Petit manuel d’autodéfense Cyber et Cypher

Pour milieu militant

Pour me présenter brièvement, j'ai évolué 6 ans dans l'univers des cryptos qui m'ont appris beaucoup de choses sur la vie privée et le self-hosting. J'ai aussi évolué pendant 10 dans l'univers des free-party où j'ai pu observer beaucoup de choses sur les manières de s'organiser pour faire des fêtes très qualitatives.

Je ne suis pas un expert en cybersécurité, mais au vu de ChatControl, de la loi RIPOST, la surveillance algorithmique, de l'avancement de l'agenda de la techno-police, des GAFAM et des boîtes d'IA, j'avais envie de prendre la plume. Car je ne crois pas que ce sont des « outils neutres ».

Peut-être l'étaient-ils avant. Mais depuis que je constate le gouffre conservateur dans lequel nous nous enfonçons, je me suis dit : « Et si j'écrivais un fanzine sur nos moyens de communications et les manières de protéger un peu mieux nos données ? ». Au pire, ça servira à informer sur quelques méthodes pour protéger nos communications et au mieux, provoquer un débat plus large pour savoir comment s'organiser pour se défendre contre la répression numérique.

Et peut-être, qui sait, qu'ensemble nous trouverons un moyen de créer des canaux éphémères d'organisation tout en préservant le savoir empirique gagné dans nos luttes lorsque ces canaux seront détruits. Car je pense qu'aujourd'hui, lorsqu'un groupe devient suffisamment grand, il devient une cible pour les forces de l'ordre ou au pire, de l'extrême droite. Or, pour faire bouger la fenêtre d'Overton, nous devons avoir un message unifié provenant d'un groupe suffisamment grand ou influent.

Le droit de communiquer

Que défendons-nous exactement ?

TOUTE PERSONNE A DROIT AU RESPECT DE SA VIE PRIVEE ET FAMILLIALE, DE SON DOMICILE ET DE SES COMMUNICATIONS

Article 7 de la chartre des droits fondamentaux de l'Union Européenne

TOUTE PERSONNE A DROIT AU RESPECT DE SA VIE PRIVEE ET FAMILLIALE, DE SON DOMICILE ET DE SA CORRESPONDANCE

Article 8 de la Chartre Européenne des Droits de l'Homme

Si on vous dit « Si vous n'avez rien à cacher, vous n'avez rien à craindre », est-ce que vous vous fichez de votre liberté de votre expression si vous n'avez rien à dire ? (Merci Edward Snowden pour la punchline)

De la même manière, si on vous dit « la confiance n'exclut pas le contrôle », hé bien si en fait. La confiance exclut *de fait* le contrôle, c'est le principe !

Seulement voilà, malgré tout ça, on est quand même surveillé massivement sous prétexte de terrorisme permanent ou pédocriminalité. Ces deux sujets sont très graves, mais est-ce au grand public de payer l'incompétence du manque de moyen de nos enquêteurs ? Car c'est bien parce que nos flics sont nuls et encouragés par la politique du chiffre qu'on se retrouve à avoir un arsenal de répression tourné contre nous et justifié par une mauvaise foi exemplaire.
C'est en réaction à cette agression de ma vie privée que j'écris

ces lignes. Si je veux envoyer des photos de nu à ma copine, ça me regarde. Si je veux raconter n'importe quoi dans mon groupe de pote, ça me regarde.

Le gouvernement veut casser le chiffrement pour lire nos conversations ? Laissez-moi rire jaune quand l'Agence Nationale des Titres Sécurisées se fait hacker par un ado de 15 ans ! Le chiffrement est une histoire de confiance, et autant dire qu'il m'en reste très peu dans la capacité du gouvernement pour protéger mes données.

DEGOOGLISONS

La place des GAFAM dans nos vies

Google connaît un peu trop de chose de nos vies. Le « Don’t be evil » est maintenant bien loin. Prendre le pari de degoogliser sa vie pour préserver la confidentialité peut être intéressant mais un peu compliqué. A quoi ça sert concrètement ? A éviter que Google transmette des infos à des personnes inopportunes on va dire.

Si vous utilisez leur service, ils pourront voir :

Votre mail
Numéro de téléphone
Historique de navigation
Historique de localisation
Contenu des mails

Si vous vous connectez avec un « se connecter avec » Google, c’est autant d’information en plus que vous donnez à Google car le site va communiquer quasiment tout dès que vous aurez utilisé ce moyen.

Vous avez évidemment le droit de penser que c’est que pour la pub. Mais sachez que les autorités peuvent, sur simple demande, accéder à toutes ces informations. Les GAFAM sont donc des complices potentielles permanentes.

Etant sur Fairphone sous LineageOS, j’ai un peu halluciné du nombre de choses qui sont dépendantes de Google :

- La localisation (beaucoup de cartes intégrées reposent sur Gmaps. Et ce sont les serveurs de Google qui nous localisent... à moins d'attendre qu'un satellite passe pour nous localiser)
- Librairies (les applis comme L'identité Numérique par la Poste ne se lancent pas)
- Les notifications

Tous ces éléments passent par leur serveurs. J'ai dû installer MicroG, qui simule une surcouche de Google pour pouvoir accéder à ces services... mais pour combien de temps ?

D'un point de vue global, c'est un peu une lutte de David contre Goliath. D'un point de vue plus local, dans ton groupe, cela permet d'apprendre à utiliser des alternatives et prendre conscience des infos que vous donnez de manière « invisible » à un GAFAM. Voici une liste d'application utile pour dégoogliser un peu votre vie :

- F-Droid ou Aurora Store pour remplacer le Play Store
- Thunderbird pour remplacer le client Gmail
- Organic Map ou Roole Map pour remplacer Gmaps
- Proton mail pour changer de fournisseur mail
- Nextcloud pour remplacer Drive (combiné avec des fichiers OpenOffice, ça fonctionne très bien)
- Obsidian pour la prise de note

Pour l'anecdote, quand j'envoyais des newsletters, je savais le temps passé de lecture, le taux d'ouverture, où les gens avaient cliqué, de quels pays ils venaient... autant d'info qui nous permettait d'identifier des profils assez précis d'utilisateurs pour le business. Je vous laisse imaginer ce qu'un outil d'analyse plus performant peut retirer comme information de

votre navigation dans un mail.

Petits conseils d’hygiène numérique

Tout comme se laver les mains peut éviter des infections non désirées, il y a quelques méthodes simples pour garder une bonne hygiène numérique. Cela rajoute des petites étapes en plus dans la vie, mais en cas de compromission, cela réduit les risques de propagation du problème.

Par défaut sur notre navigateur, supprimez les cookies + le cache + les mot de passe enregistrés lorsque vous quittez votre navigateur. En cas d’accès à votre PC, personne ne pourra poster sur les réseaux en votre nom.

Ne répondez pas aux numéros que vous ne connaissez pas : vous confirmez que votre numéro est actif. Cela évite les risques de spoofing (que quelqu’un utilise votre numéro lorsqu’il appelle).

Ne chargez pas automatiquement les images ou vidéos sur votre téléphone dans vos messageries. Pour les afficher, cela nécessite d’envoyer votre adresse IP à un serveur distant... donnant ainsi votre localisation. Les images dans les notifications ont le même défaut.

Si vous ne savez pas comment choisir un mot de passe compliqué, regardez autour de vous. Prenez un objet au hasard. Associez-lui une couleur ou ajoutez un autre objet. Séparez les deux avec un caractère spécial et ajoutez des chiffres. Plus le mot de passe est long, plus il sera compliqué à cracker.

En cas d’utilisation de gestionnaire de mot de passe, ne

sauvegardez jamais votre backup sur un cloud. Le jour où le serveur sera compromis (c'est qu'une question de temps), tous vos mots de passe le seront aussi.

Les données liés à vous sur Signal, iMessage, Whatsapp et Facebook Messenger. Pas besoin de lire pour comprendre qui pompe vos données

La préparation contre la surveillance

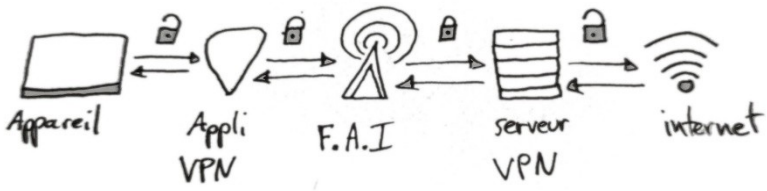
On se prépare à la guerre avant qu'elle ne soit là

Dans les pays où internet a moins de chance d'être coupé, votre navigation est surveillée. Que cela soit votre Adresse IP, votre Fournisseur d'accès à internet, votre Navigateur, votre système d'exploitation, votre pays ou la taille d'écran, tout ça un simple site le voit.

Et encore, ça, c'est les trucs de base.

Pour se préparer à ça, il faut prévoir un plan assez simple comme : un site = une identité ou une catégorie de site (hors réseau social) = une identité. Quand je dis « identité », je parle d'une adresse mail ou d'un numéro de téléphone. Avoir plusieurs adresses mails est essentiel aujourd'hui pour générer plusieurs inscriptions en ligne.

Pour protéger son adresse IP (qui donne une localisation de votre connexion), un VPN sera nécessaire.



Plusieurs entreprises en propose, je recommande celles qui ne gardent pas vos logs de connexion et qui ont un site accessible via TOR.

En résumé, TOR est un navigateur qui vous permet d'accéder à

un site en passant par plusieurs nœuds avant d'y arriver. Cela permet de contourner des sanctions d'accès à certains sites interdits sur tel ou tel territoire. Ce sont surtout les journalistes, les avocats et l'armée qui utilisent ce logiciel.

Tout ça, ce sont des solutions accessibles pour le grand public. Si vous voulez pousser plus loin votre préparation, vous pouvez vous-même configurer un serveur qui hébergera aussi bien un VPN personnel qu'une machine virtuelle (un ordinateur dans un ordinateur, pas mal non ?) vous permettant d'ajouter toujours plus de couche de sécurité. Encore une fois, cela dépend de vos besoins et de votre niveau de paranoïa.

Si vous en avez les moyens, prévoyez plusieurs appareils dédiés. 2-3 Smartphones. 2-3 ordinateurs portables. Cela permet de fractionner encore plus vos utilisations et surtout, pouvoir ruser si vous vous sentez observés.

Si vous êtes dans un pays autoritaire, l'accès à internet sera compliqué. S'il est coupé, des alternatives existent comme des badgers, des applis comme Bitchat ou un réseau Mesh. Mais cela nécessite d'être prêt à les utiliser avant qu'internet disparaisse.

Utiliser Bitchat

Développée par Jack Dorsey (fondateur de Twitter), cette application utilise le Bluetooth pour créer des groupes de discussions avec les autres propriétaires de l'application. Pas d'internet, entièrement privé. Peut aussi utiliser le réseau Mesh pour communiquer plus loin que la portée Bluetooth. Bitchat est très pratique pour savoir si quelqu'un de votre groupe

manque à l’appel dans un périmètre proche par exemple... et ne pas avoir vos communications captées par un IMSI Catcher

Le réseau Mesh

Le réseau Mesh permet d’échanger des petites quantités de donnée de manière décentralisée. Chaque nœud reçoit, envoie et relaie des données, formant un grand filet qui évite les pannes lorsqu’un nœud ne répond plus. Idéal dans les zones blanches (= zones qui n’ont plus accès au réseau mobile ou internet) mais n’est pas adapté pour les gros besoins en données.

Les badgers

Avoir des appareils dédiés à la communication en réseau fermé a ses avantages : cela permet d’être très réactif dans le groupe et évite les écoutes indiscrètes de l’extérieur. Cela dit, attention où ils sont achetés, l’histoire nous a déjà montré ce qu’Israël était capable de faire au Liban en distribuant des badgers piégés à l’explosif. L’exemple est extrême, mais ils pourraient être compromis avec un composant pour vous écouter tout simplement.

La Ruse

Le meilleur moyen d’échapper à la surveillance repose beaucoup sur la préparation et les mathématiques. Mais un

autre élément peut être très utile : la ruse.

La technique la plus simple est d'utiliser des **leurres**. Certains de ces leurres peuvent être dormants et servir de backup au besoin. D'autres peuvent être éphémères. Le but du leurre est de **divertir** votre adversaire de sa cible principale.

Si vous utilisez votre adresse Gmail quotidiennement, continuez de le faire. Identifiez tous les liens qui sont rattachés à cette adresse. Puis de manière aléatoire dans le temps, mettez en place vos préparatifs du chapitre précédent. Une fois tout ça mis en place (VPN, nouveau système d'exploitation, TOR...), initialisez votre appareil sans le connecter à internet. Il est préférable d'être « hors réseau » (pas de wifi, pas de réseau data) pour configurer votre appareil dédié. L'autre appareil, surveillé avec votre utilisation quotidienne, devient l'outil parfait pour détourner l'attention. Restez crédibles, c'est le plus important.

On vit dans une société où tout le monde utilise les réseaux des GAFAM. Si vous êtes à 100% à contre-courant, c'est comme se balader avec une gyrophare sur la tête dans le métro en heure de pointe. Utiliser Linux avec un VPN over TOR en fenêtre diminué est plus visible qu'une énième identité numérique bien construite.

Ne négligez pas vos personas. Une habitude de langage par exemple, se repère assez vite...

Organisation d'un groupe

Maintenant que tu as préparé tes appareils et tes personnalités numériques, concrètement, comment mettre en place un espace

de discussion avec tes potes l'esprit tranquille ? L'un des seuls moyens d'y arriver est d'improviser quelques jours en zone blanche (vous pouvez aussi laisser vos téléphones chez vous). Ça sera le moment de parler de vos **stratégies, échanges de codes et rituels** totalement « off the grid ».

Si tu discutes en ligne, la règle est simple : aucune sécurité n'est parfaite. Ton pire ennemi est le **sentiment de fausse sécurité**. Ton groupe de discussion devra avoir des messages éphémères par défaut, vous n'avez pas besoin d'archiver tout votre blabla. Libre à vous de garder l'historique pour les nouveaux arrivants mais je ne le recommande pas. Un bon briefing avant d'intégrer un groupe est moins risqué.

En résumé ton groupe de discussion est découpé en trois couches :

- Identité (durable et portable, Signal sur ton téléphone par ex)
- Espace (jetable par conception, un groupe de discussion)
- Savoir (Backups copiés transportables)

Son parcours de vie pourrait ressembler à quelque chose comme ça :

1) Naissance : le groupe se créé
2) Vie : Les échanges ont lieu
3) Checkpoint : De temps en temps, le groupe rédige les leçons et les signe collectivement
4) Mort : Le groupe est dissout. Seuls les backups

survivent

5) Renaissance : Un nouveau groupe est créé, amorcé par le backup vérifié

La vérification des archives est primordiale. En effet, comment vérifier qu'il n'y a pas de traître dans ce nouveau groupe ?

Vérifier les archives

Dans l'idée de transmission du savoir, avoir une archive ou un endroit pour garder les infos importantes est capital mais c'est une arme à double tranchant : Ce qui sera gardé dedans peut aussi bien être utile que compromettant pour le groupe.

Pourtant, nous l'avons vu avant, l'objectif est de **posséder et transmettre un savoir empirique** tout en évitant de le concentrer au même endroit ou au sein de la même personne. Alors, comment avoir plusieurs copies de la même information sans que cela puisse être incriminant ?

Ecrivez les **leçons** tirées de vos actions passées. Les **apprentissages** de vos expériences. Les **pièges** à éviter. Pas besoin d'écrire des noms, des lieux, des dates ou autres.

Régulièrement, dans vos discussions, prenez un moment pour rédiger les leçons de vos expériences. Signez collectivement (par exemple, chacun met un pouce dans votre groupe sur le lien vers le document) pour valider puis gardez chacun-e une copie de ce backup. Cela permettra d'avancer collectivement sans compromettre l'identité des auteurs des idées.

Que vous créez un groupe avec les mêmes personnes ensuite ou si le groupe se scinde, le savoir se transmettra. Dans l'évolution de ce document, les techniques évolueront, se mélangeront, brouillant ainsi encore plus l'identité individuelle des auteurs précédents. L'identité collective fera foi quant au sérieux des informations transmises et vous saurez quel document est fiable ou non. En cas de doute, l'information est probablement non fiable, donc vérifiez et faites des tests avant de passer aux choses sérieuses.

Le backup de vos leçons devient donc une force plutôt qu'une faiblesse si découverte. Même si quelqu'un découvre vos méthodes d'organisation, rien ne confirmera que vous serez encore en train de les utiliser.

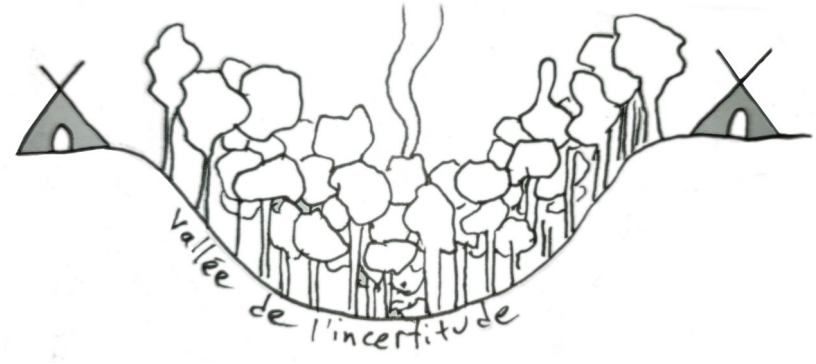
Généraux et théorie des jeux

Ça fait beaucoup de théorie, et si on laissait place à un peu de pratique avec des petits jeux ? Trouvez-vous au moins deux potes, installez-vous dans votre canap', mettez vos téléphones dans une autre pièce et éteignez les. Voici quelques situations dont vous allez débattre et qui vous permettront de préparer au

mieux vos stratégies collectives.

Les réponses sont à la fin du fanzine ;)

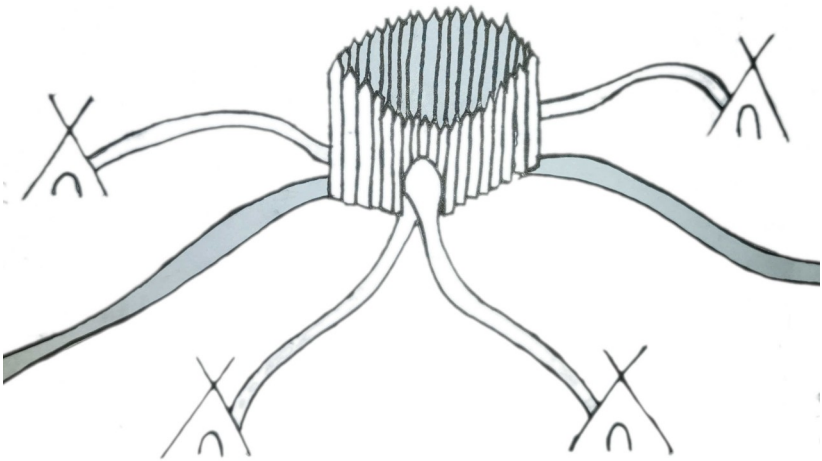
Les 2 généraux



Deux généraux doivent attaquer un ennemi caché dans une vallée. Seulement voilà : attaquer seul mène à coup sûr à la défaite. Attaquer à deux = victoire assurée.

Comment coordonner l'attaque ? Le seul moyen de communiquer est d'envoyer un messager dans la Vallée de l'Incertitude. Mais comment savoir que le camp adverse a bien reçu l'info de l'heure d'attaque ?

Les généraux byzantins



Cette fois l’affaire se corse. Encore une fois, tout le monde doit attaquer en même temps pour remporter la victoire. Vos messagers peuvent circuler librement mais il est plus facile de passer par le camp ennemi. Seulement voilà, un ou des traîtres se cachent parmi les généraux. Si le général C, qui est un traître, se fait passer pour le général B, vous courrez à la catastrophe. Comment être sûr que le message qui vous arrive ne soit pas un faux ?

Savoir quand passer à l’attaque est important. Savoir qui ment aussi. Mais tout aussi important : savoir faire des choix quand cela est nécessaire. Est-ce qu’il faut s’entraider ? Agresser ? Ne rien faire ?

Le dilemme du prisonnier

Toi et ton pote venez de vous faire arrêter pour vol mais une suspicion de délit de fuite plane. On vous sépare pendant le trajet puis on vous interroge dans deux salles séparées. Vous avez le choix entre se taire ou balancer l'autre. Voici le « deal » proposé par les flics :

- Si vous vous taisez tous les deux = 1 an de taule chacun-e

- L'un-e balance l'autre, l'autre se tait = l'un est libre, l'autre prend 10 ans

- Vous vous balancez mutuellement = 5 ans chacun-e

Que feras-tu ? Et si on réitère l'expérience ?

Le paradoxe de Schelling

Imaginez que vous devez retrouver un inconnu demain à Paris, sans communication. Devinez où vous aller vous retrouver ? A quelle heure ?

Les faucons et les colombes

Deux stratégies : être une colombe ou être un faucon. Le faucon se bat si besoin quand il y a une concurrence pour une récompense. La colombe entame une démonstration agressive mais ne répond pas à un conflit non cérémonial.

- Si la colombe entre en conflit avec le faucon, la colombe fuit

- Si les deux sont des colombes, chacun a autant de chance d'avoir la récompense

- Si les deux sont des faucons, il y a un conflit physique. Chaque faucon a 50% de chance d'avoir la récompense mais le perdant sera blessé

Est-ce qu'il faut fuir le combat ? Prendre le risque d'être blessé ?

Ces situations peuvent être transposées dans beaucoup de moment de la vie militante. Quel est le ratio bénéfice/risque de telle ou telle stratégie ? Comment se coordonner efficacement ? A quel moment être rationnel ? Être irrationnel ? Quand coopérer ou au contraire, trahir ? A quel stade les menaces deviennent crédibles pour dissuader l'adversaire ?

Je vais vous donner les leçons des exercices aux pages suivantes. Mais gardez en tête les discussions que vous venez d'avoir avec les situations précédentes. Elles sont précieuses car elles forgent l'identité de votre groupe. Autant d'éléments non-reproductibles par une personne extérieure. Autant d'éléments de signatures secrètes que seuls vous pourrez connaître.

Les leçons des jeux

Vous l’aurez sans doute compris en discutant ensemble, il n’y a pas de solution toute faite aux jeux proposés. Mais voici les leçons « officielles ». Si vous en trouvez qui vous conviennent, tant mieux, il y a beaucoup de variantes !

Les 2 généraux

Aucun protocole n’existe pour avoir une **connaissance commune** sur un canal non fiable. Le dernier message envoyé est toujours celui dont l’expéditeur ignore le sort. On abandonne la certitude et on adopte un « il va **probablement agir** comme demandé dans mon dernier message ». Si le plan a été établi par avance, pas besoin de confirmation

Les généraux Byzantins

Ici, c’est mathématique : les traitres doivent rester sous le tiers du groupe. Avec 3 généraux dont 1 traitre, le traître peut scinder le camp des loyaux en 2 camps de taille égale et voter dans les deux sens à la fois. Pour éviter les faux: une **signature infalsifiable** (Signal le fait très bien). En cas de doute : plusieurs messagers avec le même message.

Le dilemme du prisonnier

Cet exercice sert à mieux vous connaître et vous préparer psychologiquement si votre groupe venait à être interrogé séparément.

Ici, la bonne réponse est... ça dépend. Avec quelqu’un que vous ne connaissez pas, rationnellement, les deux se balancent. Mais les expériences ont prouvé qu’avec la répétition du jeu avec les mêmes personnes, cela devient : on coopère (silence), puis les

coups suivants dépendent de qu'a fait l'autre précédemment. La traitrise entraîne la traitrise... et la solution long-terme est le pardon. Une variante du dilemme du prisonnier est le jeu des colocataire. Qui va faire la vaisselle aujourd'hui ? Derrière cette question : comment les normes sociales peuvent aider à vaincre les motivations individuelles de conflit excessif ?

Le paradoxe de Schelling

Cet exercice sert à vous préparer en cas de perte totale de communication avec votre groupe.

La réponse est : à la Tour Eiffel à midi. C'est ce qu'on appelle le **point focal**. Un endroit que chacun devine que l'autre devinera. Un lieu de repli évident, une heure canonique (13h12 ?), une convention partagée.

Les faucons et les colombes

Cet exercice sert à savoir quand vous devez adopter une posture agressive dans vos actions ou à l'inverse, quand il faut se retirer.

S'il n'y a que des faucons dans le groupe, à terme, il n'y aura que des blessés. S'il n'y a que des colombes, aucun combat ne sera mené. Le « bon » ratio est : 5 faucons pour 1 colombe.

Que vous choisissez vos stratégies de manière rationnelle ou aléatoire, la proportion évolutivement stable du faucon (5/6) est égale aussi à la probabilité d'équilibre dans l'équilibre de Nash en stratégies mixtes du jeu. En gros, la nature s'équilibre elle-même sur cette proportion

L’auto-défense numérique par la pratique

Ce petit manuel est fini. J’espère qu’il vous permettra d’adopter des stratégies de défense vis-à-vis d’intrusions de plus en plus permanente dans nos vie numériques. Bien entendu, c’est une première version. Le but est d’alimenter les débats, qu’il soit reprit et adapté à votre sauce. Je ne suis pas un expert en cybersécurité donc navré pour tous les experts et pro que j’ai fait bondir avec des approximations et des raccourcis. N’hésitez pas à y apporter vos ajouts pour qu’on devienne collectivement plus intelligent :) Mais n’oubliez pas que nous sommes nombreuses et nombreux à ne pas avoir fait math sup’ ni savoir coder (et NON c’est pas « facile de coder »).

Les messages que j’espère avoir transmis sont les suivants :

- La force d’une chaîne est égale à son maillon le plus faible
- Aucune OPSEC n’est parfaite. Acceptez une marge d’erreur
- Restez mobile et flexible
- Soyez préparés avant la guerre. Pendant, c’est trop tard
- Faites confiance, mais vérifiez comme disait l’autre
- Le papier a de beaux jours devant lui
- Ne paniquez pas, soyez résilients

Bon courage dans vos luttes !

Merci à Mizae pour la relecture

Lexique et références

Equilibre de Nash : Situation dans laquelle aucun des joueurs ne peut trouver de meilleure stratégie de jeu, compte tenu des stratégies choisies par les autres joueur

Optimum de Pareto : Situation dans laquelle on ne peut améliorer la satisfaction d'un individu sans réduire la satisfaction d'une autre personne

Cypher : Chiffrement. Il est d'origine Arabe (صفر - Sifer) qui signifie en français Zéro.

Donnée secrète : qui ne doit être partagée avec personne

OPSEC : Sécurité Opérationnelle. Processus de sécurité et de gestion des risques.

VPN : Réseau privé virtuel.

GAFAM : Google Amazon Facebook Apple Microsoft

Fenêtre d'Overton : Métaphore qui désigne l'ensemble des idées, opinions ou pratiques considérées comme plus ou moins acceptables par l'opinion publique d'une société donnée.

« La théorie des jeux en image » par Tuvana Pastine et Ivan Pastine, à commander dans votre librairie indépendante préférée.

Mon site : https://konohime.xyz