Auto-défense numérique – *rudiments*

En attendant les indispensables prochains ateliers d'«auto-défense numérique», voici quelques pratiques d'hygiène courante rudimentaire, à adopter sans attendre pour limiter les zones de vulnérabilité les plus grossières en matière d'informatique, et ce dans le domaine où elles sont les plus nombreuses : le transfert de données par Internet.

Ces questions de sécurité deviennent d'une banalité assourdissante – si bien qu'une partie des astuces ci-dessous sont reprises jusque dans une pleine page A3 du bimensuel des mutualités chrétiennes! – et ne sont donc pas le propre de personnes particulièrement paranoïaques. C'est une des raisons pour lesquelles ce petit aperçu est diffusé largement et structuré selon des degrés de précaution croissants, adaptable en fonction des usages.

En trois lignes, donc :

1 - Connaître le terrain

La situation est bien plus critique qu'il n'y paraît. C'est-à-dire que, d'une part, les moyens élaborés pour optimiser les flux d'information et perfectionner les capacités de contrôle sur ceux-ci, les méthodes de systématisation du profilage et la puissance d'exploitation des données générées, vont déjà bien au-delà de ce qui est communément admis et publicisé ; et que, d'autre part, les ripostes, esquives et contournements multiples qui s'inventent, à flux tout aussi tendus, face à cela nécessitent une mise-à-jour fréquente, sinon permanente, pour rester efficaces – efficaces «dans les limites des connaissances actuelles (dlca)».

Il s'agit donc d'une course de vitesse – qu'il est possible de ne pas perdre.

Tout le monde n'est pas enclin à développer les connaissances requises pour coller de près aux manœuvres adverses. Il est dès lors pratique de pouvoir s'appuyer sur des sources de confiance pour se fournir des moyens simples et non excessivement contraignants d'opérer en milieu informatique, et qui n'impliquent pas d'en comprendre exhaustivement les fondements ni d'en maîtriser la mécanique.

Les recommandations qui suivent sont susceptibles de varier au fil des changements – fulgurants – dans le domaine. Il est donc important de faire la distinction entre, d'un côté, ce qu'il s'agit de bien comprendre : le fonctionnement d'un outil, là où il intervient et ce qu'il permet de faire ; et, de l'autre, ce qui peut être choisi et suggéré par des personnes plus expertes : la marque, le modèle et la couleur dudit outil.

Dès lors, avant même d'essayer de colmater des passoires, il est préférable, de manière générale, de bien séparer les domaines d'utilisation, et cela *en amont*. Il s'agit de savoir sur quel terrain la partie se déroule, d'évaluer s'il est vraiment indispensable de renoncer au niveau de sécurité disponible et dans quelle mesure – sinon, autant optimiser celui-ci quel que soit l'usage ; et, surtout, de savoir ce que cela implique. C'est un premier pas hors de la paranoïa.

2 - S'équiper selon l'usage

En ce domaine davantage qu'en beaucoup d'autres, il est souvent plus dommageable d'agir sans cohérence que de ne pas agir du tout ; une mauvaise évaluation de l'adéquation entre l'usage et les moyens de protection pouvant conduire à un niveau d'exposition plus élevé qu'à l'accoutumée.

Voici quelques astuces, outils et habitudes élémentaires pour réduire les possibilités de traçage, d'identification et de prélèvement lors d'un usage somme toute courant du réseau Internet. Elles sont classées dans un ordre croissant de précaution (et, possiblement, de prise de tête) mais leur priorité dépend aussi de chaque cas :

Navigateur et paramétrage

- Utiliser «Firefox» comme navigateur. Ajouter les extensions élémentaires pour limiter les traces (voir les propositions sur «help.riseup.net») ; paramétrer la navigation privée par défaut ou, au moins, effacer régulièrement – au minimum à la fermeture – les «cookies», voire l'historique et autres persistances ; garder en tête que «tout ce que vous y ferez pourra être retenu contre vous», les sites visités, les informations transmises hors canaux sécurisés, les adresses électroniques utilisées (émettrices et réceptrices), etc'.

Information personnelle et mots de passe

- Ne pas laisser traîner son nom partout. La machine n'a pas besoin de savoir quoi que ce soit quant à la personne qui l'utilise pour fonctionner. De même, une adresse électronique sert à trouver le chemin entre deux points du réseau, pas à décliner son CV – il n'est pas nécessaire d'y inclure ses noms, données biométriques et coordonnées GPS. En ce qui concerne les mots de passe, c'est un sujet à part entière, très touffu, et fonction de ce qu'ils sont censés protéger. Un bon début : variés, longs, hétérogènes en types de caractère.

Serveurs et services

- Se débarrasser de «Gmail», «Hotmail», «Yahoo !», sans reste. Créer une adresse «@riseup.net» (ou d'autres proposées sur «help.riseup.net»), de préférence anonyme. Il s'agit d'un serveur très scrupuleux sur les techniques de protection informatique qui propose également d'autres outils sécurisés. Pour tout ce qui, jadis, passait par «Google» (agenda, rendez-vous, partage de fichiers, visio-conférence, etc'), il existe une trentaine de services semblables – le profilage en moins – sur «Framasoft».

TOR – navigation délocalisée (proxy)

- Utiliser tant que possible «TOR bundle». Il s'agit d'une application comprenant une version du navigateur «Firefox» paramétrée pour se connecter à Internet au travers du réseau «TOR». Celui-ci permet de masquer l'adresse IP assignée à la connexion et rend impossible (dlca) – à moins d'y mettre des moyens conséquents – de savoir à quel site la machine est connectée et d'où provient la connexion à un site visité. L'usage en est aussi simple qu'un navigateur standard et, hormis quelques restrictions détaillées sur le site, peut être généralisé à toutes les connexions à Internet – «www.torproject.org»

Système d'(auto-)exploitation

- Se débarrasser de «Windows», sans reste. Dans les cas marginaux où cette taupe mondiale s'est rendue incontournable (boulot, logiciel vital, addiction-sevrage...), ne la conserver que pour cet usage spécifique – au mieux, sur une machine y dédiée ; au pire, sur une autre partition du disque. Certains conseils repris ici ne sont pas entièrement inopérants sous «Windows», ils y sont cependant plus hasardeux. Quoi qu'il en soit, utiliser ce système pour un usage courant est risqué, et il est vivement conseillé de s'en défaire dès que et tant que possible. Par souci de simplicité, admettons que, mutatis mutandis, il en va de même pour «Mac OS».

Il existe une pléthore de systèmes d'exploitation moins suspects, pour tous les goûts ; toutefois, en guise d'introduction, «Ubuntu» est un système relativement accessible qui ne devrait pas paraître trop exotique aux accros de «Windows» ; c'est gratuit, complet, et vous trouverez certainement une personne habilitée qui peut vous l'installer le temps d'un café.

TAILS – navigation furtive et exploitation «propre»

- Un cran plus loin, «Tails» est un système installé sur un disque externe qui permet de démarrer l'ordinateur depuis ce disque, dont les applications sont optimisées en terme de sécurité (dlca), et qui force les connexions à passer par le réseau «TOR». De plus, comme il tourne depuis un disque externe sur la mémoire vive de la machine, et qu'il efface celle-ci après chaque usage, il ne laisse théoriquement aucune trace de l'activité, en ou hors ligne, sur l'ordinateur – «www.tails.boum.org»

Pas à pas – PGP, chiffrement

- Pour qui voudrait explorer un peu plus avant les possibilités non plus seulement de délocalisation et d'anonymisation mais aussi de rendre inexploitable (dlca) par des personnes indiscrètes les données présentes sur un disque ou transmises à d'autres, et ainsi, au passage, contribuer à rendre cette pratique aussi répandue que banale, les méthodes de chiffrement symétrique et asymétrique utilisant «PGP» sont relativement simples et accessibles – cependant, dans le cadre de la transmission de données, il faut être au moins deux et consentants pour jouer à ce jeux.

3 - Rester sur ses gardes et trouver des complices

Prendre un peu de temps pour acquérir une certaine autonomie en la matière – et pouvoir déjà palier très rapidement les lacunes de cette courte note – est requis afin de ne pas se leurrer quant à l'efficacité des suggestions précitées. Toutes ces parades peuvent devenir obsolètes si elles ne sont pas régulièrement mises à jour et si leurs effets sont mal compris. Pour cela, outre les mécanismes d'avertissement et les mises-à-jour automatiques, sont heureusement disponibles des sources relativement fiables (plus que celle-ci), plutôt au taquet, et qu'il y a tout intérêt à soutenir et à diffuser.

Faire de ces questions un sujet de discussion récurrent et rendre ces pratiques anodines, banales et répandues autant que possible, reste incontestablement plus efficace que de les maintenir dans des niches spécialisées – à la pointe, certes, mais confidentielles, circonscrites et localisables. C'est pourquoi il n'est pas vain de lourdement insister pour que d'autres s'y mettent dès maintenant, quand bien même «on n'aurait rien à se reprocher» – puisque, si vous avez bien suivi, vous savez que là n'est pas la question. Diffuser ceci aussi largement qu'il est matériellement possible, transférer ses habitudes vers des services dignes de confiance (dlca) et forcer la propagation autour de soi – une adresse sûre qui ne communique qu'avec d'autres adresses sûres – est un bon début pour se familiariser avec des considérations qui deviennent de plus en plus incontournables.

Vous ne pouvez vous passer des «réseaux sociaux» ?, essayez «Crabgrass» («we.riseup.net») ou «Diaspora» ; rendre vos contacts directs plus sûrs ?, filez-leur ceci et coupez toute communication jusqu'à migration complète hors des dispositifs de capture et de contrôle ; pour le premier de l'an ?, offrez une clef «Tails», ou un «kit de survie en milieu informatique»...

En cas de doute, *faites de ceci un livre de chevet !* : **«https://guide.boum.org»**