

Journaliste d'investigation et sureté de l'information

Quelques propositions

Paul Guermonprez - paul@guermonprez.eu

25 octobre 2010

Table des matières

1	Astuces minimales en 5mn	3
2	Cas pratiques	3
2.1	Poste de travail	3
2.1.1	Intégrité physique	3
2.1.2	Intégrité logicielle	3
2.1.3	Intégrité du réseau	4
2.1.4	Chiffrer votre disque	4
2.2	Stocker vos fichiers	5
2.2.1	GnuPG	5
2.2.2	Rigueur	5
2.3	Mots de passe	5
2.3.1	Un bon mot de passe ?	5
2.3.2	Rigueur	6
2.4	Organiser la fuite de documents	6
2.4.1	Analogique	6
2.4.2	Numérique	6
2.5	Protéger son enquête en ligne	7
2.6	Protéger son enquête de terrain	7

Résumé

Public : Vous êtes journaliste d'investigation, vous pensez que la sensibilité de vos enquêtes peut vous conduire à être l'objet de divers actes de malveillance ou procédures d'écoute. Légales ou pas, justifiées ou pas, de la part des forces de l'ordre ou d'individus. Vous n'avez pas de compétences en sécurité informatique.

Besoin : Vous ne cherchez pas à vous dissimuler puisque vous êtes donc une cible identifiée a priori (contrairement à un terroriste inconnu). Vous cherchez par contre à vous prémunir de ces intrusions de premier niveau. Le niveau d'attaque subie est haut mais pas maximal (vous n'êtes pas la cible des services secrets sur le long terme non plus).

Légalité : Vous cherchez à rester dans la légalité, mais à ne montrer que le minimum, pour n'avoir à communiquer à la justice que le minimum, et au moment où vous aurez décidé de le faire.

Éthique : Un journaliste ne devrait pas avoir à se cacher pour enquêter. Toutes les atteintes au secret devraient découler d'une procédure judiciaire juste et raisonnable. Or ce n'est plus forcément le cas en France, comme l'ont démontré certaines affaires. Le recours à des techniques de prévention efficaces, bien que dangereuses si utilisées à mauvais escient, deviennent donc éthiquement justifiées.

Solution : Le passage de l'analogique (ondes-papier) au numérique (fichiers-internet) a démultiplié les capacités et l'échelle des interventions possibles, mais il déplace le sujet sur un terrain que vous pouvez maîtriser. Ou au moins tenter. Ce document présente donc quelques éléments techniques qu'un journaliste d'investigation devrait avoir à l'esprit. Il doit se concevoir comme une base minimale, pas comme une assurance de résultat. Il sera corrigé et enrichi par des contributions ultérieures.

Pratique : Des labs d'initiation/réflexion pratiques et gratuits sont possibles, mais uniquement pour des journalistes et en région parisienne. Contact : paul@guermonprez.eu

1 Astuces minimales en 5mn

Si vous n'avez pas le temps de tout lire, les mesures les plus simples à mettre en place améliorant raisonnablement la sureté de l'information sont :

1. Avoir un second mobile à part avec une sim à part pour chaque enquête. Surtout pas un smart phone, le plus simple possible et les options de journal d'appels désactivés. Cacher son existence et son utilisation. Le garder éteint autant que possible et activer les codes SIMs et téléphone.
2. Pour éditer les fichiers les plus sensibles, avoir un PC séparé dédié, réinstallé souvent avec les CDs d'usine (ou mieux démarré avec une clé USB linux), accédant des données chiffrées sur une clé USB, sans jamais accéder au réseau. PC secret et bien caché, idéalement dans un coffre. (un petit netbook à 250e sera parfait).
3. Original et Sauvegardes chiffrées de vos fichiers sensibles. Important !
4. Pour les fuites, ne demandez que le texte au format .txt et procédez par une clé USB que vous détruirez et transférerez le contenu.
5. Réinstallez souvent votre poste principal, celui accédant à internet, par exemple avant de commencer un article, et mettez le à jour des que vous êtes sur internet.

Attention, l'accumulation de demi mesures peu fiables nuit car elles vous apportent un faux sentiment de confiance. Réciproquement, l'ingénierie sociale (la ruse) est plus efficace que bien des mesures techniques à moitié maîtrisées.

2 Cas pratiques

2.1 Poste de travail

Votre poste de travail quotidien peut être volé pour obtenir vos informations passées, ou pour vous en priver. Il peut aussi subir des altérations matérielles ou logicielles pour permettre l'écoute numérique ou aspirer vos fichiers.

2.1.1 Intégrité physique

Il n'y a pas de sureté de l'information sans respect de l'intégrité physique du matériel qui la traite. Le matériel peut vous donner toutes les apparences de sécurité, vous pouvez ajouter tous les mots de passes logiciels, ils ne serviront à rien si une personne a eu physiquement accès à un moment à votre poste, même temporairement, pour l'altérer.

Idéalement, vous vous procurerez un poste sur le marché public (pour éviter le stock de PCs de votre employeur) lors d'un achat physique sans precommande (pour recevoir un exemplaire non altéré), sans laisser de traces de votre achat (savoir quel modèle vous utilisez est en effet très utile). En clair : passez par un tiers et payez en liquide dans un magasin sans prévenir.

Ranger votre pc portable dans un coffre est idéal. Le but n'est pas tant de se protéger des vols que de savoir lorsque votre pc a pu être accédé par un tiers, signe qu'il est temps d'en changer.

2.1.2 Intégrité logicielle

Voilà la point le plus délicat. Tous les OS utilisés et maintenus par l'utilisateur moyen sont en général faiblement protégés, et les logiciels de sécurité mal utilisés. Ils sont facile-

ment la cible de mesures d'écoute/accès à distance. Or les sécuriser demande compétences techniques et rigueur.

Une mesure facile à mettre en place : réinstallez votre PC "à neuf" à partir du CD d'installation fourni par votre fabricant, par exemple à chaque fois que vous voulez accéder à un document très sensible. Cette procédure est simple à effectuer par tout le monde. Il faut cependant avoir une sauvegarde de vos données, et pouvoir réinstaller les logiciels rapidement. Détail important : pensez à garder les CDs de réinstallation dans un endroit séparé et secret, pour éviter leur compromission.

Très efficace mais nécessitant de travailler sous linux : il existe des clés USBs/CDs "live" qui contiennent un OS complet et permettent de démarrer en 30 secondes n'importe quel PC pour effectuer une tâche sensible sans risque qu'une compromission passée n'impacte cette opération. Votre disque dur n'est plus un problème, puis qu'il n'est plus utilisé. Ces clés peuvent contenir tous les outils utiles, comme une suite bureautique OpenOffice pour éditer de longs textes. Détail important : pensez à garder ces clés dans un endroit séparé et secret, pour éviter leur compromission.

2.1.3 Intégrité du réseau

Le réseau peut être utilisé pour mettre en place une écoute logicielle à distance, et bien souvent pour envoyer les le contenu de ces écoutes à son destinataire, quel que soit leur mode d'action.

Ne pas utiliser de réseau (internet, réseau local ou bluetooth) est une solution qui testera la détermination et la légitimité de votre adversaire : il devra passer du piratage logiciel anonymes à l'effraction physique incarnée.

Des qu'un ordinateur est connecté à un réseau, quel qu'il soit, même une seule fois, il doit être considéré comme compromis. Lors de la réinstallation de votre ordinateur à partir des CDs constructeur, faites ce que vous avez à faire sur celui ci sans vous connecter à aucun réseau, puis réinstallez. Alors seulement vous pourrez vous reconnecter. Vous serez alors raisonnablement protégé de l'espionnage logiciel, mais pas du matériel.

Avoir un ordinateur apparemment éteint mais connecté (cable ou wifi) à un réseau n'est pas une protection, puis qu'il peut être contrôlé à distance et s'allumer. Donc pas de câble branché, et faites usage du bouton physique de désactivation du Wifi/Bluetooth.

Si vous utilisez un réseau, préférez les câbles. Si vous utilisez un Wifi, n'acceptez rien de moins que la norme "WPA2" (réglage possible dans l'interface de votre fournisseur internet) et un mot de passe fort. Évitez les appareils bluetooth.

2.1.4 Chiffrer votre disque

Le disque dur est le point faible. Il existe des modèles de portables (Lenovo par exemple) dont le disque peut être chiffré. L'opération se fait au niveau matériel, et le code vous est demandé au démarrage, dès la première seconde. Ce chiffrement n'a qu'un mot de passe faible mais constitue une première protection qui nécessite un matériel spécialisé pour le casser. Nettoyez bien le clavier à l'alcool pour effacer les traces physiques des touches utilisées ou tapez sur toutes les chiffres pour brouillez les traces.

Chiffrement logiciel en bloc : Si le code vous est demandé plus tard, c'est que le chiffrement opère à un plus haut niveau, moins fiable mais complémentaire. (Option "chiffrer votre dossier personnel" de votre système d'exploitation par exemple).

Notez que ces chiffrements ne sont utiles que lorsque votre poste est éteint. Dès que vous l'allumez et tapez un mot de passe tout est déchiffré et le restera (mise en veille, certains

types d'hibernation). Pensez donc à éteindre complètement votre ordinateur pour être protégé. Éventuellement débranchez la batterie et l'alimentation.

D'une manière générale, le chiffage du disque dur apparait comme un bouclier trop parfait pour être utile. Il protège tout d'un bloc, donc rien en particulier.

2.2 Stocker vos fichiers

Vous ne pouvez pas vous prémunir efficacement contre les vols ou les cambriolages. Vous pouvez par contre faire en sorte que vos documents sensibles soient inutilisables en dehors de vos périodes d'édition. Pour cela il vous faut chiffrer vos fichiers.

2.2.1 GnuPG

Le standard dans le domaine : GnuPG. Le concept : vous avez une clé privée secrète pour déchiffrer, et une clé publique pour chiffrer. Les clés publiques s'échangent librement, permettant de chiffrer un fichier à destination d'un collègue. Plus compliqué qu'une simple archive protégée par mot de passe, mais aussi beaucoup plus solide.

L'usage de la clé privée est protégé par un mot de passe. La clé privée, qui se présente sous forme d'un petit fichier doit être gardée dans un endroit secret, même si elle est inutile sans le mot de passe. Il est utile d'avoir plusieurs clés pour différents niveaux de sureté : une clé pour le quotidien présente sur votre ordinateur, une clé pour les fichiers les plus sensibles, rarement accédés.

Avec des sauvegardes non chiffrées vous avez le choix entre ne pas en faire et risquer de perdre vos données au premier vol ou faire des sauvegardes non chiffrées et propager involontairement vos données. La compromission des sauvegardes est un problème classique. Chiffrer des fichiers est particulièrement utile pour faire des sauvegardes sécurisées ou échanger des documents avec des tiers identifiés (après échange des clés).

2.2.2 Rigueur

Même si le chiffrement est accessible à tous, il demande un apprentissage et une certaine rigueur. Utiliser une clé sur un poste non sur est un risque, taper son mot de passe sans se cacher est une faille classique. Donc chiffrer peu mais chiffrer bien. Faites le pour les documents les plus sensibles, depuis un poste réinstallé à neuf pour l'occasion et encore jamais connecte à internet. Choisissez un mot de passe vraiment tordu et protégez vous lors de la saisie.

Dernier point : un fichier une fois chiffré, l'original reste présent. Vous devez non pas l'effacer (ce qui ne fait que le cacher superficiellement) mais faire un "wipe", sorte d'effacement beaucoup profond. N'essayez pas de chiffrer des fichiers sur un disque dur classique, stockez vos fichiers sur une clé USB au format "FAT32". En effet tout ce que vous créez sur un disque dur standard ne peut que très difficilement être effacé.

2.3 Mots de passe

Du chiffrement à votre compte email, les mots de passe sont partout. Mais la sureté de l'information n'est nulle part.

2.3.1 Un bon mot de passe ?

Pour casser un mot de passe, un indiscret à plusieurs méthodes :

- Brutale : Un logiciel utilise les dictionnaires de toutes les langues et teste tous les mots, les combinaisons, mais aussi de nombreuses transformations couramment utilisées (nous avons tous les même fausse bonnes idées).
- Fine : Des éléments aléatoires de tout ce qui peut être récolté sur vous est associée à la recherche, du nom de votre chien à vos copains d'enfance (internet est une mine d'or), de tous les livres que vous avez à votre liste de lecture musicale. Si vous écrivez tout le vocabulaire et les champs lexicaux de vos textes y passeront aussi.
- Pattern : Si un autre mot de passe utilisé pour des services peu sûrs a été trouvé, les règles qui seront apprises de ce mot de passe seront ajoutées à la recherche. Ne recyclez pas vos mots de passe, et n'utilisez pas de règles pour les imaginer.

Toujours aussi sur de vos mots de passe? Votre mot de passe vous semble tordu, mais résistera t il à des millions d'essais par secondes pendant des heures? des jours? des semaines? Un bon mot de passe : le plus long possible (8 minimum) en utilisant tout l'éventail de caractères possibles (accentuation comprise). L'aléatoire total est l'idéal absolu.

2.3.2 Rigueur

Quand bien même votre mot de passe serait bon, il est souvent mal utilisé. Vous tapez votre mdp sur un poste partagé au bureau ou dans un webcafé, mais si ces postes sont vérolés et l'enregistrent? Facile : les taches de graisses sur les touches (vous n'êtes jamais entre dans un immeuble à digicode, en quelques essais grâce à cela?). Plus délicat : vous avez un poste sur, mais une petite camera dans votre bureau est pointée sur votre clavier? (un classique).

Puisque vous n'avez pas envie de maintenir une rigueur sans faille au quotidien, organisez des compartiments. Créez un mot de passe fantastique, que vous n'utiliserez que sur un netbook rangé dans un coffre pour consulter et éditer vos fichiers les plus sensibles. Ce netbook ne sera jamais connecté à internet. Vous ne taperez ce mot de passe que sur ce clavier, sous un tissu, et penserez à nettoyer le clavier à l'alcool juste après.

2.4 Organiser la fuite de documents

La matière du journaliste d'investigation est souvent faite de documents transmis par sources anonymes qui aimeraient le rester. Un problème typique serait de confondre la sureté de l'information en elle même et de l'identité de l'informateur (exemple en utilisant Skype).

Vient alors le débat : sous forme numérique ou analogique? Un fichier .doc par email ou une copie papier?

2.4.1 Analogique

Tout procédé analogique laisse des traces uniques, qui peuvent être identifiées. Un fax laisse des imperfections uniques, une imprimante aussi, sans parler du papier ou de vos empreintes sur celui ci. Mais il s'agit plus de confirmer une provenance suspectée que de la trouver.

2.4.2 Numérique

Le numérique laisse aussi des traces.

- Dans le contenu : un fichier .doc est truffé de détails techniques sur la machine qui a servi à éditer le fichier, les fontes, l'utilisateur, et souvent les différentes éditions

successives. Il est presque impossible de les nettoyer. Le transformer en .pdf n'aide que marginalement. Pareil pour les photos et images, qui gardent en elles des métadonnées très précises sur l'appareil, les circonstances, l'optique utilisée, le logiciel de transfert ...

- Sur le poste d'édition : Le logiciel d'édition laisse des fichiers temporaires pour récupérer après un plantage par exemple. Combiné avec l'incapacité à effacer correctement un fichier, le poste de travail est un piège qui trahira l'auteur de la fuite. Si votre informateur est censé être en possession du document sur son poste, il ne sera par contre pas inquiété.

Solution : ne traiter que le texte, l'information brute, dans un éditeur simple et prévisible comme notepad et enregistrer au format .txt.

Mais le gros problème du fichier numérique, c'est son transfert anonyme et discret.

- Un email laisse des traces indélébiles sur son parcours, et tous les emails et leur fichiers attachés sont scannés au départ ou à l'arrivée. Scannés pour filtrer les virus, mais la recherche de mots clés n'en est qu'une extension très facile à installer.
- Même sans ces traces, le média en lui-même en dit long sur le poste créateur et son auteur, qu'il s'agisse d'email, clé USB ou CD.

Utiliser un média physique comme un CD (ou une clé USB) contenant uniquement un fichier .txt, média qui sera détruit dès la réception est probablement la meilleure option.

2.5 Protéger son enquête en ligne

Puisqu'une partie de votre enquête se déroule en ligne, vos recherches et consultations vous trahissent aussi.

De votre côté, votre navigateur garde par défaut en mémoire les pages consultées, vos mots de passe. La fonction "Effacer mes traces" ne peut malheureusement que les effacer superficiellement. Le mode anonyme des navigateurs récents est lui plus efficace.

Du côté du serveur, tout ce qui vous caractérise, de votre dernière page visitée à la localisation géographique supposée, et bien sûr des détails sur votre poste de travail est disponible dès que vous chargez une simple page, ou que vous recevez un simple email (si vous chargez les images dans la mise en page du mail).

Si vous surfez en étant connecté à votre compte GMail par exemple, vos recherches sont stockées et consultables depuis n'importe quel poste qui aura votre mot de passe.

Côté communication audio-video, des solutions comme Skype existent, mais elles ne font que chiffrer la communication, pas l'anonymiser. Votre fournisseur saura à quel poste (à quelle IP distante) vous parlez. Les gouvernements ont souvent accès, eux, au contenu. Dans tous les cas un petit logiciel sur votre poste pourra tout enregistrer.

Cote email, choisissez un prestataire situé dans un pays où le sujet que vous traitez n'a pas de prise, et qui n'a pas de filiale en France. Au-delà des actions en justice, les "indiscrétions" sont plus faciles lorsque l'indiscret et la donnée sont à moins de 10km qu'à 5000km.

2.6 Protéger son enquête de terrain

Vous avez sur vous un mouchard fantastique : votre mobile. Il donne votre localisation en temps réel par votre opérateur. Son signal bluetooth vous identifie partout où vous passez (auprès de tout le monde).

Les réseaux Wifi que vous croisez (même sans les utiliser) vous localisent. Voir dans la mémoire de votre mobile intelligent la liste de tous les réseaux croisés au cours de la

journée retrace votre itinéraire.

Les logiciels que vous chargez typiquement sur votre mobile (ou que d'autres chargent pour vous) font ce qu'ils veulent de ces données sans vous en avertir et les transmettent sur internet. Sans parler des classiques journaux d'appels, sur le mobile lui même ou par votre opérateur.

Par ailleurs, le GPS de votre voiture a une excellente mémoire.

Pour faire simple, la seule solution à peu près efficace consiste à avoir un second mobile extrêmement rudimentaire, avec une carte SIM dédiée que vous aurez acquis auprès d'un tiers. Ce mobile restera éteint l'essentiel du temps et vous ne montrerez à personne que vous le possédez ou l'utilisez. Vous changerez de mobile régulièrement et mélangerez les fournisseurs pour les SIM.

Vous n'emporterez pas votre mobile habituel lors de vos enquêtes de terrain et rendez vous sensibles.

La fouille de données automatisée peut aussi vous trahir. Exemple : vous utilisez une carte SIM qu'un ami de classe primaire en province vous a fourni. Il n'a rien à voir avec votre travail, ni même Paris. Vous utilisez cette SIM pour téléphoner à un employé d'un cabinet ministériel. Plus tard, une enquête peu respectueuse du respect des sources est menée pour savoir si un des membres du ministère a eu des contacts avec un des journaliste de votre journal. Il est fort possible qu'un logiciel fasse indirectement le lien qu'un humain n'aurait pas réussi à faire directement.