Hygiène numérique

C'est quoi l'hygiène numérique ?

Parmi les mesures techniques que les militant.es peuvent prendre pour garantir leur sécurité personnelle et celle du mouvement, on qualifie les plus simples et élémentaires d’entre elles d’hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.

Lien de la formation : https://xr-secu.vercel.app/

Faire un nettoyage de printemps

> L’hygiène implique avant toute chose de nettoyer.

Ordinateurs & téléphones cumulent des données, prenant ainsi une place conséquente sur le système au fur et à mesure des jours, mais laissant aussi une plus grande fenêtre ouverte aux attaques et fraudes en ligne. C’est pour cette raison qu’il est primordial de **faire un nettoyage régulier de ces appareils en supprimant les données inutiles**, comme l’**historique de navigation**, la **corbeille**, les **cookies**, les **applications qui ne vous servent pas**, les **anciens emails sur son adresse protonmail** et les **téléchargements**.

Le fait de retirer ces éléments vous permettra d’alléger votre appareil en ôtant les éléments qui peuvent l’encombrer et le ralentir, donc de libérer de la place et d’améliorer sa vitesse de fonctionnement. C’est aussi un bon moyen de réduire les risques de cyberattaques.

Il est aussi très important de supprimer régulièrement ses messages Mattermost & Signal.

Une boucle Signal utilisée pour partager des informations sensibles / organiser une action ne devrait pas avoir une expiration de message supérieure à 24h.

Idem pour Mattermost, si vous utilisez un canal privé pour organiser des actions, il est **très fortement recommandé** de supprimer ses messages au fur et à mesure (l'expiration automatique n'existant pas sur MM) pour éviter tout problème.

Aussi, lorsque vous envoyez par exemple un mot de passe d'un cryptpad sécurisé à une personne en message privé sur MM, pensez à supprimer votre message contenant le mot de passe une fois que la personne a copié le mot de passe. Cela permettera de laisser le moins de trace possible sur les outils numériques.

Les mots de passe

Utiliser des mots de passes & uniques

Il est recommandé d'utiliser des mots de passe complexes & différent pour chaque site internet (XR ou non XR). Un mot de passe complexe c'est :

- Au moins 12 caractères (plus c'est long, mieux c'est)
- Des majuscules
- Des minuscules
- Des caractères spéciaux (@%*!?)
- Des chiffres
- Aléatoire

> Il est aussi fortement recommandé de ne pas utiliser des mots de passe en rapport avec des éléments de sa vie privée, car les FDO peuvent retrouver très facilement vos mots de passe s'il contient le nom de votre chat et votre code postal.

Utiliser un gestionnaire de mot de passe

Il est **fortement conseillé** (ça devrait être obligatoire) d'utiliser un gestionnaire de mots de passe. Ce type d'outil permet en effet non seulement de conserver tous vos mots de passe, ce qui évite d'avoir à les noter ou à les retenir, de les protéger, mais aussi de générer des mots de passe forts, difficilement déchiffrables par les pirates et les FDOs. Il propose également souvent d'autres fonctionnalités pratiques.

Il existe de nombreux gestionnaires de mots de passe, comme par exemple Keepass, ou Bitwarden, etc. Certains sont payants et d'autres gratuits.

> Personnellement, je recommande vivement **Bitwarden** qui est gratuit et très bien conçu. Il y a une extension pour Google Chrome, Firefox, Safari, iOs & Android.

Utiliser la double authentification

Dès que possible, utilisez la double authentification (2FA) sur les applications. Grâce à une application (comme Google Authenticator), vous aurez un mot de passe à usage unique à rentrer en plus de votre mot de passe classique. Si une personne découvre votre mot de passe, elle ne pourra pas se connecter sans le code à usage unique.

Certains sites utilisent seulement les SMS comme second facteur d'authentification. Outre la faiblesse du mécanisme (face à des attaquants disposant d'IMSI catchers, ou faisant du SIM swapping), cela lie aussi votre numéro de téléphone à votre identité sur le site en question.

□□ Sauvegarder régulièrement vos données

Il est extrêmement important de sauvegarder régulièrement vos données importantes, de les avoir en plusieurs exemplaires au cas où un problème surviendrait, comme par exemple une panne informatique, un virus, un appareil brisé ou volé. Tout ce que vous souhaitez et tout ce dont vous avez besoin ne doit pas dépendre d'un seul et même support. Les mettre bien à l'abri dans différents endroits vous permettra de limiter les dommages et de ne pas perdre ces précieux éléments.

□□Être discret.es

Chaque clic sur internet laisse des traces quelque part (votre routeurs et autre équipements du réseau - de votre fournisseur, mais pas que -, sur les serveurs des sites visités, etc.). Pour cela il est important d'être le plus discret possible.

Utilisation de TOR, ou d'un VPN

Lorsque vous consultez Google Maps ou encore le site internet de Total Energies, votre IP (adresse numérique) est enregistrée dans leurs serveurs. Cette IP peut permettre aux FDOs de remonter jusqu'à vous. Pour brouiller les pistes, l'idéal est d'utiliser le réseau TOR (via le navigateur TOR - https://torproject.org/), ou à défaut un VPN.

Il existe une infinité de VPN et les meilleurs sont payants. On peut citer par exemple ProtonVPN, Mullvad VPN ou NordVPN sont deux VPN très solides et avec beaucoup de possibilité.

Certains fournisseurs de VPN collectent les données de leurs utilisateurs, et peuvent les donner aux FDOs qui en font la demande.

Certains fournisseurs VPN (notamment ceux dont les services sont gratuits) sont à éviter car ils revendent les données collectées sur leurs utilisateur.ices.

Divulgation d'informations sur les messageries

Gardez en tête qu'aucun outil numérique n'est safe à 100%, même Signal, ProtonMail, ou Mattermost. Cependant on ne peut pas utiliser de pigeons voyageurs pour faire vivre le

mouvement et organiser des actions, on doit donc utiliser des outils numériques.

Essayez un maximum de n'utilisez aucun autre canaux numériques pour échanger des informations sensibles : pas de sms, pas de coup de téléphone si possible (ou via Signal), pas de WhatsApp, Messenger, Telegram ou autre.

Nous sommes sur écoute, partout, tout le temps.

Les FDOs ont les moyens techniques d'allumer les caméras, et les microphones de nos appareils à distance. C'est (encore) illégal, les données ainsi collectées sont inutilisables lors d'un procès, mais rien n'indique que ces moyens ne sont pas utilisés lors d'enquêtes.

À partir du moment où vous vous retrouvez à plusieurs pour discuter d'informations sensibles, que ce soit chez vous ou alors dans un parc, il faut éteindre tous les portables et appareils connectés, et les mettre à distance. Cela peut paraître extrême, mais mieux vaut prévenir que guérir.

□□ Protéger vos appareils

Passons maintenant à la protection de vos appareils, et là plusieurs armes sont à votre disposition pour vous défendre d’éventuelles attaques :

- **Installez un anti-virus et anti-malware**. Ces logiciels de cybersécurité indispensables permettent de détecter les programmes malveillants, d'assurer une protection contre ces derniers et de les supprimer de l’appareil concerné.
- **Installez un firewall ou « pare-feu »**, un appareil de sécurité chargé de surveiller et de contrôler les applications et les flux de données sur le réseau entrant et le réseau sortant. Il existe des firewalls logiciels ou matériels, le mieux étant bien évidemment d’installer les deux.
- **Faites la différence entre HTTPS et HTTP**. Ces deux protocoles permettent l’affichage des données web sur votre écran, cependant le HTTPS est plus sécurisé que le HTTP. Ainsi, avant de rentrer des données sensibles sur un site, comme des informations de paiement par exemple, vérifiez dans la barre d’état que la mention « HTTPS » est bien indiquée.
- **Privilégier au maximum les réseaux de Wi-Fi sécurisés** et évitez le plus possible les connexions sur Wi-Fi public car ces dernières peuvent laisser la porte ouverte à des individus malveillants qui pourront, via cette connexion publique, entrer dans votre système et accéder à vos informations. Lorsque vous êtes sur un réseau public, évitez les opérations « sensibles » comme les transactions bancaires, les achats en ligne ou l’envoi de documents importants.

□□ SPAM et phishing : attention aux messages douteux d'origine inconnue

Reçus par mail, ou par messagerie (SMS, Signal, etc.), ce type de courriers indésirables envahit nos vies comme de la mauvaise herbe, et peut aller du simple courrier envahissant à l'attaque ciblée, en passant par la véritable arnaque. Il existe trois types de spams différents : le spam publicitaire qui est le plus courant et disons le moins dangereux, ainsi que le phishing et l'escroquerie. Ces deux derniers présentent des risques bien plus élevés car il peuvent amener au vol de données confidentielles (mots de passe, coordonnées bancaires, etc.) et/ou à l'usurpation d'identité si le destinataire du message n'est pas prudent.

Il est donc impératif de toujours rester sur vos gardes et de vous méfiez des messages dont l'origine vous semble douteuse ou dont vous ne connaissez pas l'expéditeur. Ne cliquez jamais sur un lien et n'ouvrez jamais de pièce jointe à un message de ce genre. L'orthographe du contenu et de l'adresse de l'envoyeur peuvent être de bons indicateurs de l'origine frauduleuse.

□□ Éviter le partage de renseignements personnels sur les réseaux sociaux

Il est plus que conseillé de choisir soigneusement les informations personnelles que vous acceptez d'indiquer et/ou de divulguer par message comme sur vos comptes. Limitez-les le plus possible. Vous pouvez aussi utiliser les paramètres de confidentialité pour mieux contrôler les informations diffusées sur votre profil.

Il est aussi recommandé de ne pas avoir de compte militant avec votre prénom / pseudo affiché sur la même page ou des comptes qui permettent de relier votre identité militante avec votre identité personnelle. En effet, il est très facile pour les FDO de demander une réquisition à Facebook, Instagram ou Tiktok pour récupérer toutes les données associées à votre compte sur le réseau social.

> Gardez vos identités militante & personnelle séparées le plus possible sur les réseaux sociaux

□□ Gérer ses notifications

Qui dit applications, dit notifications. Ainsi, en plus de votre appareil qui peut sonner/bipper sous le coup d'un appel, d'une alarme ou d'un sms reçu, il se manifeste également en cas d'alerte comme un like, un commentaire, un message, etc.

Il est recommandé d'activer l'option pour cacher le contenu des notifications sur l'écran verouiller de votre téléphone. Dans le cas d'une GAV, les FDO pourront très bien lire toutes vos notifcations sans même avoir besoin de vous demander le code de votre téléphone.

Une autre alternative est de désactiver les notifications des applications XR (Mattermost, Signal, ProtonMail), notamment lors des actions si vous tenez à prendre votre téléphone.

Savoir si votre compte a été piraté

Comment savoir si votre compte a été piraté ? Plusieurs sites permettent en effet de vérifier si la sécurité d'un ou plusieurs de vos comptes est compromise.

L'outil Have I Been Pwned permet de vérifier si vos données personnelles (adresse email ou téléphone) ont été compromises via une fuite de donnée sur internet et risquent ainsi d'être utilisées à des fins malveillantes.

Certains sites et services permettent de lister l'historique des connections à votre compte. On peut y observer si des connections inhabituelles ont eu lieu.

> Il est possible pour un attaquant sachant rester discret de cacher la compromission de vos comptes et de vos appareils.

Mettre à jour votre matériel et vos applications

Effectuez régulièrement des mises à jour sur vos appareils, vos systèmes d'exploitation, vos logiciels et vos applications permet de corriger les éventuelles failles de sécurité déjà présentes ou pouvant apparaître. Ces mêmes failles laissent la place aux attaques en ligne, aux logiciels malveillants, et aux FDOs qui peuvent s'y engouffrer, d'où l'importance d'effectuer ces mises à jour dès qu'elles sont disponibles.

Lorsque vous le faites, ne téléchargez que les mises à jour proposées par les sites ou dispositifs officiels. Vous pouvez aussi, si vous le souhaitez, utiliser l'option de mise à jour et d'installation automatiques.

Désactivez les assistants vocaux de vos appareils

Nombreux sont celles et ceux qui utilisent désormais les assistants vocaux numériques proposés par leurs divers appareils, comme Siri, Alexa, Google et bien d'autres. Basés sur le principe d'écoute active, ces derniers sont donc supposés écouter en permanence ce que vous dites lorsqu'ils sont branchés. Bien que pour l'instant il n'y ait pas de faits rapportés quant à des incidents de sécurité causés par ces assistants ou d'espionnage volontaire, il est tout de même conseillé de les désactiver quand vous n'en n'avez pas besoin, ou par exemple lorsque vous discutez de sujets pouvant contenir des informations confidentielles.

Aller encore plus loin

Chiffrer son disque dur

Même avec un mot de passe compliqué sur votre ordinateur, si votre disque dur n'est pas chiffré, il est très facile pour les FDOs de récupérer les données de votre ordinateur. Pour cela il est recommandé de chiffrer son disque dur.

Pour les mêmes raisons, il est très fortement recommandé de chiffrer ses autres disques et clefs USB où peuvent-être sauvegardées des données sensibles.

Tutoriel Windows

Tutoriel MacOS

Utilisation d'un portable d'action / XR

Pour encore plus de sécurité, vous pouvez utiliser un autre téléphone pour les actions XR. Dans l'idéal, ce téléphone ne contiendrait aucune de vos informations personnelles, uniquement les applications nécessaires à XR. Cela permet d'avoir un téléphone d'action sans aucune trâce de votre vie privée et sans avoir besoin de supprimer mattermost & signal à chaque action.

> Vous pouvez même utiliser un deuxième numéro pour votre portable d'action pour encore plus brouiller les pistes

Réinitialiser régulièrement son téléphone

Cela peut sonner comme de la paranoia, mais il peut être utile de réinitialiser régulièrement votre téléphone. Non seulement vous allez gagner en rapidité sur votre appareil, mais les potentiels malwares ou logiciels espions seront supprimés à chaque réinstallation de votre appareil.

Installer Linux sur son ordinateur

Pour avoir un système plus difficilement attaquable par les virus & les cyberattaques, vous pouvez installer Linux sur votre machine.

Il existe une infinité de distribution, pour les débutant.es, Ubuntu est un bon point de départ :

https://www.ubuntu-fr.org/

Révision #16
Créé 13 September 2022 18:41:24 par amitabha
Mis à jour 5 March 2024 23:21:45 par Lag