GUIDE DE PROTECTION NUMÉRIQUE

ZEKA // NOTHING2HIDE

DÉCEMBRE 2019

AVANT-PROPOS

Nothing2hide anime des formations autour de la sécurité numérique en école de journalisme, auprès des professionnels en exercice et auprès des défenseurs des droits humains.

Nothing2hide a rédigé de nombreux supports pédagogiques pour ces formations.

Zeka publie aujourd'hui une compilation (mise à jour) de ces ressources, sous la forme d'un guide de protection numérique. Il est diffusé sous licence Creative Commons CC BY SA.

Partagez, copiez, réutilisez et diffusez !

https://nothing2hide.org/fr/

https://zeka.noblogs.org

Note à l'attention des lecteurs

Certains hyperliens présents dans le présent document ne sont pas pris en charge. Nous vous recommandons de les recopier manuellement dans votre navigateur

TABLE DES MATIÈRES

Pour commencer

Protéger ses données

Protéger ses communications

Protéger son anonymat

Pour aller plus loin

POUR COMMENCER

LES CONSEILS DE BASE

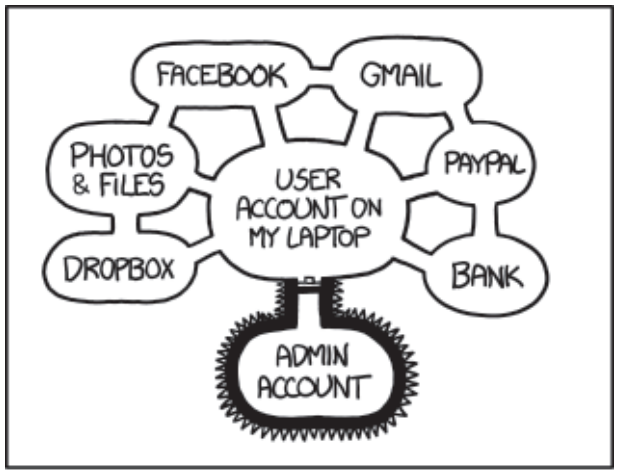
Entre la chaise et le clavier

Avant même d'allumer son ordinateur, smartphone ou tablette, il y a quelques conseils de bon sens à appliquer.

Évitez de travailler dos à une fenêtre

En voyage, dans le train ou en avion, appliquez un filtre de confidentialité sur votre écran. Le filtre de confidentialité est une feuille transparente qui une fois appliquée sur votre écran restreint la vision latérale. Ainsi seule la personne située en face (vous) est capable de voir l'écran.

Ne laissez pas votre ordinateur portable ou votre smartphone sans surveillance ! Cela permet d'éviter qu'un individu malveillant ne puisse récupérer des fichiers de votre ordinateur ou ne puisse y introduire un cheval de Troie.



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS, BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

Tous les systèmes d'exploitation (Windows, Mac OS et Linux) permettent de protéger votre session avec un mot de passe. N'hésitez pas à utiliser cette fonctionnalité.

Les bases sur un ordinateur

Une fois l'ordinateur allumé,

Installez les mises à jour de votre système d'exploitation (libres) et vos logiciels (libres)

Utilisez un antivirus **ClamXav**, **ClamTk**, **Avast**, **MSE**, **Mc Afee**, **Norton** (même sur Mac).

Sur Windows, **Windows Defender** fera l'affaire à 100%. En 2013, Adobe était victime d'un large piratage informatique, faisant craindre une nouvelle génération d'attaques contre plusieurs produits, dont le très répandu **Adobe PDF reader** pour les documents PDF.

https://frama.link/nxtnpct-adobe-40go

Sur smartphone, nous vous recommandons l'utilisation de **MuPDF** pour lire vos fichiers PDF.

Activez votre Firewall sur Windows et sur Mac.

Ne cliquez pas n'importe où !

S'il est important d'installer un antivirus sur son poste, il est encore plus important de faire preuve de bon sens lorsque vous recevez un lien ou une pièce jointe par e-mails, ou Twitter, Facebook ou Skype.

Les services sociaux et les outils de communication sont les principaux vecteurs de transmission de virus.

La méthode la plus efficace est d'agir en amont, avant qu'un logiciel malveillant n'infecte votre ordinateur ou votre smartphone.

Ne téléchargez pas de fichiers ou ne cliquez pas sur des liens qui vous sont envoyés par des expéditeurs inconnus.

Vérifiez soigneusement l'adresse mail ou le compte Twitter de ceux qui partagent un lien avec vous. En cas de doute, vérifiez l'identité de l'expéditeur auprès d'autres contacts ou par l'intermédiaire d'un moteur de recherche.

Enfin si le fichier et l'expéditeur vous semblent suspects, contactez des experts qui pourront vous aider. Le ***Citizen Lab*** est un organisme qui analyse les virus envoyés par des dissidents ou activistes et les aide à mieux se protéger.

https://citizenlab.ca/

Effacez vos traces sur un ordinateur public

Si vous travaillez dans un cybercafé ou sur un ordinateur qui n'est pas le vôtre, veillez à ne pas laisser de traces une fois votre travail terminé :

Si vous avez consulté votre boite mail, votre compte Facebook ou votre compte Twitter, surtout, **pensez à vous déconnecter**.

Effacer votre historique de navigation. Celui-ci comporte de nombreuses informations et pour un individu expert peut également permettre d'accéder à certains de vos comptes en ligne.
Sur un ordinateur public, **ne stockez jamais** votre mot de passe dans le navigateur. Si par mégarde vous l'avez fait, pensez à les effacer de la mémoire du navigateur une fois votre travail terminé

Effacez les champs de formulaire

Supprimez les cookies

Le nettoyage de ces données se fait différemment selon les navigateurs. Un bon moyen d'éviter les impairs est d'utiliser le mode « navigation privée » de **Firefox**.

Quel est le meilleur navigateur ? Google a créé un navigateur pour traquer les utilisateurs, Chrome. Firefox fait-il mieux ? Rien n'est moins sûr…

Il n'existe donc pas de "meilleur navigateur", même si **Tor Browser** (cf. page 6 et page 25) peut vous offrir une navigation hautement sécurisée en comparaison de Chrome, Firefox ou Safari.

POUR COMMENCER

Les mots de passe

La plupart des services en ligne que vous utilisez, messagerie, réseaux sociaux, banque en ligne, etc. sont protégés par des mots de passe. Avant de lire ce qui suit, vous pouvez tout de suite tester la robustesse de vos mots de passe sur notre vérificateur de mot de passe. Si le résultat est terrible, voire catastrophique, lisez la suite !

La longueur d'un mot de passe est le facteur principal pour créer un mot de passe solide, capable de résister à une attaque par force brute. Mélanger les chiffres, les caractères spéciaux, les minuscules et les majuscules a souvent pour résultat de créer un mot de passe faible et difficile à retenir. Si, en lieu et place de « mot » de passe, vous utilisez des « phrases » de passe, vous obtiendrez une chaîne de caractère facile à mémoriser et d'une longueur bien supérieure à vos anciens mots de passe.

Th#$^jHTo%46 : court et difficile à retenir

@QueJaimeAFaireApprendreUnNombreUtileAuxSages ! : facile à retenir et très difficile à deviner pour un attaquant.

Utilisez un gestionnaire de mots de passe

Avoir un mot de passe différent par service peut poser problème à ceux d'entre nous qui n'ont pas beaucoup de mémoire. Pas de panique, il existe des outils pour enregistrer l'ensemble de vos mots de passe.

LastPass est un gestionnaire de mot de passe. Disponible sous forme d'extension pour **Firefox**, **Chrome** et **Safari**, **LastPass** permet d'enregistrer l'ensemble de vos mots de passe. L'accès à votre coffre-fort **LastPass** est protégé par une phrase de passe unique. Il vous suffit alors de retenir cette seule phrase pour accéder à tous vos services en ligne. Tout comme le service de mail de Google, Gmail, **LastPass** offre la possibilité de mettre en œuvre la validation en deux étapes. Si vous utilisez **LastPass**, il est fortement recommandé de choisir une longue phrase de passe et de configurer la validation en deux étapes.

Cependant, gardez à l'esprit que LastPass est développé par une société lointaine. Leurs données sont centralisées sur leurs serveurs et ne sont donc pas à l'abri d'un piratage informatique.

De plus, si vous vivez dans/traversez les frontières d'un pays totalitaire : le gestionnaire de mots de passe est à proscrire. En effet, certains pays peuvent vous réclamer le contenu de vos appareils.

La double authentification

La plupart des services en ligne permettent de récupérer un mot de passe perdu grâce à l'envoi d'un mot de passe dans votre boite mail. Il est donc capital de protéger votre boite mail le mieux possible. Si celle-ci est compromise, très souvent, c'est toute votre identité numérique qui le sera également.

La plupart des services mail permettent de mettre en œuvre une sécurité supplémentaire : la « validation en deux étapes ». Ce service permet de protéger votre compte mail avec :

un nom d'utilisateur
un mot de passe
un code que vous recevrez sur votre téléphone portable chaque fois que vous vous connecterez

SÉCURISER SON SURF

Ainsi, sans votre téléphone portable, il est plus difficile pour un pirate (ou un gouvernement) d'accéder à vos mails.

Encore une fois, la protection par double authentification est plus efficace que par SMS. Notamment si vos SMS peuvent être lus sans déverrouiller votre téléphone (au travail, dans les transports en commun, etc.)

https://frama.link/sms2factors

Le saviez-vous ?

Tout votre trafic web est potentiellement accessible par votre fournisseur d'accès. Et plus largement par tous intermédiaires qui se situent entre votre ordinateur et le site que vous visitez : borne WiFi, routeurs, FAI, ordinateurs relais sur Internet, etc.

Voici quelques solutions pour protéger votre activité web des regards indiscrets.

Boostez votre navigateur avec des extensions

Il est possible d'ajouter des fonctionnalités à Firefox et Chrome à l'aide de plug-ins. Chrome, s'il met également l'accent sur la sécurité, n'est pas libre et n'offre pas les mêmes garanties en matière de respect de la vie privée.

L'installation de **HTTPS everywhere** vous garantira que votre navigateur utilisera dès qu'il pourra la version sécurisée (HTTPS donc) du site visité.

Noscript vous permet de contrôler les scripts JavaScript lancés sur les sites web visités. JavaScript est un langage de programmation largement utilisé sur le web. Il s'exécute dans votre navigateur et peut parfois être utilisé dans le cadre de certaines attaques (XSS et XSRF). Vous avez la possibilité d'autoriser certains sites à faire tourner JavaScript et l'extension retient vos choix. Fastidieux au départ, mais indispensable pour surfer couvert. L'équivalent pour Chrome est **scriptsafe**.

Web of trust fonctionne sur le principe du crowd-sourcing (information donnée et vérifiée par une multitude d'utilisateurs) et vous indique si un site est sûr en fonction de l'avis d'autres internautes.

Si vous débarquez sur un site réputé être un nid de scripts malveillants, **Web of trust** vous affichera une alerte avant que la page ne se charge.

UOrigin fait la même chose que **Web of trust**. C'est aussi un bloqueur de publicités beaucoup plus efficace que le très controversé **AdBlock**.

DuckDuckGo Privacy Essentials « protège » vos données lorsque vous effectuez une recherche et naviguez : blocage des pistages, cryptage plus intelligent, recherche privée et plus encore.

POUR COMMENCER

QUELQUES RECOMMANDATIONS

Attention au HTTPS

Lorsque vous allez sur le web avec votre portable ou votre ordinateur, vous utilisez le protocole HTTP (hyper texte transfert protocole). Un protocole est un ensemble de règles et de normes qui permettent à deux machines de communiquer ensemble. **HTTPS** est la version sécurisée du protocole HTTP.

En réalité, rien de ce qui est basé sur les certificats n'est véritablement sûr. C'est une vaste escroquerie intellectuelle ! Sur Chrome, par défaut, le navigateur n'affiche même pas de mis en garde en cas certificat ne correspondant pas au site.

Le HTTPS et le cadenas vert ne font pas tout ! L'actualité récente nous en donné la preuve au Kazakhstan :

https://frama.link/kazakhstanhttps

Chiffrer votre surf

Le problème de HTTPS est que son activation ne dépend pas de vous, mais du webmaster du site que vous visitez. Tous les sites n'utilisent pas HTTPS et une grosse partie de votre surf n'est donc pas chiffrée. Heureusement, il existe des logiciels qui permettent de chiffrer votre connexion et de protéger votre identité en ligne. L'un d'entre eux est le navigateur TOR Browser :

https://www.torproject.org/fr/

Le VPN comme contournement de la censure ?

Certains états surveillent et espionnent les contenus des connexions de leurs populations et, au besoin, n'hésitent pas à filtrer l'accès à certains sites ou services qu'ils jugent contraire à leurs intérêts. Le VPN permet de contourner ce filtrage. La différence majeure est que le fournisseur de VPN vous connecte « réellement » à Internet et, de ce fait, Internet vous voit désormais connecté depuis la Suède et non depuis votre pays. Ainsi, le filtrage mis en place par votre pays ne s'applique plus.

En utilisant un outil légal, **le VPN**, vous pouvez publier vos contenus sur Internet, consulter vos e-mails, surfer de façon sécurisée. Votre pays ne verra plus l'utilisation que vous faites d'Internet, car vous accédez désormais à Internet via un tunnel chiffré dont la sortie se trouve ailleurs, dans un pays où le réseau Internet ne peut être contrôlé par votre gouvernement.

Quelques fournisseurs de VPN reconnus comme étant sûrs : VyprVPN, Astrill VPN, VPN Tunnel, RiseUp VPN, Tunnelbear.

ATTENTION : Dans le cas de l'utilisation d'un VPN, ce n'est plus votre FAI (fournisseur d'accès internet) qui saura ce que vous faites mais… le fournisseur du VPN que vous utilisez !

LES RÉSEAUX SOCIAUX

Contrôler sa présence en ligne

Les réseaux sociaux sont des outils de communication. Vous n'y êtes pas anonyme. Même si vous utiliser un pseudonyme, votre réseau de connaissance est accessible pour chacun de vos amis, voire à tous si votre profil est public.

Par ailleurs, Facebook, Twitter, Instagram, Snapchat, etc. possèdent de nombreuses informations sur vous (adresse IP, heures de connexion, temps de connexion, fichiers ou pages consultées, etc.) en plus de celles que vous renseignez délibérément.

Vous devez contrôler les informations que vous donnez à voir. Ces tutoriels et services en ligne vous aideront à mieux contrôler votre présence en ligne :

Vérifier votre présence sur Internet avec namechecker
- *https://www.namecheckr.com/*

Sécurisez votre compte Twitter
- *https://frama.link/twitter-privacy*

Maîtrisez les paramètres de vie privée dans Facebook
- *https://frama.link/facebook-privacy*

Gardez un œil sur les changements récents dans Facebook

- *https://frama.link/recent-change-facebook*

Contre le harcèlement en ligne

Les réseaux sociaux sont de plus en plus souvent le lieu de harcèlement. Cette technique est utilisée pour faire taire un ou une internaute et consiste à inonder son compte Facebook, Twitter ou autre d'insultes et de menaces. Dans l'idéal, la meilleure réponse à ce phénomène est de faire appel à la justice pour diffamation insultes ou menaces. Cependant c'est un processus long et hors État de droit le recours à la justice est tout simplement impossible.

Il existe des techniques à mettre en place pour lutter contre harcèlement en ligne :

Le guide **Zen and the art of making tech work for you** (*https://frama.link/gendersec*) fournit de nombreux moyens de lutter contre le harcèlement :

- **Outils techniques de contrôle de trolls**
- **Prise de parole sous pseudonyme**
- **Contrôle de ses infos perso**

POUR COMMENCER

LES RÉSEAUX SOCIAUX

La grosse artillerie : BlockTogether

Blocktogether.org est une application en ligne sur laquelle vous pouvez vous inscrire avec votre compte Twitter. **Blocktogether** utilise l'API de Twitter pour bloquer automatiquement des comptes sur la base des listes de blocage d'utilisateurs de Twitter.

Chaque fois que cette liste est mise à jour, si vous passez par l'application, votre compte Twitter bloquera automatiquement les nouveaux comptes ajoutés. Lorsqu'un compte est débloqué, il est débloqué également pour tous les comptes Twitter ayant souscrit à cette liste.

Important : blocktogether ne bloquera jamais un compte que vous suivez déjà, même s'il se trouve dans la liste.

Anonyme sur les réseaux sociaux, vraiment ?

Pseudonymat et anonymat

Il est difficile d'être anonyme sur les réseaux sociaux. L'anonymat ne consiste pas simplement à utiliser autre chose que son vrai nom — un pseudonyme — pour s'enregistrer sur une plate-forme.

On parle ici non pas d'anonymat, mais de **pseudonymat**. L'anonymat consiste à supprimer tout élément qui permettrait de remonter jusqu'à votre identité civile. Il est difficile à obtenir, mais pas impossible (explication page suivante).

Supposons que vous vous créez un profil *@Machintruc* sur Twitter depuis un Cybercafé. Tant que vous ne commettez pas l'erreur de vous y connecter depuis chez vous, avec l'adresse IP fournie par votre FAI, ça passe. Mais personne n'est à l'abri d'une erreur ou d'un oubli. Il suffit d'une seconde pour que tout ce que vous avez mis des mois, voire des années à construire ne s'effondre.

Devenir anonyme

Pour quoi faire ?

Les plates-formes de réseaux sociaux possèdent de nombreuses informations sur vous. Elles peuvent les exploiter à des fins commerciales, mais elles peuvent également les transmettre aux gouvernements qui en feraient la demande. En 2013, l'EFF a recensé le degré de résistance de quelques plates-formes ; celui-ci est assez variable.

- ***https://www.eff.org/who-has-your-back-2013***

Comment ?

L'enregistrement sur une plate-forme avec un e-mail anonyme ou créé pour l'occasion, en utilisant un outil d'anonymisation technique tel que Tor est un bon moyen de créer un compte anonyme.

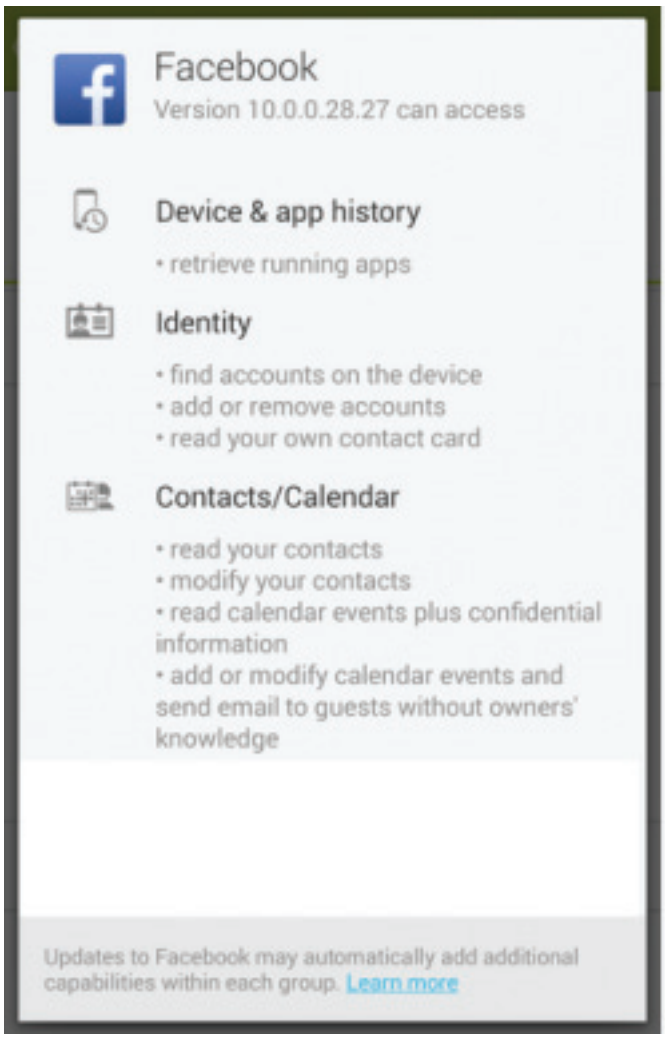
Attention, de nombreux services mail vous imposent désormais de renseigner un numéro de téléphone lors de la création d'un compte. Vous pouvez soit acheter une carte SIM pour l'occasion (un peu lourd), soit utiliser des services qui n'exigent pas de numéro de téléphone, tel que **Tutanota** (payant), **Protonmail**, **Caliopen** ou **GMX mail**.

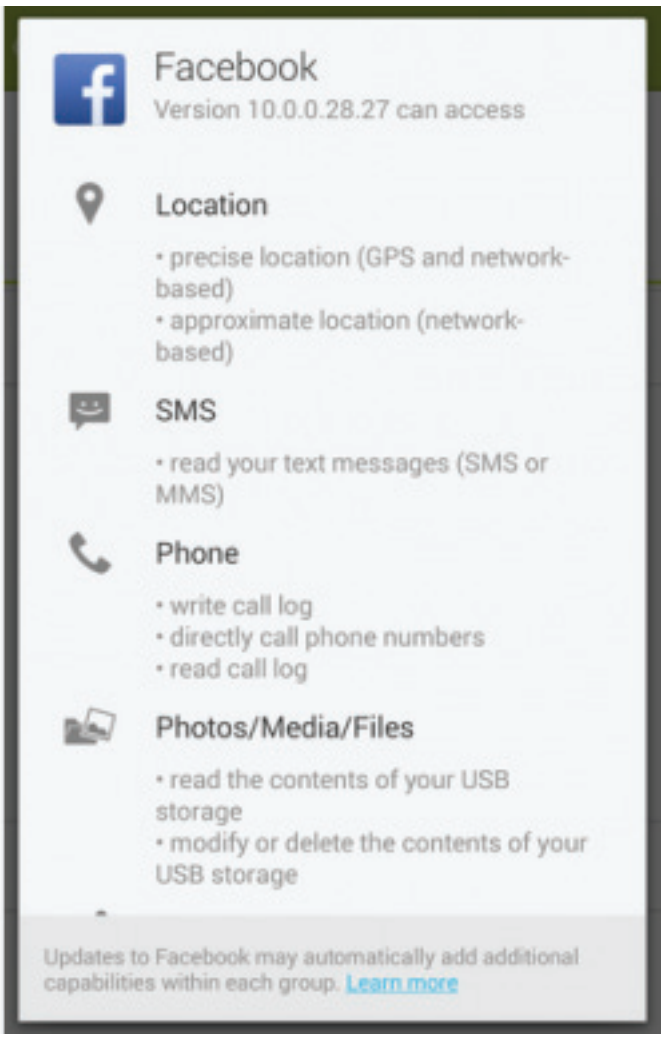
Facebook et les smartphones

Attention, utiliser un compte Facebook sur un smartphone est une très mauvaise idée :

Facebook s'octroie l'accès à de nombreuses données sur votre smartphone et rien ne peut vous garantir que ces données ne sont pas fuitées, au contraire (voir scandale *Cambridge Analytica*, par exemple).

Conserver un compte anonyme sur le long terme est également assez difficile puisque cela suppose de ne jamais se connecter depuis son domicile ou son lieu de travail, ou d'utiliser systématiquement **Tor Browser** (cf. page 6 et page 25).





POUR COMMENCER

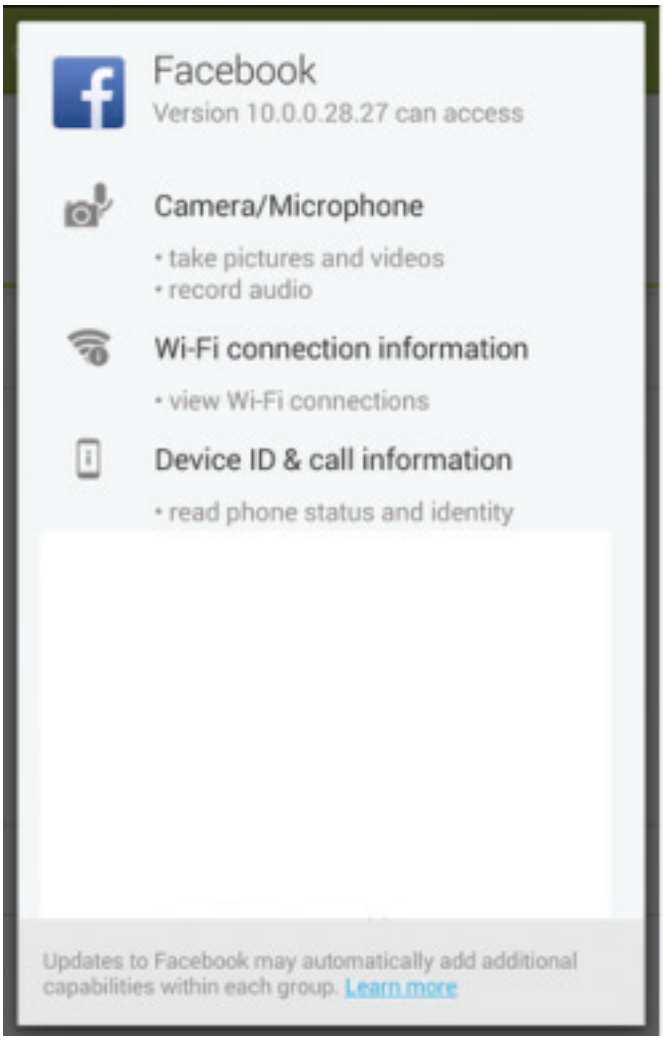
LES RÉSEAUX SOCIAUX

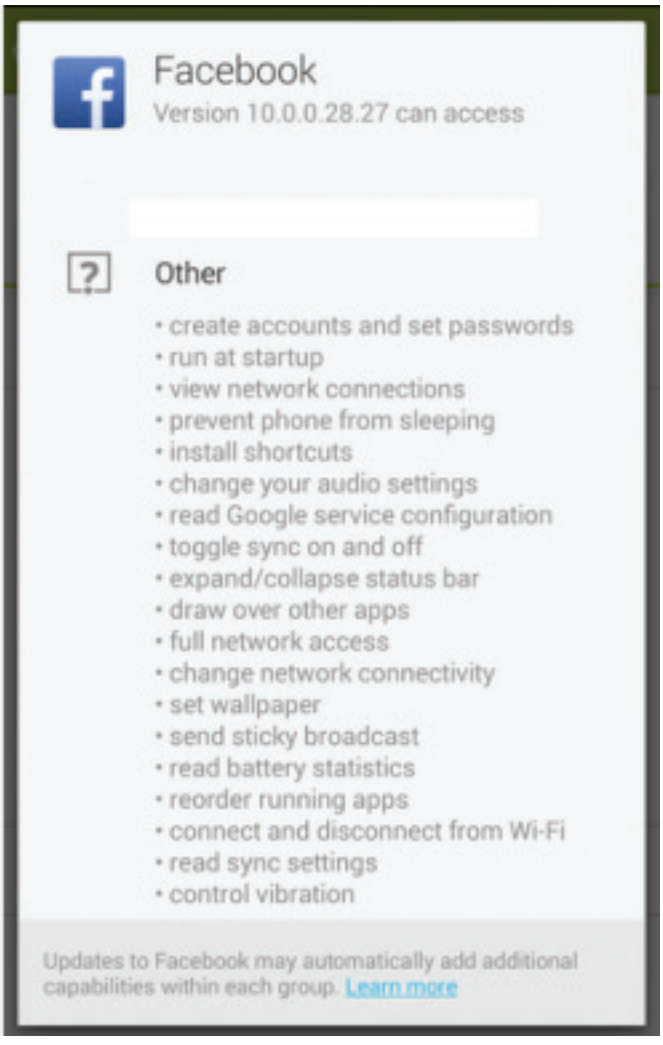
Un bon moyen de s'assurer de conserver un compte vraiment anonyme sur le long terme est de ne s'y connecter qu'en utilisant **le système d'exploitation Tails** :

- ***https://tails.boum.org/***

Pour renforcer l'anonymat et la sécurité d'un compte Facebook on peut également s'y connecter depuis la version hébergée sur le réseau Tor de Facebook dont l'adresse est :

- ***https://facebookcorewwwi.onion/***





Élaborer un modèle de menace

• ***https://frama.link/n2h-atelier-menace***

Bonus : testez votre mot de passe

Vous pouvez tester la robustesse de votre mot de passe grâce au formulaire mis à disposition par **Nothing2Hide**. Il vous indiquera le temps nécessaire pour le craquer :

• ***https://frama.link/n2h-boostermdp***

QUELLES ALTERNATIVES ?

Framasoft s'est donné comme objectif de proposer une trentaine de services libres alternatifs face aux services qui aspirent nos données et nous enferment (Google, Amazon, Facebook, Apple, Microsoft, etc.) Vous trouverez ci-dessous une liste qui récapitule les alternatives présentées par Framasoft :

• ***https://degooglisons-internet.org/fr/alternatives***

Un YouTube sans YouTube ?

Si vous utilisez fréquemment YouTube, vous pourriez être intéressé par **PeerTube :**
• ***https://joinpeertube.org/***

Ou par ***https://invidio.us/***, un « moyen de consommation alternatif » open source et auto-hébergé.

https://framasoft.org/

PROTÉGER SES DONNÉES

GUIDE DE PROTECTION DE VOS DONNÉES ET DE VOTRE ANONYMAT SUR TÉLÉPHONE

De nombreux militants sont pistés via leurs téléphones portables. Certains pays poussent la surveillance plus que d'autres. Il est donc nécessaire d'évaluer le risque de vos activités en prenant en compte les pratiques en cours dans votre pays, le caractère vulnérable de votre travail et les expériences passées des membres de votre groupe.

Les opérateurs téléphoniques ont la possibilité de récupérer des informations relatives à l'utilisation de votre téléphone portable, y compris votre position géographique, et éventuellement de partager ces informations avec le gouvernement si celui-ci le demande. Il est également possible d'installer un logiciel de surveillance sur un téléphone sans que son propriétaire en soit informé. Il y a donc un risque, si vous n'avez pas été en possession physique de votre portable pendant un certain laps de temps.

Les données transmises par mon téléphone

Allumé, hors communication

Quand votre téléphone est allumé, il envoie en continu les informations suivantes aux tours relais avoisinantes :

- Le numéro IMEI — un numéro unique qui identifie le matériel informatique de votre téléphone
- Le numéro IMSI — un numéro unique qui identifie votre carte SIM — c'est ce à quoi votre numéro de portable est lié.
- Le numéro TMSI — un numéro temporaire régulièrement réassigné en fonction du changement de la situation géographique ou du réseau (couverture) qui peut être pisté par des systèmes d'écoute en vente dans le commerce.
- La cellule réseau dans laquelle le téléphone est situé. De quelques mètres jusqu'à plusieurs kilomètres, les cellules peuvent couvrir plusieurs tailles de zones géographiques, avec des cellules beaucoup plus petites dans les zones urbaines et encore plus petites dans les immeubles qui utilisent une antenne relais pour renforcer les signaux.
- La position géographique de l'abonné grâce à cette cellule, déterminée en triangulant le signal depuis la tour relais avoisinante. Là encore, la situation géographique exacte du téléphone dépend de la taille de la cellule — plus une zone géographique est pourvue de tours-relais, plus la position géographique du portable sera précise.

Allumé, en communication

Quand votre téléphone est allumé et communique avec les tours-relais, il peut être utilisé comme un moyen d'écoute pour ceux qui ont accès aux informations des opérateurs téléphoniques. Celles-ci incluent :

- Vos appels téléphoniques reçus et émis
- Vos SMS reçus et envoyés, incluant les informations de l'expéditeur et du récepteur.
- Tout type de données transmis (par exemple les activités de navigations sur le web, hors HTTPS, les messages instantanés non chiffrés) ainsi que le volume de données envoyé (par exemple « Avez-vous uploadé des vidéos sur YouTube ?)
- Votre situation géographique approximative (d'une précision variant entre quelques mètres à quelques kilomètres en fonction de la densité des tours-relais installées).

Il est important de préciser que si vous pensez faire l'objet d'une surveillance quelconque, changer de carte SIM n'est pas suffisant : vous pouvez être suivi grâce au numéro IMEI de votre téléphone. Celui-ci contient également énormément d'informations qui peuvent être utilisées contre vous s'il vous est confisqué ou dérobé.

Tous les téléphones portables disposent en effet d'un espace de stockage situé sur la carte SIM ainsi que d'une mémoire interne. De plus, de nombreux téléphones portables sont aujourd'hui équipés de cartes SD (ou micro SD). De manière générale, stocker des données sur une carte SIM ou sur une carte micro SD (si disponible) est plus recommandé que de stocker ses données sur la mémoire interne du téléphone : une carte SIM ou une carte micro SD est plus facile à cacher ou à détruire qu'un téléphone portable.

Allumé ou non : les données stockées en local

Les données stockées dans votre téléphone, que ce soit sur la carte SIM, dans la mémoire interne ou sur une carte mémoire SD incluent :

- Votre répertoire : les noms et numéros de téléphone de vos contacts.
- L'historique de vos appels : qui avez-vous appelé, qui vous a appelé, et à quel moment les appels ont eu lieu ?
- Les SMS que vous avez envoyés ou reçus
- Les données des applications que vous utilisez, comme un calendrier ou une liste de choses à faire.
- Les photos ou vidéos que vous avez prises avec votre téléphone, si votre téléphone le permet. La plupart des téléphones conservent l'heure et la date auxquelles a été prise la photo, et parfois même la situation géographique.

Si votre téléphone vous permet de surfer sur Internet, vous devriez vous préoccuper de votre historique de navigation. Si possible, ne conservez pas d'historique de navigation. Le danger est bien plus grand si un agresseur accède à vos mails que s'il accède à votre carte SIM ou à la mémoire de votre téléphone.

PROTÉGER SES DONNÉES

GUIDE DE PROTECTION DE VOS DONNÉES ET DE VOTRE ANONYMAT SUR TÉLÉPHONE

Tout comme le disque dur de votre ordinateur, la mémoire SIM de votre téléphone mobile conserve toute donnée sauvegardée jusqu'à ce que la mémoire soit pleine et que de nouelles données sauvegardées viennent écraser les anciennes.

Ainsi, les SMS, l'historique des appels ou les contacts effacés peuvent potentiellement être exhumés de la mémoire SIM. (Il existe une application gratuite pour cela qui ne nécessite qu'un lecteur de carte). Il en est de même pour les téléphones disposant d'espaces de stockage supplémentaires, que ce soit sur la mémoire interne du téléphone ou sur une carte mémoire externe. De manière générale, plus la mémoire du téléphone est importante et plus les éléments effacés, même depuis longtemps, sont potentiellement retrouvables.

Les stratégies à mettre en place

Si les téléphones portables peuvent être des outils efficaces pour les militants, ils peuvent également devenir d'incroyables handicaps si le gouvernement ou les forces de sécurité s'associent avec les compagnies téléphoniques pour vous traquer. Si vous vous situez dans un pays qui met en œuvre des moyens de surveillance pour les téléphones portables ou si vous pensez être surveillé de près à cause de vos activités militantes, il est préférable de ne pas utiliser de téléphone portable pour communiquer. Préférez les rencontres en face-à-face.

Au final, c'est à vous de choisir le risque que vous acceptez de courir : si vous pensez ne pas faire l'objet de surveillance à cause de vos activités militantes ou plus largement par une campagne de surveillance et que vous souhaitez utiliser votre téléphone pour communiquer avec vos camarades militants, prendre des photos et vidéos, ou alors diffuser de l'information par ce biais, vous pouvez utiliser les tactiques suivantes :

- Créez et utilisez un système codé pour communiquer avec les autres militants. « Bippez » vos contacts pour communiquer (laissez sonner une fois ou deux le téléphone de votre correspondant et raccrochez aussitôt afin de lui indiquer que vous êtes bien arrivé à un endroit donné, ou que tout va bien par exemple).

- N'utilisez pas les vrais noms de vos contacts dans vos répertoires téléphoniques. Attribuez-leur des numéros ou des pseudonymes. De cette manière, si jamais les forces de sécurité saisissent votre téléphone ou votre carte SIM, elles ne disposeront pas de l'ensemble de votre réseau.

- Amenez des cartes SIM de rechange lors des manifestations si vous pensez qu'elles risquent d'être confisquées. Il est très important que vous ayez sur vous un téléphone portable qui fonctionne. Si jamais vous devez vous débarrasser de votre carte SIM, essayer de la détruire physiquement.

- Si votre téléphone vous le permet, verrouillez votre téléphone avec un mot de passe. Toute carte SIM dispose d'un code PIN par défaut. Changez le et verrouillez votre carte SIM avec ce code SIM. Un mot de passe (votre code PIN) vous sera demandé à chaque fois que vous utiliserez votre téléphone.

- Si vous pensez qu'une manifestation va se terminer par une forte répression des forces de sécurité, activez le mode avion de votre téléphone. Vous ne serez plus en mesure d'émettre ou de recevoir des appels, mais vous pourrez toujours prendre des photos ou des vidéos et les uploader sur des sites Internet plus tard. Cette tactique est également utile si vous pensez que les forces de sécurité vont cibler en priorité les personnes disposant d'un téléphone portable lors de la manifestation. Plus tard, le gouvernement pourra demander les enregistrements d'appels, de SMS ou de données téléphoniques de tout individu qui se trouvait à un endroit donné à un moment donné afin de procéder à des arrestations en masse.

- Désactivez les fonctions de géolocalisation de vos applications à moins que vous n'utilisiez cette fonction à des fins militantes en taguant certains médias lors d'un événement. Si vous utilisez votre téléphone portable pour diffuser de la vidéo en streaming live, désactivez les fonctions de GPS et de géolocalisation.

- Si votre téléphone fonctionne avec le système d'exploitation **Android**, vous pouvez utilisez de nombreux outils pour chiffrer votre navigation Internet, vos chats, SMS et messages vocaux via les outils créés par le **Guardian Project** et **Whispersys**.

- Lorsque vous utilisez votre portable pour accéder au web, utilisez le HTTPS lorsque cela est possible.

Quelques applications que vous pourriez utiliser pour communiquer plus librement :

- **Silence** (chiffrement des SMS)
- **Orfox / Orbot** (Tor pour Androïd & iPhone)

PROTÉGER SES DONNÉES

VERACRYPT : COMMENT CHIFFRER LE CONTENU DE SON ORDINATEUR ?

Le logiciel Veracrypt permet de chiffrer un simple fichier, une partition entière d'un disque dur ou un périphérique, comme une clé USB. Chiffrer ses données permet de transformer une information afin qu'elle ne soit pas accessible par des tiers non autorisés. En cas de perte ou de vol de votre ordinateur (ou de votre clé USB), il est impossible d'accéder aux données chiffrées sans connaître le mot de passe que vous aurez défini.

Cette rubrique étant assez ardue pour un néophyte, nous vous invitons à visionner cet excellent tutoriel (en français) qui vous apprendra à chiffrer un support de stockage (clé USB, dossier, etc) :

• ***https://frama.link/veracrypt-howto***

Le principe

Ce tutoriel aborde la création d'un volume (ou conteneur) chiffré permettant de chiffrer un ensemble de fichiers. Ce conteneur ou volume peut se trouver sur votre disque dur, une clé USB, une carte mémoire, etc.

Pour en comprendre le fonctionnement, il faut comparer l'utilisation des volumes ou conteneurs **Veracrypt** à celle d'un coffre fort. Chaque fois que vous souhaitez stocker un fichier chiffré, vous ouvrez le volume **Veracrypt** pour l'y déposer. Une fois le fichier stocké, vous fermez le volume. Le fichier est alors chiffré et protégé.

Avant de commencer

Téléchargez et installez **Veracrypt** sur votre ordinateur. **Veracrypt** est un logiciel libre, gratuit, disponible sur **Windows**, **Mac** et **Linux**.

• ***https://www.veracrypt.fr/en/Downloads.html***

Le volume Veracrypt s'ouvre à l'aide d'un mot de passe. Vous devez donc :

- Créer une phrase de passe solide : une phrase à vous (pas de citation ou réplique de film), un mot de passe aléatoire… Quelque chose de long et compliqué qu'on ne peut pas trouver dans un dictionnaire.
- À moins d'utiliser **un gestionnaire de mots de passe**, vous devez impérativement retenir votre phrase de passe ! En cas d'oubli, vous ne pourrez pas récupérer les données du volume chiffré.
- Ne pas écrire votre phrase de passe en clair où que ce soit : le meilleur mot de passe ne vaut rien si on peut le trouver… Collé sous votre clavier par exemple.

Création du volume chiffré

Pour créer un volume chiffré, après avoir lancé le logiciel **Veracrypt**, cliquez sur le bouton **Create Volume.**

Vous avez le choix entre 3 options. La première est la création d'un volume dans un fichier, la seconde dans une partition et la dernière concerne votre système d'exploitation. Sélectionnez la première option **Create an encrypted file container** et cliquez sur **Next**.

Vous avez le choix entre créer un volume chiffré standard et créer un espace protégé invisible (nous y reviendrons plus tard).

Cliquez sur le premier, **Standard Veracrypt volume** puis **Next**.

Vous devez maintenant sélectionner l'emplacement où sera stocké votre volume chiffré. Il peut se trouver sur votre disque dur (dans votre ordinateur), un support de stockage externe (clé USB, disque externe, NAS...), dans un service de stockage en ligne, etc. Cliquez sur **Select File** pour choisir votre emplacement de sauvegarde.

Positionnez-vous dans le répertoire voulu et donnez un nom au fichier (explicite ou non, tel que « Mes Photos.tc » ou alors « Données chiffrés.tc ». Enfin, cliquez sur **Enregistrer**.

Le chemin du fichier apparaît à présent dans le champ de sélection de l'emplacement. Cliquez sur **Next**.

Choisissez l'algorithme proposé par défaut : **AES.**

AES est l'algorithme le plus performant en terme de débit. Il est utilisé aujourd'hui comme standard par les organisations gouvernementales (non militaires) depuis 2000.

Attention : Un algorithme très utilisé est un algorithme très attaqué.

Il y a, en théorie, un risque plus important pour qu'une faille significative soit découverte (un peu à l'image de Microsoft Windows) dans AES que dans les deux autres algorithmes proposés, **Twofish** et **Serpent**, moins vulnérable, car moins utilisés, mais légèrement moins performant en terme de débit.

La méthode la plus sûre est l'utilisation en combinaisons de deux ou trois algorithmes. Si vos documents ne sont pas des informations d'état mettant en jeu la sécurité de votre pays, AES suffira largement, sinon préférez-lui une combinaison d'algorithme.

Sélectionnez à présent l'algorithme de chiffrement voulu. Il y a un deuxième choix à faire, celui du **Hash**. Le hash permet de transformer votre mot de passe en un code irréversible. Si vous ne savez pas lequel choisir, prenez le SHA-512 (également utilisé par les organisations gouvernementales des USA). Une fois votre sélection faite, cliquez sur **Next**.

Indiquez la taille du fichier à créer. Les mesures sont exprimées en KB, MB et GB, l'équivalent européen des Ko, Mo et Go (1 Go = 1 000 Mo = 1 000 000 Ko). Si vous ne savez pas quoi mettre, voici les tailles moyennes de fichiers courants :

un document Word : 200 Ko,
une photo (d'un appareil photo) : 1 Mo,
un fichier audio (MP3) : 4 Mo,
un film (encodé en DivX) : 700 Mo.

Aujourd'hui, un ordinateur portable est vendu avec un disque dur de 160 Go à 320 Go et une clé USB de 2 Go à 16 Go. Après avoir indiqué la taille de votre espace de stockage, cliquez sur **Next**.

PROTÉGER SES DONNÉES

VERACRYPT : COMMENT CHIFFRER LE CONTENU DE SON ORDINATEUR ?

Vous devez à présent définir le mot de passe permettant de chiffrer et déchiffrer vos données. Il est conseillé d'avoir un mot de passe d'au moins 20 caractères.

Vous pouvez composer une phrase pour vous en rappeler plus facilement ou choisir un mot de passe aléatoire (plus difficile à cracker). Votre phrase ne doit pas être connue : citations, répliques de film et titres de chansons sont à éviter. Cliquez sur **Next**.

Veracrypt n'autorise pas l'utilisation de lettres accentuées (tel que : é à ï ô ù…) dans le mot de passe.

Remplacez les lettres accentuées par leurs équivalents non accentués. Il est possible d'utiliser des chiffres et des signes de ponctuation pour complexifier le mot de passe.

Optionnel : Cette fenêtre n'apparaît que si vous avez choisi de créer un volume de stockage supérieur à 4096 Mo (soit plus de 4 Go). Le système de fichier FAT32 limite la taille des fichiers à 4096 Mo. Pour outrepasser cette limite, choisissez le format **NTFS de Microsoft**. Si vous n'avez pas de connaissances approfondies en informatique, sélectionnez **No**. Cliquez ensuite sur **Next**.

Le conteneur **Veracrypt** va maintenant être créé. Si vous ne savez pas à quoi correspondent les options de cet écran, conservez les choix par défaut.

Utilisateurs expérimentés : nous déconseillons de cocher la case **Dynamic**. Cette option permet d'augmenter la taille du volume **Veracrypt** dynamiquement, mais pose un problème de sécurité, car cette fonctionnalité peut permettre à un attaquant de connaître la taille réelle des données stockées.

Vous allez à présent formater le volume de stockage. Le programme remplit de données aléatoires l'espace non utilisé de votre conteneur. Lancer le formatage en cliquant sur le bouton **Format**.

La progression peut être longue, elle est en fonction de la taille de votre fichier, des performances du support physique et de votre processeur.

Bravo ! Vous venez de créer votre fichier chiffré ! Pour finir, cliquez sur **Exit**

Ouverture du volume chiffré

Pour accéder à vos données, cliquez sur **Select File**.

Sélectionner le volume chiffré là où il a été enregistré puis cliquer sur **Ouvrir**.

Il est également possible d'accéder au volume chiffré en double-cliquant dessus dans votre explorateur de fichier.

Le chemin de votre volume chiffré apparaît dans le champ **Volume**. Sélectionner dans la liste, la lettre

du lecteur virtuel par laquelle vous souhaitez accéder à vos données chiffrées (généralement la première convient). Cliquez sur le bouton **Mount**.

Entrez le mot de passe défini lors de la création du volume **Veracrypt** puis cliquez sur **OK**.

Le volume chiffré est à présent accessible en clair depuis votre explorateur de fichiers comme un support de stockage classique.

Vous pouvez maintenant accéder au contenu de votre volume chiffré directement par votre explorateur de fichiers, en double cliquant sur la ligne où se trouve votre espace chiffré ou en faisant un clic droit sur cette ligne et en sélectionnant **Open**.

Utilisation du Volume chiffré

Nous allons chiffrer un fichier se trouvant sur notre disque dur : une image. Celle-ci se trouve actuellement dans le dossier Images. Après l'avoir sélectionnée, nous la « coupons » afin qu'elle ne soit plus disponible à son emplacement d'origine en version non chiffrée.

Une fois positionnée dans le volume **Veracrypt**, nous la « collons ». Elle est désormais en sécurité dans notre volume chiffré. Notre image et tous les fichiers que nous y mettrons à l'avenir seront chiffrés. Pour y accéder, le mot de passé défini lors de la création du volume sera nécessaire.

Une fois les fichiers déplacés dans le coffre fort numérique (le volume **Veracrypt**), il faut en refermer l'accès (l'accès est automatiquement fermé lorsque l'ordinateur s'éteint) : c'est l'opération dite de « démontage ». Pour cela, cliquez sur l'élément à refermer et sélectionnez **Dismount** (démonter). Vous pouvez aussi cliquer sur le bouton du bas **Dismount All** (démonter tout).

Veracrypt et le déni plausible

Veracrypt offre la possibilité de créer un volume caché pour prévenir le cas où on est forcé de donner son mot de passe. C'est le principe de la valise à double fond ou, en cryptographie, déni plausible.

Au lieu de créer un volume chiffré unique, **Veracrypt** en créera deux, un volume extérieur (outer volume) et un volume caché (hidden volume). Chaque volume s'ouvrira avec des mots de passe différents. L'un fera office de leurre, l'autre contiendra les données vraiment confidentielles. Même si le mot de passe du volume extérieur est révélé, il ne permettra pas d'accéder au volume caché qui est lui protégé par un autre mot de passe. Il est impossible de savoir si un espace chiffré avec **Veracrypt** contient un ou deux volumes.

Pour créer un volume chiffré caché, suivez les mêmes étapes que lors de la création d'un volume simple :

Cliquez sur le bouton **Create Volume**

Sélectionnez l'option **Create an encrypted file container** puis cliquez sur **Next.**

Vous avez le choix entre créer un volume chiffré standard et créer un espace protégé invisible. Cliquez sur **Hidden Veracrypt Volume** puis sur **Next.**
Le procédé de création du volume est alors le même que celui décrit plus haut à ceci près que

PROTÉGER SES DONNÉES

VERACRYPT : COMMENT CHIFFRER LE CONTENU DE SON ORDINATEUR ?

vous créerez deux volumes successivement, le volume extérieur d'abord, le volume caché ensuite, chacun avec des mots de passe différents.
L'utilisation d'un volume caché présente quelques inconvénients :

- La création d'un container caché fait perdre de la place.
- Vous devrez retenir un mot de passe supplémentaire (sauf si vous utilisez un gestionnaire de mots de passe).
- Si vous avez mis le déni plausible en place il y a un certain temps et que vous n'avez pas touché à la partition cachée depuis, votre agresseur, s'il sait ce qu'il cherche et s'il sait regarder la date de dernière modification d'un fichier, aura tôt fait de s'apercevoir de l'astuce.
- Il existe d'autres moyens de dissimuler des données : il est possible de cacher un conteneur **Veracrypt** dans des fichiers image et/ou vidéo.

Cette solution (la stéganographie) est moins facile à mettre en œuvre, mais plus crédible en terme de camouflage :

- ***https://frama.link/stegano-veracrypt***

Ce chapitre est basé sur un article de Korben :

- ***http://wiki.korben.info/Truecrypt***

Pour aller plus loin :

Chiffrer le contenu de son Mac avec Filevault :

- ***https://frama.link/n2h-guidevoyagehostile***

Chiffrer le contenu de son smartphone Android :

- ***https://frama.link/n2h-guideandroid***

Chiffrer le contenu de son iPhone :

- ***https://frama.link/n2h-guideiphone***

PROTÉGER SES COMMUNICATIONS

PROTÉGER SES E-MAILS

Le mail est probablement l'outil de communication le plus utilisé sur Internet. Et il risque de le rester pour encore quelques dizaines d'années. Mauvaise nouvelle, sécuriser ses mails sur Internet n'est pas la chose la plus aisée à faire.

Premier problème : l'e-mail par défaut n'est pas chiffré. Envoyer des informations confidentielles par mail via Internet revient à peu près au même qu'envoyer ses codes de carte bleue par carte postale (sans enveloppe) : c'est une très mauvaise idée !

Chiffrement des e-mails, le problème

Bonne nouvelle, il existe un une solution permettant de chiffrer le contenu d'un e-mail : openPGP.

Problème, l'e-mail par défaut n'ayant pas été prévu lors de sa conception pour assurer un minimum de confidentialité lors des échanges, le chiffrement de mail avec **openPGP** ressemble plutôt à une rustine qu'à une roue toute neuve. L'installation et l'utilisation d'**openPGP** sont assez ardues et requièrent beaucoup de pratique pour être vraiment efficaces et sûres.

Par ailleurs, quand bien même vous seriez un champion de PGP — ce qui n'est pas à exclure après la lecture de ce guide — le chiffrement de mail via PGP comporte quelques défauts : seuls le contenu des e-mails, le corps de texte et les éventuelles pièces jointes sont chiffrés. Ni l'objet, ni les noms et adresses des expéditeurs et destinataires ne sont chiffrés. Ainsi, si vous envoyez un e-mail chiffré, il est toujours possible pour quelqu'un placé stratégiquement sur le réseau de savoir avec qui vous correspondez.

Avant d'apprendre à chiffrer vos mails, la question à se poser est : ai-je vraiment besoin de chiffrer mes e-mails ?

N'existe-t-il pas un autre outil de communication chiffrée (**Signal**, **Wire**) qui conviendrait mieux à mes besoins ? Si la réponse est non et que vous avez absolument besoin de chiffrer vos mails, vous avez là encore deux alternatives :

• Chiffrer vos mails depuis n'importe quel fournisseur de service avec **Enigmail** dans Thunderbird (***https://www.enigmail.net/index.php/en/***) ou **Mailvelope** directement dans votre navigateur :

• ***https://www.mailvelope.com/en/***

• Utiliser un fournisseur de mail qui propose en standard une implémentation d'**openPGP** transparent pour l'utilisateur.

PROTÉGER SES COMMUNICATIONS

PROTÉGER SES E-MAILS

Les fournisseurs de mails chiffrés

La solution la plus simple pour chiffrer ses mails consiste à utiliser un service qui le fait pour vous, tels que Tutanota ou Protonmail. Ce n'est pas aussi sécurisé que de chiffrer ses mails sur son ordinateur à l'aide d'enigmail ou Mailveloppe, mais c'est déjà très sûr.

Les clés privées (voir plus loin pour l'explication du **système de clés**) qui servent à chiffrer les mails sont stockées chiffrées sur les serveurs de Protonmail, là où avec **enigmail** ou **Mailveloppe** ces dernières ne quittent jamais votre ordinateur.

C'est là la principale différence entre un service clés en main et une implémentation logicielle (**engimail** ou **Mailveloppe**). Le premier est plus simple, mais vos clés privées transitent — bien que chiffrées — via Internet. Ce qui n'est pas la meilleure des idées selon votre modèle de menace.

Protonmail fonctionne sur un modèle freemium et propose un service gratuit avec 500 Mo de stockage :

- ***https://protonmail.com/***

Tutanota est le service d'e-mails le plus sécurisé au monde. L'ouverture d'un compte est gratuite, mais vous pouvez bénéficier de nombreux autres avantages à partir de 12 €/an :

- ***https://tutanota.com/fr/***

Riseup est un petit collectif créé à Seattle en 1999 dans le but de rendre accessible aux mouvements sociaux une certaine forme d'autodétermination numérique.

Riseup fournit des outils de communication en ligne pour les personnes et les groupes qui militent en faveur d'un changement social libérateur. C'est un projet pour créer des alternatives démocratiques et pour pratiquer l'autodétermination en contrôlant nos propres moyens de communication sécurisés.

Attention : l'inscription à Riseup se fait grâce à 4 codes d'invitation, afin de limiter les intrusions des services étatiques, policiers, etc.

- ***https://riseup.net/fr/***

Disroot est une plateforme qui fournit des services en ligne basés sur les principes de liberté, de respect de la vie privée, de fédération et de décentralisation :

- ***https://disroot.org/fr/***

Des outils de chats sécurisés sur smartphone

- **Signal** pour Android et iPhone
- **Wire** pour iOS ou Android

- ***https://frama.link/polemique-whatsapp***

PROTÉGER SON ANONYMAT

EFFACEMENT SÉCURISÉ DES DONNÉES

Lorsque vous effacez un fichier de votre ordinateur, celui-ci va dans la corbeille. Une fois la corbeille vidée, il est quand même possible de récupérer ce fichier. En d'autres mots : lorsque vous effacez un fichier sur votre ordinateur, il peut quand même être restauré.

Il faut imaginer votre ordinateur et sa façon de gérer les fichiers comme un livre avec une table des matières. Lorsque vous videz votre corbeille, vous ne faites que supprimer la référence du fichier dans la table des matières. Le fichier lui est toujours sur le disque dur. Le récupérer n'est pas si complexe, des logiciels libres et gratuits tels que **Photo Recovery** (*https://frama.link/photrecovery*) vous permettent de le faire.

Si vous souhaitez vraiment effacer un fichier depuis votre ordinateur, il faut donc non seulement supprimer sa référence, mais également l'effacer de votre disque dur.

Sur Mac

Si vous disposez d'un système d'exploitation (OS) antérieur à El Capitan, il suffit de faire un clic droit sur la corbeille tout en maintenant la touche option appuyée. Une nouvelle option dans le menu apparaît : **Vider la corbeille en mode sécurisé**

Dans le cas contraire, téléchargez et installez le freeware **OnyX**. Dans les options de nettoyage du logiciel, il est possible de choisir un effacement sécurisé des données présentes dans la corbeille.

Télécharger OnyX :

- *https://www.titanium-software.fr/en/onyx.html*

Windows

Sous Windows, il vous faut installer un logiciel supplémentaire : *https://eraser.heidi.ie/*. Une fois le logiciel installé, vous aurez une nouvelle option dans le menu contextuel lorsque vous cliquerez (clic droit) sur un fichier : **Erase** ou **erase on restart.** Comme son nom l'indique, vous pouvez choisir d'effacer le fichier (et sa référence) immédiatement ou au redémarrage de votre ordinateur.

Linux

Sous Linux, deux programmes très utiles :

Wipe:
- *https://doc.ubuntu-fr.org/wipe*

Shred:
- *https://doc.ubuntu-fr.org/shred*

PROTÉGER SON ANONYMAT

SUPPRIMER LES MÉTA DONNÉES DE VOS FICHIERS

Lorsque vous transmettez un document, de nombreuses données associées transitent avec lui. Peu d'internautes en ont conscience, pourtant, de nombreux formats de fichiers contiennent des données cachées, les fameuses « métadonnées ».

Vos fichiers parlent pour vous

Des traitements de textes ou des PDF sont susceptibles de contenir le nom de l'auteur, la date et l'heure de la création du fichier, et même parfois une partie de l'historique de l'édition de ce fichier. Ces données cachées dépendent du format du fichier ainsi que du logiciel utilisé.

Les formats d'images tels que TIFF ou JPEG sont parmi les formats les plus bavards. Ces fichiers, créés par des appareils photo numériques ou des téléphones portables, contiennent des métadonnées au format **EXIF**, qui peuvent renseigner la date, l'heure, voire les données GPS de l'image, la marque, le numéro de série de l'appareil ainsi qu'une image en taille réduite de l'image originale. Des logiciels de traitement d'image tendent à conserver intactes ces données.

Internet abonde de ces images floutées dont le fichier EXIF contient toujours le document avant floutage.

Pour info, certains sites de partage d'images en ligne ou réseaux sociaux **Facebook** ou **Flickr** par exemple, effacent — ou tout du moins ne republient pas — les méta données des fichiers. Attention, cela ne signifie pas que ces méta données n'existent pas. Elles existent toujours… chez Facebook.

Afficher les métadonnées

Il existe plusieurs méthodes pour accéder à ces métadonnées. La plus simple consiste à vérifier les propriétés du fichier. Un simple clic droit vous donnera beaucoup d'informations. Les fichiers bureautiques de type Office peuvent comporter des informations sur l'auteur ou l'entreprise qui a créé le document. Vous avez la possibilité de les supprimer avec le logiciel de création du document, que ce soit **Microsoft Word** ou **Open Office** : **Menu Fichier > Propriétés.**

Les fichiers PDF peuvent aussi faire office de mouchards. Ils comportent souvent le nom de l'auteur. Celui-ci est accessible dans les propriétés du fichier et modifiable à l'aide d'un logiciel d'édition de fichiers PDF. Avec **Acrobat Writer**, sous Windows ou Mac, il suffit d'aller dans le menu **Fichier > Propriétés** pour modifier l'auteur du document. Sous Gnu/Linux, il existe des alternatives libres et gratuites telles que **PDF Mod** qui permettent d'éditer aussi simplement les métadonnées des fichiers PDF.

L'extension Firefox **Exif Viewer** permet d'afficher les métadonnées des images JPEG.

Modifier les méta données

Il existe des outils plus sophistiqués permettant d'éditer l'ensemble des métadonnées, quel que soit le type du fichier à manipuler : PDF, JPEG, GIF, etc. Leur usage requiert un peu plus d'expérience cependant.

ExifTool : le plus simple à utiliser, ce logiciel avec une interface graphique disponible sous Windows

- ***http://owl.phy.queensu.ca/~phil/exiftool/***

Il existe de nombreux tutoriels et exemples pour l'utiliser : ***https://frama.link/exiftool-tuto***

JHead : logiciel de manipulation de JPG, disponible sous Gnu/Linux, Windows et Mac OSX.

- ***http://www.sentex.net/~mwandel/jhead/***

VerExif : voir et supprimer les données EXIF directement depuis votre navigateur.

- ***http://www.verexif.com/fr/***

LE NAVIGATEUR TOR BROWSER

Nous avons vu que, lors de nos navigations sur le web, les sites visités peuvent enregistrer notre adresse IP et donc qu'un adversaire peut facilement remonter à nous par ce biais. D'où, parfois, la nécessité de dissimuler cette adresse IP.

Tor est un logiciel permettant de faire transiter notre connexion au sein d'un réseau de « nœuds », masquant ainsi notre IP réelle. On appelle cela **le routage en oignon**.

Pour pouvoir utiliser le réseau d'anonymisation Tor, il faut paramétrer le logiciel Tor lui-même, mais également les logiciels qui vont l'utiliser, comme le navigateur web par exemple. Ces paramétrages sont souvent complexes, à tel point qu'il est difficile d'être sûr de l'anonymat qui en résulte.

C'est pourquoi il est conseillé, pour utiliser Tor, de se servir soit d'un système live dédié à cet usage, soit d'utiliser un « kit prêt à l'emploi » : **le Navigateur Tor.**

Apprenez à installer/configurer Tor :

- ***https://frama.link/boomtor***

POUR ALLER PLUS LOIN

COMMENT SÉCURISER SON ORDINATEUR TOUT EN RESTANT DISCRET ?

L'objectif n'est pas ici de se cacher de Google ou de se protéger d'un gouvernement ou de logiciels espions type **FinFisher** (***https://frama.link/rsf***) ou **DaVinci** (***https://frama.link/rsfhackteam***), mais de se prémunir des menaces standards et de ne rien conserver de sensible sur son ordinateur. Utile pour passer les frontières et les check-points, comme c'est le cas dans certaines régions du monde où il peut légalement vous être demandé d'afficher le contenu de vos appareils.

Mise en œuvre : facile
prérequis : une connexion Internet
Ingrédients : un peu de technique et beaucoup de bon sens (« information management » comme disent les Anglo-saxons).

Le principe

Cette configuration repose sur la compartimentation et le **déni plausible**. L'idée est de n'avoir aucun élément sensible sur son ordinateur, ni contacts ni outils de sécurité qui pourraient éveiller les soupçons (**Tor**, **Veracrypt**, etc.). L'utilisateur devra faire l'effort d'identifier les informations sensibles qu'il devra placer sur ses comptes et sa messagerie de terroriste de l'Internet.

Ce qu'il faut avoir

- **HTTPS everywhere :**

- ***https://www.eff.org/https-everywhere***

- **Un antivirus**
- **Un outil permettant l'effacement sécurisé**

Ce qu'on peut avoir (et c'est bien)

- **Open VPN** sur Windows ou **Tunnelblick** sur Mac
- **Adium** sur Mac ou **Pidgin** avec le plug-in **OTR** sur Windows

Ce qu'il ne faut pas avoir

- Un carnet d'adresses rempli de contacts sensibles
- Un historique web
- Des e-mails en local sur son ordinateur (avec Outlook, ou Thunderbird)
- Tout outil de crypto sauf ceux mentionnés ci-dessus (car facile à supprimer et pas du tout identifiés comme « outils d'activistes »)
- Des clés PGP
- Des clés SSH
- Des fichiers ou containers chiffrés

Ce qu'il faut mémoriser

• Le mot de passe de la messagerie et des comptes de réseaux sociaux. Ces mots de passe ne doivent jamais être stockés sur l'ordinateur. Ça ne fait que quelques phrases de passe à mémoriser.

La pratique

- Utiliser la navigation privée (pas de traces sur l'ordi) et un **VPN** (pas de traces en ligne)
- Effacer de manière sécurisée tous les fichiers sensibles sur l'ordinateur
- Dans le cloud, sur un compte **Protonmail**, **Fastmail**, **Cozy** ou **NextCloud**. **On y stocke :** les fichiers, les contacts, sans client local type Google drive ou logiciel Dropbox, sans enregistrer lesdits comptes dans les apps natives de l'OS (puisque tout est stocké sur l'ordi) que ce soit Windows, Mac ou Linux.
- supprimer quand nécessaire les fichiers avec **Eraser** ou **l'effacement sécurisé** sous mac

S'il vous faut absolument stocker des informations localement

S'il vous faut stocker des fichiers volumineux, utilisez une clé USB externe avec un container **Veracrypt** – le mieux en mode stéganographie (***https://frama.link/stegano-truecrypt***) pour les plus furieux, et le logiciel Veracrypt dessus.
Ne rien stocker sur l'ordinateur. Il est plus facile de détruire une clé qu'un disque dur.

Ou : stockez vos données sur la carte SD de votre téléphone en fichier TXT caché dans l'arborescence d'Android, au format mp3 au milieu de votre/musique… ça reste simple et ludique à faire (juste avoir de l'imagination).

Le risque principal

L'erreur humaine est ici hautement probable :

- laisser traîner un mot de passe,
- ne pas naviguer en navigation sécurisée et laisser traîner des sites dans votre historique ou, pire, des mots de passe enregistrés dans le navigateur (ne JAMAIS enregistrer des mots de passe dans son navigateur),
- oublier d'effacer un fichier sensible,
- se connecter sans VPN. La plupart des clients VPN peuvent se paramétrer pour se lancer automatiquement.

Divers

Choix du service mail :

Se créer un compte mail éphémère sur gmx.com ou autre et activer la redirection dessus vers son vrai compte mail pro est une solution valable pour que votre « vrai » e-mail ne transit pas sur le réseau du pays où vous êtes.

Veracrypt peut être camouflé simplement sous Windows ou autre en changeant l'icône tout simplement.

POUR ALLER PLUS LOIN

COMMENT SÉCURISER SON ORDINATEUR TOUT EN RESTANT DISCRET ?

Les services Google ou Microsoft live sont à proscrire, dans tous les cas de figure !

Fastmail ou **Protonmail** proposent les mêmes fonctions que Google ou Microsoft avec l'énorme avantage de ne pas être hébergé aux USA. Inconvénient : c'est payant.

Un e-mail et des services autohébergés (ou hébergé par une connaissance) type **Yunohost**.

ATTENTION à l'autohébergement et le black-listing e-mail :

Le contexte du lieu est important, se noyer dans la masse reste un point important. Il vaut mieux utiliser une adresse Gmail, Yahoo, Hotmail dans certaines circonstances qu'une adresse Riseup.

Ça va sans dire, mais on le dit quand même

Vos comptes compartimentés ne doivent pas contenir d'informations personnelles type nom/prénom.

> LE MEILLEUR MOYEN DE PROTÉGER SES DONNÉES, C'EST DE N'EN AVOIR AUCUNE…

Surtout pas de **prenom.nom@gmail.com** ou **prenom75@live.com**. On ne devient pas activiste du jour au lendemain et on peut avoir échangé des e-mails éventuellement compromettants avec son e-mail usuel (identifiable **nom.prenom@service.com**). Il faut dans ce cas les transférer sur une autre messagerie dédiée (IMAP est très bien pour ça) et les effacer de la précédente messagerie.

Ce chapitre a été rédigé après une rencontre avec des activistes syriens qui font des allers-retours réguliers entre Londres, Raqqa, Alep et Damas.

POUR ALLER PLUS LOIN

PRÉCAUTIONS À PRENDRE AVANT D'ALLER COUVRIR UN ÉVÉNEMENT

Le guide de prévention pour smartphone

Vous avez besoin de votre smartphone lors d'une manifestation ou d'un événement, mais vous êtes inquiet de ce que pourrait se passer si celui-ci est confisqué ? Voici sept étapes à mettre en œuvre avant de sortir de chez vous.

Traduction de l'infographie de la **Press Freedom Foundation, Mobile Security Prevention Tips**

- ***https://frama.link/tips-activists***

1. Chiffrez votre téléphone

Cela signifie que vos données ne seront pas lisibles sans le mot de passe que vous utilisez pour accéder à votre téléphone lorsque celui-ci est éteint, et ce même si quelqu'un réussit à copier l'intégralité des données de votre téléphone. Le chiffrement est activé par défaut sur iPhone depuis iOS8 et sur Android depuis Android6 (**mashmallow**).

2. Verrouillez votre téléphone

Changez les paramètres de votre téléphone pour que celui-ci se verrouille : dès qu'il se met en veille, lorsque vous appuyez sur le bouton on/off

3. Masquez vos messages

Paramétrez votre téléphone pour que les SMS ne s'affichent pas sur l'écran lorsque votre téléphone est verrouillé.

4. Verrouillez votre carte SIM et assignez un code à votre carte SIM.

5. Utilisez des mots de passe forts

Utilisez des phrases de passe, l'authentification à deux facteurs et des mots de passe différents pour chacun de vos comptes.

6. Faites la liste de vos comptes sensibles

Avoir une liste des comptes sensibles auxquels il faudra apporter une attention toute particulière en cas de compromission ou vol de votre smartphone vous fera gagner un temps précieux.

7. Effacez votre historique de navigation

Effacez régulièrement l'historique de votre navigateur web.

POUR ALLER PLUS LOIN

QUE FAIRE SI VOTRE TÉLÉPHONE A ÉTÉ COMPROMIS ?

Lorsque vous participez à une action organisée, votre téléphone est susceptible d'être confisqué, fouillé ou manipulé par les autorités. Vous pouvez minimiser les conséquences en cas de confiscation de votre téléphone en suivant les étapes de ce guide.

Traduit de l'article de la **Press Freedom Foundation Rapid Responses For Compromised Phones** (***https://frama.link/compromisedphone***).

Que faire en cas de compromission de votre smartphone ? Vol, ou suspicion d'infection.

- Préservez votre carte SD et votre carte SIM
- Sortez votre carte SIM et votre carte SD et conservez-les quelque part.
- Auditez l'activité de votre compte
- Sur un autre ordinateur (de confiance), vérifiez l'activité de votre compte et cherchez des indices permettant de voir que quelqu'un d'autre s'est connecté à votre compte. Prenez des captures-écrans et notez toutes les nouvelles adresses IP, les géolocalisations et les périphériques qui accèdent à votre compte.
- Cherchez des traces d'activité inhabituelle sur les réseaux sociaux
- Cherchez des signes permettant de savoir si quelqu'un a infiltré votre réseau et celui de vos contacts. Documentez et prenez des captures-écrans de toute activité inhabituelle.
- Déconnectez-vous de tous vos comptes sensibles.

En vous déconnectant, vous signalez à votre fournisseur de service que votre session est terminée. Cela évite qu'un attaquant ne reprenne et réactive votre session à partir des cookies de connexion qu'il aurait pu copier.

Réinitialiser votre téléphone

Après toute compromission ou même suspicion de compromission, vous devriez effectuer une remise à zéro, aux paramètres d'usine, de votre smartphone. Si possible, prenez en un nouveau.

Réinitialisez vos mots de passe

Sur un autre ordinateur, de confiance, réinitialisez les mots de passe de vos comptes et profitez-en pour utiliser des phrases de passe.

- ***https://frama.link/n2h-mdprobuste***

Si vous aviez activé la double authentification pour un de vos services, les paramètres d'authentification vont aussi être réinitialisés.

Prenez une nouvelle carte SIM

Prenez une nouvelle carte SIM. C'est une opération très simple à effectuer. Demandez à votre opérateur ou faites-le en magasin. Veillez à ramener deux pièces d'identité. Certains opérateurs de télécoms peuvent l'exiger pour des raisons de sécurité.

D'autres, au contraire, ne vérifient pas les justificatifs demandés : **LycaMobile** par exemple (utilisation de fausses cartes d'identité possible).

Formatez votre carte SD

Vous ne pouvez plus avoir confiance en votre ancienne carte SD ? Formatez-la. C'est la procédure la plus simple. Toutes les données seront perdues, mais vous repartirez avec une carte SD vierge.

REMARQUE IMPORTANTE : Il y a une sorte de BIOS (Basic Input Output System) sur les cartes SD. Si ce dernier a été modifié, un simple formatage de la carte ne permet pas de remettre un BIOS « propre ». Ce programme étant difficilement accessible, la meilleure solution est encore de **changer de carte SD.**

LOI LPM 2019/2025

Le saviez-vous ? Depuis la loi LPM (Loi de propagation militaire 2019-2025), les services de renseignements et les services de police peuvent introduire des logiciels espions dans les matériels électroniques de n'importe quel utilisateur (soit physiquement soit à distance), avec le concours des opérateurs télécoms et sans avoir besoin de l'autorisation d'un juge.

Selon le journal Allemand **Der Spiegel**, « *la France s'est dotée de la loi la plus répressive du monde en matière de cybercriminalité, passant devant l'Australie, déjà réputée pour sa sévérité en la matière*. »

Source : ***https://www.spiegel.de/international/europe/the-big-brother-of-europe-france-moves-closer-to-unprecedented-internet-regulation-a-678508.html***

POUR ALLER PLUS LOIN

AUTRES RESSOURCES & LIENS UTILES

Parce que d'autres organisations, auteurs, blogueurs, journalistes, etc. font un très bon travail de vulgarisation sur la sécurité numérique, voici une sélection de ressources sur le sujet.

Français

Boîte à outils pour le chiffrement et l'anonymat en ligne :

https://frama.link/n2h-toolbox

Security in a box : très bon guide édité par l'ONG Tactical Tech. Régulièrement mis à jour. Plutôt orienté activistes et défenseurs des droits humains :

https://securityinabox.org/fr/

Le c**hiffrement de mails** expliqué en infographie :

https://emailselfdefense.fsf.org/fr/infographic.html

Un guide complet de chiffrement des e-mails avec GnuPG (Windows, Mac, Linux) :

https://emailselfdefense.fsf.org/fr/windows.html

Guide d'auto défense numérique :

https://guide.boum.org/

Pourquoi la sécurité numérique ne peut pas être la même pour tous les journalistes ?

https://frama.link/secujournalistes

PrivacyNightmare : Cette page vise à réunir des articles, études et rapports faisant état des risques et dérives entrainés par une faible protection des données personnelles.

https://wiki.laquadrature.net/PrivacyNightmare(fr)

Tentatives d'hameçonnages avec les caractères unicodes Une méthode plus élaborée pour masquer le nom de domaine réel consiste à utiliser des caractères bien choisis parmi les dizaines de milliers de caractères du répertoire Unicode. En effet, certains caractères spéciaux ont l'apparence des caractères de l'alphabet latin.

https://frama.link/hackunicode

English

The Motherboard guide to not getting hacked

https://frama.link/guidetonotgettinghacked

Surveillance self defense guide By EFF : one of the best guide out there with tutorials, overviews articles and detailed guides for specific situations.

https://ssd.eff.org/

Why doesn't your website enforce https ?
Https isn't a magic wand to "make everything secure", especially not in the current age where certain projects have completely trivialized the https.

https://frama.link/websitehttps

Mobile Security Prevention Tips visual guide

https://frama.link/mobsecuretips

Rapid Responses For Compromised Phones visual guide

https://frama.link/compromisedphone

Digital Security Resources (juillet 2017)

https://frama.link/digital-security-resources

How to Lose Friends and Anger Journalists with PGP

https://frama.link/journalists-pgp

Zen and the art of making tech work for you : a community-built resource for women and trans activists, human rights defenders and technologists

https://frama.link/gendersec-tacticalmanual

Reporters Whitout Borders Safety Guide for Journalists include a specific chapters on digital safety

https://frama.link/rsf-guide-journalists

Exposing the invisible more about new tools of online investigation than sources protection. However extremely interesting though a little bit technical.

https://exposingtheinvisible.org/

Security in a box : specifically aimed at activists and human rights defenders

https://securityinabox.org/en/

Arabe

Cyber Arabs : Un très bon guide réalisé par l'ONG IWPR (Institute for Women's Policy Research).

https://www.cyber-arabs.com/

Security in a box

https://securityinabox.org/ar/

GUIDE DE PROTECTION NUMÉRIQUE

DÉCEMBRE 2019