Auto-défense numérique syndicale

Solidaires Informatique 2024

Ce guide a pour priorité de vous protéger numériquement contre les groupes hostiles aux syndicats (l'extrême-droite, le patronat) et, dans une relative mesure, contre une surveillance légère de l'État.
D'autres guides existent pour la protection physique des locaux, des militant·e·s et de leurs proches.

Il ne cherche pas particulièrement la protection informatique des travailleuses et travailleurs contre leur employeur qui mériterait un autre guide.

Quant à une surveillance ciblée par l'État, elle mériterait un niveau de sécurité encore supérieur qui dépasse la simple auto-défense numérique.

* * *

L'objectif de ces conseils est de renforcer la sécurité numérique des structures. Les moyens envisagés ici ne constituent pas une stratégie d'ensemble, mais une série de mesures qui permettent de limiter rapidement les problèmes les plus fréquents en nécessitant le moins de connaissances techniques.

* * *

💡 N'hésitez pas à contacter Solidaires Informatique (contact@solidairesinformatique.org) pour obtenir de l'aide.

Sommaire

Contexte

Depuis 50 ans le monde s'est transformé. Nos engagements et modalités d'engagement aussi.

Il y a 25 ans la police faisait ses réquisitions dans les bibliothèques pour savoir qui empruntait des livres suspicieux. Elle mettait des téléphones fixes sur écoute.

Aujourd'hui, elle sonorise des véhicules. Elle trace nos déplacements sur simple réquisition des opérateurs mobiles. Elle déploie des technologies de surveillance massive couplant des intrusions dans des locaux à des modalités de vidéosurveillance algorithmique de l'espace public. Elle dispose d'une base de données d'ADN inimaginable, et cherche à pouvoir utiliser les fichiers des pièces d'identité pour faire de la reconnaissance faciale dans l'espace public. Juridiquement, la police a maintenant le droit d'enregistrer non des faits mais nos préférences sportives, politiques, nos pratiques religieuses ou nos lectures philosophiques.

À une époque, les fascistes infiltraient les réunions des syndicats ou des collectifs en lutte. Aujourd'hui, ils infiltrent nos boucles de messagerie instantanée, dont certaines technologies vont même jusqu'à communiquer en temps réel nos positions géograhiques. Ils arrivent ainsi à savoir quand, quoi et où frapper. Ils peuvent anticiper nos manifestations, trouver des camarades isolé·e·s, et nous mettre en danger.

Tout ceci est une réalité en France et dans le monde de 2024.

25 ans après l'avènement d'Internet, il est essentiel de considérer la sécurité numérique comme un aspect essentiel de la sécurité de nos groupes, de nos actions et de nos personnes.

Globalement nous, les militant·e·s, avons accumulé du retard. Le rattraper peut sembler être un saut de géant. Mais pensons à nos camarades et à ce que nous défendons : c'est toujours le maillon le plus faible d'une chaîne qui en détermine sa robustesse d'ensemble. Où est mon organisation, où suis-je dans cette chaîne ?

Pour bien rendre compte des moyens déployés par les forces de l'ordre contre nous autres et nos camarades, cet article est passionnant et donne des motivations pour suivre ce qui suit : https://lessoulevementsdelaterre.org/blog/affaire-lafarge.les-moyens-denquete-utilises-et-quelques-attentions-a-en-tirer

Sécurité physique des lieux et des matériels

- Suivre les recommandations de sécurité des locaux distribuées par l'USS et penser à :
  - Mettre un mot de passe aux sessions d'ordinateurs
  - Verrouiller l'ordinateur dès que vous le quittez, même pour 2 secondes
  - Éteindre son ordinateur en partant

Sauvegarder vos données

- Récupérer les données en ligne, elles pourraient être effacées si quelqu'un accède à votre ordinateur :
  - Si vous utilisez Google Drive, suivre ce guide
  - Si vous utilisez OneDrive, suivre ce guide
  - Si vous utilisez iCloud, suivre ce guide
- Sauvegarder régulièrement ces données sur un ordinateur situé dans un lieu différent

Minimiser les données en notre possession

- Supprimer les fichiers inutiles des ordinateurs et des téléphones
- Supprimer les données inutiles/obsolètes des fichiers

Chiffrer les disques durs

- Les postes sont sous Windows : suivre le guide de Microsoft.
- Les postes sont sous macOS : suivre le guide d'Apple.
- Les postes sont sous Linux : contactez celui ou celle qui vous l'a installé

💡 un disque chiffré n'est utile que si l'ordinateur/téléphone est éteint. Allumé, il n'est pas chiffré. Éteignez !

Avoir un mot de passe solide

- Détruire tout papier avec un mot de passe. Pas de mot de passe écrit
- Utiliser des gestionnaires de mots de passe comme KeePass ou BitWarden
- Générer un bon mot de passe. Un bon mot de passe est composé de plusieurs mots
  Exemple : J3-Mange3-Un3-Banan3-Hapagnan-107
- S'assurer que les mots de passe ne sont pas en lien avec l'orga ou la vie familiale
  Exemples de termes à proscrire : Solidaires/SUD, votre nom/prénom, celui du partenaire, dates…

Ne pas brancher un disque dur ou une clé USB de source inconnue

Ces périphériques peuvent avoir été laissés là avec des logiciels malveillants pour infecter vos ordinateurs.

- Demander si le périphérique appartient à quelqu'un
- Détruire rapidement le matériel concerné si personne ne le réclame

Si vous avez des données stockées sur ces supports, ils ne doivent pas rester au local

Sécurité numérique des appareils

Si votre matériel est saisi par police ou des individus hostiles, ou si un virus y a été installé, ces conseils vous permettront de limiter les dégâts

Protection du téléphone

- S'assurer que le disque dur du téléphone est chiffré, voir section suivante.
- Éteindre votre téléphone en manifestation/action si vous n'attendez pas de message urgent
- Mettez vos objets connectés dans un tissu dans une boîte à biscuits métallique, ils seront isolés efficacement

En cas de garde à vue, la police analysera votre téléphone, même sans votre code PIN. Elle n'y arrivera que très difficilement s'il est chiffré et éteint

IPhone

Le téléphone est déjà chiffré

- Définir un code d'accès à 6 chiffres au téléphone si ce n'est pas déjà fait
  Réglages – Face ID et code
- Paramétrer l'effacement du téléphone en cas de trop nombreuses tentatives de connexion
  Réglages – Général – Face ID et code – Effacer les données (tout en bas). 10 échecs consécutifs effaceront les données du téléphone
- Activer la protection contre le vol
  Réglages – Général – Face ID et code – Protection en cas de vol de l'appareil

Android

Les téléphones récents sont chiffrés, les plus anciens ne le sont pas. Pour vérifier, suivre ce guide

- Définir un code à 6 chiffres *(pas de schéma, trop fragile)*, suivre ce guide

Protection de l'ordinateur

- Avoir un mot de passe de session (et ne pas l'écrire sur un post-it à côté !)
- Chiffrer ses disques durs :
  - Pour Windows : suivre ce guide
  - Pour MacOS : suivre ce guide
  - Pour Linux : consulter la personne qui a installé l'ordinateur

Sécurité des communications

Pseudonymat

- Utiliser un pseudonyme dédié aux échanges syndicaux. Ce pseudonyme ne doit servir nulle par ailleurs
  - Assurez-vous que ce pseudonyme ne puisse pas être relié à votre véritable identité par une recherche en ligne (pas de code postal, pas de référence à un pseudonyme…)

Favoriser Firefox pour naviguer

- Utiliser Firefox, sur ordinateur comme sur téléphone, pour naviguer
- Installer le bloqueur de publicités uBlock Origin également utile contre le pistage
- Ne pas enregistrer les mots de passe dans le navigateur
  - préférer un logiciel dédié de gestion de mots de passe

Favoriser Signal pour chatter

- Utiliser Signal pour vos échanges numériques
  Ne plus utiliser plus Telegram, Messenger, Instagram… pour les communications militantes
- Créer un identifiant signal
  Ainsi v*otre numéro de téléphone ne sera pas visible par les participant·e·s à un groupe de discussion*
- Basculer votre organisation syndicale sur Signal
- Fixer une durée de vie maximale pour les messages dans un groupe
- Détruire le groupe une fois par an et le recréer

Protéger sa boîte mail

- Activer la double authentification (par exemple login + SMS) – Voir comment faire pour Gmail
- Purger régulièrement la boîte mail : identifiants bancaires, mots de passes transmis, etc.
- Changer le mot de passe une fois par an, surtout s'il s'agit d'une boîte mail collective

Suivi des activités téléphoniques – Fadettes

L'accès aux factures détaillées permet d'en savoir beaucoup sur vous. Si vous êtes curieux, lire cet article.
Pour se prémunir de cette vulnérabilité, par ordre décroissant de priorité, vous devez :

- Arrêter tout appel ou SMS « en clair », c'est-à-dire en dehors d'une app sécurisée
- Appeler et "texter" via Signal (https://www.signal.org/)
- Passer en mode avion / désactiver votre carte SIM le plus tôt possible avant d'arriver en réunion ou laisser votre téléphone à votre domicile quand vous vous déplacez à une réunion

Quand cela est absolument nécessaire, se doter d'une connexion au réseau GSM via des cartes prépayées (« *burner* »), voir cet article pour obtenir des instructions détaillées

Image publique

Ici, il y a triple danger. D'abord, indiquer que des camarades non-protégés sont syndiqués et risquer de leur faire perdre leur emploi. Ensuite donner des indications sur les camarades les plus actifs et risquer d'en faire des proies faciles pour les milices fascistes. Et enfin, le risque d'usurpation d'identité et création de situations confuses (désinformation, vol de données, détournement de fonds…)

Sites web

- Limiter les données présentes sur le site au nécessaire (des tracts, communiqués, visuels).
- Privilégier Signal et le mail comme moyens de contact
- Cacher au maximum :
  - les informations sur les élu·e·s et les personnes (même les prénoms ou juste une photo non-floutée)
  - retirez les informations nominatives, comme les professions de foi, au plus vite après leur usage
- Tenir à jour le logiciel de votre site web. Contactez le support de votre prestataire pour cela si besoin
- Définir un mot de passe fort et qui n'est utilisé nulle part ailleurs (éviter qu'en le piratant, on accède aussi à vos mails)

Réseaux sociaux

- Mettre en place une double authentification
  - Pour Twitter/X : https://help.x.com/fr/managing-your-account/two-factor-authentication
  - Pour Facebook : https://fr-fr.facebook.com/help/148233965247823/
  - Pour Instagram : https://fr-fr.facebook.com/help/instagram/566810106808145/
- Flouter tous les visages sur les photos publiées

Réseaux sociaux personnels

Avec juste votre nom et quelques informations relativement faciles à trouver (employeur, région…), il peut être très facile de vous pister.

- Restreindre la visibilité de vos informations (infos perso, amis, photos) pour qu'elles ne soient pas visibles du public
- Favoriser l'utilisation d'un pseudonyme distinct de celui que vous utilisez pour militer
- Créer un profil dédié à votre activité militante sans possibilité de lien avec votre profil pour votre vie privée
- Faire de même sur les réseaux sociaux professionnels (LinkedIn, réseau social de l'entreprise) et sur les réseaux sociaux sportifs (Strava…)

Gestion des crises (curatif)

Que faire quand un·e camarade est en GAV ou perquisitionné ?

En GaV

- Dire être prêt à communiquer ses codes dès que vous aurez vu votre avocat
- Avertir son avocat des contenus de son téléphone/ordinateur
- Demander à son avocat d'avertir les camarades de la saisie du matériel

Immédiatement

- En informer en toute discrétion les camarades concerné·e·s directement ou indirectement
- Le retirer de toutes les boucles de messagerie instantanée, ce qui implique de ne jamais laisser un admin unique sur une boucle
- Réfléchir à ce à quoi la Police peut avoir accès immédiatement, et couper cet accès à la camarade, prendre des mesures concernant les informations en leur possession (ex : notes de réunion…)

Dès que possible

- Envisager la réinitialisation/réinstallation de tout matériel numérique ayant été en la possession, même temporaire, de la Police
- Changer les comptes de la personne ayant accès à des espaces numériques d'échange ou de stockage sensibles, ou *a minima* réinitialiser les mots de passe

Dès que la personne est sortie de la crise immédiate

- Faire un débrief collectif pour amortir le choc personnel, mais aussi pour faire le point sur l'exposition du groupe suite à cet événement… Penser à revenir jusqu'à un an en arrière et envisager l'avenir
- Prendre des mesures suite à ce qui aura été envisagé durant le débrief

Que faire quand un téléphone/ordinateur a été volé/en la possession d'un groupe constituant une menace ?

cf. « camarade en GAV ou perquisitionné »

À la récupération du téléphone/ordinateur, *a minima* changer le code PIN/mot de passe. Idéalement, réinitialiser le téléphone aux paramètres d'usine/réinstaller totalement l'ordinateur.

Avertir les camarades dans tous les cas, de manière à leur permettre d'ajuster leurs propres mesures de sécurité

Que faire quand une boucle de messagerie a été dévoilée à un groupe constituant une menace ?

- Avertir les camarades concernés

- Contrôler ce qui était accessible dans la boucle et les informations potentiellement dévoilées (mots de passe, informations privées…)
- Détruire la boucle et récréez-la à 0

Que faire quand les locaux ont été visités ?

- Lister le matériel qui a disparu, avertir les camarades et sections concernées
- Contrôler toute trace d'utilisation du matériel qui est resté sur place, au besoin se faire aider
- Changer les mots de passe qui étaient enregistrés sur les ordinateurs, Réinstaller les ordinateurs à 0, au besoin se faire aider, et en attendant, laisser le matériel éteint
- Inspecter les lieux minutieusement pour repérer d'éventuels dispositifs d'écoute
- Prévenir les camarades concerné·e·s, de manière à leur permettre d'ajuster leurs propres mesures de sécurité

Annexes

Des ressources pour aller plus loin

https://expansive.info/Vague-de-perquis-en-ce-moment-comment-on-s-y-prepare-4005
https://expansive.info/Retour-d-experience-sur-la-securite-informatique-en-nomade-3068
https://expansive.info/Comment-s-organiser-en-ligne-Une-brochure-pour-lutter-2168#Mail-Chiffre-avec-PGP-GPG
https://atelier.mediaslibres.org/M-I-F-I-P-5-pratiques-de-base-pour.html

Des analyses / états des lieux de l'actualité répressive

https://expansive.info/Une-analyse-du-proces-du-8-12-4277
https://expansive.info/Affaire-Lafarge-Les-moyens-d-enquete-utilises-et-quelques-attentions-a-en-tirer-4130

Des documents techniques

https://telmob.0id.org/
https://infokiosques.net/informatique
notamment :
— https://infokiosques.net/spip.php?article1849 – Guide de survie en protection numérique à l'usage des militante
— https://infokiosques.net/spip.php?article2017 – Comment se protéger et protéger nos luttes
— https://infokiosques.net/spip.php?article1975 – Téléphonie mobile
— https://infokiosques.net/spip.php?article1726 – TuTORiel Tails 5.4
— https://guide.boum.org/ – Guide d'Autodéfense Numérique

Des outils

https://tails.net/
https://riseup.net/
https://riseup.net/fr/email
https://riseup.net/fr/vpn
https://we.riseup.net/
https://cryptpad.fr

Des podcasts

https://www.lacoalition.fr/Bibliographie-commentee-autodefense-juridique-et-numerique ?