-tu plutôt, par souci de discrétion, te contenter d'une adresse « gmail.com » ?

D'une manière ou d'une autre, vous devez garder à l'esprit que chaque message a un expéditeur et au moins un destinataire. Vous, personnellement, n'êtes qu'un élément de l'équation. Même si vous accédez à votre compte de façon sécurisée, vous devez considérer les précautions que vos contacts prennent (ou ne prennent pas) lorsqu'ils envoient, lisent ou répondent à vos messages. Si possible, demandez à vos correspondants de vous indiquer où sont situés leurs fournisseurs de service de courriel. Certains pays sont plus agressifs que d'autres en ce qui concerne la surveillance des communications par courrier électronique. **Pour assurer la confidentialité de vos communications, vos correspondants et vous devriez tous utiliser des services sécurisés hébergés dans des pays relativement sûrs.** Si vous voulez être absolument certain que vos messages ne soient pas interceptés entre votre serveur de courriel et celui de votre correspondant, il serait pertinent que vous adoptiez tous deux des comptes courriels du même fournisseur. À cet égard, Riseup est un excellent choix.

Conseils supplémentaires pour améliorer la sécurité de vos correspondances par courriel

- Soyez toujours prudent lorsque vous ouvrez des pièces jointes que vous n'attendiez pas, qui proviennent de personnes que vous ne connaissez pas ou dont la ligne d'objet est douteuse. Lorsque vous ouvrez des messages de ce type, vous devriez toujours, 1) vous assurer que votre programme antivirus soit actualisé et 2) rester particulièrement attentif aux avertissements lancés par votre navigateur ou votre programme de courriel.
- Vous devriez utiliser un programme de connexion anonyme, comme *Tor* [137]. Ce programme, abordé au chapitre ***8. Préserver votre anonymat et contourner la censure sur Internet*** [138], peut vous aider à cacher votre service de courriel à ceux qui pourraient être en train de surveiller votre connexion Internet. Selon le degré de filtrage des courriels qui prévaut dans votre pays, il vous sera peut-être nécessaire d'utiliser Tor, ou un autre des outils de *contournement* [139] décrits au ***chapitre 8*** [138], ne serait-ce que pour accéder à un fournisseur de services de courriel sécurisés comme Riseup ou Gmail.
- Au moment de créer un compte que vous avez l'intention d'utiliser anonymement (pour communiquer avec vos destinataires ou participer à des forums par courriel), faites attention à ne pas enregistrer un nom d'utilisateur ou un « Nom complet » qui se rapporte à votre vie personnelle ou professionnelle. Dans ces cas-là, il est également indiqué d'éviter les comptes Hotmail, Yahoo, ou tout autre fournisseur de webmail qui inclut automatiquement votre adresse IP dans les messages que vous envoyez.
- Compte tenu des personnes qui ont physiquement accès à votre ordinateur, le nettoyage régulier des fichiers temporaires liés à l'utilisation des services de courriel est tout aussi important que la protection des messages envoyés sur Internet. À ce sujet, voir le chapitre ***6. Détruire définitivement des données sensibles*** [98] et le ***Guide pratique CCleaner*** [112].
- Vous pouvez envisager d'utiliser plusieurs comptes de messagerie anonymes pour communiquer avec différents groupes de personnes et assurer ainsi la protection de votre réseau de contacts. Vous pouvez également utiliser d'autres comptes de messagerie pour vous inscrire à des services Internet exigeant une adresse électronique.
- Au-delà de toutes ces précautions, prenez garde à ce que vous écrivez dans vos emails et aux conséquences qu'ils pourraient avoir s'ils tombaient entre de mauvaises mains. Un moyen d'accroître la sécurité de tout échange de données consiste à créer un système de code réservé à l'échange de données sensibles et vous permettant de ne pas nommer les gens par leur propre nom, ni de citer des adresses réelles, etc.

Que faire si vous soupçonnez que vos communications par courriel sont surveillées

Si vous soupçonnez que votre compte courriel a été piraté ou compromis, vous pouvez prendre des mesures pour limiter les dégâts. Bien qu'il soit difficile d'en être certain, vous pouvez vous faire une idée si :

- vous remarquez des changements dans le contenu de votre compte ou dans les paramètres, que vous n'avez pas faits vous-même ;
- vos contacts vous ont informé qu'ils ont reçu un courriel provenant de votre adresse et que vous ne l'avez pas envoyé ;
- vous ne pouvez pas vous connecter à votre compte alors que vous êtes certain de votre mot de passe et que les autres paramètres sont corrects ;
- il arrive régulièrement que vous ne receviez pas certains messages de vos collègues qui affirment pourtant vous les avoir envoyés ;
- certaines informations privées qui ont été envoyées ou reçues exclusivement par courriel ont été portées à la connaissance d'un tiers alors que ni vous, ni votre correspondant ne les avez partagées avec une autre personne ;
- si l'historique des connexions de votre compte (si cela est possible chez votre fournisseur de service de courriel) indique que ce dernier a été consulté à des heures dont vous ne vous souvenez pas ou depuis des lieux (ou adresse IP) où vous ne vous êtes pas rendus.

Dans de telles situations, il serait prudent de prendre des mesures de précaution :

- **Cessez d'utiliser ce compte pour échanger des informations sensibles**, au moins jusqu'à ce que la situation vous paraisse meilleure.
- **Changez votre mot de passe dès que possible**. Consultez le *Chapitre 3: Créer et sauvegarder des mots de passe*

sûrs [140]. Pour pouvoir changer le mot de passe de votre compte (ou d'autres comptes), vous devrez vous familiariser avec la façon de procéder sur votre système de courriel, afin que lorsque vous devrez le faire, cela soit rapide. **Changez votre mot de passe de tous les autres comptes lorsqu'il est le même ou semblable**, car ces comptes sont peut-être aussi compromis.

- Utiliser des mots de passe différents et forts pour chaque compte. Vous pouvez aussi changer les mots de passe de tous les autres comptes que vous possédez. Envisagez d'utiliser *KeePass* [141] pour stocker et gérer tous vos mots de passe. Changez vos questions de sécurité (si vous en utilisez) pour tous vos comptes, afin qu'elles soient impossibles à deviner, que la réponse ne puisse être trouvée par quelqu'un qui fait des recherches sur vous. Il s'agit d'une précaution au cas où votre ordinateur serait infecté par un logiciel espion, qui pourrait alors rendre vos autres comptes vulnérables.
- **Si vous ne parvenez pas à vous connecter** à votre compte pour changer votre mot de passe, pensez à entrer en contact avec votre fournisseur de service de courriel pour tenter de récupérer votre compte. Certains fournisseurs ont des procédures spéciales pour aider les utilisateurs dans de telles circonstances. Il est aussi utile de connaître ces procédures à l'avance.
- **Atténuez la perte d'information et l'impact** sur votre communauté. Il est aussi important de mettre en place un plan de réponse. En sachant quel genre d'information sensible vous aviez sur votre compte et en déterminant les personnes avec lesquelles vous échangez des informations via ce compte, décidez qui vous devriez alerter et quels autres comptes devront être changés ou fermés. Déterminez quels services (web, financiers, etc.) vous devrez revoir ou annuler. Il est important de **vérifier les dossiers de votre compte** (si vous le pouvez), pour rechercher ce qui pourrait avoir été envoyé depuis votre compte, et agissez en fonction. **Pour informer vos contacts**, vous devrez conserver une sauvegarde à part de votre carnet d'adresse. Vérifiez **aussi les paramètres de votre compte** afin de voir les changements qui ont pu être faits. Vérifiez l'option signature des comptes et veillez à ce qu'il n'y ait pas de lien ou de logiciels néfastes, l'option pour transférer un message qui permettrait de copier les courriels que vous recevez sur un compte tiers, les messages d'absence, l'affichage du nom, etc.
- **Chercher comment votre compte a pu être compromis**. Était-ce parce que votre mot de passe était faible ou à cause d'une infection par un logiciel néfaste, etc. Plus vous en saurez à ce sujet, mieux vous pourrez répondre à la situation et mieux vous pourrez protéger vos contacts.
- **Revoyez la sécurité de tous** vos systèmes qui accèdent à vos courriels sur ce compte et les systèmes sur lesquels vous stockez le mot de passe de ce compte. Voir les chapitres ***1. Protéger votre ordinateur contre les logiciels malveillants et les pirates*** [142], ***2. Assurer la sécurité physique de vos données*** [143] et ***11. Utiliser votre smartphone en sécurité (autant que possible...)*** [144]. Revoyez votre logiciel antivirus (voir les guides pratiques Avast - antivirus et Spybot - anti-mouchard). Scannez votre ordinateur : lisez ***4.1 Comment faire face efficacement à une attaque de virus*** [145]. Utilisez un CD ou une clé USB de secours (rescue CD) – lisez ***4.9 Méthodes avancées de suppression de virus*** [146]. Si vous n'êtes pas certain de pouvoir nettoyer votre système, pensez à réinstaller tous vos tous les logiciels, y compris le système d'exploitation, à partir d'une source fiable. Envisagez de changer pour des programmes plus sécurisés tels que *Firefox* [147], *Thunderbird* [94], *LibreOffice* [148] et d'autres programmes *libres et open source* [8]. Après avoir apporté les améliorations à la sécurité de votre système, changez de nouveau les mots de passe de vos comptes, assurez-vous qu'ils soient forts.
- Pensez à signaler le piratage de votre compte à votre fournisseur.
- Pensez à utilisez un autre compte plus sécurisé, par exemple un qui vous informe et empêche l'accès depuis des lieux ou des appareils inhabituels. Envisagez d'utiliser un compte hébergé hors de votre pays. Pensez à utilisez le chiffrement des courriels – lisez gpg4usb – chiffrement de courriel et de dossiers ou Thunderbird avec Enigmail et GPG – Client de courriel sécurisé.
- Pensez à éviter de stocker les courriels lus sur le serveur de courriel sur votre compte. Songez plutôt à les télécharger sur votre ordinateur. Analysez la sécurité liée à la façon dont vous accédez à votre compte et les appareils que vous utilisez pour cela.

Il est important d'agir rapidement et avec précision dans de telles situations. Avoir un plan prêt que vous avez répété peut vous aider.

Si vous avez de bonnes raisons de croire que quelqu'un surveille vos courriels, il serait pertinent de créer un nouveau compte et de garder l'ancien comme diversion. Rappelez-vous tout de même que tous les comptes avec lesquels vous avez pu échanger des messages dans le passé pourraient très bien être surveillés également. En conséquence, vous devriez prendre quelques précautions supplémentaires :

Vous et tous vos correspondants récents devriez créer de nouveaux comptes et vous y connecter à partir d'ordinateurs que vous n'avez jamais utilisés auparavant, comme ceux que l'on trouve dans des cafés Internet. Nous recommandons cette stratégie pour empêcher que les connexions établies à partir de votre ordinateur habituel ne révèle l'emplacement de votre nouveau compte. Si vous n'avez d'autre choix que de vous connecter à partir de votre ordinateur habituel, vous pouvez utiliser l'un des programmes décrits au ***Chapitre 8. Préserver votre anonymat et contourner la censure sur Internet*** [149] pour cacher ces connexions.

- Échangez les renseignements relatifs à ces comptes via des voies de communications sécurisées, que ce soit en personne, par messagerie instantanée sécurisée ou par conversation *VoIP* [150] chiffrée.

- Essayez de maintenir une fréquence plus ou moins habituelle d'échanges sur votre ancien compte, au moins pour quelque temps. Vous devez laisser croire à l'espion que vous utilisez toujours ce compte pour effectuer des communications de nature délicate. Évidemment, vous éviterez désormais de révéler des renseignements importants, mais vous devriez aussi donner l'apparence que vos habitudes sont inchangées. Comme vous pouvez l'imaginer, cela pose un certain défi.

- Faites en sorte qu'il soit difficile d'établir un lien direct entre votre identité réelle et votre nouveau compte. N'envoyez pas de messages entre votre nouveau compte et l'ancien (ou ceux de vos contacts que vous soupçonnez être sous

surveillance).

- Faites attention à ce que vous écrivez lorsque vous utilisez votre nouveau compte. Il est préférable d'éviter d'utiliser des vrais noms et adresses, ou de formuler des phrases comme « droits humains » ou « torture ». Vous pouvez aussi concevoir un système codifié (que vous modifiez périodiquement) pour communiquer avec vos correspondants par courriel.
- Rappelez-vous que pour assurer la sécurité de vos communications par courrier électronique, il ne suffit pas de mettre en place des moyens de défense techniques efficaces. Il est aussi essentiel de faire très attention à la façon dont vos correspondants et vous utilisez le courriel, et de maintenir une discipline de fer quant à vos habitudes sécuritaires non techniques.

Sécuriser vos autres outils de communication par Internet

Tout comme le courrier électronique, les programmes de messagerie instantanée et de *VoIP* [120] peuvent être sécurisés ou non, selon les outils que vous choisissez et l'utilisation que vous en faites.

Sécuriser votre programme de messagerie instantanée

La messagerie instantanée, aussi appelée *chat* ou « clavardage », n'est habituellement pas sécurisée et, à cet égard, peut s'avérer tout aussi vulnérable que le courrier électronique. Heureusement, il existe des logiciels conçus pour garantir la confidentialité de vos séances de clavardage. Comme pour les courriels, cependant, une voie de communication sécurisée exige que vos correspondants par *chat* et vous utilisiez les mêmes logiciels et respectiez les mêmes mesures de précaution.

Pidgin [123] est un programme de clavardage qui fonctionne avec la plupart des protocoles de messagerie instantanée existants, ce qui signifie que vous pouvez facilement commencer à l'utiliser sans pour autant devoir changer vos noms de comptes ou recréer votre liste de contacts. Pour mener des conversations confidentielles *chiffrées* [41] avec Pidgin, vous devrez installer et activer le module complémentaire Off-the-Record (*OTR* [122]). Heureusement, cette opération est plutôt simple.

Expérience pratique : se lancer avec le *Guide pratique Pidgin* [151]

Pablo : Si le service webmail de Yahoo n'est pas sécurisé, est-ce que cela signifie que Yahoo Chat est également non sécurisé ?

Claudia : Tu dois surtout te rappeler que si l'on veut utiliser la messagerie instantanée pour discuter de ce rapport, on doit d'abord s'assurer que chacune des personnes impliquées a installé et configuré Pidgin et le module OTR. Si c'est le cas, nous pouvons utiliser Yahoo Chat ou n'importe quel autres service semblable.

Sécuriser votre programme de VOIP (voix sur IP)

Les appels entre utilisateurs de VoIP sont habituellement gratuits. Certains programmes vous permettent de placer des appels bon marché à des téléphones réguliers, y compris vers l'étranger. Inutile de dire que ces outils peuvent s'avérer extrêmement utiles. Skype [152], Jitsi [153], Google Talk [154], Yahoo! Voice [155] et MSN Messenger [156] figurent parmi les programmes de VoIP les plus répandus.

Normalement, les communications par voix sur réseau IP ne sont pas plus sûres que les courriels ou les chats non sécurisés. Lorsque vous utilisez ce type de communication pour échanger des informations sensibles, il est important de choisir un programme en état de chiffrer l'appel depuis votre ordinateur jusqu'à celui du destinataire. De même, il vaut mieux utiliser des logiciels libres et Open Source ; de préférence ceux qui ont été examinés, testés et recommandés par un groupe ou une communauté en lesquels vous avez confiance. En considération des critères exposés ci-dessus, nous conseillons l'utilisation de *Jitsi* [153] comme logiciel de VoIP.

Remarques sur la sécurité de Skype

Skype [78] est un logiciel de messagerie instantanée et vocale très courant, et avec lequel on peut également effectuer des appels à destination de numéros fixes comme mobiles. Malgré sa popularité, ce logiciel n'est pas un choix sûr pour plusieurs raisons. Certaines de ces raisons sont décrites ci-dessous.

Selon Skype, les messages et les appels vocaux sont *chiffrés* [78]. Ceci ne peut donc être le cas que lorsque toutes les personnes impliquées dans l'échange utilisent un logiciel Skype. Skype ne chiffre donc ni les appels à destination de

téléphones ni les textes envoyés sous forme de SMS.

Si toutes les personnes impliquées dans l'échange utilisent un logiciel Skype (authentique), son chiffrement peut être plus sûr que lors d'un appel ordinaire via téléphone. Mais comme Skype est un logiciel à code source fermé, ce qui rend impossible tout contrôle ou évaluation indépendamment de ses déclarations, il est également impossible de vérifier si Skype protège vraiment ses utilisateurs, leurs informations et communications. Le ***chapitre 1. Protéger votre ordinateur contre les logiciels malveillants et les pirates*** *[142]* présente clairement les avantages des logiciels Free/Libre Open-Source (*FLOSS* [74]), à la section ***Actualiser vos logiciels*** [157].

Nous ne recommandons donc pas l'usage de Skype. Si vous décidez toutefois de l'utiliser pour échanger des informations sensibles, prenez un certain nombre de précautions:

- Téléchargez Skype à partir de son site officiel www.skype.com [152] afin d'éviter un programme Skype infecté par un logiciel espion. Il est important de toujours vérifier l'URL afin d'être sûr que vous êtes connecté au site officiel. Dans certains pays, le site de Skype est bloqué et/ou de faux sites prétendant être Skype circulent sur le net. Dans de nombreux cas, la version de Skype disponible est probablement infectée par un logiciel malveillant, conçu pour espionner les communications. Utilisez les outils de contournement décrits dans le ***chapitre 8. Préserver votre anonymat et contourner la censure sur Internet*** *[149]* pour vous connecter au site Internet de Skype et télécharger une version authentique du logiciel ; que vous souhaitiez l'installer ou le mettre à jour.

- Il est très important de modifier votre mot de passe Skype régulièrement. Skype assure des connexions multiples à partir d'emplacements différents et ne vous informe pas sur le nombre de sessions simultanées. Si votre mot de passe est compromis, vous courez le risque que n'importe qui puisse se connecter à votre place. Toutes les sessions connectées reçoivent toutes les communications par texte et ont accès à l'historique des appels. Le seul moyen de stopper ces sessions sournoises est de modifier son mot de passe (en forçant une reconnexion).

- Il est également conseillé de régler les paramètres de confidentialité sur Skype de façon à ce que l'historique des conversations ne soit pas conservé.

- Il est recommandé de désactiver la fonction d'acceptation automatique de fichiers entrants. C'est par ce biais que des logiciels malveillants/espions ont pu parfois être introduits sur des ordinateurs.

- Vérifiez toujours indépendamment l'identité de la personne avec laquelle vous communiquez. Ceci est plus facile à effectuer lors de communications vocales - si vous connaissez la personne à laquelle vous souhaitez parler.

- Demandez-vous s'il est nécessaire que votre nom d'utilisateur Skype soit votre nom réel ou celui de votre organisation.

- Prévoyez d'autres moyens de communication - Skype peut devenir indisponible à tout moment.

- Exprimez-vous prudemment. Développez un système codé pour discuter des sujets sensibles sans avoir à utiliser la terminologie spécifique.

Malgré la popularité de Skype, les préoccupations mentionnées ci-dessus font douter de son efficacité en matière de sécurité. Bref, vous avez tout avantage à utiliser des logiciels tels que Jitsi pour vos communications vocales et *Pidgin* [78] avec le module complémentaire *OTR* [78] pour une messagerie instantanée sécurisée.

Principes de sécurité avancée

Les outils et concepts présentés ci-dessous sont recommandés aux utilisateurs expérimentés.

Utiliser le chiffrement asymétrique pour vos courriels

Il est possible d'améliorer davantage le niveau de confidentialité de vos communications par courriel, et ce, même en employant un compte de courriel non sécurisé. Pour ce faire, vous devrez apprendre à utiliser le *chiffrement* [41] asymétrique. Cette technique permet de chiffrer un message individuellement de telle sorte que seul le destinataire visé puisse le lire. L'aspect ingénieux du chiffrement asymétrique est que vous n'êtes pas obligé d'échanger des renseignements secrets avec vos correspondants pour leur indiquer comment vous coderez vos messages à l'avenir.

Pablo : Mais comment ça fonctionne ?

Claudia : Avec des mathématiques sophistiquées ! Tu dois encoder les messages que tu envoies à un correspondant en particulier à l'aide de sa « clé publique », qu'il t'a préalablement fait parvenir et qu'il est libre de partager avec n'importe qui. Ensuite, cette personne utilise sa « clé privée », dont elle garde rigoureusement le secret, pour décoder les messages. En retour, ton correspondant utilise ta clé publique pour chiffrer les messages qu'il t'envoie. Au bout du compte, vous devez échanger vos clés publiques, mais vous n'avez pas à vous inquiéter qu'elles soient interceptées, puisqu'une clé publique, sans la clé privée correspondante, est parfaitement inutile.

Cette technique peut être employée avec n'importe quel service de courriel, même ceux qui n'offrent pas de connexion

sécurisée, parce que les messages sont chiffrés avant même de quitter votre ordinateur. N'oubliez pas, toutefois, que l'utilisation de procédés de chiffrement pourrait attirer sur vous une attention non désirée. Le type de chiffrement employé pour accéder à un site Internet sécurisé ou à un compte webmail attire habituellement moins de suspicion que le chiffrement asymétrique abordé dans cette section. Dans certaines circonstances, si un message contenant des données chiffrées de cette manière est intercepté ou publié sur un forum public, il pourrait incriminer la personne qui l'a envoyé, et ce, même si le message lui-même ne contient rien d'incriminant. Il faut parfois choisir entre la confidentialité de vos messages et l'importance de passer inaperçu.

Chiffrer et authentifier des messages individuellement

Le chiffrement asymétrique peut sembler complexe de prime abord, mais le procédé est relativement simple, pourvu que vous en saisissiez les principes élémentaires. Par ailleurs, les outils sont très faciles à utiliser. Le client de messagerie *Mozilla Thunderbird* [93] peut être utilisé avec un module complémentaire appelé *Enigmail* [124] pour chiffrer et déchiffrer des messages en un tournemain.

Expérience pratique : se lancer avec le *Guide pratique Thunderbird* *[136]*

VaultletSuite 2 Go [158], un programme (*gratuiciel* [7]) de courriel chiffré, est encore plus facile à utiliser que Thunderbird, pourvu que vous soyez disposé à faire confiance aux distributeurs de logiciel et à leur permettre de faire un peu de travail pour vous.

Expérience pratique : se lancer avec le *Guide pratique VaultletSuite 2Go* *[159]*

L'authenticité de vos courriels est un autre aspect important de la sécurité des communications. Quiconque dispose d'un accès Internet et des bons programmes peut usurper votre identité en envoyant des messages à partir d'une fausse adresse identique à la vôtre. On comprend mieux ce danger lorsqu'on le considère depuis la perspective de vos destinataires. Imaginez, par exemple, la menace posée par un message qui semble provenir d'une source fiable mais qui en réalité est émis par un tiers dont l'intention est de perturber vos activité ou d'obtenir des renseignements sensibles à propos de votre organisme.

Puisqu'il est impossible de voir ou d'entendre nos correspondants par courriel, nous nous fions habituellement à l'adresse de l'expéditeur pour vérifier son identité. C'est pourquoi l'on peut facilement se laisser berner par de fausses adresses. Les *signatures numériques* [160], qui reposent elles aussi sur un procédé de chiffrement asymétrique, offrent un moyen plus sûr de vérifier l'identité d'un correspondant lorsque vous recevez ou envoyez des messages. La section ***Comment utiliser Enigmail avec Thunderbird*** [161] du ***Guide pratique Thunderbird*** [136] explique comment utiliser cette fonction.

Pablo : J'ai un collègue qui a déjà reçu un courriel de moi que je ne lui avais jamais envoyé. Nous avons déterminé que c'était probablement un pourriel, mais je me rends bien compte maintenant des problèmes qui pourraient survenir si un faux courriel aboutissait dans la corbeille d'arrivée de la mauvaise personne, au mauvais moment. J'ai lu quelque part qu'il est possible d'éviter ce genre de situation en recourant aux signatures numériques. Mais de quoi s'agit-il ?

Claudia : Une signature numérique est un peu comme un cachet de cire que l'on utilise pour sceller une enveloppe contenant une lettre importante. Il est impossible de contrefaire une telle signature. Elle prouve que tu es bel et bien l'expéditeur du message et que celui-ci n'a pas été intercepté ni falsifié en chemin.

Lecture complémentaire

- Pour en savoir plus sur les moyens par lesquels il est possible d'usurper une identité numérique, veuillez consulter la section Spoofing [162] du chapitre 2.5 du manuel Digital Security and Privacy for Human Rights Defenders [27].[5]
- Il existe une faille de sécurité bien connue du procédé de chiffrement SSL : l'attaque de l'homme du milieu (*Man in the Middle attack*) [163].[5]
- La Charte de confidentialité de Gmail [164] [6], que vous devez accepter à la création d'un compte Gmail, explique que « Google assure la maintenance et le traitement de votre compte Gmail et de son contenu afin de vous fournir le service Gmail et d'améliorer nos prestations ». En fait, dans une certaine mesure, tous les fournisseurs de services de courriel examinent vos messages pour améliorer leurs fonctions anti-pourriel et autres fonctionnalités du même genre. Mais Gmail va plus loin, cependant, afin d'afficher des « annonces pertinentes » selon le contenu de vos messages. Cela peut s'avérer dangereux si les renseignements stockés par Gmail devaient un jour être révélés, intentionnellement ou accidentellement.
- Une série d'entretiens menés en 2008 portait sur les politiques de confidentialité et de chiffrement [165] [7] de plusieurs services de messagerie instantanée.
- En plus des guides pratiques *Riseup* et *Thunderbird*, il existe un certain nombre de sites Internet qui expliquent comment utiliser votre programme de courrier électronique avec plusieurs fournisseurs de services courriel répandus

tout en laissant une copie de vos messages sur le serveur de courriel distant :

- Le site Internet de Riseup [166].[8]
- Des consignes pour l'utilisation de Gmail [167].[9]
- Des consignes pour l'importation de vos contacts Gmail dans Thunderbird [168].[10]
- Pour des renseignements sur l'utilisation d'autres services de courriel de cette façon, effectuez une recherche dans la section « Aide » du fournisseur de service, avec des mots-clés comme 'POP', 'IMAP' et 'SMTP'.

Liens

[1] www.gizmo5.com/pc [169]
[2] www.google.com/talk [154]
[3] www.voice.yahoo.com [170]
[4] www.download.live.com/?sku=messenger [171]
[5] www.frontlinedefenders.org/manual/en/esecman [49]
[6] https://mail.google.com/mail/help/intl/fr/privacy.html [172]
[7] www.news.cnet.com/8301-13578_3-9962106-38.html [173]
[8] http://help.riseup.net/mail/mail-clients [174]
[9] https://mail.google.com/support/bin/topic.py?topic=12805 [175]
[10] www.email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm [176]

8. Préserver votre anonymat et contourner la censure sur Internet

Plusieurs gouvernements nationaux, un peu partout sur la planète, ont choisi d'installer des programmes spéciaux pour empêcher les internautes de leurs pays respectifs d'accéder à certains sites et services Internet. Des sociétés privées, des écoles et des bibliothèques publiques emploient des logiciels similaires pour protéger leurs employés, étudiants et clients contre des contenus jugés dérangeants ou nocifs. Ces technologies de filtrage se présentent sous diverses formes. Certains filtres bloquent des sites par leur *adresse IP* [132], alors que d'autres dressent des « *listes noires* [177] » de *noms de domaine* [178] ou effectuent des recherches à travers l'ensemble des communications non chiffrées sur Internet pour y détecter certains mots-clé particuliers.

D'une manière ou d'une autre, il est quasiment toujours possible de contourner ces méthodes de filtrage en utilisant des ordinateurs intermédiaires, à l'extérieur de votre pays, pour accéder aux services qui vous sont interdits. Ce procédé est souvent appelé « contournement de la censure », ou tout simplement *contournement* [139], et les ordinateurs intermédiaires sont appelés « *mandataires* [179] » ou « proxys ». (N.D.T. Dans ce chapitre nous utiliserons plutôt le terme *proxy* [179], puisque les spécialistes et les logiciels spécialisés tendent à utiliser davantage ce mot que l'équivalent français.) Les ordinateurs ou serveurs proxys, eux aussi, peuvent prendre plusieurs formes. Ce chapitre comporte une brève présentation des réseaux de connexion anonyme par proxys multiples, suivie d'une description plus détaillée des méthodes de contournement par proxy unique et de leur fonctionnement.

Ces deux méthodes constituent des moyens efficaces de contournement des filtres sur Internet, bien que le premier soit davantage approprié que le second, si vous êtes toutefois disposé à sacrifier la vitesse de connexion pour assurer que vos activités sur Internet restent tout à fait confidentielles. Si vous connaissez bien l'individu ou l'organisme qui gère votre serveur proxy et que vous lui faites confiance, ou si la performance vous importe plus que l'anonymat, le contournement par serveur proxy unique vous conviendra sans doute.

Scénario de départ

Mansour et Magda sont frère et soeur. Ils habitent un pays arabophone où ils gèrent ensemble un blog pour dénoncer diverses violations de droits humains et faire campagne en faveur de changements politiques. Jusqu'à présent, les autorités de leur pays n'ont pas réussi à fermer leur site parce que ce dernier est hébergé dans un autre pays. Par contre le gouvernement a à plusieurs reprises tenté d'apprendre l'identité des administrateurs du blog en interrogeant d'autres activistes. Mansour et Magda craignent que les autorités parviennent à découvrir leur identité en contrôlant les mises à jour apportées au site. De plus, ils veulent se préparer à l'éventualité où le gouvernement parviendrait à filtrer leur site, pas uniquement pour être en mesure de continuer à l'actualiser régulièrement, mais aussi pour offrir de bons conseils de contournement aux lecteurs qui se trouvent dans leur pays et qui, autrement, perdraient complètement accès au blog.

Qu'apprendrez-vous dans ce chapitre

- Comment accéder à un site Internet qui est bloqué dans votre pays ;
- Comment empêcher que les sites que vous visitez puissent servir à déterminer votre position ;

- Comment vous assurer que ni votre *FSI* [129] ni aucun organisme de surveillance implanté dans votre pays ne soit en mesure de déterminer quels sites Internet vous visitez et quels services vous utilisez.

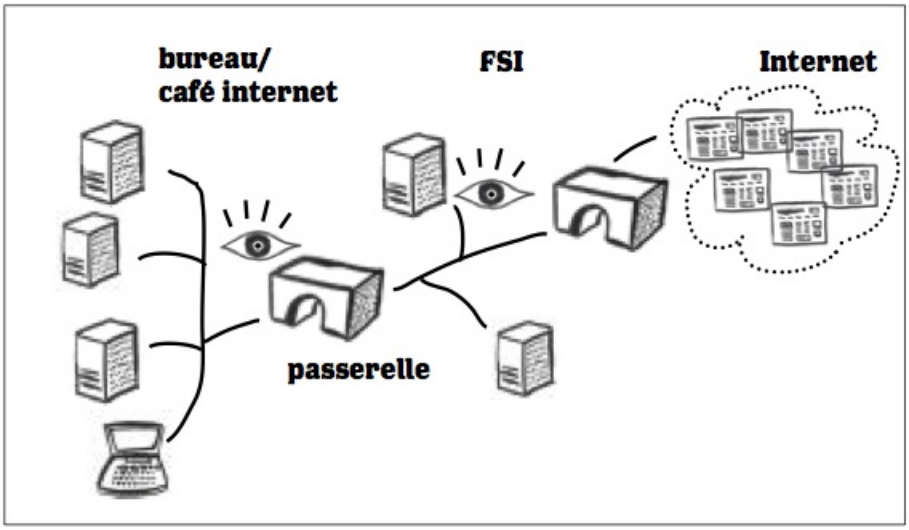
Comprendre la censure sur Internet

Des recherches menées par des organismes comme OpenNet Initiative (ONI) [180] [1] et Reporters sans frontières (RSF) [181] [2] indiquent que plusieurs pays ont recours au filtrage d'un vaste éventail de contenus à caractère social ou politique (et/ou de renseignements étant rattachés au concept de « sécurité nationale »), sans toutefois publier des listes précises des contenus bloqués. Bien entendu, les agences qui souhaitent limiter l'accès de leurs citoyens à Internet font aussi de leur mieux pour bloquer les serveurs *proxy* [179] et les sites Internet qui offrent des outils et des instructions pour aider les utilisateurs à *contourner* [139] les mesures de filtrage.

Malgré le droit à l'information garanti par l'article 19 de la Déclaration universelle des droits de la personne, le nombre des pays qui emploient des mesures de censure sur Internet n'a pas cessé d'augmenter au cours des quelques dernières années. Alors que le filtrage des contenus sur Internet est de plus en plus répandu, il en va de même des techniques et outils de contournement créés, déployés et distribués par des activistes, des programmeurs et des bénévoles un peu partout dans le monde.

Avant d'explorer les diverses méthodes par lesquelles il est possible de contourner la censure sur Internet, vous devriez d'abord avoir une bonne compréhension du fonctionnement de ces filtres. Pour ce faire, il est utile de se représenter un modèle simplifié de votre connexion Internet.

Votre connexion Internet



La première étape de votre connexion à Internet est habituellement le lien qui est établi par votre *fournisseur de services Internet (FSI)* [129] à votre domicile, bureau, école, bibliothèque ou café Internet. Le FSI assigne à votre ordinateur une *adresse IP* [132], que divers services Internet utilisent pour vous identifier et vous transmettre de l'information, tel que les courriels et les sites Internet que vous cherchez. Quiconque connaît votre adresse IP peut plus ou moins facilement déterminer dans quelle ville vous vous trouvez. Certaines agences influentes dans votre pays peuvent même utiliser ce renseignement pour déterminer très exactement votre position.

- **Votre FSI** peut déterminer à quelle adresse vous êtes situé ou quelle ligne téléphonique vous utilisez si vous accédez à Internet via un modem.
- **Le café Internet, la bibliothèque ou le commerce privé d'où vous travaillez** peut déterminer quel ordinateur vous utilisez à tel ou tel moment, ainsi que le port ou le point d'accès sans-fil par lequel vous êtes connecté.
- **Les agences gouvernementales** peuvent facilement obtenir ces renseignements, du fait de leur influence sur ces organismes.

À ce point, votre FSI s'en remet à l'infrastructure du réseau existant dans votre pays pour connecter ses utilisateurs, vous y compris, au reste du monde. À l'autre bout de la connexion, le site ou le service Internet auquel vous accédez a dû passer par un processus similaire, ayant lui aussi reçu des adresses IP de la part d'un FSI dans le pays où il est hébergé. Même sans plus de détails techniques, un modèle simplifié comme celui-là pourra vous être utile pour tenir compte des différents outils qui permettent de contourner les filtres tout en restant anonyme sur Internet.

Comment les sites Internet sont-ils bloqués

Essentiellement, lorsque vous souhaitez visiter une page Web, vous indiquez l'adresse IP du site en question à votre FSI et vous lui demandez d'établir une connexion entre vous et le FSI du serveur Web où est hébergé ce site. Si vous avez une connexion Internet non filtrée, c'est précisément ce qu'il fera. Par contre, si vous vous trouvez dans un pays qui exerce de la censure sur Internet, il consultera d'abord une « *liste noire* [177] » de sites interdits et déterminera ensuite s'il peut consentir ou non à votre requête.

Dans certains cas, c'est une agence centrale, et non pas les FSI, qui s'occupe du filtrage. La plupart du temps, une « liste noire » contient des *noms de domaine* [178], comme www.blogger.com [182], plutôt que des adresses IP. Dans certains pays, des logiciels de filtrage contrôlent carrément votre connexion au lieu de bloquer votre accès à certaines adresses en particulier. Ce type de programme balaie toutes les requêtes que vous effectuez (et tous les sites Internet qui tentent de vous répondre) afin de détecter certains mots-clé et, selon ses conclusions, décider si vous pouvez ou non voir les résultats de vos requêtes.

Pire encore, lorsqu'un site Internet est bloqué, il est fort possible que vous ne le sachiez même pas. Alors que certains filtres présentent une « page de blocage », qui vous explique pourquoi une page en particulier a été censurée, d'autres affichent des messages d'erreur pour tromper les utilisateurs. Ces messages indiquent que la page ne peut être trouvée, par exemple, ou qu'il y a une erreur dans l'adresse.

En général, quand il est question de censure sur Internet, il est plus simple d'adopter une attitude carrément « pessimiste » que d'étudier attentivement toutes les forces et les faiblesses des technologies de filtrage utilisées dans votre pays. En d'autres termes, vous avez avantage à tenir pour acquis que :

- Quelqu'un contrôle vos activités sur Internet pour détecter certains mots-clé ;
- Le filtrage se produit directement au niveau du FSI ;
- Les sites bloqués sont mis à l'index selon leurs adresses IP et leurs noms de domaine ;
- Il est fort probable que l'on vous fournisse une raison ambiguë ou trompeuse pour expliquer pourquoi la connexion à un site donné a échoué.

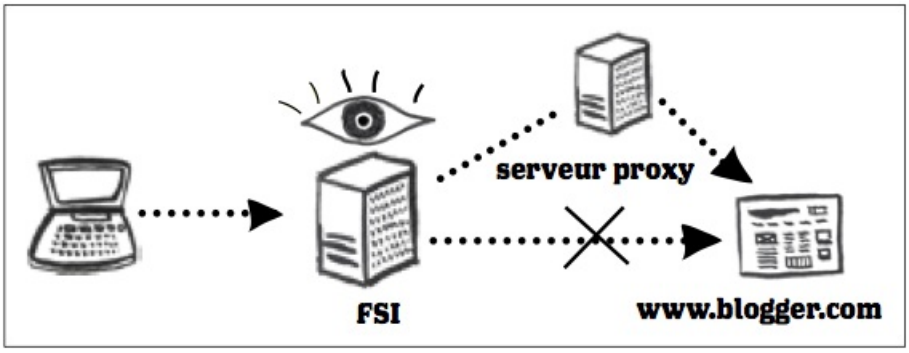
Comme les outils de contournement les plus efficaces peuvent aussi bien être utilisés contre l'une ou l'autre de ces méthodes de filtrage, il est en fait plutôt utile d'adhérer à ces hypothèses « pessimistes ».

Mansour : Alors, si un jour ou l'autre je ne peux plus accéder au blog, mais qu'un camarade dans un autre pays y parvient toujours, est-ce que cela signifie que le gouvernement a finalement réussi à le bloquer ?

Magda : Pas nécessairement. Il est possible qu'un problème d'une toute autre nature touche uniquement les utilisateurs qui tentent de joindre le site à partir d'ici. Il peut aussi s'agir d'un problème avec ton ordinateur qui ne survient qu'avec certains types de pages Web. Cela dit, tu es sur la bonne voie. Pour en avoir le cœur net, tu devrais essayer de visiter le site à l'aide d'un outil de contournement. Après tout, la plupart de ces programmes reposent sur l'utilisation de serveurs proxy externes, ce qui revient à peu près à demander à un ami à l'étranger de tester le site pour toi, sauf que tu le fais toi-même.

Comprendre le contournement de la censure

Si vous ne pouvez pas établir une connexion directe à un site parce qu'il est bloqué par l'une des méthodes présentées ci-dessus, il vous faudra trouver un moyen pour *contourner* [139] l'obstruction. Un serveur *proxy* [179] sûr, situé dans un pays qui ne filtre pas l'Internet, peut vous permettre ce type de contournement en allant chercher pour vous les pages auxquelles vous voulez accéder. Du point de vue de votre *FSI* [129], vous donnerez simplement l'impression d'avoir établi une communication sécurisée avec un ordinateur inconnu (le serveur proxy) quelque part sur Internet.



Bien sûr, l'agence gouvernementale responsable de la censure dans votre pays (ou la compagnie qui fait les mises à jour des programmes de filtrage) pourrait éventuellement découvrir que cet « ordinateur inconnu » est en réalité un proxy de contournement. Si cela se produit, l'*adresse IP* [132] du proxy pourrait être ajoutée à la « *liste noire* [177] » et, le cas échéant, ce dernier cessera de fonctionner pour vous. Cela dit, il faut habituellement un certain temps avant que les serveurs proxy ne soit identifiés et bloqués, et les gens qui conçoivent et améliorent ces outils sont au fait de ces risques. En général, ils se défendent en ayant recours à l'une ou l'autre des méthodes suivantes :

- Les **proxys cachés** sont plus difficile à identifier que les proxys normaux. C'est l'une des raisons pour lesquelles il est important d'utiliser des proxys sécurisés, lesquels sont habituellement plus discrets. Cependant, le *chiffrement* [41]

n'est qu'une partie de la solution. Les administrateurs d'un proxy, s'ils veulent que ce dernier reste caché, doivent être très prudents lorsqu'ils en révèlent l'emplacement à de nouveaux utilisateurs.

- Les **proxys jetables** peuvent facilement être remplacés lorsqu'ils sont bloqués. Il n'est pas particulièrement sécuritaire d'indiquer publiquement aux utilisateurs où ils peuvent trouver des proxys de rechange. C'est pourquoi les outils de contournement de ce type, la plupart du temps, essaient tout simplement de déjouer les censeurs en distribuant les nouveaux proxys plus vite que ces derniers sont capables de les bloquer.

Au bout du compte, tant et aussi longtemps que vous serez en mesure de joindre un proxy pour chercher les services dont vous avez besoin, tout ce que vous aurez à faire est d'effectuer la requête et de visualiser les résultats à l'aide de l'application Internet appropriée. Habituellement, les détails de ce processus sont gérés soit automatiquement par le logiciel de contournement que vous installez sur votre ordinateur, soit en modifiant les paramètres de votre navigateur, ou encore en pointant votre navigateur vers la page d'un proxy basé sur le Web. Le réseau de connexion anonyme *Tor* [137], abordé à la prochaine section, utilise la première méthode. Après cela, nous verrons quelques outils de contournement par proxy unique, dont le fonctionnement varie légèrement d'un modèle à un autre.

Les réseaux de connexion anonyme et les proxys uniques

Les réseaux de connexion anonyme

Les réseaux de connexion anonyme font généralement « rebondir » votre connexion entre plusieurs *proxys* [179] sécurisés pour occulter l'origine de vos requêtes et la nature des sites que vous tentez de joindre. Cela peut réduire considérablement la vitesse à laquelle vous pourrez charger des sites ou accéder à des services Internet. Par contre, le programme *Tor* [137] offre un moyen de *contournement* [139] sûr, fiable et public, dont l'utilisation toute simple vous épargne beaucoup d'inquiétude. Comme toujours, vous devez vous assurer que votre connexion à un site Internet donné soit sécurisée (avec le HTTPS) avant de commencer à échanger des renseignements sensibles comme des mots de passe et des courriels par l'intermédiaire d'un navigateur.

Pour utiliser Tor, il vous faudra installer le logiciel, mais vous serez ensuite en mesure de préserver votre anonymat, en plus de contourner efficacement les mesures de censure. Chaque fois que vous vous connectez au réseau Tor, vous passez par un chemin complètement aléatoire, par le truchement de trois proxys Tor sécurisés. Cela vous assure que ni votre *FSI* [129], ni les proxys eux-mêmes, ne soient en mesure de connaître à la fois l'*adresse IP* [132] de votre ordinateur et la position des services Internet que vous recherchez. Pour plus d'information au sujet de ce programme, veuillez consulter le ***Guide pratique Tor*** [183].

Expérience pratique : se lancer avec le *Guide pratique Tor* [183]

Une des plus grandes forces du programme Tor est qu'en plus de pouvoir être utilisé avec un navigateur, il est compatible avec d'autres logiciels. Des clients de messagerie comme *Mozilla Thunderbird* [93] et des programmes de messagerie instantanée comme *Pidgin* [123] fonctionnent très bien avec Tor, que ce soit pour accéder à des services filtrés ou pour occulter votre utilisation de ces services.

Proxys de contournement uniques

Il y a trois éléments essentiels dont vous devez tenir compte au moment de choisir un proxy de contournement unique. Premièrement, s'agit-il d'un outil basé sur le Web, ou devez-vous plutôt modifier des paramètres ou installer un logiciel sur votre ordinateur ? Deuxièmement, est-ce un service sécurisé ? Troisièmement, est-ce un service privé ou public ?

Proxys Web et autres types de proxys :

Les proxys Web sont probablement les plus faciles à utiliser. Vous n'avez pour ce faire qu'à pointer votre navigateur vers la page du proxy, saisir l'adresse filtrée que vous souhaitez visiter et cliquer sur un bouton. Le proxy affichera alors le contenu de la page filtrée à l'intérieur de sa propre page. Vous pouvez aussi suivre les hyperliens ou saisir une nouvelle adresse dans le proxy si vous souhaitez visualiser une autre page. Vous n'avez aucun logiciel à installer ni aucun paramètre à modifier dans votre navigateur, ce qui signifie que les proxys Web sont :

- Faciles à utiliser ;
- Joignables à partir d'ordinateurs publics (par exemple les ordinateurs d'un café Internet) qui ne vous permettent pas, en temps normal, d'installer des logiciels ou de modifier des paramètres ;
- Possiblement plus sûrs que d'autres méthodes si vous craignez d'être « pris » avec des programmes de contournement sur votre ordinateur.

Les proxys Web comportent néanmoins certains inconvénients. Ils n'affichent pas toujours les pages correctement et plusieurs proxys Web sont tout simplement incapables de charger les sites Internet complexes et les flux de données

audio et vidéo. De plus, malgré que tous les proxys tendent à ralentir proportionnellement au nombre d'utilisateurs qui s'y connectent, ce désagrément est encore plus prononcé avec les proxys Web publics. Par ailleurs, les proxys Web ne fonctionnent évidemment qu'avec les pages Web. Vous ne pouvez pas, par exemple, utiliser un programme de messagerie instantanée ou un client de messagerie pour accéder à certains services bloqués via un proxy Web. Finalement, les proxys Web sécurisés ne peuvent offrir qu'une confidentialité limitée parce qu'ils doivent eux-mêmes intercepter et modifier les données qui vous sont envoyées par les sites que vous visitez. S'ils ne le faisaient pas, vous ne pourriez pas cliquer sur un lien sans automatiquement quitter le proxy pour tenter d'établir une connexion directe à la page Web visée. Nous reviendrons sur ce détail à la prochaine section.

Les autres types de proxys exigent habituellement que vous installiez un programme ou que vous configuriez une adresse de proxy externe dans les paramètres de votre navigateur ou de votre système d'exploitation. Dans le premier cas, le programme de contournement vous offre habituellement la possibilité d'activer et de désactiver l'outil pour indiquer à votre navigateur d'utiliser ou non le proxy. Souvent, ces logiciels vous permettent également, lorsqu'un proxy est bloqué, d'en trouver automatiquement un nouveau (comme nous avons vu ci-dessus). Dans le second cas, vous devrez apprendre à utiliser la bonne adresse de proxy, laquelle doit être modifiée si ledit proxy est bloqué ou s'il ralentit tellement qu'il en devient inutilisable.

Bien qu'elle soit légèrement plus difficile à utiliser qu'un proxy Web, cette méthode est plus susceptible d'afficher des pages complexes correctement. Elle devrait également rester efficace plus longtemps avant de commencer à ralentir en raison du nombre élevé d'utilisateurs qui s'y connectent. De plus, différents proxyspeuvent être utilisés pour divers types d'applications Internet. Il existe par exemple des proxys HTTP pour les navigateurs, des proxys SOCKS pour les programmes de courriel et de messagerie instantanée et des proxys VPN, qui peuvent être utilisés pour rediriger la totalité de vos activités sur Internet afin d'éviter le filtrage.

Proxys sécurisés et proxys non sécurisés :

Un proxy sécurisé, dans ce chapitre, désigne tout proxy qui donne la possibilité aux utilisateurs d'établir des connexions *chiffrées* [41]. Un proxy non sécurisé vous permettra tout de même de contourner plusieurs types de filtrage, mais vous sera moins utile si votre connexion Internet est l'objet d'une recherche de mots-clé ou d'adresses Web ciblées. C'est une idée particulièrement mauvaise d'utiliser un proxy non sécurisé pour accéder à des sites Internet habituellement chiffrés, comme des comptes de webmail ou des sites de services bancaires. En faisant cela, il est possible que vous exposiez des renseignements sensibles qui seraient normalement restés cachés. De plus, comme nous l'avons vu ci-dessus, les proxys non sécurisés sont plus faciles à identifier et à bloquer que les proxys sécurisés pour ceux dont c'est le travail d'actualiser les logiciels de filtrage. En fin de compte, le fait qu'il existe d'excellents proxys gratuits, rapides et sécurisés signifie qu'il y a très peu de raisons valides d'employer un proxy non sécurisé.

Vous pouvez déterminer si un proxy Web est sécurisé ou non en tentant de vous connecter au site du proxy avec une adresse HTTPS. Tout comme avec les services webmail, il est possible que les connexions sécurisées et non sécurisées soient toutes deux possibles. C'est pourquoi vous devriez toujours vous assurer d'utiliser l'adresse sécurisée. La plupart du temps, dans de tels cas, vous devez accepter un « *certificat de sécurité* [131] » (exigé par votre navigateur) afin de continuer. Tel est le cas du proxy *Peacefire* [184], abordés ci-dessous. Les avertissements de votre navigateur concernant les certificats de sécurité vous indiquent que quelqu'un, comme votre FSI ou un *pirate informatique* [18], pourrait être en train de contrôler votre connexion au proxy. Malgré l'utilité de ces avertissements, il est toujours conseillé d'utiliser, autant que possible, des proxys sécurisés. Par contre, lorsque votre méthode de contournement dépend exclusivement d'un proxy de ce type, vous devriez éviter de visiter des sites Internet sécurisés, de saisir des mots de passe ou d'échanger des renseignements sensibles, à moins que vous ne soyez en mesure de vérifier l'authenticité de la signature *SSL* [130] du proxy. Pour ce faire, vous aurez besoin d'une voie de communication avec l'administrateur du proxy.

L'annexe C du Guide de l'utilisateur de Psiphon [3] explique les étapes que vous et l'administrateur du proxy devez suivre pour vérifier l'empreinte numérique du proxy.

Vous devriez également éviter d'accéder à des données sensibles par le truchement d'un proxy Web, à moins que vous ne fassiez totalement confiance à son administrateur. Cette mesure de précaution s'impose, que vous receviez ou non un avertissement de certificat de sécurité lorsque vous visitez le proxy. Elle s'impose même si vous connaissez assez bien l'administrateur du proxy pour vérifier l'empreinte du serveur avant d'indiquer à votre navigateur d'accepter le certificat de sécurité. Lorsque vous dépendez d'un serveur proxy unique pour contourner les mesures de filtrage, les administrateurs dudit proxy connaîtront votre adresse IP et les sites Web que vous visitez. Qui plus est, si ce proxy est basé sur le Web, un administrateur malveillant pourrait facilement accéder à toutes les données qui circulent entre votre navigateur et les sites Internet que vous visitez, y compris le contenu de vos courriels et vos mots de passe.

Quant aux proxys non Web, vous devrez peut-être effectuer quelques recherches pour déterminer si les connexions sécurisées sont permises ou non. Tous les proxys et réseaux de connexion anonyme recommandés dans ce chapitre sont sécurisés.

Proxys privés et proxys publics :

Les proxys publics acceptent des connexions de n'importe qui, alors que les proxys privés exigent habituellement un nom d'utilisateur et un mot de passe. Bien que les proxys publics comportent l'avantage évident d'être librement accessibles, dans la mesure où on peut les trouver, ils tendent bien souvent à être rapidement très achalandés. En conséquence, même si les proxys publics sont aussi sophistiqués et bien administrés que les proxys privés, ils sont souvent plutôt lents. Finalement, les proxys privés sont habituellement gérés soit par des entreprises commerciales, soit par des administrateurs qui créent des comptes pour les utilisateurs qu'ils connaissent personnellement ou socialement. Il est donc assez facile, dans la majorité des cas, de déterminer les motivations des administrateurs de proxys privés. Vous ne

devriez pas tenir pour acquis, cependant, que les proxys privés sont plus dignes de confiances que leurs pendants publics. Après tout, il est déjà arrivé que l'appât du profit mène les administrateurs de certains services numériques à dénoncer leurs utilisateurs.

Des proxys publics uniques non sécurisés peuvent souvent être trouvés en exécutant une recherche avec des mots-clé comme « public proxy » dans un moteur de recherche, mais vous ne devriez pas vous fier aux services trouvés de cette manière. Si vous avez le choix, il est préférable d'utiliser un proxy privé sécurisé, administré par des gens que vous connaissez (personnellement ou de réputation) et en qui vous avez confiance, et qui ont les aptitudes techniques nécessaires pour préserver la sécurité de leur serveur. Votre choix d'utiliser ou non un proxy Web dépendra de vos besoins particuliers et de vos préférences personnelles. Chaque fois que vous utilisez un proxy pour contourner des mesures de censure, il est fortement conseillé d'employer le navigateur *Firefox* [14] et d'installer le module complémentaire *NoScript* [15], tel qu'indiqué dans le ***Guide pratique Firefox*** [17]. Cela vous protégera contre les proxys malveillants et les sites Internet qui pourraient tenter de découvrir votre vraie adresse IP. Finalement, n'oubliez pas qu'un proxy chiffré ne transformera pas magiquement un site non sécurisé en site sécurisé. Vous devez toujours vous assurer d'avoir établi une connexion HTTPS avant d'envoyer ou de recevoir des renseignements sensibles.

Si vous n'êtes pas en mesure de trouver un individu, un organisme ou une compagnie dont le service de proxy vous semble digne de confiance, abordable et facilement accessible depuis votre pays, vous devriez sérieusement considérer l'utilisation du réseau de connexion anonyme Tor, que nous avons brièvement abordé ci-dessus, à la section ***Réseaux de connexion anonyme***.

Proxys de contournement particuliers

Voici quelques outils et *proxys* [179] particuliers qui pourront vous aider à *contourner* [139] le filtrage sur Internet. De nouveaux programmes de contournement sont conçus régulièrement et ceux qui ont déjà fait leurs preuves sont constamment améliorés. Nous vous invitons donc à visiter le site Internet de Security in-a-Box, ainsi que les sites mentionnés à la section ***Lecture complémentaire*** [185], ci-dessous.

Proxys de type VPN (Réseau privé virtuel)

Voici une liste de proxys de type VPN qui feront passer toute votre connexion Internet par le proxy lorsque vous êtes « connecté ». Cela peut être utile si vous utilisez des services de messagerie instantanée ou électronique qui sont filtrés dans votre pays.

Riseup VPN est destiné aux utilisateurs dont le compte de messagerie se trouve sur le serveur *Riseup*. Le collectif offre la possibilité de se connecter à un serveur proxy de type VPN gratuit, sécurisé, privé. Merci de consulter le site de *Riseup VPN pour plus d'infos* [186] générales et sur *la façon de s'y connecter* [187].

Hotspot Shield est un gratuiciel de contournement public, sécurisé et VPN. Pour l'utiliser, il faut *télécharger l'outil* [188] et l'installer. La société qui développe Hotspot Shield obtient des revenus de la publicité, alors vous verrez des banderoles publicitaires dans le haut de votre navigateur lorsque vous utiliserez ce logiciel pour visiter des sites internet non sécurisés. De plus, il est impossible de corroborer l'affirmation de la société à l'effet qu'elle supprime les *adresses IP* [132] des utilisateurs du logiciel au lieu de les archiver ou de les refiler au acheteurs de publicité.

Your-Freedom est un proxy de contournement privé, sécurisé et VPN/SOCKS. C'est un gratuiciel qui peut être employé pour accéder à un service de contournement gratuit. Le débit binaire ainsi que le temps d'utilisation (3 heures par jour jusqu'à 9 heures par semaine) y sont limités. Vous pouvez également payer un tarif modique pour accéder à un service commercial plus rapide et moins limité. Pour utiliser Your-Freedom, vous devrez *télécharger l'outil* [189] et *créer un compte* [190], deux opérations que vous pouvez effectuer à partir du *site Internet de Your-Freedom* [191]. Vous devrez également configurer votre navigateur afin d'utiliser le proxy *OpenVPN* [192] lorsque vous vous connecterez à Internet. Merci de consulter le site de *documentation de Your-Freedom pour plus d'infos* [193].

Freegate est un proxy de contournement gratuit, privé, sécurisé et VPN. Vous pouvez télécharger la dernière version de Freegate [190] et consulter des articles informatifs [194] à ce sujet.

SecurityKISS est un proxy de contournement gratuit, privé, sécurisé et VPN. Pour l'utiliser, vous devez télécharger et exécuter un programme gratuit [195]. Il n'est pas nécessaire de créer un compte. Les utilisateurs gratuits sont limités à une utilisation de 300MB par jour ainsi que par un trafic plus important sur internet via le proxy. Les abonnements payants offrent une utilisation sans restrictions et plus de serveurs VPN..

Psiphon3 est un outil public de contournement qui utilise la technologie VPN, SSH et HTTP Proxy et qui vous permet de contourner la censure sur internet. Pour l'utiliser, vous devez télécharger le programme sur la *page d'accueil Psiphon3* [196] et le lancer pour sélectionner le mode que vous souhaitez utiliser *VPN, SSH, SSH+*. Psiphon3 fonctionne aussi avec le système Androïd. Consultez-la page d'accueil [196] pour en savoir plus.

Proxys web

Peacefire entretient un vaste parc de proxys Web publics, qui peuvent être sécurisés ou non, selon la méthode que vous choisissez pour y accéder. Lorsque vous utilisez un proxy *Peacefire* [184], vous devez saisir manuellement ***https*** [130] dans la barre de navigation pour vous assurer que la connexion entre votre ordinateur et le proxy soit sécurisée. Les nouveaux

proxys sont annoncés régulièrement sur une liste de diffusion. Vous pouvez vous inscrire sur le *site internet de Peacefire* [197] pour recevoir des mises à jour régulières.

Lecture complémentaire

- Voir les chapitres *2.5 Internet Surveillance and Monitoring* et *2.6 Censorship circumvention* du manuel Digital Security and Privacy Manual for Human Rights Defenders [198].
- Un guide pratique intitulé How to Bypass Internet Censorship [199] est disponible sur le site Internet des FLOSS Manuals.
- Le Internet Censorship Wiki [200] , rédigé par Freerk, est disponible en anglais, en allemand et en espagnol.
- CitizenLab a produit un guide intitulé Everyone's guide to by-passing Internet Censorship [201] actuellement en cours de traduction vers le birman, l'anglais, le français, le russe, l'espagnol et l'urdu.
- L'organisme Reporters sans frontières en est à la seconde édition de son Guide pratique du blogger et du cyberdissident [202] disponible en arabe, birman, chinois, anglais, farsi, français, russe et espagnol.
- Ethan Zuckerman, de Global Voices Online, a publié un guide pratique intitulé Anonymous Blogging with Wordpress and Tor [203].

9. Savoir se protéger sur les sites de réseautage social

Les communautés en ligne existent depuis les tous débuts d'Internet. Il y a d'abord eu les babillards électroniques, puis les listes de diffusion, qui ont permis à des millions de personnes de partout sur la planète d'entrer en contact les unes avec les autres, de communiquer et de partager de l'information sur des intérêts communs. De nos jours, en permettant aux utilisateurs de partager instantanément des messages, des photos, des fichiers et des mises à jour en temps réel de leurs activités et déplacements, les nouveaux sites de réseautage social ont considérablement accru la gamme des interactions possibles sur Internet. Ces fonctions ne sont cependant pas nouvelles ou uniques, car il est possible de mener chacune de ces actions sur Internet sans pour autant s'inscrire à un site de réseautage social.

Même si ces réseaux peuvent être utiles à plusieurs égards et faciliter les interactions sociales, autant en ligne que dans la vie réelle, leur utilisation peut rendre certains de vos renseignements considérablement vulnérables. Figurez-vous un site de réseautage social comme une immense réception. Il y a là des gens que vous connaissez bien, mais d'autres que vous ne connaissez pas du tout. Imaginez-vous déambuler parmi les invités avec un écriteau collé au dos où sont inscrites toutes vos coordonnées personnelles (ainsi que des mises à jour de minute en minute de vos réflexions intimes !), de telle sorte que tout le monde puisse les lire sans même que vous vous en rendiez compte. Voulez-vous vraiment que tout le monde sache tout à votre sujet ?

N'oubliez pas que les sites de réseautage social sont la propriété de sociétés privées. Ces dernières font de l'argent en recueillant des renseignements sur les utilisateurs de leurs services et en revendant ces données à des annonceurs commerciaux. Lorsque vous vous connectez à un site de réseautage social, vous abandonnez les libertés qu'offrent l'Internet pour pénétrer dans un réseau privé gouverné et réglementé par les propriétaires du site. Les paramètres de confidentialité ne vous protègent que des autres membres du réseau social ; ils ne vous mettent pas à l'abri des propriétaires du service. En fait, en créant un compte, vous confiez tous vos renseignements personnels à ces derniers et n'avez d'autre choix que de leur faire confiance.

Si vous manipulez des renseignements sensibles ou travaillez sur des enjeux sensibles, mais êtes tout de même intéressé à utiliser les services de réseautage social, il est très important que vous soyez conscient des problèmes de sécurité et de confidentialité que cela implique. Les défenseurs des droits de la personne sont particulièrement vulnérables aux dangers que posent les sites de réseautage social et doivent conséquemment être très prudents avec les renseignements qu'ils dévoilent à propos d'eux-mêmes et des gens avec qui ils travaillent. Avant d'utiliser les sites de réseautage social, il importe de comprendre les risques auxquels ceux-ci vous exposent et d'appliquer les mesures nécessaires pour vous protéger, vous et les personnes avec qui vous travaillez. Ce guide vous aidera à comprendre les enjeux de sécurité liés à l'utilisation des sites de réseautage social.

Scénario de départ :

Mansour et Magda se portent à la défense des droits de la personne dans un pays d'Afrique du Nord. Ils organisent une marche qui doit bientôt avoir lieu au centre de la plus grande ville du pays. Ils veulent utiliser Facebook pour faire la promotion de leur événement, mais ils ont peur que les autorités en soient informées et soient ensuite en mesure d'identifier les personnes qui ont signalé leur intérêt. Ils ont également l'intention d'utiliser Twitter pendant la marche pour diffuser des mises à jour sur sa progression. Mais si la police surveille leurs *tweets*, ne peut-elle pas s'en servir pour déployer ses forces et intercepter les manifestants ? Mansour et Magda veulent également partager des photos et vidéos de la manifestation, mais sont soucieux de préserver la confidentialité des participants pour éviter que ceux-ci deviennent la cible de persécutions.

Le but de ce chapitre n'est pas de vous inciter à renoncer complètement aux services de réseautage social. Par contre, il est nécessaire que vous preniez les mesures appropriées pour éviter que ces outils vous exposent à des risques inutiles, vous et les personnes avec qui vous interagissez.

Qu'apprendrez-vous dans ce chapitre

- Comment les sites de réseautage social facilitent la fuite involontaire de renseignements privés ou sensibles.
- Comment protéger les renseignements qui vous concernent, vous et les personnes avec qui vous interagissez, lorsque vous utilisez des sites de réseautage social.

Conseils généraux concernant l'utilisation des outils de réseautage social

Demandez-vous toujours :

- Qui peut voir l'information que je mets en ligne ?
- Qui est propriétaire de l'information que je publie sur le site de réseautage social ?
- Quels renseignements à mon sujet mes contacts peuvent-ils transférer à d'autres parties ?
- Est-ce que mes contacts sont à l'aise avec le fait que je partage leurs renseignements avec d'autres ?

- Fais-je bien confiance à toutes les personnes avec qui je suis en réseau ?

- Assurez-vous de toujours employer des **mots de passe sûrs** pour vous connectez à des réseaux sociaux. Si quelqu'un d'autre arrive à se connecter à votre compte, cette personnes accèdera directement à une banque de renseignements à votre sujet et au sujet de toutes les personnes avec qui vous êtes connecté par l'interface de ce réseau. Changez de mots de passe régulièrement ; faites en un routine. Veuillez consulter le chapitre 3. Créer et sauvegarder des mots de passe sûrs [140] pour plus d'information à ce sujet.

- Assurez-vous de bien comprendre les **paramètres de confidentialité** établis par défaut sur les sites de réseautage social. Sachez aussi les modifier en conséquence.

- Envisagez la possibilité d'utiliser **des comptes/identités différents** (ou d'adopter différents pseudonymes) pour vos différentes campagnes et activités. N'oubliez pas que la considération la plus importante, pour utiliser ces réseaux de façon sûre, est de pouvoir faire confiance à ses membres. La création de comptes séparés peut s'avérer un bon moyen d'atteindre un bon niveau de confiance.

- Faites très attention lorsque vous vous connectez à un réseau social sur Internet à partir d'un point d'accès public. **Supprimez vos historiques de mots de passe et de navigation** lorsque vous accédez à Internet depuis un lieu public. À ce sujet, voir le chapitre 6. Détruire définitivement des données sensibles [80].

- **N'accédez aux sites de réseautage social qu'avec le protocole https://** pour protéger vos noms d'utilisateur, vos mots de passe et les autres renseignements que vous y publiez. L'utilisation de https:// plutôt que http:// ajoute un élément de sécurité supplémentaire en chiffrant le trafic entre votre navigateur et le site de réseautage social. À ce sujet, voir le chapitre 8. Préserver votre anonymat et contourner la censure sur Internet [149].

- Faites attention aux renseignements que vous publiez dans **votre statut**. Même si vous faites confiance aux personnes de votre réseau, il est facile de recopier les items que vous publiez.

- La plupart des réseaux sociaux permettent à leurs utilisateurs d'intégrer leur contenu avec d'autres réseaux. Par exemple, il est possible de publier une mise à jour depuis votre compte Twitter et de faire en sorte qu'il soit automatiquement repris sur votre compte Facebook. **Faites particulièrement attention lorsque vous intégrez les contenus de vos différents comptes de réseau sociaux !** Il est possible que vous soyez anonyme sur un site mais complètement exposé sur un autre.

- Soyez soucieux de la sécurité de vos contenus sur les sites de réseautage social. **Ne vous fiez jamais aux sites de réseautage social comme principal support de vos contenus** ou de vos renseignements. Pour les agences gouvernementales, il est très facile de bloquer l'accès aux services de réseautage social à l'intérieur de leurs frontières nationales si elles jugent que certains contenus sont répréhensibles. Les administrateurs des réseaux sociaux peuvent aussi décider de retirer certains contenus qu'ils jugent répréhensibles, plutôt que de subir la censure dans un pays donné.

Publier des renseignements personnels

Lorsque vous créez un compte, les sites de réseautage social vous demandent une grande quantité de renseignements à votre sujet pour aider les autres utilisateurs à entrer en contact avec vous. Le plus grand risque que cela entraîne pour les utilisateurs de ces sites est la possibilité de vol d'identité, une pratique qui est de plus en plus répandue. Par ailleurs, plus vous dévoilez d'information à votre sujet, plus il est facile aux autorités de vous identifier et d'épier vos activités. Il est déjà arrivé que les activités en ligne de militants de la diaspora de certains pays aient entraîné la persécution des membres de leurs familles dans leur pays d'origine.

Pensez-y bien : est-il vraiment nécessaire de publier les renseignements suivants en ligne ?

- Votre date de naissance
- Votre numéro de téléphone

- Votre adresse
- Des détails concernant les membres de votre famille
- Votre orientation sexuelle
- Votre historique d'éducation et d'emploi

Mansour : Notre amie vient d'être interpellée à la frontière et placée de force sur un vol de retour vers son pays. Les agents frontaliers lui ont demandé si elle avait écrit un article critique du régime. Comment peuvent-ils être au courant si son article n'a pas été publié dans ce pays ?

Magda : Les agents frontaliers effectuent des recherches sur Internet des noms des personnes qui passent aux frontières. Ils ont probablement vu le CV qu'elle a affiché sur son compte Facebook.

Amis, abonnés et contacts

La première chose que l'on fait après avoir fourni ses renseignements personnels sur un site de réseautage social est de chercher des personnes avec qui établir des connexions. On suppose que ces contacts sont des gens que vous connaissez et en qui vous avez confiance, mais il est également possible que vous vous joigniez à une communauté virtuelle composée d'individus avec qui vous avez des affinités mais que vous ne connaissez pas personnellement. La chose la plus importante à cette étape-ci est de déterminer à quels renseignements vous permettez à cette communauté virtuelle d'accéder.

Lorsque vous utilisez un compte de réseau social comme Facebook, où plusieurs renseignements à votre sujet sont affichés, considérez la possibilité de connecter exclusivement avec des personnes que vous connaissez et en qui vous avez totalement confiance (c.-à-d. des personnes qui ne feront pas un usage abusif de vos renseignements).

Mansour : Wow ! Depuis la manifestation, j'ai reçu des douzaines de demandes de personnes qui veulent être mon ami sur Facebook. C'est un moyen fantastique d'étendre notre portée et d'informer les gens de nos prochaines manifestations !

Magda : Attends un minute ! Est-ce que tu connais vraiment toutes ces personnes ? Comment peux-tu être sûr que ce n'est pas la police ou des agents du gouvernement qui essaient d'obtenir des renseignements au sujet des prochaines manifestations ?

Statuts

Sur Twitter, Facebook ou d'autres réseaux semblables, les mises à jour de statuts servent à répondre aux questions suivantes : Qu'est-ce que je fais maintenant ? Que se passe-t-il dans ma vie ? Le critère le plus important à déterminer au sujet des mises à jour du statut est la catégorie d'utilisateurs qui peuvent les lire. Dans la plupart des applications de réseautage social, les paramètres par défaut sont réglés de telle sorte que n'importe quel utilisateur d'Internet peut les lire. Si vous voulez plutôt faire en sorte que seuls vos contacts soient en mesure de consulter votre statut, vous devez modifier les paramètres de l'application pour cacher vos mises à jour à la vue de tous les autres utilisateurs.

Pour faire cela dans Twitter, cherchez le lien « Protéger mes tweets ». Dans Facebook, modifiez vos paramètres de confidentialité afin de partager vos statuts avec vos « Amis seulement ». Même si vous suivez ces indications, n'oubliez pas qu'il est facile pour vos amis et abonnés de re-publier vos commentaires. Entendez-vous avec les amis de votre réseau sur une méthode commune concernant le transfert des renseignements publiés sur vos comptes de réseaux sociaux respectifs. Dans le même ordre d'idée, vous devriez réfléchir aux renseignements que vous révélez au sujet de vos amis et que ceux-ci pourraient vouloir garder confidentiels. Il est important d'être sensible à ces questions et de demander à vos amis d'être également sensibles aux renseignements qu'ils dévoilent à votre sujet.

Il est déjà arrivé que des renseignements publiés par des utilisateurs de réseaux sociaux soient par la suite utilisés contre eux. Des enseignants aux États-Unis ont été congédiés après avoir confié leurs impressions au sujet de leurs étudiants ; d'autres employés ont perdu leur emploi après avoir publié des commentaires au sujet de leur employeur. C'est une question à laquelle pratiquement tout le monde doit faire très attention.

Partager du contenu Internet

Il est très facile d'attirer l'attention de vos amis en partageant de partager un lien vers un site Internet. Mais qui d'autre porte attention ? Et quelle sera leur réaction ? Si vous signalez que vous aimez un site qui, d'une manière ou d'une autre, est lié à une intention politique de défaire un régime répressif, les agents de ce régime pourraient soudainement s'intéresser à vous. Si vous voulez faire en sorte qu'uniquement vos amis soient en mesure de voir les éléments et les liens que vous marquez comme intéressants, assurez-vous de modifier vos paramètres de confidentialité en conséquence.

Révéler votre emplacement

La plupart des sites de réseautage social affichent votre emplacement si cette donnée est disponible. Cette fonction est habituellement fournie lorsque vous utilisez un téléphone mobile muni d'un GPS pour interagir avec un réseau social. Mais ne présumez pas qu'une telle chose est impossible si vous ne vous connectez pas à partir d'un téléphone mobile. Le réseau auquel votre ordinateur est branché peut également fournir des coordonnées d'emplacement. La meilleur façon d'en avoir le coeur net est de bien vérifier vos paramètres de confidentialité.

Faites particulièrement attention aux paramètres d'emplacement sur les sites de partage de photos et de vidéos. Ne tenez

pas pour acquis qu'ils ne partagent pas votre emplacement : vérifiez vos paramètres pour en être sûr.

À ce sujet, voir également On Locational Privacy, and How to Avoid Losing it Forever [204] sur le site Internet de Electronic Frontier Foundation.

Partager des photos/vidéos

Les photos et vidéos versées dans le domaine public peuvent très facilement servir à révéler l'identité des gens. Il est important que vous ayez le consentement des personnes qui figurent dans les photos ou vidéos que vous publiez en ligne. Si vous publiez l'image de quelqu'un, sachez que vous compromettez possiblement la confidentialité et la sécurité de cette personne. Ne publiez jamais une photo ou une vidéo d'une personne sans d'abord avoir obtenu son consentement.

Les photos et vidéos peuvent aussi révéler beaucoup d'information involontairement. Plusieurs modèles de caméra intègrent des données cachées (des balises méta) qui révèlent la date, l'heure et le lieu où la photo a été prise, le type de caméra, etc. Il est possible que les sites de partage de photos et de vidéos affichent ces données lorsque vous y téléversez du contenu.

Mansour : Savais-tu que les autorités birmanes ont été capables d'identifier plusieurs des prêtres impliqués dans les manifestations de la « Révolution safran » à l'aides des photos et vidéos publiées à l'étranger ? Toutes les personnes qu'ils ont réussi à identifier ont été jetées en prison.

Magda : Oui, nous devons nous assurer qu'aucun visage n'apparaît clairement sur les photos des manifestations que nous publions en ligne. Nous devrions brouiller les visages ou n'utiliser que les photos où on voit les personnes de dos.

Messageries instantanées

Plusieurs sites de réseautage social comportent des outils qui vous permettent de discuter avec vos amis en temps réel. Ces outils fonctionnent comme des messageries instantanées et constituent un des moyens les moins sûrs de communiquer sur Internet. Pour vous assurer que vos séances de messagerie instantanée soient sécurisées, vous et vos amis devriez vous connecter à vos comptes de réseau social par https://, ou mieux encore, utiliser un client de messagerie comme Pidgin avec le module complémentaire Off-the-Record, qui utilise une forme avancée de chiffrement. À ce sujet, veuillez lire le guide pratique 'Pidgin+OTR messagerie instantanée sécurisée'.

Créer/se joindre à des groupes, événements et communautés

Quelle information révélez-vous lorsque vous vous joignez à un groupe ou à une communauté ? Qu'est-ce que vous révélez à votre sujet ? Similairement, qu'est-ce que les gens révèlent à leur propre sujet lorsqu'ils se joignent à des groupes ou des événements que vous avez créés ? Est-il possible que vous placiez ces personnes en situation de risque ?

Lorsque vous vous joignez à un groupe ou à une communauté en ligne, cela révèle quelque chose à votre sujet. De façon générale, on pourrait être portés à croire que vous soutenez ou êtes d'accord avec ce que ce groupe dit ou fait. Cela peut vous rendre vulnérable si vous vous alignez ouvertement avec des groupes politiques contestataires, par exemple. Si vous vous joignez à un groupe qui compte un grand nombre de membres que vous ne connaissez pas, cela risque de compromettre les paramètres de sécurité et de confidentialité que vous avez établis pour votre compte. Réfléchissez bien aux renseignements que vous révélez avant de vous joindre à un groupe. Avez-vous utilisé votre photo et votre vrai nom, de sorte que des étrangers puissent facilement vous identifier ?

Similairement, si vous créez un groupe, qu'est-ce que les personnes qui choisissent de s'y joindre révèlent-elles à leur sujet ? Par exemple, s'il s'agit d'un groupe d'entraide pour gays et lesbiennes que vous avez créé pour soutenir cette cause, les membres du groupe s'identifient ouvertement comme gay ou « gay-friendly » et risquent peut-être de s'attirer des ennuis dans le monde réel. Il faut être conscient des risques.

Mansour : Nos amis syriens ne peuvent pas venir à notre conférence à Istanbul parce qu'ils se sont joints à un groupe Facebook appelé « Mettons fin à l'interdiction de voyager à l'étranger imposé par l'État syrien »... et ils se sont fait interdire de voyager !

Magda : Peut-être devrait-on créer un groupe avec le nom « Vive l'interdiction de voyager à l'étranger imposé par l'État syrien »... nos amis pourraient s'y joindre et l'interdiction serait peut-être levée !?

Expérience pratique: se lancer avec le *Guide pratique pour les outiles de résautage social* [205]

10. Utiliser votre téléphone mobile en sécurité (autant que possible...)

Les téléphones mobiles font désormais partie intégrante de nos communications quotidiennes. Tous les téléphones mobiles ont maintenant la possibilité d'envoyer et de recevoir des appels vocaux et des messages textes. Leur petit format, leur coût relativement bas et leurs multiples usages font de ces appareils des outils indispensables pour les défenseurs de droits de la personne, qui les utilisent de plus en plus pour communiquer et mener à bien leur travail.

Récemment, on trouve sur le marché des appareils munis de nombreuses nouvelles fonctions. On en trouve par exemple qui sont munis d'un GPS [206], de fonctions multimédia (photo, vidéo, enregistrement audio, et parfois même transmission de signal), traitement de données et accès à Internet. Par contre, le fonctionnement et l'infrastructure des réseaux de téléphonie mobile sont extrêmement différents du fonctionnement d'Internet. Cela donne lieu à de nouveaux défis en matière de sécurité et engendre de nouveaux risques pour la vie privée des utilisateurs et l'intégrité de leurs communications et de leurs renseignements.

Scénario de départ

Borna et son fils Delir sont tous deux ouvriers dans une usine et militent actuellement pour la création d'un syndicat. Les propriétaires de l'usine, qui ont des relations dans le gouvernement local, nuisent à leurs efforts. Le superviseur de Borna l'a averti qu'il était peut-être sous surveillance et qu'il devait faire très attention à qui il parlait. Borna a acheté un téléphone mobile pour son travail syndical. Delir aide son père à utiliser son nouveau mobile de façon sûre pour ses activités militantes.

Qu'apprendrez-vous dans ce chapitre

- Pourquoi les communications par téléphone mobile et le stockage de données sur les téléphones mobiles ne sont pas des pratiques sûres ;
- Comment accroître votre sécurité lorsque vous utilisez un téléphone mobile ;
- Comment minimiser les risques d'être espionné ou suivi à la trace par le truchement de votre téléphone mobile ;
- Comment augmenter les chances de préserver votre anonymat lorsque vous utilisez un téléphone mobile.

Les téléphones mobiles et la sécurité

Lorsqu'on utilise un téléphone mobile, il est important de prendre des décisions importantes en toute connaissance de cause. Cela est également important pour votre protection personnelle que pour celle de vos contacts et de vos données. Le fonctionnement et l'infrastructure des réseaux de téléphonie cellulaire ont une influence significative sur la faculté qu'ont les utilisateurs de préserver la sécurité et la confidentialité de leurs données et communications.

- Les réseaux de téléphonie cellulaire sont des réseaux privés administrés par des entités commerciales, qui peuvent ou non être sous le contrôle unique du gouvernement. L'entité commerciale (ou le gouvernement) dispose d'un accès pratiquement illimité aux renseignements et aux communications de ses clients. De plus, elle a la possibilité d'intercepter n'importe quel appel ou message texte et peut déterminer en tout temps l'emplacement de chaque appareil (et donc de son utilisateur).

- Les systèmes d'exploitation utilisés par les téléphones mobiles sont conçus sur mesure ou configurés par les fabricants, selon les spécifications imposées par les fournisseurs de services, pour être compatibles avec les réseaux privés de ces mêmes compagnies. En conséquence, les systèmes d'exploitation peuvent très bien comporter des fonctions cachées permettant au fournisseur de service un contrôle plus serré de chaque appareil branché à son réseau.

- Le nombre des fonctions incluses dans les téléphones mobiles a nettement augmenté au cours des dernières années. Les nouveaux appareils sont en fait des mini-ordinateurs portables capables de se connecter à Internet et présentant des fonctions de téléphonie mobile.

Afin de déterminer quels aspects de vos communications ont le plus besoin d'être protégés, il peut être utile de vous pencher sur un certain nombre de questions : Quel est le contenu et la teneur de vos appels vocaux et de vos messages textes ? Avec qui communiquez-vous, et à quelle occasion ? D'où appelez-vous ? Vos renseignements sont vulnérables de plusieurs façons :

- **Les renseignements sont vulnérables quand ils sont envoyés à partir d'un téléphone mobile**
  Exemple : Chaque fournisseur de service de téléphonie mobile a un accès illimité à tous les appels et messages textes transmis sur son réseau. Dans la plupart des pays, les fournisseurs de service ont l'obligation de conserver un registre de l'ensemble des communications effectuées sur leur réseau. Dans certains pays, les fournisseurs de service sont carrément sous le contrôle unique du gouvernement. Les appels vocaux et les messages textes peuvent également être placés sous écoute par une tierce partie située à proximité de l'appareil, à l'aide d'un équipement facilement accessible.

- **Les renseignements sont vulnérables à même les appareils respectifs de l'expéditeur et du destinataire**
  Exemple : Les téléphones mobiles peuvent stocker toutes sortes de données : l'historique des appels, les messages textes envoyés et reçus, les entrées au carnet d'adresses, des photos, clips vidéos, fichiers textes, etc. Ces données peuvent révéler vos contacts, ainsi que des renseignements personnels sur vous et vos collègues. Il est très difficile, voire impossible avec certains appareils, de sécuriser ces renseignements. Les plus récents modèles sont ni plus ni moins que des ordinateurs de poche. Avec ces fonctions additionnelles viennent malheureusement de plus grands risques. De plus, les appareils qui ont la possibilité de se connecter à Internet sont évidemment vulnérables aux menaces inhérentes aux ordinateurs et à l'Internet.

- **Les appareils révèlent leur emplacement**
  Exemple : Dans le cadre des opérations normales, chaque appareil de téléphonie mobile communique

automatiquement et régulièrement son emplacement au fournisseur de service. Qui plus est, plusieurs appareils comportent maintenant des fonctions GPS [206], et des données de position très précises peuvent être intégrées à d'autres données, comme aux photos, aux SMS et aux requêtes Web envoyées depuis le téléphone.

L'évolution de la technologie introduit de nouvelles fonctions mais entraîne également de nouveaux risques.

Borna : Mon fils, à partir de maintenant, j'ai décidé d'utiliser uniquement ce téléphone mobile pour organiser nos réunions. J'ai l'impression qu'ils ont placé le téléphone du plancher de l'usine sous écoute, et peut-être même notre téléphone à la maison. Delir : Père, c'est une bonne chose que tu aies enfin acquis un mobile, mais sais-tu ce que cet appareil peut et ne peut pas faire ? Borna : Bien sûr, c'est un téléphone ! On appelle quelqu'un, on lui parle et il nous répond. On peut faire ça peu importe où on se trouve. ET je peux envoyer des courts messages, à toi ou à d'autres, et ils vont apparaître sur ton téléphone.

Delir : Tout ça est vrai, mais ce n'est pas tout. De nos jours, il y a plusieurs autres choses qu'on peut faire avec ce type d'appareils. Mais parlons d'abord des risques et des précautions, surtout si tu as l'impression que quelqu'un est intéressé à savoir ce que tu dis et avec qui tu communiques.

La prochaine section aborde un certain nombre de moyens faciles que vous pouvez prendre pour réduire les risques de sécurité associés à l'utilisation d'un téléphone mobile.

La mobilité et la vulnérabilité des données

Les gens transportent souvent avec eux des téléphones mobiles qui contiennent des données sensibles. L'historique des communications, les messages textes et vocaux, les carnets d'adresses, les calendriers, les photos et plusieurs autres fonctions utiles peuvent sérieusement compromettre votre sécurité si le téléphone est perdu ou volé. Il est essentiel que vous soyez toujours conscient des renseignements qui sont stockés, passivement et activement, sur votre téléphone mobile. Les renseignements stockés sur un téléphone mobile peuvent compromettre la sécurité de la personne qui utilise l'appareil, mais également celle des personnes listées dans le carnet d'adresses ou dans la boîte de réception des messages, qui figurent dans l'album photo, etc.

Les téléphones qui ont la possibilité de se connecter à Internet sont également exposés aux risques et vulnérabilités associés à l'Internet et aux ordinateurs, comme nous l'avons vu dans les chapitres de ce livret portant sur la sécurité des données, l'anonymat, la récupération, la perte, le vol et l'interception de données.

Afin de réduire certains des risques de sécurité mentionnés ci-dessus, les utilisateurs devraient toujours être conscients des potentielles failles que présente leur appareil et configurer leurs options en conséquence. Une fois que vous avez cerné les problèmes potentiels, il est peut-être possible de mettre en place des moyens de sauvegarde et des mesures préventives appropriées.

Borna : Un des avantages du téléphone mobile est qu'ils ne pourront pas savoir où sont nos réunions si nous les organisons par téléphone mobile en marchant au marché, par exemple, alors qu'ils peuvent facilement tendre l'oreille ou nous placer sous écoute si nous utilisons un téléphone normal.

Delir : Et bien, ne m'as-tu pas dit qu'ils ont des relations au sein de la compagnie de téléphone ?

Borna : Quelqu'un m'a dit qu'ils soudoient les techniciens du téléphone pour obtenir des renseignements.

Delir : Si tu t'es inscrit au service de téléphonie mobile en utilisant ta propre adresse et ta propre identité, le téléphone est associé à ton nom, et chaque fois que tu place un appel, une entrée de registre est associée à ton compte et à ton identité. Père, t'es-tu inscrit avec ta propre identité ?

Borna : Non, j'ai pris un téléphone usagé à la boutique de ton oncle ; il m'a assuré que le téléphone était « propre » et que je pouvais l'utiliser en toute sécurité. Il m'a aussi aidé à acheter une de ces puces prépayées qu'on met dans le téléphone.

Delir : Oui, c'est ce qu'on appelle une carte SIM [207]. La compagnie de téléphone retrace chaque appel ou transmission avec le numéro de téléphone et le numéro d'identification de la carte SIM, ET le numéro d'identification du téléphone. Alors, s'ils savent quel numéro de téléphone, OU quel le numéro d'identification du téléphone, OU quel numéro de carte SIM t'appartient, ils peuvent faire jouer leurs relations pour connaître tes habitudes d'utilisation du téléphone.

Borna : Et je suppose qu'ils peuvent aussi écouter mes conversations par téléphone mobile ?

Delir : Dans ton cas particulier, et il faut remercier mon oncle pour cela, le téléphone n'est pas enregistré à ton nom et la carte SIM n'est aucunement associée à ton nom. Alors, même s'ils arrivent à retracer l'emplacement de la carte SIM et/ou du téléphone, ils n'ont pas nécessairement la possibilité de savoir que tu es associé à la carte SIM ou au téléphone.

- 9.2.1 Pratiques exemplaires en matière de sécurité mobile [208]
- 9.2.2 Fonctions de base, traçabilité et anonymat [209]
- 9.2.3 Communications par texte - SMS / Messages textes [210]
- 9.2.4 Autres fonctions des appareils mobiles [211]

Pratiques exemplaires en matière de sécurité mobile

Comme c'est le cas avec d'autres types d'appareils, la première ligne de défense pour les renseignements contenus sur votre téléphone mobile est la protection physique de l'appareil et de sa carte SIM [207] contre le vol et les dommages.

- Conservez votre appareil avec vous en tous temps. Ne le laissez jamais sans surveillance. Évitez d'exhiber votre téléphone en public.
- Utilisez toujours les codes de sécurité ou le numéro d'identification personnel (NIP) du téléphone et gardez-en le secret (ne les révélez à personne). Ne conservez jamais les codes et numéros de sécurité par défaut du fabricant.
- Faites une marque physique (dessinée) sur la carte SIM, la carte mémoire de rechange, la pile et le téléphone. Cette marque devrait être unique et ne devrait pas être évidente aux yeux d'un étranger (faites une petite marque, un dessin, des lettres ou des chiffres, et/ou utilisez un marqueur ultraviolet, dont l'encre est invisible à la lumière normale). Collez des étiquettes de sécurité indécachetable ou du ruban adhésif sur les joints du téléphone. De cette façon, vous pourrez voir immédiatement si ces items ont été trafiqués ou remplacés (par exemple, l'étiquette ou le ruban adhésif sera mal aligné ou laissera un résidu visible).
- Assurez-vous de savoir en tous temps quels renseignements sont stockés sur votre carte SIM, sur vos cartes mémoire additionnelles et dans la mémoire interne de votre téléphone. Ne stockez pas de renseignements sensibles sur votre téléphone. Si vous devez stocker des renseignements que vous jugez sensibles, envisagez la possibilité de les charger sur une carte mémoire externe, qui peut facilement être détruite. Ne laissez pas des renseignements aussi importants dans la mémoire interne du téléphone.
- Protégez votre carte SIM et votre carte mémoire supplémentaire (si votre téléphone en a une), puisqu'elles peuvent contenir des renseignements importants comme des coordonnées personnelles et des messages SMS. Par exemple, assurez-vous de ne pas les laisser à l'atelier de réparation lorsque vous faites réparer votre appareil.
- Lorsque vous vous débarrassez de votre appareil, assurez-vous de ne laisser aucun renseignement dans la mémoire interne du téléphone ou sur la carte SIM (même si le téléphone ou la carte SIM sont brisés ou défectueux). La meilleure solution est probablement de détruire physiquement la carte SIM. Si vous avez l'intention de donner, revendre ou réutiliser votre appareil, assurez-vous d'abord que tous les renseignements en soient supprimés.
- Envisagez de ne faire affaire qu'avec des marchands et réparateurs de confiance. Cela réduit considérablement votre niveau de vulnérabilité si vous achetez un téléphone usagé ou si vous faites réparer votre appareil. Vous pouvez également envisager d'acheter votre appareil d'un marchand autorisé mais choisi complètement au hasard. Ainsi, vous réduisez les risques que votre appareil ait été préparé spécialement pour vous avec des logiciels d'espionnage installés à l'avance.
- Faites régulièrement des copies de sauvegarde, sur un ordinateur sécurisé, des renseignements contenus dans votre téléphone. Stockez la copie de sauvegarde de façon sécurisée (voir le chapitre : **4. Protéger les données sensibles stockées sur votre ordinateur** [63]). Cela vous permettra de récupérer vos données si vous perdez votre téléphone. De plus, si vous avez une copie de sauvegarde, vous saurez exactement quels renseignements peuvent être compromis (si votre appareil est perdu ou volé) et pourrez prendre des mesures en conséquence.
- Le numéro de série à 15 caractères, ou IIEM (Identité internationale d'équipement mobile), permet d'identifier votre téléphone et peut être affiché sur la plupart des appareils en composant *#06#. Sinon, ce numéro est habituellement inscrit sous la pile, ou vous pouvez le retrouver en consultant les paramètres de l'appareil. Notez ce numéro quelque part et gardez cette note à l'écart de votre téléphone, puisque ce numéro peut être utile pour retracer le téléphone et en prouver la propriété si l'appareil est volé.
- Prenez le temps de bien considérer les avantages et désavantages d'enregistrer votre téléphone auprès d'un fournisseur de service. Si votre téléphone est volé, le fournisseur de service devrait être en mesure d'en interrompre immédiatement l'usage. Par contre, l'enregistrement de votre appareil signifie que son usage est associé directement à votre identité.

Fonctions de base, traçabilité et anonymat

Pour que votre appareil soit en mesure d'envoyer ou de recevoir des communications, il doit constamment signaler sa présence aux tours de transmission qui se trouvent à proximité. Conséquemment, le fournisseur de service qui gère le réseau est en mesure de savoir précisément où se trouve votre appareil à tout moment.

Borna : Y a t-il autre chose que je devrais savoir à propos de ce téléphone ?

Delir : Oui, je suppose, mais ça dépend... est-ce que tu soupçonnes qu'ils te suivent à la trace.

Borna : Je ne crois pas, mais peuvent-ils faire ça ?

Delir : Et bien oui, si le téléphone est sous tension ET que les techniciens ont accès au trafic du réseau ET qu'ils savent exactement quel téléphone est le tien.

Borna : Aucun risque, puisque je ne ferai pas d'appels avec mon téléphone quand je serai sur place.

Delir : Ça n'a pas d'importance, père. Tant que tu auras le téléphone avec toi, chargé et prêt à être utilisé, l'appareil émet un signal aux tours qui se trouvent à proximité pour permettre à celles-ci de le localiser, tout simplement parce que c'est nécessaire à son fonctionnement. Donc, à tout moment, ton emplacement exact est forcément quelque part entre les tours de transmission qui se trouvent à proximité.

Borna : Je devrais donc éteindre l'appareil jusqu'à ce que je sois arrivé à destination ?

Delir : Et bien, la meilleure solution est de ne pas transporter le téléphone avec toi. La deuxième meilleure option est d'éteindre l'appareil ET de retirer la pile avant de partir, et de pas le remettre sous tension avant ton retour.

Borna : Quoi !? Ça ne suffit pas de le mettre hors tension ?

Delir : Et bien, juste pour mettre toutes les chances de ton côté, il est préférable de retirer la pile, et voici pourquoi : le téléphone mobile est un dispositif de transmission de signaux, donc tant que la pile est connectée, il y a toujours un risque que quelqu'un, d'une manière ou d'une autre, trouve le moyen de mettre l'appareil sous tension à ton insu.

À propos de l'anonymat

Si vous menez des conversations ou envoyez des messages textes de nature sensible à partir de votre téléphone mobile, prenez garde aux fonctions de traçabilité dont il est question ci-dessus. Envisagez d'adopter les pratiques suivantes :

- Faites vos appels chaque fois à partir d'emplacements différents, et choisissez des lieux auxquels on ne peux pas facilement vous associer.
- Gardez votre appareil hors tension, avec la pile déconnectée, rendez vous au lieu déterminé, mettez votre appareil sous tension et faites votre communication, puis éteignez-le à nouveau et retirez la pile. En prenant cette habitude chaque fois que vous devez utiliser votre téléphone mobile, le réseau ne sera pas en mesure de vous suivre à la trace.
- Changer de téléphone et de cartes SIM [207] régulièrement. Échangez-les entre camarades ou fréquentez les marchands d'appareils usagés.
- Utilisez des cartes SIM prépayées non enregistrées si cette option est possible dans votre région. Évitez d'acheter un téléphone ou une carte SIM à l'aide d'une carte de crédit, car cela créerait évidemment un lien direct entre vous et ces items.

Borna : Es-tu en train de me dire que mon appareil signale mon emplacement aux tours de transmissions même si je l'ai mis hors tension ?

Delir : Oui, et ce n'est pas le pire, père. Borna: Ah bon ?

Delir : Il y a apparemment des programmes qui peuvent être installés sur ton appareil et qui permettent de le mettre sous tension secrètement et à distance, et de lui faire composer un numéro à ton insu. Ensuite, alors que tu mènes ta réunion, ton téléphone peut être utilisé à distance comme dispositif d'enregistrement et de transmission !

Borna : Non, vraiment !?

Delir : Et bien, c'est quelque chose que la technologie actuelle permet de faire assez facilement. Mais rien de cela n'est possible si la pile est retirée du boîtier, alors tu n'auras jamais de problème si tu prends cette précaution.

Borna : Je vais donc éviter de transporter mon mobile si je veux être particulièrement prudent. Mais je commence à me demander sérieusement si c'est une bonne idée d'utiliser ce bidule...

Delir : Je t'en prie, père... Tu m'as toujours dit qu'il ne faut pas avoir peur de la nouveauté... Les téléphones mobiles sont comme ça, il faut en connaître les avantages et les risques, c'est tout. Il faut simplement faire attention. Si tu connais les risques, tu peux prendre les moyens appropriées pour les éviter.

À propos de l'écoute intrusive

Votre téléphone peut être utilisé pour enregistrer et transmettre les sons qui sont émis dans la portée de son microphone, et ce, sans même que vous vous en rendiez compte. Certains appareils peuvent être mis sous tension à distance et actionné de cette façon, même s'ils ont l'apparence d'être hors tension.

- Ne laissez jamais une personne en qui vous n'avez pas confiance s'approcher physiquement de votre téléphone ; c'est un moyen répandu d'installer des logiciels d'espionnage sur votre appareil.
- Si vous menez des réunions importantes ou de nature privée, mettez votre téléphone hors tension et retirez la pile du boîtier. Ou n'apportez tout simplement pas l'appareil avec vous si vous avez la possibilité de le laisser en lieu sûr.
- Assurez-vous que toutes les personnes avec qui vous communiquez respectent également les précautions décrites ici.
- De plus, n'oubliez pas que l'utilisation d'un téléphone mobile en public, ou dans un lieu dont vous vous méfiez, vous

rend vulnérable aux techniques d'écoute traditionnelles, ou même aux agressions et au vol.

À propos de l'interception des appels

Habituellement, le chiffrement des communications vocales (et des messages textes) qui circulent par voie de téléphonie mobile est relativement faible. Il existe des techniques facilement accessibles par lesquelles des tierces parties peuvent intercepter vos communications écrites ou écouter vos conversations si elle se trouvent à proximité de l'appareil et sont en mesure de recevoir les transmissions qui en émanent. Et bien sûr, les fournisseurs de service ont accès à toutes vos communications. Il est actuellement plutôt cher et/ou techniquement compliqué de chiffrer vos appels téléphoniques de sorte que même les fournisseurs de service de téléphonie mobile ne soient pas en mesure de les intercepter. Par contre, il est prévu que ces outils deviennent bientôt plus abordables. Pour déployer une stratégie de chiffrement, il faudrait d'abord que vous installiez une application de chiffrement à même votre appareil ainsi que dans l'appareil de la personne avec qui vous souhaitez communiquer. Vous utiliseriez ensuite cette application pour envoyer et recevoir des appels et/ou des messages chiffrés. Les logiciels de chiffrement ne sont pour l'instant supportés que sur certains modèles de téléphones dits « intelligents ».

Les conversations menées par Skype sur des téléphones mobiles ne sont pas chiffrées non plus, puisque le signal doit nécessairement transiter par le réseau de téléphonie mobile, où aucun processus de chiffrement n'est en place.

Communications par texte - SMS / Messages textes

Vous ne devriez jamais vous fier aux services de messagerie texte pour transmettre des renseignements de nature sensible. Les messages sont transmis en texte clair, ce qui les rend inappropriés à l'échange de renseignements confidentiels.

Borna : Et si je ne me servais jamais de mon téléphone pour faire des appels, mais seulement pour envoyer et recevoir des courts messages. Ils ne peuvent pas écouter si personne ne dit quoi que ce soit, et en plus c'est rapide, non ?

Delir : Une petite minute, père... Ces messages sont aussi très faciles à intercepter, et quiconque a accès au trafic de la compagnie de téléphone, ou même une tierce partie avec le bon équipement, peut intercepter et lire ces messages. Ces messages circulent en texte clair et sont sauvegardés d'une tour de transmission à l'autre.

Borna : C'est idiot. Que doit-on faire, alors ? Écrire des messages codés, comme on faisait pendant la guerre ?

Delir : Et bien parfois, les vieilles chaussures sont les plus confortables...

Les messages SMS peuvent être interceptés par les fournisseurs de service ou par des tierces parties dotées d'un équipement facilement accessible. Ces messages transportent avec eux les numéros de téléphone de l'expéditeur et du destinataire ainsi que le contenu des messages en texte clair. De plus, les messages SMS peuvent facilement être altérés et falsifiés par des tierces parties.

Envisagez la possibilité d'établir un système codé entre vous et vos correspondants. Un système de codes peut sécuriser vos communications, en plus d'offrir un moyen supplémentaire de confirmer l'identité de la personne avec qui vous communiquez. Les systèmes de codes doivent être sécurisés et changés fréquemment.

Les messages SMS sont accessibles après la transmission :

- Dans plusieurs pays, la législation (ou d'autres formes d'influence) exige que les administrateurs de réseaux conservent un registre à long terme de tous les messages textes envoyés par leurs utilisateurs. Dans la plupart des cas, les messages SMS sont conservés par les fournisseurs de service à des fins commerciales, comptables ou juridiques.
- Les message sauvegardés dans votre téléphone peuvent facilement être consultés par une personne qui arriverait à mettre la main sur l'appareil. Considérez la possibilité de supprimer immédiatement tous les messages envoyés et reçus.
- Certains modèles de téléphone offrent la possibilité de désactiver la fonction d'historique des appels et des messages textes. Cette option peut s'avérer particulièrement utile pour les personnes qui ont des activités de nature sensible. Vous devriez toujours vous assurer de bien connaître toutes les fonctionnalités de votre appareil. Lisez attentivement le manuel de l'utilisateur !

Autres fonctions des appareils mobiles

Les téléphones mobiles ressemblent de plus en plus à des ordinateurs portables, avec leurs propres systèmes d'exploitation et applications disponibles en téléchargement, qui offrent divers services avancés aux utilisateurs. Conséquemment, les virus et les logiciels espions ont également pénétré le monde de la téléphonie cellulaire. Des virus peuvent être implantés dans votre téléphone ou être transportés avec des applications, des sonneries ou des messages multimédia téléchargées depuis Internet.

Même si les modèles plus anciens ont peu ou pas de fonctions Internet, il est tout de même important d'observer les précautions décrites ci-dessous avec tous les téléphones pour vous assurer que la sécurité de votre appareil n'est pas

compromise à votre insu. Certaines de ces précautions ne s'appliquent uniquement qu'aux téléphones « intelligents », mais il est très important de connaître exactement les possibilités qu'offrent votre appareil afin d'être bien certain d'avoir pris les mesures de sécurité appropriées :

- Ne stockez aucun fichier ni aucune photo de nature confidentielle sur votre téléphone mobile. Transférez-les aussitôt que possible vers un emplacement sûr, tel qu'indiqué au chapitre 4. Protéger les données sensibles stockées sur votre ordinateur [63].
- Supprimez fréquemment vos historiques d'appels et de messagerie, vos carnets d'adresses, vos photos, etc.
- Si vous utilisez votre téléphone pour naviguer sur Internet, suivez les mêmes pratiques exemplaires que lorsque vous utilisez un ordinateur (par exemple, envoyez toujours vos communications par connexion chiffrée HTTPS [212]).
- Ne connectez votre téléphone à un ordinateur que si vous êtes bien certain que ce dernier n'est infecté par aucun logiciel malveillant. Voir à ce sujet le chapitre 1. Protéger votre ordinateur contre les logiciels malveillants et les pirates [142].
- N'acceptez et n'installez aucun programme inconnu sur votre téléphone, y compris les sonneries, les papiers peints, les applications Java [213] ou toute autre application provenant d'une source non sollicitée ou inconnue. Ces fichiers pourraient contenir des virus, des logiciels malveillants ou des programmes espions.
- Observez attentivement le comportement et le fonctionnement de votre appareil. Méfiez-vous des programmes et des processus inconnus, des messages étranges et des opérations instables. Si vous ne connaissez pas ou n'utilisez pas certaines fonctions ou applications qui se trouvent sur votre téléphone portable, désactivez-les ou désinstallez-les, dans la mesure du possible.
- Soyez vigilant lorsque vous vous connectez à un point d'accès WiFi qui n'exige aucun mot de passe, de la même façon que lorsque vous utilisez un ordinateur pour vous connecter à un accès WiFi. Votre téléphone mobile est essentiellement comme un ordinateur et est donc vulnérable aux mêmes risques de sécurité que les ordinateurs connectés à Internet
- Assurez-vous d'éteindre et de désactiver les canaux de communication Infrared (IrDA) [214], Bluetooth [215] et Wireless Internet (WiFi) si vous ne les utilisez pas. N'activez ces fonctions que lorsque vous en avez besoin. Ne les utilisez que dans des lieux sûrs et des situations de confiance. Considérez la possibilité de vous passez entièrement de la fonction Bluetooth, puisqu'il est relativement facile de placer cette forme de communication sous écoute. Au lieu du Bluetooth, transférez les données à l'aide d'un câble entre le téléphone et votre casque d'écoute main libre ou votre ordinateur.

Lecture complémentaire

- The Mobile Advocacy Toolkit [216] publié par le Tactical Technology Collective. Entre autres choses, cette trousse d'information contient des descriptions détaillées et des guides pour la sécurité des téléphones portables [217], ainsi qu'une vaste gamme d'outils alternatifs et d'exemples liés à leur utilisation.
- Sécurité pour les militants – Un Guide pratique pour les militants et les campagnes [218].
- Un guide sur les téléphones portables – un guide court pour les militants sur l'utilisation des téléphones portables en toute sécurité. [219].
- Un guide sur la sécurité mobile des journalistes-citoyens [5] publié par MobileActive.org [220] publié par MobileActive.org
- Une brève introduction à la messagerie par SMS sécurisée en MIDP – Guide Nokia du développeur [221]
- Téléphones utilisés comme système d'espionnage [222]

11. Utiliser votre smartphone en sécurité (autant que possible...)

Dans le ***chapitre 10 : Utiliser votre téléphone mobile en sécurité (autant que possible...)*** [223], nous avons examiné les défis de sécurité liés à l'utilisation de téléphones mobiles de base – y compris les problèmes liés à la communication vocale et les services de messagerie textuelle (SMS/MMS). Ces téléphones utilisent principalement (si non exclusivement) des réseaux mobiles pour transférer des appels et des données.

Les progrès technologiques permettent aujourd'hui de profiter de nombreux services et fonctionnalités similaires à ceux dispensés par un ordinateur de bureau ou portable via un téléphone mobile. Ces smartphones offrent de nombreuses façons nouvelles de communiquer, capturer et diffuser des médias. Pour fournir ces nouvelles fonctionnalités, les smartphones n'utilisent pas seulement le réseau mobile mais se connectent également à Internet soit via une connexion Wifi (de la même façon qu'un ordinateur portable dans un cybercafé), soit via des connexions de données par l'intermédiaire de l'opérateur du réseau mobile.

Vous pouvez donc certes faire des appels avec un smartphone, il vaut toutefois mieux le considérer comme un dispositif informatique de petite taille. Ceci signifie que les informations dispensées dans cette boîte à outils sont applicables à l'utilisation de votre smartphone comme de votre ordinateur.

Les smartphones subviennent généralement à un large eventail de fonctionnalités – navigation sur le web, courrier électronique, messagerie vocale et instantanée sur Internet, capture, stockage et transmission d'audio, de vidéos et de photos, utilisation de réseaux sociaux, de jeux multi-utilisateurs, services bancaires électroniques et d'autres nombreuses activités. Cependants, beaucoup de ces outils et fonctionnalités présentent de nouveaux problèmes de sécurité, ou augmentent des risques déjà existant.

Par exemple, certains smartphones ont intégré la fonctionnalité de géolocalisation (*GPS* [224]), par laquelle votre emplacement précis peut être fourni par défaut à votre opérateur de réseau mobile et à de nombreuses applications que vous utilisez sur votre téléphone (telles qu'entre autres de réseaux sociaux, de cartographie ou de navigation). Comme mentionné précédemment, les téléphones mobiles relaient déjà votre localisation à votre opérateur de réseau mobile (dans le cadre des fonctions normales de votre téléphone). Toutefois, la fonctionnalité additionnelle du GPS augmente non seulement la précision des informations sur votre localisation, mais aussi la quantité des lieux où ces informations peuvent être distribuées.

Cela vaut la peine de reconsulter les risques associés aux téléphones mobiles présentés dans le ***chapitre 10 : Utiliser votre téléphone mobile en sécurité (autant que possible...)*** [223] dans la mesure où tous valent pour l'utilisation d'un smartphone. Le ***chapitre 10*** [223] couvre les questions d'écoute, d'interception de SMS ou d'appels téléphoniques, les problèmes liés à la carte SIM et des usages plus conseillés.

Dans ce chapitre, nous allons considérer d'autres problèmes de sécurité posés par les smartphones.

Sacs à main, porte-feuille, smartphones

Nous connaissons intuitivement la valeur de ce que contient notre sac à main ou porte-feuille dans la mesure où ceux-ci détiennent énormément de renseignements très personnels ou sensibles nous concernant. Les perdre compromettrait notre vie privée et notre sécurité. Les gens sont bien moins conscients de la quantité d'informations personnelles qu'ils transportent dans leur smartphone et considèrent leur perte plutôt comme une contrariété que comme un risque. Si vous percevez le smartphone comme un dispositif informatique toujours connecté à un réseau et constamment sur vous, alors vous constaterez facilement la grande différence existant entre un support d'informations discrètes, passives (tel un porte-feuille) et un objet actif et interactif tel le smartphone.

Un exercice simple peut aider à illustrer ce propos :

Videz le contenu de votre sac à main ou de votre porte-feuille et prenez en compte les objets sensibles. En général, vous trouvez : - Photos de proches (~5 photos) - Papiers d'identité (permis de conduire, cartes de membre, cartes de sécurité sociale) - Assurances et santé (~2 cartes) - Argent (~5 billets) - Cartes de paiement (~3 cartes)

Maintenant, examinez le contenu de votre smartphone. Un utilisateur type de smartphone trouvera certainement bien plus d'objets sensibles que dans son porte-monnaie, et parfois d'une plus grande valeur :

- Photos de vos proches (~100 photos)
- Applications de messagerie et leurs mots de passe
- Emails (~500 courriels)
- Vidéos (~50 vidéos)
- Applications de réseaux sociaux et leurs mots de passe
- Applications bancaires (avec l'accès aux comptes bancaires)
- Documents sensibles
- Documentation de communications sensibles
- Une connexion directe à vos informations privées

Plus votre usage du smartphone augmente, plus il vous faut devenir conscient des risques associés et prendre des précautions appropriées. Les smartphones sont de puissants amplificateurs et distributeurs de vos données personnelles. Ils sont conçus pour fournir une connectivité aussi constante que possible et assurer la connexion aux services de réseautage social par défaut. Car, vos données personnelles représentent des renseignements précieux pouvant être regroupés, recherchés et vendus.

Dans le ***chapitre 5 : Récupérer des données perdues*** [225], nous avons exposé l'importance de la sauvegarde des données. Ceci s'applique tout particulièrement aux smartphones. Perdre votre téléphone peut avoir des conséquences désastreuses si vous n'avez pas sauvegardé vos données les plus importantes (tels vos contacts) dans un endroit sûr. Outre la sauvegarde de vos données, assurez-vous que vous savez également comment restaurer les données. Conserver une copie imprimée des étapes à suivre de façon à pouvoir agir vite en cas d'urgence.

Dans ce chapitre, nous allons tout d'abord vous présenter quelques indications générales sur le smartphone – une description des différentes plateformes et des procédures de configuration de base pour sécuriser vos informations et communications. Les autres parties de ce chapitre porteront sur des précautions spéficiques liées à des utilisations courantes du smartphone. Les sections suivantes porteront sur les aspects de sécurité suivants :

Plateformes, configuration et installation

Plateformes et systèmes d'exploitation

Au moment de la rédaction de ces lignes, les smartphones les plus couramment utilisés sont l'iPhone d'Apple et l'Android de Google, suivis par les Blackberry et les Windows Phones. La principale différence entre l'Android et d'autres systèmes d'exploitation se trouve dans le fait qu'Android est le plus souvent un système open source (*FOSS* [226]), qui permet au système d'exploitation d'être audité indépendamment afin de vérifier s'il protège correctement les informations et communications des utilisateurs. Il soutient également le développement d'applications de sécurité pour cette plateforme. De nombreux analystes programmeurs sensibles à la sécurité développent des applications Android en prenant en compte la sûreté des utilisateurs. Certains d'entre eux seront mentionnés plus tard dans ce chapitre.

Quel que soit le type de smartphone que vous utilisez, il vous faut être au courant de certains faits liés à l'utilisation d'un téléphone connecté à Internet et livré avec des fonctionnalités telles que le *GPS* [227] ou la possibilité de mise en réseau sans fil. Dans ce chapitre, nous nous concentrons sur les appareils équipés de la plateforme Android, car, comme mentionné ci-dessus, il y est plus facile de sécuriser les données et communications. Néanmoins, les guides de configuration de base et quelques applications pour d'autres appareils que les téléphones Android seront également exposés.

Les téléphones Blackberry ont été présentés comme des appareils de messagerie texte et email « sûrs » dans la mesure où les messages et emails transitent par des serveurs Blackberry, hors de portée d'oreilles indiscrètes potentielles. Malheureusement, de plus en plus de gouvernements réclament l'accès à ces communications, invoquant la nécessité de se prémunir contre le terrorisme et le crime organisé. Les gouvernements d'Inde, des Émirats arabes unis, d'Arabie Saoudite, d'Indonésie et du Liban ont par exemple examiné attentivement l'utilisation des appareils Blackberry et exigé l'accès aux données des utilisateurs dans leur pays.

Mobiles classiques (ou feature phones)

Les 'feature phones' (par exemple le 7705 Twist de Nokia ou le Rogue de Samsung) constituent une autre catégorie de téléphones mobiles. Ceux-ci ont depuis peu augmenté leurs fonctionnalités de façon à inclure celles de certains smartphones. Mais de manière générale, les systèmes d'exploitation des feature phones restent moins accessibles, les possibilités de développement d'applications de sécurité ou de perfectionnement sont donc limitées. Nous ne traitons pas spécifiquement des feature phones, toutefois de nombreuses mesures présentées ici valent également pour ceux-ci.

Smartphones labellisés et simlockés

Les smartphones sont généralement vendus labellisés ou simlockés. Un smartphone simlocké est un appareil qui ne peut fonctionner qu'avec la carte SIM fournie par l'opérateur. Généralement, les opérateurs de réseau mobile simlockent un téléphone en y installant leur propre firmware ou logiciel. Ils peuvent également désactiver certaines fonctionnalités ou en ajouter d'autres. Le simlockage permet aux entreprises d'augmenter leurs gains en orientant votre utilisation du smartphone, souvent aussi en collectant des données sur la façon dont vous utilisez votre téléphone ou en permettant l'accès à votre smartphone à distance.

Pour ces raisons, nous recommandons l'achat d'un téléphone non simlocké, si possible. Un téléphone simlocké présente un risque plus élevé dans la mesure où toutes vos données sont acheminées par un seul opérateur, qui centralise vos flux de données, empêche de changer de carte SIM et donc de diffuser des données via d'autres opérateurs. Si votre téléphone est simlocké, demandez à quelqu'un en qui vous avez confiance de le désimlocker.

Configuration générale

Les smartphones ont de nombreux paramètres contrôlant la sûreté de l'appareil. Il est important de prêter attention à la configuration de votre smartphone. Dans les guides pratiques ci-dessous, nous vous signalons certains paramètres de sécurité qui sont disponibles mais non actifs par défaut, tout comme d'autres qui sont actifs par défaut et rendent votre téléphone vulnérable.

Expérience pratique : se lancer avec le *guide de configuration générale pour Android* [228].

Installation et mise à jour des applications

La façon habituelle d'installer un nouveau logiciel sur votre smartphone consiste à utiliser l'Appstore d'iPhone ou le Play Store de Google, de s'y connecter avec vos accréditations d'utilisateur et, de télécharger et installer l'application désirée. En vous connectant, vous associez votre usage de la boutique en ligne à votre compte d'utilisateur connecté. Les propriétaires de la boutique en ligne d'applications conservent des registres indiquant l'historique de la navigation de l'utilisateur et des applications choisies.

Les applications proposées dans les boutiques en ligne officielles sont censées êtres vérifiées par les propriétaires des boutiques (Google ou Apple), mais ceci fournit en réalité une protection faible contre ce que les applications peuvent engendrer une fois installées sur votre téléphone. Par exemple, certaines applications sont en état de copier et de communiquer votre carnet d'adresses après avoir été installées sur votre téléphone. Dans le cas des téléphones Android, toute application doit demander durant le processus d'installation ce qu'elle est en droit d'accomplir à partir du moment où elle est en service. Vous devez porter une attention toute particulière aux autorisations qui vous sont demandées et si ces autorisations sont en rapport avec la fonction de l'application que vous installez. Par exemple, si vous envisagez d'installer un « lecteur de nouvelles » et vous découvrez qu'il demande le droit d'envoyer vos contacts via une connexion de

données mobile à un tiers, vous feriez mieux de chercher une autre application dont l'accès et les demandes de droits sont plus appropriés.

Les applications Android sont également disponibles à partir de sources situées en dehors des canaux officiels de Google. Pour utiliser ces sites de téléchargement, il vous suffit de cocher l'option *Sources inconnues* dans les *paramètres des applications*.

Il est utile de tenir compte de ces autres sites si vous souhaitez minimiser le contact avec Google. Nous recommandons **F-Droid** [229] ('Free Droid'), qui ne propose que des applications *FOSS* [230]. Dans ce guide, F-Droid constitue le dépôt principal des applications que nous recommandons et nous ne faisons référence à Google Play que si F-Droid ne dispose pas du type d'app recherché.

Si vous ne voulez (ou ne pouvez) pas vous connecter à Internet pour accéder à ces apps, vous pouvez transférer les apps à partir du téléphone de quelqu'un d'autre en envoyant des fichiers *.apk* [231] ('android application package') via bluetooth. Vous pouvez soit télécharger le fichier .apk sur la carte Micro SD de votre téléphone, soit utiliser un câble USB afin de l'y déplacer à partir d'un PC. Quand vous avez reçu le fichier, il suffit de cliquer le nom du fichier assez longtemps jusqu'à ce que vous soyez invité à l'installer. (**Note** : soyez particulièrement prudent lorsque vous utilisez bluetooth - infos à ce sujet dans le ***chapitre 10 : Autres fonctions des appareils mobiles*** [232]).

Communication (voix et messagerie) via smartphone

Parler en toute sécurité

Téléphonie de base

Dans la section ***Fonctions de base, traçabilité et anonymat*** [233] du Chapitre 10, nous avons présenté diférentes mesures à suivre afin de réduire le risque d'interception lors de l'utilisation du réseau opérateur de téléphonie mobile pour votre communication vocale.

Le fait d'utiliser Internet par le biais de votre smartphone via des connexions de données mobiles ou WiFi peut permettre une communication plus sûre, à savoir en utilisant *VoIP* [234] et des moyens de sécurisation de ce canal de communication. Certains outils de smartphone peuvent même étendre la sécurité au-delà de VoIP, aux appels à partir d'un téléphone mobile aussi (Voir **Redphone** ci-dessous).

Voici une liste de quelques outils, leurs avantages et inconvénients :

Skype

La plus populaire des applications VoIP commerciales, *Skype* [235], est disponible sur toutes les plateformes de smartphone et fonctionne bien si votre connectivité sans fil est fiable. Elle est moins fiable via une connexion de données mobile.

Dans la section ***Sécuriser vos autres outils de communication par Internet*** [236] du ***chapitre 7 : Préserver la confidentialité de vos communications sur Internet*** [237], nous avons discuté des risques liés à l'utilisation de Skype et pourquoi il vaut mieux, dans la mesure du possible, l'éviter. En résumé, Skype est un logiciel non open-source qui fait qu'il est très difficile d'en confirmer indépendamment le niveau de sécurité. De plus, Skype appartient à Microsoft, qui a un intérêt commercial à savoir quand et d'où vous utilisez Skype. Skype peut également permettre à des organismes chargés de l'application de la loi d'accéder rétrospectivement à l'historique de vos communications.

D'autres VoIP

L'utilisation de VoIP est généralement gratuite (ou nettement moins chère que les appels téléphoniques mobiles) et laisse peu de traces de données. De fait, un appel VoIP sécurisé peut être le moyen le plus sûr de communiquer.

CSipSimple [238] est un client VoIP solide pour téléphones Android, qui est bien entretenu et livré avec de nombreux assistants simples pour saisir les paramètres de différents services VoIP.

Le projet du **Open Secure Telephony Network (OSTN)** [239] et le serveur entretenu par le Guardian Project **ostel.me** [240] proposent actuellement l'un des moyens les plus sûrs de communication vocale. Bien connaître et faire confiance à l'entité qui exploite le serveur que vous utilisez pour vos communications vocales est extrêmement important. Les hôtes de ce service – le **Guardian Project** [241] – sont très connus et respectés dans la communauté.

Lors de l'utilisation de CSipSimple, vous ne communiquez jamais directement avec votre interlocuteur; toutes vos données passent par le serveur Ostel. Il est alors beaucoup plus difficile de retracer vos données et de découvrir à qui vous parlez. En outre, Ostel ne conserve aucune de ces données, mises à part les données du compte dont vous avez besoin pour vous connecter. Tout ce que vous dites est chiffré et même vos métadonnées, qui sont normalement difficiles à dissimuler, sont floues puisque le trafic se fait à travers le serveur ostel.me. Si vous téléchargez CSipSimple depuis ostel.me, vous le recevrez préconfiguré pour ostel.me; ce qui rend son installation et utilisation d'autant plus faciles.

RedPhone [242] est une application logicielle libre et open source qui permet de chiffrer les données de communication vocale envoyées entre deux appareils qui utilisent cette application. Elle est facile à installer et très facile à utiliser puisqu'elle s'intègre dans votre numérotation normale et dans votre schéma des contacts. Mais les gens auxquels vous

souhaitez parler doivent également installer et utiliser RedPhone. Pour une utilisation facile de RedPhone, prenez votre numéro de téléphone mobile comme identificateur (tel un nom d'utilisateur dans d'autres services VoIP). Toutefois, sachez qu'il devient de plus en plus facile d'analyser le trafic produit et de remonter jusqu'à vous par le biais de votre numéro de mobile. RedPhone utilise un serveur central, qui est un point de centralisation et place RedPhone dans une position de force (celle d'avoir le contrôle sur certaines de ces données).

Des guides pratiques pour CSipSimple, Ostel.me et Redphone sont en prévision. En attendant, des informations supplémentaires sont disponibles en cliquant sur les liens mentionnés ci-dessus.

Envoyer des messages en toute sécurité

Certaines précautions sont à prendre lors de l'envoi de SMS et l'utilisation de la messagerie instantanée ou de discussions en ligne sur votre smartphone.

SMS

Comme décrit dans le ***chapitre 9.2.3 : Communications par texte – SMS / Messages textes*** [243], la communication par SMS est non sûre par défaut. Toute personne ayant accès à un réseau de télécommunication mobile peut intercepter ces messages facilement, ce qui est un fait quotidien dans de nombreuses situations. Ne comptez pas sur l'envoi SMS non sécurisés lors de situations critiques. Il est de surcroît impossible d'authentifier les messages SMS, de savoir si le contenu d'un message a été modifié en chemin ou si l'expéditeur est bien la personne qu'il prétend être.

SMS sécurisés

TextSecure [244] est un outil *FOSS* [230] qui permet d'envoyer et de recevoir des SMS sécurisés via un téléphone Android. Il fonctionne à la fois pour des messages chiffrés et non chiffrés si bien que vous pouvez l'utiliser comme votre application SMS par défaut. Pour échanger des messages chiffrés, cet outil doit être installé par l'expéditeur et par le destinataire. Vous devrez donc amener les gens avec lesquels vous communiquez régulièrement à l'utiliser également. TextSecure détecte automatiquement lorsqu'un message chiffré est reçu par un autre utilisateur de TextSecure. Il vous permet également d'envoyer des messages chiffrés à plusieurs personnes. Les messages sont automatiquement signés; ce qui rend presque impossible la falsification du contenu. Dans notre guide pratique consacré à TextSecure, nous expliquons en détail les caractéristiques de cet outil et comment l'utiliser.

Expérience pratique : se lancer avec le *guide pratique TextSecure* [245].

Chat sécurisé

L'utilisation de la messagerie instantanée ou le fait de chatter avec votre téléphone produit un grand nombre d'informations qui peuvent être interceptées. Vous courez ainsi le risque que ces conversations soient utilisées plus tard contre vous par des adversaires. Vous devez donc être extrêmement prudent sur les informations que vous divulguez lorsque vous envoyez des messages ou chattez avec votre téléphone.

Il existe des moyens de chatter et d'envoyer des messages instantanés en toute sécurité. Le meilleur moyen est d'utiliser le chiffrement de bout en bout, qui assure que la personne à l'autre bout du fil est bien celle que vous souhaitez.

Pour les téléphones Android, nous recommandons **Gibberbot** [246] comme application de messagerie instantanée sécurisée. Gibberbot permet un chiffrement de vos chats facile et résistant avec protocole de messagerie *Off-the-Record* [247]. Ce chiffrement assure à la fois l'authenticité (vous pouvez vérifier que vous chattez avec la bonne personne) et la sécurisation autonome de chaque session : s'il arrive que le chiffrement d'une session de chat soit compromise, d'autres sessions passées ou futures ne seront pas concernées.

Gibberbot a été conçu pour être utilisé avec Orbot; de sorte que vos messages de chat peuvent passer par le réseau anonymisant *Tor* [248]. Tout échange est ainsi rendu intraçable voire comme n'ayant jamais eu lieu.

Expérience pratique : se lancer avec le *guide pratique Gibberbot* [249].

Pour les iPhones, le client **ChatSecure** [250] offre les mêmes fonctionnalités. Il n'est toutefois pas évident à utiliser avec le réseau *Tor* [248].

Un guide pratique pour ChatSecure va bientôt paraître. En attendant, des informations supplémentaires sont disponibles sur la page d'accueil [250].

Quelle que soit l'application que vous utilisez, réfléchissez bien au type de compte duquel vous voulez chatter. Par exemple, quand vous utilisez Google Talk, vos informations d'identification et l'heure de votre session de discussion sont connus par Google. De même, mettez-vous d'accord avec vos interlocuteurs sur le fait que l'historique des discussions ne doit en aucun cas être sauvegardé - surtout si les discussions ne sont pas chiffrées.

Stocker des informations sur votre smartphone

Les smartphones disposent de grandes capacités de stockage de données. Malheureusement, les données stockées sur votre appareil peuvent être facilement accessibles à des tiers, soit à distance, soit physiquement. Quelques précautions de

base pour réduire tout accès inapproprié à ces informations sont formulées dans le ***guide de configuration générale pour Android*** [228]. En outre, vous pouvez prendre des mesures pour chiffrer toute information sensible dans votre téléphone à l'aide d'outils spécifiques.

Outils de chiffrement des données

Android Privacy Guard (APG) [251] permet de chiffrer fichiers et courriels au format OpenPGP. Il peut être utilisé pour conserver vos fichiers et documents en toute sécurité sur votre téléphone, tout comme lorsque vous communiquez par courriel.

Expérience pratique : se lancer avec le *guide pratique APG* [251].

Cryptonite [252] est un autre outil de chiffrement de fichiers *FOSS* [230]. Cryptonite dispose de fonctionnalités plus avancées sur les téléphones Android rootés spécialement préparés avec un firmware personnalisé. Consultez la section ***Utilisation avancée du smartphone*** [253] pour en savoir plus.

Experience pratique : se lancer avec le *guide Cryptonite* [254].

Sécurisation du mot de passe

Vous pouvez conserver tous vos mots de passe en un fichier sécurisé et chiffré en utilisant **Keepass**. Vous n'aurez besoin de vous souvenir que d'un seul mot de passe principal pour accéder aux autres. Avec Keepass, vous pouvez utiliser des mots de passe très forts pour chaque compte en votre possession dans la mesure où Keepass s'en souviendra pour vous; il fournit de surcroît un générateur de mots de passe pour créer de nouveaux mots de passe. Vous pouvez synchroniser les base de données de mots de passe Keepass entre votre téléphone et votre ordinateur. Nous vous recommandons de synchroniser uniquement les mots de passe que vous allez réellement utiliser sur votre téléphone mobile. Vous pouvez créer une base de données de mots de passe séparée plus petite sur l'ordinateur et synchroniser celle-ci au lieu de copier toute une base de données comprenant tous les mots de passe que vous utilisez sur votre smartphone. Aussi, étant donné que tous les mots de passe sont protégés par votre mot de passe principal, il est essentiel d'utiliser un mot de passe très fort pour votre base de données Keepass. Consultez le ***chapitre 3 : Créer et sauvegarder des mots de passe sûrs*** [140].

Expérience pratique : se lancer avec le *guide pratique KeePassDroid* [255].

Envoyer des courriels avec votre smartphone

Dans cette section, nous allons examiner brièvement l'usage du courrier électronique sur smartphone. Nous vous encourageons à consulter les sections ***Sécuriser votre courriel*** [256] et ***Que faire si vous soupçonnez que vos communications par courriel sont surveillées*** [257] du ***chapitre 7: Préserver la confidentialité de vos communications sur Internet*** [237] dans lesquels nous nous penchons sur la sécurité de base du courrier électronique.

En premier lieu, demandez-vous si vous avez vraiment besoin d'utiliser votre smartphone pour accéder à vos courriels. Sécuriser un ordinateur et son contenu est généralement plus simple que de le faire pour un appareil mobile tel qu'un smartphone. Un smartphone est plus prédisposé au vol, à la surveillance et à l'intrusion.

S'il vous est absolument indispensable d'accéder à vos courriels sur votre smartphone, certaines mesures sont à prendre pour minimiser les risques.

- Ne vous fiez pas à votre smartphone comme moyen principal pour accéder à vos courriels. Télécharger (et supprimer) des courriels à partir d'un serveur de messagerie et les stocker uniquement sur votre smartphone n'est pas conseillé. Vous pouvez configurer votre application courriel de façon à n'utiliser que des copies de courriels.
- Si vous utilisez le chiffrement email avec certains de vos contacts, envisagez de l'installer également sur votre smartphone. L'avantage supplémentaire qui en découle tient au fait que les courriels chiffrés resteront secrets si jamais votre téléphone devait tomber entre de mauvaises mains.

Le stockage de votre clé privée de chiffrement sur votre appareil mobile peut paraître risqué. Mais l'avantage d'être en mesure d'envoyer et de stocker des courriels soigneusement chiffrés sur l'appareil mobile peut l'emporter sur les risques. Envisagez la création d'une paire de clés de chiffrement seulement mobile (en utilisant **APG** [251]) pour votre utilisation sur le smartphone de sorte que vous ne copiiez pas votre clé privée de chiffrement à partir de votre ordinateur sur votre appareil mobile. Notez que ceci nécessite que vous demandiez aux gens avec lesquels vous communiquez de chiffrer également leurs courriels en utilisant votre clé de chiffrement seulement mobile.

Expérience pratique : se lancer avec le *guide pratique K9 et APG* [258]

Capture de médias avec un smartphone

La capture d'images, de vidéos ou d'audio avec votre smartphone peut être un moyen effectif de documenter et partager des événements importants. Toutefois, il est important d'être prudent et respectueux de la vie privée et de la sécurité des personnes photographiées, filmées ou enregistrées. Par exemple, si vous prenez des photos ou faites des enregistrements audio ou vidéo d'un événement important, cela peut engendrer une situation dangereuse pour vous ou

pour ceux qui apparaissent dans les enregistrements si votre téléphone tombe entre de mauvaises mains. Dans ce cas, les suggestions suivantes peuvent être utiles :

- Disposez d'un mécanisme permettant de télécharger les fichiers multimédias enregistrés en toute sécurité vers des emplacements en ligne protégés et retirez-les du téléphone instantanément (ou dès que vous le pouvez) après l'enregistrement.
- Utilisez des outils pour flouter les visages de ceux qui apparaissent dans les images ou vidéos, ou pour déformer les voix dans les enregistrements audio ou vidéo et ne stockez que des copies de fichiers multimédias floutées et déformées sur votre périphérique mobile.
- Protégez ou supprimez toute méta-information indiquant le temps et le lieu dans les fichiers multimédias.

Le **Guardian Project** [241] a créé une application *FOSS* [230] appelée **ObscuraCam** [259] pour détecter les visages sur des photos et les flouter. Vous pouvez bien sûr choisir le mode de floutage et ce que vous souhaitez flouter. Obscuracam supprime également les photos originales et si vous avez mis en place un serveur pour télécharger les médias capturés, il fournit des fonctionnalités simples pour les télécharger.

Expérience pratique : se lancer avec le *guide pratique Obscuracam* [260].

Au moment de la rédaction de ces lignes, l'organisation des droits de l'homme **Witness** [261] travaille avec le Guardian Project à une solution quant aux trois points mentionnés ci-dessus.

Accéder à Internet en toute sécurité avec un smartphone

Comme nous en avons discuté dans le ***chapitre 7 : Préserver la confidentialité de vos communications sur Internet*** [237] et le ***chapitre 8 : Préserver votre anonymat et contourner la censure sur Internet*** [149], accéder à des contenus sur Internet ou publier du matériel en ligne tel que des photos ou des vidéos, laisse de nombreuses traces indiquant qui et où vous êtes et ce que vous faites. Cela peut vous mettre en danger. Utiliser votre smartphone pour communiquer avec Internet amplifie ce risque.

Accès par WiFi ou données mobiles

Les smartphones vous permettent de contrôler la façon dont vous accédez à Internet : via une connexion sans fil fournie par un point d'accès (tel qu'un cybercafé), ou via une connexion données mobile telle que GPRS, EDGE ou UMTS, fournies par votre opérateur de réseau mobile.

L'utilisation d'une connexion WiFi réduit les traces de données que vous pourriez laisser auprès de votre opérateur de réseau mobile (en n'utilisant pas votre forfait de téléphonie mobile pour vous connecter). Toutefois, une connexion données mobile est parfois le seul moyen d'être en ligne. Malheureusement, les protocoles de connexion données mobile (telles EDGE ou UMTS) ne sont pas des standards ouverts. Les développeurs indépendants et les ingénieurs de sécurité ne peuvent pas analyser ces protocoles pour voir comment ils sont mis en oeuvre par des supports de données mobiles.

Dans certains pays, les opérateurs de réseau mobile opèrent conformément à une législation différente de celle des fournisseurs d'accès à Internet, ce qui peut conduire à une surveillance plus directe de la part des gouvernements et des transporteurs.

Quel que soit le chemin que vous prenez pour vos communications numériques avec un smartphone, vous pouvez réduire les risques d'exposition des données en utilisant des outils d'anonymisation et de chiffrement.

Anonymiser

Pour accéder à du contenu en ligne de façon anonyme, vous pouvez utiliser une app Android appelée **Orbot** [262]. Orbot fait passer vos communications sur Internet par le réseau anonyme Tor.

Expérience pratique : se lancer avec le *guide pratique Orbot* [263].

Une autre app, Orweb, est un navigateur web qui offre des fonctionnalités améliorant la confidentialité en passant par des serveurs mandataires et en ne conservant pas d'historique local de la navigation. Orbot et Orweb contournent ensemble les filtres et pare-feux du réseau, et procurent une navigation anonyme.

Expérience pratique : se lancer avec le *guide pratique Orweb* [264].

Proxies

La version mobile *Firefox* [265] – **Firefox mobile** [266] peut-être équipée d'extensions proxy qui dirigent le trafic vers un serveur proxy (appelé aussi mandataire). De là, votre trafic est acheminé vers le site que vous souhaitez. Ceci est très utile en cas de censure, mais peut toujours encore révéler vos demandes, à moins que la connexion de votre client au proxy soit chiffrée. Nous recommandons l'extension **Proxy Mobile** [267], (également du **Guardian Project** [268], qui rend facile l'utilisation de serveurs mandataires avec Firefox. Il s'agit également du seul moyen de canaliser les communications

mobiles via Firefox vers Orbot et d'utiliser le réseau *Tor* [248].

Sécurité avancée pour votre smartphone

Obtenez l'accès complet à votre smartphone

La plupart des smartphones peuvent plus que ce que leur système d'exploitation, que ce que les logiciels des fabricants (firmware) et les programmes des opérateurs mobiles permettent. À l'inverse, certaines fonctionnalités sont 'bloquées' si bien que l'utilisateur ne peut ni contrôler ni modifier ces fonctions; elles restent hors de portée. Dans la plupart des cas, ces fonctionnalités sont inutiles. Certaines applications et fonctionnalités permettent cependant parfois d'améliorer la sécurité des données et des communications sur un smartphone. Il existe également d'autres fonctionnalités dont la suppression permet d'éviter des risques.

C'est pour cela, et pour d'autres raisons, que certains utilisateurs de smartphone décident de manipuler les différents logiciels et programmes tournant sous leur smartphone dans le but d'obtenir des passe-droits appropriés leur permettant d'installer des fonctionnalités améliorées, d'en supprimer, ou d'en amoindrir d'autres.

La procédure de dépassement des limites imposées par les opérateurs mobiles ou fabricants de systèmes d'exploitation est appelé rooting (dans le cas des appareils Android), ou jailbreaking, débridage (dans le cas des appareils iOS tels l'iPhone ou l'iPad). En règle générale, un rooting ou débridage réussi a pour conséquence que vous obtenez tous les passe-droits dont vous avez besoin pour installer et utiliser d'autres applications, modifier des configurations autrement verrouillées, et le contrôle complet sur le stockage de données et la mémoire du smartphone.

ATTENTION: Le rooting ou jailbreaking peut être irréversible et demande une certaine expérience quant à l'installation et la configuration de logiciels. Considérez ce qui suit :

- Vous risquez de rendre votre smartphone définitivement inutilisable, de le 'bricker' (cad de le réduire à l'état de 'brique').
- La garantie du fabricant ou de l'opérateur mobile peut être annulée.
- Dans certains endroits, cette procédure peut être illégale.

Mais si vous faites attention, un appareil rooté est un moyen simple de gagner plus de contrôle sur votre smartphone et de le rendre ainsi beaucoup plus sûr.

Firmware alternatifs

Les firmware (appelés aussi micrologiciels) se réfèrent à des programmes étroitement liés à l'appareil en particulier. Ils coopèrent avec le système d'exploitation de l'appareil et sont responsables des fonctions de base du matériel informatique de votre smartphone, telles que le haut-parleur, le microphone, les caméras, l'écran tactile, la mémoire, les clés, les antennes, etc.

Si vous avez un téléphone Android, vous pouvez envisager l'installation d'un firmware alternatif pour renforcer vos possibilités de contrôle de votre téléphone. Notez que pour installer un firmware alternatif, vous devez rooter votre téléphone.

Un firmware alternatif pour Android est par exemple le **Cyanogenmod** [269] qui, entre autres, vous permet de désinstaller des applications au niveau du système de votre téléphone (cad celles installées par le fabricant du téléphone ou votre opérateur de réseau mobile). En faisant cela, vous pouvez réduire les possibilités de contrôle de votre appareil, telles que l'envoi de données à votre fournisseur de services à votre insu.

En outre, Cyanogenmod est livré par défaut avec une application OpenVPN qui peut sinon être fastidieuse à installer. VPN (Virtual Private Network) est l'un des moyens de transiter vos communications en ligne à travers un autre serveur en toute sécurité.

Cyanogenmod propose également un mode de navigation incognito dans lequel l'historique de vos communications n'est pas enregistré sur votre smartphone.

Cyanogenmod est livré avec de nombreuses autres fonctionnalités. Toutefois, il n'est pas compatible avec tous les appareils Android, donc avant de commencer, consultez la liste des appareils compatibles [270].

Chiffrement de volumes entiers

Si votre téléphone est rooté, vous pouvez envisager de chiffrer l'intégralité des données stockées ou de créer un volume sur le smartphone pour protéger certaines informations sur le téléphone.

Luks Manager [271] permet un chiffrement à la volée simple et solide de volumes avec une interface conviviale. Nous vous recommandons fortement d'installer cet outil avant de commencer à stocker des données importantes sur votre appareil Android et d'utiliser les volumes chiffrés que Luks Manager fournit pour stocker toutes vos données.

Le projet Whisper Systems est en train de développer l'application **WhisperCore** [272] qui permettra le chiffrement complet de votre appareil Android.

Réseau Privé Virtuel (virtual private network VPN)

Un VPN fournit un tunnel chiffré à travers Internet entre votre appareil et un serveur VPN. On parle de tunnel parce que contrairement à d'autres trafics chiffrés, comme https, il cache tous les services, protocoles et contenus. Une connexion VPN est configurée une fois et n'est résiliée que lorsque vous en décidez.

Notez que depuis que votre trafic passe par le serveur proxy ou VPN, un intermédiaire a seulement besoin d'accéder au proxy pour analyser vos activités. Par conséquent, il est important de bien choisir parmi les services proxy et VPN. Il est également conseillé d'utiliser différents proxies et/ou VPNs car le fait de répartir vos flux de données réduit les conséquences d'un service compromis.

Nous recommandons d'utiliser le serveur **RiseUp VPN** [273]. Vous pouvez utiliser RiseUp VPN sur un appareil Android après avoir installé Cyanogenmod (voir ci-dessus). Il est également facile d'établir la connexion à RiseUp VPN sur l'iPhone - en savoir plus ici [274].

Glossaire

Voici quelques uns des termes techniques les plus courants accompagnés d'une courte description. Vous trouverez ces termes sur ce site Internet ou dans d'autres ressources similaires.

- ***Adresse IP (Internet Protocol Address)*** – Réfère au numéro unique qui est utilisé pour identifier un ordinateur donné lorsqu'il est connecté à Internet.
- ***Android*** - Un système d'exploitation open source basé sur Linux pour les smartphones et les tablettes, développé par Google.
- ***APG - Android Privacy Guard*** : Application libre et open source pour les smartphones Android facilitant le chiffrement OpenPGP. Il peut être intégré avec K-9 Mail.
- ***App Store*** - Le dépôt par défaut à partir duquel on peut trouver et télécharger des applications iPhone.
- ***Avast*** - Un gratuiciel antivirus.
- ***Base de données de mots de passe sécurisée*** - Un outil utilisé pour chiffrer et stocker plusieurs mots de passe derrière un seul mot de passe principal.
- ***BIOS - Basic Input/Output System (ou système d'entrée-sortie de base)*** - C'est le premier degré de logiciel d'un ordinateur. Le BIOS permet de configurer plusieurs préférences avancées liées au matériel installé sur un ordinateur, y compris un mot de passe au démarrage.
- ***Blackberry*** - Une marque de smartphones utilisant le système d'exploitation BlackBerry développé par Research In Motion (RIM).
- ***Câble de sécurité*** - Un câble que l'on peut cadenasser pour sécuriser un ordinateur portable ou toute autre matériel informatique (dont les disques durs externes et certains ordinateurs de bureau) en l'attachant a un mur ou un bureau et en empêcher le vol.
- ***Carte d'identification de l'abonné (carte SIM)*** - Une petite carte amovible insérée dans un téléphone portable pour établir un service avec une compagnie de téléphonie cellulaire. Les cartes SIM peuvent aussi servir à stocker des listes de numéros de téléphone et des messages texte.
- ***CCleaner*** - Un gratuiciel qui permet de supprimer les fichiers temporaires et toutes les traces de données potentiellement sensibles laissées sur votre disque dur par des programmes que vous avez utilisés récemment (et/ou par le système d'exploitation Windows lui-même).
- ***Certificat de sécurité*** - Moyen par lequel des sites et services Internet sécurisés peuvent prouver, par procédé de chiffrement, qu'ils sont bel et bien ce qu'ils prétendent être. Pour que votre navigateur soit en mesure de reconnaitre la validité d'un certificat de sécurité, le service en question doit payer pour obtenir une signature numérique de la part d'un organisme de confiance. Parce que cela coûte de l'argent, il se peut que vous receviez à l'occasion un message d'erreur même lorsque le service sécurisé est valide.
- ***Chiffrement*** - Un moyen d'employer des mathématiques avancées pour *chiffrer*, ou brouiller, des renseignements qui sont communiqués entre deux parties de telle sorte que ces renseignements ne puissent être *déchiffrés* que par la ou les personnes qui détiennent l'information particulière à cet effet, comme un mot de passe ou une *clé de chiffrement*.
- ***Clam Win*** - Un outil antivirus sous licence FLOSS.
- ***Cobian Backup*** - Un logiciel FLOSS servant à créer automatiquement des copies de sauvegarde de vos données. La plus récente version de Cobian est un gratuiciel de source fermée, mais les sources précédentes étaient publiées sous licence FLOSS.
- ***Code source*** - Le code sous-jacent d'un logiciel, composé par des programmeurs informatique. Le code source d'un outil révèle son fonctionnement et montre s'il est non sûr ou malveillant.
- ***Comodo Firewall*** - Un pare-feu sous licence FLOSS.
- ***Contournement (de la censure / du filtrage)*** - L'action de contourner des filtres Internet pour accéder à des sites et/ou services Internet bloqués.
- ***Cookie*** - Un minuscule fichier, sauvegardé sur votre ordinateur par le navigateur, qui peut être utilisé pour stocker de l'information à l'intention d'un site Internet particulier et/ou pour vous identifier auprès d'un site.
- ***Cryptonite*** - Une application libre et open source pour le chiffrement de fichiers sur les smartphones Android.
- ***Démarrage (ou Booting)*** - L'action de faire démarrer un ordinateur.
- ***Dispositif d'alimentation sans interruption - ASI (ou Uninterruptable Power Supply - UPS)*** - Un dispositif électrique qui permet à un ordinateur ou à certaines pièces d'équipement particulièrement importantes de rester en fonction, ou de s'éteindre normalement, en cas de perte d'électricité ou de chute de courant.
- ***EDGE, GPRS, UMTS*** - Enhanced Data Rates for GSM Evolution, General Packet Radio Service et Universal Mobile Telecommunications System sont des technologies permettant aux appareils mobiles de se connecter à Internet.

- ***Enigmail*** - Un module complémentaire pour le client de messagerie Thunderbird qui permet d'envoyer et recevoir des messages chiffrés et signés numériquement.
- ***Enregistreur de frappe (ou Keylogger)*** - Il s'agit d'un type de logiciel malveillant qui enregistre toutes les touches que vous frappez sur le clavier de votre ordinateur pour ensuite retransmettre les séquences enregistrées à un tiers. Ces logiciels sont régulièrment utilisé pour voler des mots de passe de courriel et autres.
- ***Eraser*** - Un outil qui permet de supprimer, de façon sûre et définitive, des données d'un ordinateur ou d'un dispositif de stockage portable.
- ***F-Droid*** - Un depôt alternatif à partir duquel on peut trouver et télécharger de nombreuses applications libres et open source Android.
- ***Fichier .apk*** - L'extension de fichier utilisée pour les applications Android.
- ***Fichier d'échange (ou Swap file)*** - Un fichier où des données (qui peuvent être de nature sensible) sont parfois sauvegardées automatiquement afin d'améliorer la performance générale de l'ordinateur.
- ***Firefox*** - Un navigateur Web sous licence FLOSS qui constitue une alternative populaire à Microsoft Internet Explorer.
- ***FLOSS*** - Free/Libre Open-Source Software. Les logiciels appartenant à cette famille sont gratuits et ne comportent aucune restrictions juridiques servant à empêcher les utilisateurs de les tester, les partager ou les modifier.
- ***FSI ou FAI (ou ISP)*** - Fournisseur de services Internet ou Fournisseur d'accès à Internet. Il s'agit de la compagnie ou de l'organisme qui vous fournit votre connexion initiale à Internet. Plusieurs gouvernements nationaux exercent un contrôle sur l'accès à Internet (y compris le filtrage et la surveillance) par l'intermédiaire du FSI qui dessert les utilisateurs de ce pays.
- ***Gibberbot*** - Une application libre et open source pour Android permettant de chatter en toute sécurité via XMPP protocol (également utilisé par Google Talk). Elle est compatible avec Off-the-Record et, utilisée en conjonction avec Orbot, peut router des conversations vocales via le réseau Tor.
- ***GNU/Linux*** - Un système d'exploitation sous licence FLOSS qui constitue une alternative de plus en plus populaire à Microsoft Windows.
- ***Google Play*** - Le dépôt par défaut à partir duquel on peut trouver et télécharger des applications Android.
- ***Gratuiciel (ou Freeware)*** - Désigne les logiciels qui sont gratuits mais qui comportent des restrictions juridiques qui servent à empêcher les utilisateurs d'accéder au code source employé pour les créer.
- ***Graveur de CD*** - Un lecteur de CD-ROM qui a la capacité d'écrire des données sur un disque compact vierge. Les *graveurs de DVD* ont la même fonction, mais avec des disques DVD. Les graveurs *CD-RW* et *DVD-RW* ont également la capacité de supprimer et de réécrire des données plus d'une fois sur un même disque CD-RW ou DVD-RW.
- ***Guardian Project*** - Une organisation qui crée des applications smartphones, améliore et personnalise les systèmes d'exploitation mobiles dans le but de sécuriser les échanges privés.
- ***iPhone*** - Une marque de smartphones créée par Apple utilisant le système d'opération iOS d'Apple.
- ***Jailbreak*** - Le processus de déverrouillage de fonctionnalités sur un iPhone sinon bloquées par le fabricant ou l'opérateur permettant d'obtenir un accès complet au système d'exploitation.
- ***K-9 Mail*** - Un client de messagerie libre et open source pour smartphones Android qui, utilisé avec l'application APG, permet le chiffrement OpenPGP.
- ***KeePass*** - Un outil gratuiciel permettant de créer une base de données de mots de passe sécurisée.
- ***Liste blanche*** - Une liste de sites et services Internet auxquels un certain accès est permis, là où d'autres sites et services sont automatiquement bloqués.
- ***Liste noire*** - Une liste de sites et services Internet dont l'accès est bloqué en vertu d'une politique de filtrage restrictive.
- ***LiveCD*** - Un CD qui permet de faire fonctionner temporairement votre ordinateur avec un système d'exploitation différent.
- ***Logiciel malveillant (ou Malware)*** - Un terme générique pour désigner tous les logiciels malveillants, y compris les virus, les logiciels espions, les Chevaux de Troie (*Trojan*) et autre menaces semblables.
- ***Logiciel propriétaire*** - L'opposée des FLOSS. Ces applications sont habituellement vouées à des utilisations commerciales, mais peuvent parfois être utilisées en freeware avec des conditions d'utilisation restrictives.
- ***Menace physique*** - Dans le présent contexte, il s'agit de n'importe quelle menace à vos données sensibles découlant de l'accès physique direct que peuvent avoir d'autres personnes à votre ordinateur et votre matériel physique, ou toute autre risque physique, comme des bris, des accidents ou des catastrophes naturelles.
- ***Nettoyage (ou Wiping)*** - L'action de supprimer des données de façon sécurisée et définitive.
- ***Nom de domaine*** - L'adresse, en mots, d'un site ou service Internet ; par exemple, security.ngoinabox.org
- ***NoScript*** - Un module de sécurité complémentaire pour le navigateur Firefox. NoScript vous protège contre les programmes malveillants qui pourraient se dissimuler dans le code source de sites Internet inconnus.
- ***Obscuracam*** - Une application libre et open source pour smartphones Android qui protège l'identité des personnes en facilitant l'édition des photographies tel le floutage des visages.
- ***Off the Record (OTR)*** - Un module complémentaire de chiffrement pour le programme de messagerie instantanée Pidgin.
- ***Orbot*** - Une application libre et open source pour smartphones Android qui permet à des applications telles qu'Orweb et Gibberbot de se connecter au réseau Tor.
- ***Orweb*** - Un navigateur Web libre et open source pour smartphones Android qui, utilisé en conjonction avec Orbot, facilite la navigation via le réseau Tor.
- ***Pare-feu*** - Un outil qui sert à protéger un ordinateur contre des connexions suspectes vers (ou depuis) des réseaux locaux ou Internet.
- ***Peacefire*** - Les personnes abonnées à ce service gratuit reçoivent périodiquement des messages contenant une liste actualisée de proxys qui peuvent être employés pour contourner les mesures de filtrage et de censure d'Internet.
- ***Pidgin*** - Un programme de messagerie instantanée sous licence FLOSS et compatible avec un module de chiffrement appelé *Off the Record (OTR)*.
- ***Pirate informatique (ou Hacker)*** - Dans le présent contexte, il s'agit d'un criminel informatique qui pourrait tenter

d'accéder à vos données sensibles ou de prendre le contrôle de votre ordinateur à distance.

- ***Politique de sécurité*** - Un document écrit qui décrit clairement les moyens par lesquels votre organisme peut se protéger efficacement contre diverses menaces, y compris une liste de mesures à prendre si certains problèmes de sécurité se produisent.
- ***Procédé mnémonique*** - Une astuce simple qui vous aide à vous rappeler de mots de passe complexes.
- ***Riseup*** - Un service de courrier électronique géré par des activistes (et à l'intention des activistes) auquel il est possible d'accéder par interface webmail (sur Internet) ou à l'aide d'un client de messagerie comme *Mozilla Thunderbird*.
- ***Rooting*** - Le processus de déverrouillage de fonctionnalités sur un téléphone Android sinon bloquées par le fabricant ou l'opérateur mobile permettant d'obtenir un accès complet au système d'exploitation.
- ***Routeur*** - Une pièce d'équipement informatique par lequel un ordinateur peut être connecté à un réseau local et des réseaux locaux peuvent être connectés à Internet. Les *commutateurs*, *passerelles* et *concentrateurs* ont des fonctions similaires, tout comme les *points d'accès* sans-fil pour les ordinateurs qui disposent du matériel approprié.
- ***Serveur*** - Un ordinateur qui reste en fonction et connecté à Internet en permanence pour fournir un service, comme l'hébergement d'un site Internet ou le courrier électronique, à d'autres ordinateurs.
- ***Serveur mandataire (ou Proxy)*** - Un service intermédiaire par lequel il est possible de canaliser une partie ou l'ensemble de vos communications sur Internet et qui peut être utilisé pour contourner la censure sur Internet. Un proxy peut être d'accès public ou il peut être nécessaire de s'y connecter avec un nom d'utilisateur et un mot de passe. Seulement une minorité de proxys sont sécurisés, c.-à-d. qu'ils utilisent un procédé de chiffrement pour protéger la confidentialité des renseignements qui sont communiqués entre votre ordinateur et les services Internet auxquels vous souhaitez vos connecter par l'intermédiaire du proxy.
- ***Signature numérique*** - Un moyen par lequel il est possible d'authentifier la source d'un fichier ou d'un message (c.-à-d. de prouver que l'expéditeur est bel et bien la personne qu'elle prétend être) à l'aide d'un procédé de chiffrement.
- ***Skype*** - Un outil gratuiciel de Voix sur réseau IP (VoIP) qui permet de parler gratuitement avec d'autre utilisateurs Skype et d'appeler des téléphones normaux moyennant des frais modiques. La compagnie qui gère Skype prétend que les conversations entre utilisateurs Skype sont chiffrées. Comme il s'agit d'un outil de source fermée, il est impossible de vérifier cette affirmation mais plusieurs personnes y prêtent foi. Skype offre aussi un service de messagerie instantanée.
- ***Spybot*** - Un gratuiciel anti logiciel malveillant utilisé pour balayer un ordinateur afin d'y détecter des logiciels espions et les supprimer.
- ***SSL*** – La technologie qui permet de maintenir une connexion chiffrée sécurisée entre votre ordinateur et certains des sites et services Internet que vous visitez. Lorsque vous êtes connecté à un site Internet par SSL, l'adresse du site commence par `HTTPS` plutôt que `HTTP`.
- ***Stéganographie*** - Toute méthode employée pour déguiser des données en leur donnant l'aspect d'autres types de données dans le but d'éviter d'attirer l'attention sur des renseignements sensibles.
- ***Textsecure*** - Une application libre et open source pour Android facilitant l'envoi et le chiffrement de messages texte.
- ***Thunderbird*** - Un client de messagerie sous licence FLOSS qui présente un certain nombre de fonctions de sécurité, y compris le module de chiffrement Enigmail.
  Tor - Un outil de connexion anonyme qui permet de contourner la censure sur Internet et de cacher les sites et services Internet que vous visitez à quiconque aurait intérêt à surveiller votre connexion Internet, en plus de masquer votre propre emplacement à ces sites et services.
- ***TrueCrypt*** - Un outil de chiffrement sous licence FLOSS qui permet de stocker des données sensibles de façon sécurisée.
- ***Undelete Plus*** - Un gratuiciel qui, selon les circonstances, peut restaurer des données qui ont été supprimées accidentellement.
- ***VaultletSuite 2Go*** - Un programme (gratuiciel) de courrier électronique chiffré.
- ***Voix sur IP (VoIP)*** – La technologie qui permet d'utiliser Internet pour communiquer avec la voix avec d'autres utilisateurs de VoIP.
- ***Windows Phone*** - Un système d'exploitation mobile développé par Microsoft.
- ***Your-Freedom*** - Un gratuiciel de contournement qui permet de contourner des mesures de filtrage en se connectant à Internet par l'intermédiaire d'un proxy privé. Si Your-Freedom est configuré correctement, votre connexion à ces proxys sera chiffrée afin de protéger la confidentialité de vos communications.

Liens:
[1] https://securityinabox.org/fr/glossaire#Hacker
[2] https://securityinabox.org/glossaire#Logiciel_malveillant
[3] https://securityinabox.org/glossaire#Avast
[4] https://securityinabox.org/glossaire#Spybot
[5] https://securityinabox.org/fr/glossaire#Comodo
[6] https://securityinabox.org/fr/glossaire#Gnu_Linux
[7] https://securityinabox.org/glossaire#Gratuiciel
[8] https://securityinabox.org/fr/glossaire#FLOSS
[9] https://securityinabox.org/fr/avast_principale
[10] https://securityinabox.org/avast_utiliser#Section_3.2.1
[11] https://securityinabox.org/avast_principale
[12] https://securityinabox.org/fr/spybot_principale
[13] https://securityinabox.org/glossaire#Code_source
[14] https://securityinabox.org/glossaire#Firefox
[15] https://securityinabox.org/glossaire#NoScript
[16] https://securityinabox.org/firefox_noscript
[17] https://securityinabox.org/firefox_principale
[18] https://securityinabox.org/glossaire#Hacker
[19] https://securityinabox.org/glossaire#Comodo
[20] https://securityinabox.org/fr/comodo_principale

[21] https://securityinabox.org/chapter_1_5
[22] https://securityinabox.org/glossaire#Routeur
[23] https://www.libreoffice.org/
[24] http://www.ubuntu.com/
[25] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_9.html
[26] http://www.frontlinedefenders.org/manual/en/esecman/appendix_c.html
[27] http://www.frontlinedefenders.org/manual/en/esecman/
[28] http://www.virusbtn.com
[29] http://www.marksanborn.net/howto/turn-off-unnecessary-windows-services
[30] http://tacticaltech.org
[31] http://www.askvg.com/download-free-bootable-rescue-cds-from-kaspersky-bitdefender-avira-f-secure-and-others/
[32] http://www.selectrealsecurity.com/malware-removal-guide
[33] https://securityinabox.org/fr/glossaire#Politique_de_securite
[34] https://securityinabox.org/fr/glossaire#Menace_physique
[35] https://securityinabox.org/glossaire#Menace_physique
[36] https://securityinabox.org/glossaire#Skype
[37] https://securityinabox.org/glossaire#Serveur
[38] https://securityinabox.org/glossaire#Cable_de_securite
[39] https://securityinabox.org/chapter-3
[40] https://securityinabox.org/glossaire#BIOS
[41] https://securityinabox.org/glossaire#Chiffrement
[42] https://securityinabox.org/chapter-4
[43] https://securityinabox.org/glossaire#ASI
[44] https://securityinabox.org/glossaire#Politique_de_securite
[45] https://securityinabox.org/chapter-5
[46] https://securityinabox.org/fr/chapter_2_5
[47] http://www.frontlinedefenders.org/manual/en/esecman/chapter1_2.html
[48] http://www.frontlinedefenders.org/manual/en/esecman/chapter1_3.html
[49] http://www.frontlinedefenders.org/manual/en/esecman
[50] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_1.html#2_1c
[51] http://www.frontlinedefenders.org/manual/en/esecman/chapter4.html
[52] http://www.frontlinedefenders.org/manuals/protection
[53] http://www.frontlinedefenders.org/security-training
[54] https://securityinabox.org/fr/glossaire#Chiffrement
[55] https://securityinabox.org/glossaire#BD_de_mots_de_passe_securises
[56] https://securityinabox.org/fr/glossaire#Keepass
[57] https://securityinabox.org/chapter_3_2
[58] https://securityinabox.org/glossaire#Keepass
[59] https://securityinabox.org/glossaire#Procede_mnemonique
[60] https://passfault.appspot.com/password_strength.html
[61] https://securityinabox.org/keepass_principale
[62] https://securityinabox.org/chapter_5
[63] https://securityinabox.org/fr/chapter-4
[64] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_2.html
[65] http://www.frontlinedefenders.org/manual/en/esecman/appendix_d.html
[66] http://fr.wikipedia.org/wiki/Password
[67] http://en.wikipedia.org/wiki/Password_strength
[68] http://fr.wikipedia.org/wiki/Password_cracking
[69] http://www.fr.wikipedia.org/wiki/Password
[70] http://www.en.wikipedia.org/wiki/Password_strength
[71] http://www.fr.wikipedia.org/wiki/Password_cracking
[72] https://securityinabox.org/chapter-1
[73] https://securityinabox.org/chapter-2
[74] https://securityinabox.org/glossaire#FLOSS
[75] https://securityinabox.org/glossaire#TrueCrypt
[76] https://securityinabox.org/fr/glossaire#TrueCrypt
[77] https://securityinabox.org/fr/truecrypt_principale
[78] https://securityinabox.org/fr/glossaire
[79] https://securityinabox.org/fr/chapter_4_2
[80] https://securityinabox.org/fr/chapter-6
[81] https://securityinabox.org/fr/glossaire#Logiciel_malveillant
[82] https://securityinabox.org/fr/glossaire#Steganographie
[83] https://securityinabox.org/fr/chapter_4_3
[84] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_4.html
[85] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_8.html
[86] http://www.frontlinedefenders.org/manual/en/esecman/chapter4_2.html
[87] http://www.truecrypt.org/docs/
[88] http://www.truecrypt.org/faq.php
[89] https://securityinabox.org/glossaire#Cobian
[90] https://securityinabox.org/glossaire#Undelete_Plus
[91] https://securityinabox.org/glossaire#Pare-feu
[92] https://securityinabox.org/truecrypt_principale
[93] https://securityinabox.org/glossaire#Thunderbird
[94] https://securityinabox.org/fr/thunderbird_principale
[95] https://securityinabox.org/glossaire#Graveur_CD
[96] https://securityinabox.org/chapter_5_5
[97] https://securityinabox.org/cobian_principale
[98] https://securityinabox.org/chapter-6
[99] https://securityinabox.org/fr/recuva_principale
[100] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_3.html
[101] https://www.wuala.com/fr/
[102] https://spideroak.com/
[103] https://www.google.com/intl/fr/drive/start/index.html
[104] https://tahoe-lafs.org/trac/tahoe-lafs
[105] http://fr.wikipedia.org/wiki/Récupération_de_données
[106] https://securityinabox.org/glossaire#Eraser
[107] https://securityinabox.org/glossaire#Wiping

[108] https://securityinabox.org/glossaire#CCleaner
[109] https://securityinabox.org/glossaire#Swap_file
[110] https://securityinabox.org/eraser_principale
[111] https://securityinabox.org/glossaire#Cookie
[112] https://securityinabox.org/ccleaner_principale
[113] http://support.mozilla.com/en-US/kb/Clearing+Private+Data
[114] http://www.ccleaner.com/help/faq
[115] http://www.usenix.org/publications/library/proceedings/sec96/full_papers/gutmann/
[116] http://en.wikipedia.org/wiki/Gutmann_method
[117] https://support.mozilla.com/en-US/kb/Clearing+Private+Data
[118] http://www.en.wikipedia.org/wiki/Gutmann_method
[119] https://jitsi.org/
[120] https://securityinabox.org/glossaire#VoIP
[121] https://securityinabox.org/glossaire#Riseup
[122] https://securityinabox.org/glossaire#OTR
[123] https://securityinabox.org/glossaire#Pidgin
[124] https://securityinabox.org/glossaire#Enigmail
[125] https://securityinabox.org/glossaire#Keylogger
[126] https://securityinabox.org/chapter_7_4#Chiffrer_et_authentifier_des_messages_individuellement
[127] https://securityinabox.org/chapter_7_4
[128] https://securityinabox.org/chapter_7_2
[129] https://securityinabox.org/glossaire#FSI
[130] https://securityinabox.org/glossaire#SSL
[131] https://securityinabox.org/glossaire#Certificat_de_securite
[132] https://securityinabox.org/glossaire#Adresse_IP
[133] https://securityinabox.org/chapter_7_5
[134] https://mail.riseup.net
[135] https://securityinabox.org/riseup_principale
[136] https://securityinabox.org/thunderbird_principale
[137] https://securityinabox.org/glossaire#Tor
[138] https://securityinabox.org/chapter-8
[139] https://securityinabox.org/glossaire#Contournement
[140] https://securityinabox.org/fr/chapter-3
[141] https://securityinabox.org/en/keepass_main
[142] https://securityinabox.org/fr/chapter-1
[143] https://securityinabox.org/fr/chapter-2
[144] https://securityinabox.org/fr/chatper-11
[145] https://securityinabox.org/fr/avast_virus#4.1
[146] https://securityinabox.org/fr/avast_virus#4.4
[147] https://securityinabox.org/fr/firefox_principale
[148] http://libreoffice.org
[149] https://securityinabox.org/fr/chapter-8
[150] https://securityinabox.org/fr/glossary#VoIP
[151] https://securityinabox.org/pidgin_principale
[152] http://www.skype.com
[153] http://jitsi.org/
[154] http://www.google.com/talk
[155] http://voice.yahoo.com/
[156] http://get.live.com/messenger
[157] https://securityinabox.org/chapter_1_4
[158] https://securityinabox.org/glossaire#VaultletSuite
[159] https://securityinabox.org/vaultletsuite_principale
[160] https://securityinabox.org/glossaire#Signature_numerique
[161] https://securityinabox.org/thunderbird_utiliserenigmail
[162] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_5.html#2_5b
[163] http://www.frontlinedefenders.org/manual/en/esecman/chapter2_7.html#2_7c
[164] http://mail.google.com/mail/help/intl/fr/privacy.html
[165] http://news.cnet.com/8301-13578_3-9962106-38.html
[166] http://help.riseup.net/mail/mail-clients/
[167] http://mail.google.com/support/bin/topic.py?topic=12805
[168] http://email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[169] http://www.gizmo5.com/pc
[170] http://www.voice.yahoo.com
[171] http://www.download.live.com/?sku=messenger
[172] https://mail.google.com/mail/help/intl/fr/privacy.html
[173] http://www.news.cnet.com/8301-13578_3-9962106-38.html
[174] http://help.riseup.net/mail/mail-clients
[175] https://mail.google.com/support/bin/topic.py?topic=12805
[176] http://www.email.about.com/od/mozillathunderbirdtips/qt/et_gmail_addr.htm
[177] https://securityinabox.org/glossaire#Liste_noire
[178] https://securityinabox.org/glossaire#Nom_de_domaine
[179] https://securityinabox.org/glossaire#Proxy
[180] http://opennet.net/
[181] http://www.rsf.org/
[182] http://www.blogger.com
[183] https://securityinabox.org/tor_principale
[184] https://securityinabox.org/glossaire#Peacefire
[185] https://securityinabox.org/chapter_8_5
[186] https://help.riseup.net/en/riseup-vpn
[187] https://we.riseup.net/riseuphelp+en/vpn-howto
[188] http://www.hotspotshield.com/
[189] http://www.your-freedom.net/index.php?id=3
[190] http://www.your-freedom.net/index.php?id=170
[191] http://www.your-freedom.net/
[192] https://www.your-freedom.net/index.php?id=172
[193] https://www.your-freedom.net/index.php?id=doc
[194] http://www.addictivetips.com/windows-tips/freegate-lets-you-access-blocked-websites-at-optimal-speed/

[195] http://www.securitykiss.com/resources/download/
[196] http://psiphon3.com
[197] http://www.peacefire.org/
[198] http://www.frontlinedefenders.org/esecman/
[199] http://en.flossmanuals.net/CircumventionTools
[200] http://en.cship.org/wiki/Main_Page
[201] http://www.civisec.org/sites/securitybkp.ngoinabox.org/themes/civisec/guides/everyone%27s-guide-english.pdf
[202] http://www.rsf.org/rubrique.php3?id_rubrique=527
[203] http://advocacy.globalvoicesonline.org/tools/guide/
[204] https://www.eff.org/wp/locational-privacy
[205] https://securityinabox.org/fr/social_networking_tools
[206] https://securityinabox.org/fr/glossaire#GPS
[207] https://securityinabox.org/fr/glossaire#Carte_SIM
[208] https://securityinabox.org/en/node/1777
[209] https://securityinabox.org/en/node/1778
[210] https://securityinabox.org/en/node/1779
[211] https://securityinabox.org/en/node/1780
[212] https://securityinabox.org/fr/glossaire#SSL
[213] https://securityinabox.org/fr/glossaire#Java
[214] https://securityinabox.org/fr/glossaire#IrDA
[215] https://securityinabox.org/fr/glossaire#Bluetooth
[216] http://mobiles.tacticaltech.org
[217] http://wiki.mobiles.tacticaltech.org/index.php/Security
[218] http://www.activistsecurity.org/
[219] http://www.freebeagles.org/articles/mobile_phones.html
[220] http://mobileactive.org/mobilesecurity-citizenjournalism
[221] http://sw.nokia.com/id/5274b81c-12d0-43bb-8d89-26f6a1ae111f/A_Brief_Introduction_to_Secure_SMS_Messaging_in_MIDP_en.pdf
[222] http://www.mysecured.com/?p=127
[223] https://securityinabox.org/fr/node/1899
[224] https://securityinabox.org/en/Glossary#GPS
[225] https://securityinabox.org/fr/chapter-5
[226] https://securityinabox.org/en/Glossary#FOSS
[227] https://securityinabox.org/en/glossary#GPS
[228] https://securityinabox.org/en/android_basic
[229] http://f-droid.org
[230] https://securityinabox.org/en/glossary#FOSS
[231] https://securityinabox.org/en/glossary#apk
[232] https://securityinabox.org/fr/node/1974
[233] https://securityinabox.org/fr/node/1972
[234] https://securityinabox.org/en/Glossary#VoIP
[235] https://securityinabox.org/en/glossary#skype
[236] https://securityinabox.org/fr/chapter_7_3
[237] https://securityinabox.org/fr/chapter-7
[238] http://f-droid.org/repository/browse/?fdid=com.csipsimple&fdpage=4
[239] https://guardianproject.info/wiki/OSTN
[240] https://ostel.me
[241] https://guardianproject.info
[242] https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
[243] https://securityinabox.org/fr/node/1973
[244] https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
[245] https://securityinabox.org/en/textsecure_main
[246] https://guardianproject.info/apps/gibber/
[247] https://securityinabox.org/en/glossary#OTR
[248] https://securityinabox.org/en/glossary#Tor
[249] https://securityinabox.org/en/gibberbot_main
[250] https://chatsecure.org
[251] https://securityinabox.org/en/APG_main
[252] https://code.google.com/p/cryptonite/
[253] https://securityinabox.org/fr/chapter_11_7
[254] https://securityinabox.org/en/Cryptonite_main
[255] https://securityinabox.org/fr/KeepassDroid_principale
[256] https://securityinabox.org/fr/chapter_7_1
[257] https://securityinabox.org/fr/chapter_7_2
[258] https://securityinabox.org/en/K9_APG_main
[259] https://guardianproject.info/apps/obscuracam/
[260] https://securityinabox.org/en/Obscuracam_main
[261] https://www.witness.org
[262] https://www.torproject.org/docs/android.html.en
[263] https://securityinabox.org/en/Orbot_main
[264] https://securityinabox.org/en/Orweb_main
[265] https://securityinabox.org/en/glossary#Firefox
[266] http://f-droid.org/repository/browse/?fdid=org.mozilla.firefox
[267] https://guardianproject.info/apps/proxymob-firefox-add-on/
[268] https://guardianproject.info/
[269] http://www.cyanogenmod.com
[270] http://www.cyanogenmod.com/devices
[271] http://www.whispersys.com/
[272] http://www.whispersys.com/whispercore.html
[273] https://help.riseup.net/en/vpn
[274] https://support.apple.com/kb/HT1424