Autres ressources

D'autres ressources (présentation, ressources externes) pour aller plus loin.

- Formation sur la sécurité militante
- Ressources externes de formation à l’hygiène/sécurité numérique
- Risques et bonnes pratiques pour les actions à l'étranger

Formation sur la sécurité militante

Formation "Sécurité militante de base" créée collectivement par plusieurs formateur.ices

LE BUT :

- Savoir penser autour des notions de sécurité/menaces
- Savoir estimer les menaces actuelles pour un.e militant.e en France
- Savoir agir pour renforcer sa sécurité militante

PUBLIC VISÉ :

- □ Militant.es DCNV avec un modèle de menace faible à moyen
- □ pas suffisant pour un modèle de menace fort (exemple: action de désarmement, dictature) => Formation Sécurité Militante avancée
- □ pas suffisant pour la coordination d'action => Formation Sécurité Militante avancée
- Format: Durée d'une 1h30/2h afin de pouvoir la donner lors d'une réunion de Groupe Local.

CONTENU :

□□ Formation en format audio de 50 minutes

□□ Slides dans le RDV1

Document de sécurité militante numérique créé par le GL de

Bordeaux.

LE BUT
□□ Offrir une sécurité numérique (= anonymat) aux militant.es avec des explications simples et concrètes.

IL COMPREND
□□ Le PDF du dossier complet de 21 pages + les sources
□□ Le PDF du livret qui résume tout avec des dessins, très accessible
□□ Le PDF avec des conseils et schémas pour pouvoir donner la formation
□□ Le PDF du livret pour l'imprimer, découper et agrafer facilement + un mini tuto vidéo

QUELLE ET LA LÉGITIMITÉ DE CE DOCUMENT ?
□□ Nous l'avons écrit en collaboration avec plusieurs personnes travaillant dans la sécurité informatique (pour des entreprises ou l'armée) et d'autres passionnés de sécurité numérique.

L'ENSEMBLE DES DOCUMENTS SONT TÉLÉCHARGEABLES SUR RDV2 (nom d'utilisateur: rebelles / mot de passe: Ogg?swos9): Lien vers les fichiers !

Ressources externes de formation à l’hygiène/sécurité numérique

Le post est en mode wiki, n’hésitez pas à le modifier pour rajouter un élément.

Parce qu’on n’est pas les seul.e.s à avoir besoin de propager des conseils de sécurité informatique à des personnes sans bagage technique important, autant s’appuyer sur le travail d’autres collectifs.

Quadrature du Net

dont Reconnaissance faciale et contrôle d’identité : que peut faire la police ?

Nothing2hide

Un ensemble de ressource lancée par un ancien de Telecomix et un journaliste militant. Les formulations des conseils sont simples tout en restant très pointus et factuels.
Les contributions se font sur un dokuwiki, et un pdf est recompilé régulièrement. Tout le contenu est sous license CC-BY-SA 3.0.

> “ **Nous avons tous quelque chose à cacher**. Nothing2hide est une structure associative qui s’est fixée comme objectif d’offrir aux journalistes, avocats, militants des droits humains, “simples” citoyens, les moyens de **protéger leurs**

> **informations**.

- Des **conseils de base** jusqu'au **chiffrement de vos communications** en passant par les précautions à prendre lors de la couverture d'un événement, notre Guide de protection numérique 8 vous aidera à **protéger vos informations** en toutes circonstances.
  image

- **Le pdf de "guide de protection numérique** guide-protection-numerique-2019.pdf (627,9 Ko), mis à jour régulièrement 1.
  image
- Le guide de protection numérique en format wiki 8
- Un cycle de formations à la sécurité numérique 1. Ça va de la navigation sur internet, à de la crypto avancée, en passant pas la définition du modèle de menace. Il n'y a pas de vidéos mais les slides donnant une très bonne structure si on connait le sujet.

« Guide d'autodéfense numérique »

- Guide très complet dont la dernière version à été édité en 2023.
  https://guide.boum.org 1
- Tome 1 : « Hors connexion » 180 pages
  - version web
- Tome 2 : « En ligne »156 pages
  - version web

Édité par des libristes, publié en LAL (Licence Art Libre, similaire à la CC-

- Guide de nothing2hide 2024 sur la palette d'outils à utiliser (très didactique et accessible)
- Également les privacy guides, très pertinent en complément du wiki, notamment les sections traitant d'Android, ou de ce qu'est un VPN

MOOC : Protection de la vie privée dans le monde numérique

Cours en ligne (MOOC) très intéressant fait par Inria (institut de recherche public en informatique). Le cours n'est accessible qu'en s'enregistrant sur la plateforme FUN du 6 mai au 30 juin.

- lien du MOOC 1
  image

Guide d'hygiène Informatique par l'ANSSI

L'ANSSI est l'agence gouvernementale responsable de la sécurité des systèmes d'informations. Ils ont en général de très bons conseils, mais sont assez peu écoutés par les administrations.
Un guide qui s'adresse aux administrateurs et gestionnaires des systèmes d'information des grandes entreprises.

- pdf de 72 pages 4
  image

Totem project

Formation en sécurité numérique pour activistes et journalistes

---

Fondation Frontière Electronique

Autodéfense contre la surveillance : astuces, outils et guides pratiques pour des communications en ligne plus sécurisées

Cryptolib

Ressources autour des problématiques de vie privée sur internet, de contrôle des données et des libertés numériques

Risques et bonnes pratiques pour les actions à l'étranger

Si vous participez à une action à l'étranger, voici quelques risques et bonnes pratiques à garder en tête.

Passage d'une frontière

Le passage d'une frontière, même au sein de l'espace Schengen (zone normalement sans contrôle aux frontières des personnes - Union Européenne + 5 pays), est un moment risqué car les risques de contrôle y sont plus élevés. De plus, c'est une zone sous haute surveillance, où beaucoup de données sont collectées.

Quelques conseils quand vous franchissez une frontière (que ça soit en voiture, en train ou avec un autre moyen de transport).

- Si vous avez un téléphone et/ou ordinateur, activez son chiffrement (en l'éteignant, cf: se reporter aux formations dédiées pour plus de détails)
- Mettez-vous en mode avion ou éteignez votre téléphone en amont et en aval de la frontière pour éviter de borner.
- Si possible protégez votre identité, en cachant votre visage des caméras. Au niveau des péages routiers, des caméras sont souvent situées au niveau de la voiture, il reste donc nécessaire de cacher son visage.
- Si possible, ne passez pas seul.e la frontière afin que que les autres personnes puissent faire office de base arrière en direct si vous faites arrêté.e*. Prenez le temps de vous mettre d'accord avec les personnes qui vous accompagnent afin que vous sachiez comment réagir en cas de contrôle. Par exemple, quelle est la raison de votre voyage ? Où allez-vous ? Où dormez-vous ?
- Passer une frontière en groupe peut être un atout mais aussi un risque car ça peut permettre d'identifier des groupes d'individus (exemple ci-dessous). Il peut être donc pertinent de paraître voyager seul (par exemple, en changeant de place dans le car avant la frontière ou en passant les contrôles à une distance raisonnable les unes des autres) et de s'assister qu'en cas de besoin. *Exemple: X est fichée S et voyage avec 3 autres militantes. X est contrôlée et comme elle est fichée S, les forces de l'ordre contrôlent les personnes qui l'accompagnent. Les 3 autres personnes sont maintenant identifiées comme militantes probables.*

NB: Si vous pensez être fiché.e S ou recherché.e, les risques d'arrestation ou de contrôle plus poussé (avec des questions) sont plus probables.

Choisissez le bon mode de transport

Les différents modes de transport présentent tous des intérêts et des inconvénients.

Voiture versus Car

Une voiture a moins de chance d'être contrôlé qu'un car (type Flixbus) mais les plaques d'immatriculations étant automatiquement scannées, l'identité du propriétaire de la voiture sera rattachée au passage de la frontière.

NB: Vous n'avez pas de voiture ? Faites du covoiturage ou du stop ! Un canal mattermost existe pour faciliter les covoiturages. D'autres systèmes militants sont aussi parfois proposés par l'organisation de l'action. Passer par une plateforme de covoiture non militante (type blablacar) peut permettre de passer la frontière avec un conducteur (et donc une voiture) qui a peu de chances d'être fiché.

Voiture de location

Les voitures de location ont souvent des balises GPS intégrées. Les mouvements de la voiture seront donc traçables par les forces de l'ordre s'ils ont accès aux données de la société de location.

Train

Les trains sont régulièrement contrôlés au sein de l'espace Shenghen.

Faire ou non appel à l'ambassade française

Si vous êtes citoyen français, à l'étranger, vous pouvez demander assistance à l'ambassade française, qui est la représentante de la France.
En cas de procédure policière ou judicaire à votre encontre, il n'est pas conseillé de faire appel à l'ambassade française du pays à moins que les système policiers et juridiques de pays soient très défavorables par rapport à ceux de la France (Belgique et Allemand assez proches, au Royaume-Uni ça peut être pertinent car les peines de prison y sont plus fréquentes). En effet, l'aide que l'ambassade vous apportera sera alors limité voire néfaste s'ils donnent des renseignements sur vous.

Formez-vous sur la situation dans le pays

- Quels sont les risques juridiques ? En quoi différent-ils de la France ?
- Comment les forces de l'ordre fonctionnent (méthode de contrôle et de répression, armement) ?
- Quels sont vos droits en contrôle, garde-à-vue ? En quoi différent-ils de la France ?