Quelques principes fondamentaux

Cette page est un complément de celle-ci. Si vous êtes arrivé ici par un autre chemin, allez donc la lire

Commençons par quelques définitions, histoire de bien se comprendre :

- **Vie privée :** Il s'agit du droit de contrôler l'information que vous partagez sur vous-même. En ce qui concerne internet, la vie privée se réfère souvent à la protection des informations personnelles que vous partagez en ligne, que ce soit volontairement (par exemple, lors de la création d'un compte sur un site web) ou involontairement (par exemple, lorsque votre adresse IP est enregistrée par un site web que vous visitez).
- **Anonymat :** L'anonymat sur internet signifie que votre identité réelle est inconnue. Cela peut être accompli de diverses manières, par exemple en utilisant un pseudonyme lorsque vous postez des commentaires en ligne, en utilisant une adresse IP masquée pour masquer votre localisation réelle, ou en utilisant des outils de navigation privée pour empêcher le suivi de vos activités en ligne.
- **Sécurité :** En termes d'internet, la sécurité fait référence à la protection contre les menaces en ligne. Cela inclut la protection de vos informations personnelles contre le vol ou l'exploitation, la protection de votre ordinateur contre les logiciels malveillants et les attaques, et la garantie que vos communications en ligne sont sécurisées et ne peuvent pas être interceptées ou déchiffrées par des tiers non autorisés.

En bref, ces trois concepts sont liés mais distincts : la vie privée est centrée sur le contrôle de vos propres informations, l'anonymat est centré sur la dissimulation de votre identité, et la sécurité est centrée sur la protection contre les menaces.

Il est crucial de se souvenir de ces distinctions, parce que une situation peut être excellente d'un point de vue de la sécurité, mais très mauvaise au plan de la vie privée, ou inversement. Vous serez peut être amenés à faire des choix en faveur de l'une ou l'autre de ces notions, et au détriment de l'autre. Autant les faire en connaissance de cause.

Utiliser prioritairement des protocoles et des logiciels libres

S'il est parfaitement envisageable qu'un logiciel propriétaire soit sécurisé et respectueux de votre vie privé, il est essentiellement impossible d'en être certain sans avoir accès au code. De ce fait, les logiciels libres ont un avantage structurel dans ce domaine, et **vous devriez les favoriser chaque fois que c'est possible**.

Attention cependant, ce n'est **en aucun cas une garantie**, et le simple usage de logiciels et de protocoles libres n'est pas suffisant pour sécuriser ses pratiques.

Identifier ses besoins, les enjeux et connaître les limites

En matière de sécurité et d'anonymat, il n'y a pas de solution unique qui s'adapterait à toutes les situations. Certains compromis, trop contraignant, seront inenvisageables pour votre usage quotidien, mais seront indispensable si vous cherchez un anonymat avancé. Pour être efficace, vous devrez identifier votre situation et vos besoins, et adopter des pratiques adaptées spécifiquement.

Au delà de quelques bonnes pratiques qui s'appliquent à toutes les situations, vous devrez avoir une idée relativement précise de ce que vous cherchez (par exemple, les enjeux seront bien différents si vous cherchez un anonymat complet, à communiquer de façon privé, ou bien à garantir une identité), des moyens techniques pour y parvenir, et des limites de ceux-ci

Principe du moindre privilège

Pensez à votre maison et aux clés que vous distribuez à différentes personnes. Vous donnez une clé de la porte d'entrée à vos enfants, mais probablement pas une clé de votre journal intime ou de votre coffre-fort personnel. Chacun n'a que l'accès nécessaire pour son rôle. C'est l'idée du principe de moindre privilège. **Chaque utilisateur d'un système informatique ne devrait avoir que les permissions minimales nécessaires pour accomplir ses tâches**. Par exemple, si vous partagez votre ordinateur avec d'autres membres de votre famille, vous ne donneriez probablement pas à vos enfants le même niveau d'accès que vous avez en tant qu'administrateur de l'ordinateur. Cela permet de prévenir d'éventuels problèmes, comme le téléchargement involontaire d'un logiciel malveillant.

Ce principe s'applique largement : **ne donnez aucune autorisation qui ne soit pas nécessaire à des tiers**, surtout si ces tiers sont des acteurs privés dont le métier est essentiellement de collecter des données sur vous.

Minimiser les données exposées

Si vous organisez une fête et demandez à vos invités de s'inscrire à l'avance, vous aurez probablement besoin de leur nom et peut-être de leur adresse électronique pour leur envoyer les détails de la fête. Mais demanderiez-vous leur numéro de sécurité sociale ou leur date de naissance ? Sûrement pas, car **ces informations sont inutiles pour l'organisation de la fête et, si elles étaient perdues ou volées, elles pourraient causer beaucoup de problèmes** à vos invités. C'est le concept de minimisation des données : **ne collecter, stocker et utiliser que les données absolument nécessaires à l'accomplissement de la tâche en cours**. Cela réduit le risque de violation de données, car moins de données sensibles sont stockées, et il y a donc moins de données qui pourraient être exploitées.

Ce principe fondamental s'applique essentiellement aux opérateurs de services, qui sont amenés à traiter des données en grande quantité. Mais vous avez tout intérêt à l'appliquer aussi à l'échelle individuelle. Ne divulguez aucune donnée, aucune information sur vous qui ne soit pas strictement nécessaire à la réalisation de vos objectifs (pas ceux du fournisseur de service).

Systématiser et formaliser les pratiques

Les meilleures pratiques de sécurité ne vous protégerons pas si vous ne les appliquez pas. C'est une évidence, mais cela n'empêche pas les gens les plus avertis de baisser la garde, de manquer d'attention et de faire une erreur qui peut ruiner les efforts fait habituellement.

Une fois vos besoins identifiés, **il est essentiel de formaliser et de systématiser les pratiques qui y répondent**. Pour une partie d'entre elle, ce sera facile, et pourra être automatisé, mais dans de nombreux cas, vous aurez des interventions manuelles à faire (pour chiffrer un message, pour choisir entre TOR et un VPN…). Comme toutes les habitudes, c'est difficile au début, mais cela devient plus naturel rapidement.