Formation à l'autodéfense numérique

jeudi 7 décembre 2017, par marjToussaint

3 journées de formation : jeudi 26 avril, jeudi 24 mai, jeudi 21 juin 2018

Les ordinateurs, Internet et les smartphones prennent de plus en plus de place dans la vie d'un grand nombre d'entre nous. **Le numérique a changé la manière dont certaines choses se faisaient et a vu naître de nouvelles pratiques et de nouveaux acteurs.** Les manière dont nous nous rencontrons et dont nous nous organisons s'en trouvent transformées, ainsi que les manières de travailler, de gouverner, de surveiller, etc..
Facebook, dont le modèle économique repose sur la commercialisation des données produites par ceux qui l'utilisent, propose depuis peu un Messenger pour enfant de 6 à 12 ans. En 2013, Edward Snowden révèle l'étendue de la surveillance planétaire exercée par la NSA. La banque carrefour de la sécurité sociale (belge) croise les données des distributeurs d'énergie avec la liste des bénéficiaires d'allocations de chômage pour repérer de possibles fraudes. Les caméras de sécurité prolifèrent dans les villes.
Si c'est le plus souvent individuellement que nous manions ordinateurs, smartphones ou tablettes, **le numérique** est pourtant d'emblée **collectif** et éminemment **politique**. **Qui communique avec qui et comment ? Qui cherche à collecter quelles données et à quelles fins ? Qui a quel pouvoir sur les flux de données et leur stockage ? Qui exerce quel contrôle sur quelles infrastructures matérielles ou immatérielles ?** Qui peut rendre ceci ou cela possible ou difficile ? En fin de compte, comment tout cela transforme-t-il nos existences ?

C'est afin de déployer ces questions et pour nous en ressaisir ensemble par l'expérimentation que CFS, en collaboration avec les membres de l'Usine à vapeur asbl, vous propose 3 journées de formation à l'autodéfense numérique.

Il ne s'agira pas d'affirmer notre droit à la vie privée et de nous outiller en conséquence, mais plutôt **d'explorer comment et dans quelle mesure nous est-il possible de nous rendre moins vulnérables numériquement et de nous soustraire collectivement, par nos pratiques, à la capture numérique et au gouvernement par les données.**

Objectifs

- Affiner notre perception des enjeux liés aux infrastructures numériques
- Développer, dans le cadre de l'usage de celles-ci, des pratiques adéquates au degré d'opacité désiré sans se leurrer ni sombrer dans la paranoïa
- Explorer et expérimenter le fonctionnement très concrets des appareils familiers, de leurs possibilités et de leurs limites
- Les objectifs que nous nous proposerons au cours des ateliers.
- …

Au programme

Chaque journée sera articulée autour d'une série d'expériences, de moments d'initiation et/ou d'introduction à un ensemble de questions.

JOUR 1 : « Privé ? »

- Sur le Web, une connexion sécurisée (https), c'est quoi, à quoi ça sert ? Quelle différence ça fait ? Un serveur, c'est quoi précisément ? Sur les données, leur circulation, leur stockage, leur commerce.
- Des outils et pratiques pour se rendre un peu moins vulnérables. Et des VPN, c'est quoi, à quoi ça sert ?
- Les mots de passe, ils ouvrent et ferment quoi ? Comment ça fonctionne ? Pourquoi ça se vole ? Comment ça se craque ? C'est quoi un mot de passe efficace ? Comment faire avec plusieurs mots de passe ?

JOUR 2 « Public ? »

- Atelier : « Vie privée, surveillance et profiling » par **Denis Devos** (Domaine Public : https://www.domainepublic.net/) et **Michel Cleempoel** (Etraces : http://etraces.constantvzw.org/informations)
- Réseaux sociaux, vidéo-surveillance, photos, bases de données. Sur le gouvernement par les données (mais que fait la police ?)
- Et nous, que faisons-nous de tout cela ? Comment ne pas trop en dire ? Quelles traces laissons-nous que nous pourrions effacer ? Comment nous rendre un peu moins transparents ?

JOUR 3 « Opacités »

- Crypter ?!!? (… mais je n'ai rien à cacher !). Qu'est-ce qui est crypté, sans qu'on le sache ? Ce qu'on croit crypté mais qui ne l'est pas. Pourquoi crypter ? Crypter quoi et comment ? Crypter des fichiers, de dossiers, des disque durs ; crypter ses e-mails avec GPG, crypter ses communications – avec Signal (https://signal.org), par exemple – ou avec d'autres applications.
- Être anonyme sur le net alors que l'on nous trace de tous côtés. Présentation d'outils et de techniques d'anonymisation avancées : TOR (The oinion router : https://www.torproject.org) et Tails (The Anonymous Incognito Live System : https://tails.boum.org)
- Retour collectif sur les trois journées de formation.
- Perspectives de suites et de prolongements.

La formation ne suppose pas de compétences particulières en plus de la curiosité et de l'envie d'explorer plus ! Il est cependant indispensable de se munir d'un ordinateur – portable, de préférence –, si possible familier (celui que vous utilisez d'habitude). Seuls deux ou trois machines supplémentaires seront éventuellement disponibles sur place (si vous n'en avez pas, signalez-le-nous lors de l'inscription).

Contenus

- Affiner notre perception des enjeux liés aux infrastructures numériques
- Développer, dans le cadre de l'usage de celles-ci, des pratiques adéquates au degré d'opacité désiré sans se leurrer ni sombrer dans la paranoïa
- Explorer et expérimenter le fonctionnement très concrets des appareils familiers, de leurs possibilités et de leurs limites

A qui s'adresse cette formation ?

La formation ne suppose pas de compétences particulières en plus de la curiosité et de l'envie d'explorer plus !

Il est cependant indispensable de se munir d'un ordinateur – portable, de préférence –, si possible familier (celui que vous utilisez d'habitude). Si vous n'en avez pas, signalez-le nous lors de l'inscription.

Formateurs

Étienne Carlier et **Yann De Coster** (membres de l'asbl L'Usine à vapeur) ont une expérience dans le codage, la configuration de réseau, le chiffrement, etc ; grande familiarité avec les enjeux politiques soulevés par l'expansion et l'intensification de l'usage d'appareils connectés à des réseaux de serveurs « propriétaires » ; pratique courante de transmission des expériences et connaissances dans ce domaine.

Infos pratiques

Quand ? 3 journées de formation : jeudi 26 avril, jeudi 24 mai, jeudi 21 juin 2018 (de 9h00 à 16h30)
Où ? 26 rue de la victoire, 1060 Saint-Gilles
Prix ? 45 €* (comprenant les documents pédagogiques, pause café et lunch du midi)
Pour s'inscrire ? Compléter le formulaire d'inscription en ligne (CODE : numerique2018)

* Le prix ne doit pas être un obstacle à l'inscription

ATTENTION // Il est indispensable de se munir d'un ordinateur – portable, de préférence –, si possible familier (celui que vous utilisez d'habitude). Seuls deux ou trois machines supplémentaires seront éventuellement disponibles sur place (si vous n'en avez pas, signalez-le nous lors de l'inscription).