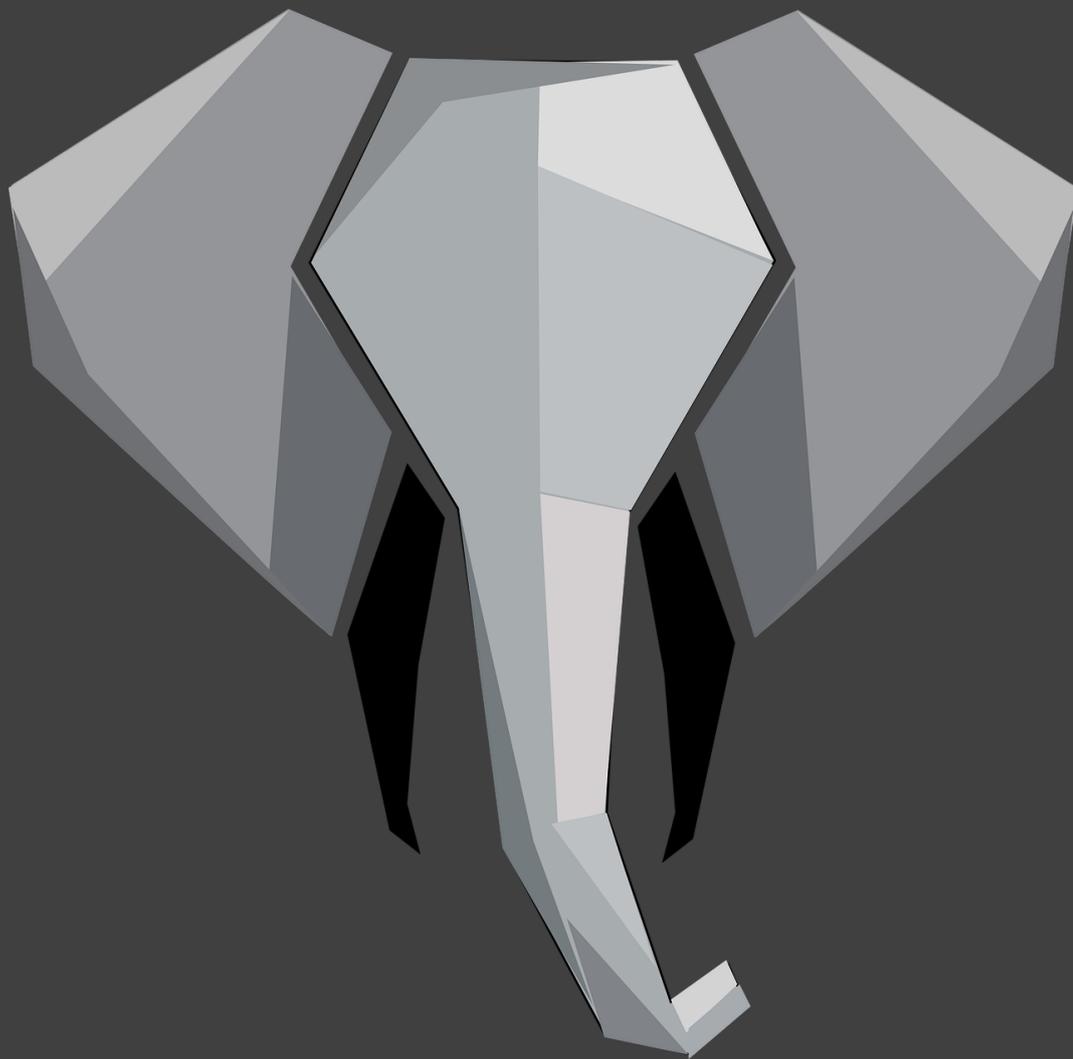


Défense Numérique
<https://defense-numerique.com>



Les 13 questions auxquelles
vous devez répondre pour
votre sécurité numérique

TABLE DES MATIÈRES

I. Merci.....	2
II. Les 13 questions auxquelles vous devez répondre pour votre sécurité numérique.....	3
1. Qui détermine les règles du jeu dans votre foyer au sujet de ce qui est permis ou pas avec vos différents équipements (smartphones, tablettes, ordinateurs, smart tv, ...) ?.....	3
2. Laissez-vous tout le monde accéder à votre ordinateur, votre tablette ou votre smartphone ?.....	4
3. Quelles sont vos premières actions lorsqu'un nouveau matériel connecté arrive chez vous ?.....	4
4. Est-ce que tous vos proches peuvent accéder à tous vos équipements, votre réseau wifi de manière permanente ?.....	5
5. Vous êtes-vous déjà demandé à combien de personnes vous aviez communiqué le code wifi de votre maison ?.....	5
6. Disposez-vous de quelques outils de protection contre les logiciels malveillants ?.....	6
7. Avez-vous bien déterminé ce qui devait être sauvegardé et que cela fonctionnait correctement ?.....	7
8. Êtes-vous certain que vos données de carte de crédit ou vos identifiants transitent de manière sécurisée ? Même depuis votre smartphone ?.....	8
9. Est-ce que vos équipements technologiques sont physiquement protégés ?.....	9
10. Avez-vous déjà vérifié l'historique de vos connexions, navigation sur vos équipements, comptes en lignes ?.....	9
11. De quand date la dernière mise à jour de chacun de vos logiciels ? Et du changement de votre mot de passe ?.....	10
12. Comment réagiriez-vous si un virus était détecté sur votre ordinateur ? Votre smartphone ? Votre tablette ?.....	11
13. Avez-vous déjà pensé à comment vous continueriez vos tâches quotidiennes pendant les premiers jours d'une indisponibilité totale de vos équipements numériques ?.....	11
III. Mots de la fin : Ce n'est que le début !	12
IV. Copyright.....	13

I. MERCI

En tant **qu'informaticien de formation et de métier**, ma famille, mes amis, les amis de mes amis, mes collègues (mais pour des besoins « perso ») me demandent souvent de les dépanner, ont besoin d'un conseil, d'un avis sur tel matériel (au sens très large du terme). Tous les informaticiens le savent, dès qu'ils sont connus pour avoir des compétences informatiques, une **avalanche de sollicitations** s'en suit.

Depuis quelques mois, les demandes ont commencé à prendre une tournure différente :

- « Que penses-tu de cet email étrange que j'ai reçu ? »
- « Pourquoi est-ce que je reçois tous ces messages ? »
- « Je crois que je me suis fait pirater ma carte de crédit, que dois-je faire ? »
- « Mon ordinateur me semble très lent, est-ce que tu peux faire quelque chose ? »
- « Est-ce que tu crois que mon ami s'est réellement fait enlever au Tadjikistan et que dois lui envoyer de l'argent par Western Union ? », etc.

Les uns et les autres, lorsqu'ils sont touchés **pour la première fois** par un acte malveillant (et même un simple email, aussi grossièrement construit soit-il) ne se sentent pas très bien. Ils se sentent personnellement visés, « Pourquoi moi ? », « Comment a-t-il obtenu mon adresse email ? », « Est-ce que je me suis fait piraté ? », « Que dois-je faire docteur ? ». Alors de longues explications commencent pour reprendre les choses depuis le début.

C'est pourquoi j'ai décidé de lancer ce blog. Pour aider le plus de personnes possibles à trouver des réponses. **N'hésitez donc pas à m'écrire en me posant vos questions** (charles@defense-numerique.com), je tenterai de vous répondre à travers un article de blog ou vous renverrai vers des articles abordant le sujet.

Dans un premier temps, je vous propose de prendre de la hauteur sur les questions à vous poser.

Un enseignement qui n'enseigne pas à se poser des questions est mauvais.
Paul Valéry – Artiste, écrivain, philosophe, poète (1871 - 1945)

Ensuite, je vous propose de suivre les différents articles de mon blog pour comprendre et trouver votre chemin dans les méandres des technologies.

Le véritable enseignement n'est point de te parler mais de te conduire.
Antoine De Saint-Exupéry – Artiste, aviateur, écrivain (1900 - 1944)

Voici donc **les 13 questions auxquelles vous devrez répondre**.

II. LES 13 QUESTIONS AUXQUELLES VOUS DEVEZ RÉPONDRE POUR VOTRE SÉCURITÉ NUMÉRIQUE

1. Qui détermine les règles du jeu dans votre foyer au sujet de ce qui est permis ou pas avec vos différents équipements (smartphones, tablettes, ordinateurs, smart tv, ...) ?

Dans un foyer, il est tout aussi important de discuter des règles d'accès aux comptes en banque que des règles d'accès aux différents matériels. Surtout maintenant que chacun d'entre nous accède à ses comptes par Internet... Car celui qui a le pouvoir de poser des règles a aussi le pouvoir **d'intercepter tous les codes d'accès !**



Sans voir le mal partout autour de soi, c'est comme laisser conduire quelqu'un en qui on a toute confiance, mais **qui n'a pas le permis !** Le lui indiquer est uniquement un geste d'attention pour soi-même et pour lui. Parlez-en chez vous et mettez-vous d'accord sur la **responsabilité confiée** (ou prise) entre vous.

2. Laissez-vous tout le monde accéder à votre ordinateur, votre tablette ou votre smartphone ?



Lorsqu'on peut accéder à un appareil, on peut faire bien des choses, volontairement ou involontairement. **Un simple SMS intercepté**, et hop, le mot de passe d'un de vos comptes en ligne est changé. Une **redirection de vos mails vers une autre boîte mail** se configure en quelques clics à qui maîtrise l'opération.

Et surtout, le cas le plus fréquent, on peut installer n'importe quelle application (+ ou – sécurisée) sur votre appareil. Et une fois l'usage terminé, **totalemment oublier de le désinstaller**.

Il est aujourd'hui possible de créer des sessions invitées sur un ordinateur, sur certains smartphones, etc.

Ce qui vaut pour les invités, **vaut également pour les enfants** ! Sans leur prêter de mauvaises intentions, leur permettre d'installer toutes les applications qu'ils veulent, voire de **réaliser des achats payants** reste un sujet à traiter. (Certains en ont eu pour leur argent...)

3. Quelles sont vos premières actions lorsqu'un nouveau matériel connecté arrive chez vous ?

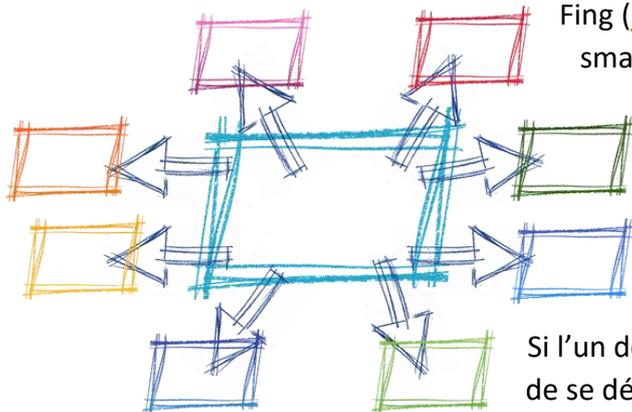
Même **une nouvelle télé** mérite qu'on s'intéresse à sa configuration avant de la connecter au wifi de la maison. C'est tout de même un équipement actif, connecté à Internet et qui peut devenir **un espion de votre foyer à votre insu** !



Avant de laisser entrer un loup dans la bergerie, partez du principe que votre nouvel équipement est maladroit et prend tout ce qu'il voit pour le communiquer à **des sociétés de publicité**. Je vous invite à aller regarder dans tous les paramètres avancés les éléments de collecte d'information qui doivent être désormais indiqués !

4. Est-ce que tous vos proches peuvent accéder à tous vos équipements, votre réseau wifi de manière permanente ?

Savez-vous qu'une fois connecté à votre wifi, n'importe quel équipement **peut « voir » tous les autres équipements** qui se trouvent sur le même réseau. Essayez-le avec l'application



Fing ([pour iPhone](#), [pour Android](#)) depuis votre smartphone. Vous aurez toutes les adresses, voire le nom et le modèle des équipements qui sont connectés sur le même réseau. C'est comme si vous entriez dans un bureau, dès que le contrôle de sécurité est passé (l'accès à votre wifi), **vous êtes libres de vos mouvements.**

Si l'un des équipements réseau possède un virus qui essaie de se déployer, soyez assuré que **vos matériels seront sollicités...**

Pour ce qui est de vos proches, pouvez-vous garantir qu'ils n'ont jamais installé un logiciel qui soit un virus ? (à l'insu de leur plein gré 😊)

5. Vous êtes-vous déjà demandé à combien de personnes vous aviez communiqué le code wifi de votre maison ?

Toutes les personnes à qui vous avez communiqué votre code d'accès Wifi ont tout naturellement suivi le mode de connexion par défaut, à savoir, avec l'**option « Reconnexion automatique » activée.**

Saviez-vous que cela signifie que dans la plupart des cas, le téléphone va demander toutes les 10/20/30 secondes « Bonjour, est-ce que le réseau « NOM DE MON WIFI » est là ? ». Il existe alors [des équipements](#) informatiques qui savent simuler le nom de n'importe quel wifi. Ainsi, il pourrait voir cette demande et dire « Oui, je suis là ». À ce moment, le téléphone envoie **les informations de connexion de votre wifi** à ce matériel inconnu. C'est ainsi que votre code wifi pourrait tomber entre de mauvaises mains. Ensuite, il suffit de faire comme précédemment, **rôder près de chez vous**, capter votre wifi et le tour est joué.



Mais là n'est pas le pire ! Je vous rappelle que votre téléphone vient de **se connecter à un équipement sans votre autorisation** et à travers lequel tout votre trafic Internet est en train de passer. C'est à ce moment que vous **dépendez de la qualité de la sécurisation mise en place, ou pas, par les différents fournisseurs** de site Internet, app ou appareil connecté.

6. Disposez-vous de quelques outils de protection contre les logiciels malveillants ?

Tout comme vous mettez **votre ceinture de sécurité** lorsque vous entrez dans votre voiture, il est nécessaire de prendre quelques précautions lorsqu'on a un ordinateur.

Le minimum est de disposer d'un **logiciel antivirus à jour**. Et contrairement aux idées reçues, **les Mac ne sont pas plus protégés que les autres systèmes d'exploitation**. Pour continuer sur cette parenthèse des systèmes d'exploitation (Windows, Mac, Linux, ...), mettez-vous du côté des fabricants de logiciels malveillants une minute. Vous avez 1h devant vous et avez le choix entre concevoir du code qui vise 10% des ordinateurs du monde ou du code qui vise les 90% restants ? C'est donc bien la réelle part de marché des ordinateurs personnels qui a favorisé **le développement de virus** pour le monde Windows au lieu des Mac. Parenthèse fermée.



Pour se protéger **des logiciels malveillants**, encore faut-il savoir ce que c'est... Je développerai ce sujet dans un prochain article sur <https://defense-numerique.com>, mais en résumé, un logiciel malveillant est tout ce qui peut exécuter des instructions sur un équipement technologique sans que vous en ayez connaissance, ni en exprimiez la demande.

Les finalités de ces logiciels sont multiples :

- **Vol de vos données personnelles**
 - Vol de vos logins / mots de passe
 - Analyse de vos comportements / habitudes
 - Vol de vos données de cartes de crédit
 - Vol de vos photos / documents
 - ...
- **Modification ou altération des données**
 - Chiffrement de tous vos documents / photos et demande de rançon en échange des clés de déchiffrement
 - Suppression pure et simple de tous vos documents / photos

Les 13 questions auxquelles vous devez répondre pour votre sécurité numérique

- Plus simplement, vous mettre des fenêtres de pubs intempestives partout sur l'ordinateur
- ...
- **Utilisation de vos ressources matérielles à votre insu**
 - Détournement de vos équipements pour en attaquer d'autres
 - Utilisation de votre puissance de calcul pour miner du bitcoin
 - ...
- **Utilisation de vos ressources matérielles contre vous**
 - Prise de contrôle de vos équipements et modification de leur fonctionnement initial
 - La version qui vous fera sourire, sauf si vous êtes le propriétaire
 - La version qui ne vous fera pas sourire, même si vous n'êtes pas le propriétaire
 - Prise de contrôle des caméras de surveillance
 - Il n'aura jamais été plus simple de savoir si vous êtes ou non à la maison...

Se protéger contre les logiciels malveillants semble plus naturel après ces quelques exemples.

7. Avez-vous bien déterminé ce qui devait être sauvegardé et que cela fonctionnait correctement ?

Quand le mot sauvegarde arrive, on pense au moins à son ordinateur, **ses fichiers et ses photos** (qui sont sur l'ordinateur). Avez-vous pensé à toutes les informations dont vous auriez besoin en cas de gros problèmes ?

Commençons par la base :

- **Vos identifiants** (j'espère que vous ne les sauvegardez pas dans le navigateur lorsque celui-ci vous le propose... Je vous en reparlerai dans un article).
- Toutes les données utiles de votre téléphone (**contacts, photos, vidéos, documents**) sauvegardées au fil des jours et des semaines.
- Idem pour **votre tablette** (photos, vidéos, documents)
- Avez-vous **une copie des licences** des différents logiciels que vous avez achetés ? Avez-vous encore une copie des **logiciels d'installation** correspondants ? Eh oui, vous



Les 13 questions auxquelles vous devez répondre pour votre sécurité numérique

n'avez peut-être pas payé chaque mise à jour, et votre licence n'est valable que pour la version d'il y a 2 ou 3 ans.

- En cherchant bien, on peut encore trouver toute une liste d'informations qu'il serait nécessaire de sauvegarder, plus ou moins importante en fonction des uns et des autres (votre **niveau de progression dans un jeu**, ...)

Une fois la liste établie de ce qu'il faudrait sauvegarder, il faudra se poser la question de **ce qu'on est prêt à perdre** et de ce qu'on a réellement envie/**besoin de restaurer**. Les photos de vos premiers pas ou de ceux de votre enfant, les photos de mariage, de vos vacances à l'autre bout du monde, de vos proches qui vous sont ou étaient chers. Ceci déterminera les moyens qu'il faudra mettre en place pour s'assurer que tout fonctionne comme prévu.

Et là, on pourra aborder **la partie restauration**. Savez-vous reconstituer votre écosystème numérique (au niveau que vous avez précédemment déterminé) ?

- Savez-vous reconstituer **tous vos accès** à tous les sites ? Et si vous aviez une amnésie ou une incapacité de parler, **est-ce que votre moitié saurait rétablir la situation** ?
- Et si on vous **volait votre téléphone** ? Est-il au moins protégé par un code PIN ?

8. Êtes-vous certain que vos données de carte de crédit ou vos identifiants transitent de manière sécurisée ? Même depuis votre smartphone ?



Normalement, on a déjà dû vous répéter à plusieurs reprises de bien veiller à voir le **logo du cadenas** à côté de l'adresse du site avant de faire un paiement sur Internet (comme celui-ci).



Malheureusement pour vous, cela peut ne pas suffire. Les sites de vente en ligne utilisent de plus en plus de systèmes d'analyse du comportement (Google Analytics par exemple, mais tant d'autres également) afin de « mieux connaître » sa clientèle. Et parfois (souvent ?), les pages de paiement continuent **d'envoyer une liste d'informations à d'autres fins** que celles du paiement. Alors, heureusement, jusqu'à preuve du contraire, ils ne sont pas nécessairement malveillants. C'est simplement que ce sont des acteurs qui **ne devraient pas avoir accès à ces informations**.

Et si on regarde de plus près vos différentes applications sur votre smartphone, êtes-vous certain d'utiliser des applications ou des mécanismes de paiement qui font transiter vos données bancaires de manière sécurisée ?

9. Est-ce que vos équipements technologiques sont physiquement protégés ?

Ici, il n'est pas question de mettre vos équipements sous-clé, mais bien de les protéger contre toute sorte d'avaries, comme les inondations ou la foudre par exemple. Et si votre disque dur, qui contient une partie de vos sauvegardes, était moins visible, cela pourrait également le protéger contre le vol (afin de pouvoir faire sa restauration !).

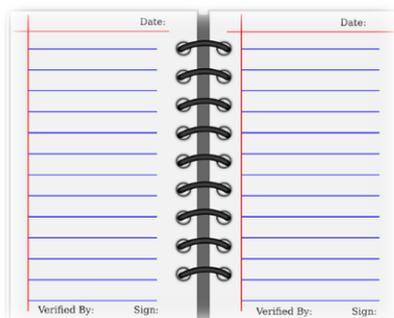


Si vous possédez des équipements qui n'ont pas besoin d'être au milieu du salon (un NAS par exemple ; c'est une version bien plus élaborée que votre disque dur externe), le placer dans un endroit moins visible le mettrait également à l'abri des chocs involontaires.

10. Avez-vous déjà vérifié l'historique de vos connexions, navigation sur vos équipements, comptes en lignes ?

De plus en plus, les fournisseurs de services en ligne vous permettent d'accéder à un historique de connexion ainsi que de l'historique des lieux de connexion. Pour les lieux de connexion, cela se base sur ce qu'on appelle votre adresse IP. Ce n'est pas très lisible par un humain, mais pour les ordinateurs, c'est très clair.

Les banques, les comptes de messageries (pour les principaux en tout cas) offrent la



possibilité de consulter ces informations de connexion. Malheureusement, c'est lorsqu'il est trop tard qu'on découvre l'importance d'aller vérifier régulièrement.

J'ai malheureusement déjà eu des cas de séparation dans mes relations où l'un des deux conjoints avait conservé les accès sur le compte mail de l'autre. Je vous laisse imaginer la suite.

11. De quand date la dernière mise à jour de chacun de vos logiciels ? Et du changement de votre mot de passe ?

Vous savez, c'est ce message qui vous demande à chaque démarrage, « est-ce que je peux faire la mise à jour ? » et vous dites toujours « Annuler », « Plus tard », etc. Encore pire, votre logiciel ne le demande même pas !

Deux raisons principales d'effectuer ces mises à jour :

- La première est qu'il existe peut-être une faille qui a été identifiée sur l'application et qu'elle est exploitée dans la nature. Souhaitez-vous être la prochaine victime ?
- La deuxième est une question de compatibilité. A un moment, des dysfonctionnements pourraient apparaître (lenteurs, incompatibilités, etc.). C'est aussi pour corriger cela que les logiciels se mettent à jour.

Vous savez pertinemment que votre voiture doit être vidangée, les roues de votre vélo regonflées ou vos skis fartés. C'est pareil pour les logiciels, mais à une fréquence un peu plus élevée. En moyenne, vous devez vous attendre à une mise à jour par mois (la principale raison est la découverte de failles...).



Par ailleurs, à moins de suivre l'actualité de tous les piratages qui ont lieu, sachez que tout aussi régulièrement, des sites se font pirater et les logins ainsi que les mots de passe se retrouvent dans la nature (vous devriez d'ailleurs aller vérifier si vos emails ne sont pas dans la nature sur [ce site](#). Celui-ci recense et collecte tout ce qu'il a trouvé dans la nature). Et malheureusement pour nous tous, ils sont très nombreux.

Au moment d'écrire ces lignes, voici les chiffres du nombre officiel de sites piratés (pwned websites), le nombre de comptes trouvés (pwned accounts), pas besoin de rentrer dans les détails des deux dernières valeurs. Pensez-vous que votre compte se trouve dans la liste ?

356	7,838,989,537	92,466	113,114,697
pwned websites	pwned accounts	pastes	paste accounts

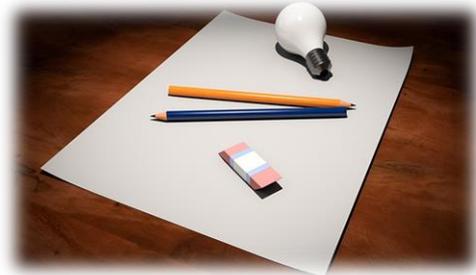
12. Comment réagiriez-vous si un virus était détecté sur votre ordinateur ? Votre smartphone ? Votre tablette ?

Se poser les questions en cas de pépin avant que ceux-ci arrivent. C'est certainement l'exercice le moins glamour. Et pourtant, nous le faisons très régulièrement pour d'autres domaines. Vous assurez bien votre véhicule et votre maison. Vous vérifiez si vous aurez droit à un véhicule de remplacement et au bout de combien de temps. Ou encore, vous regardez si vos meubles seront remboursés à neuf ou à une valeur prenant en compte l'usure en cas de problème. D'ailleurs, il vous faudra une copie des factures... que vous aviez sur l'ordinateur qui a brûlé avec l'incendie...



13. Avez-vous déjà pensé à comment vous continueriez vos tâches quotidiennes pendant les premiers jours d'une indisponibilité totale de vos équipements numériques ?

Si vous avez une activité professionnelle depuis votre domicile, cette question peut devenir essentielle pour le maintien de votre activité. Comment récupérer vos dossiers en cours alors que vous venez de vous faire cambrioler et que votre ordinateur faisait partie du butin ?



On vous vole votre téléphone, savez-vous comment bloquer votre appareil et rediriger vos appels vers un autre numéro ?

C'est l'une des questions les plus difficiles auxquelles il faut répondre, mais je tenterai article après article de vous apporter des idées de réponse. Vous avez aussi le droit de continuer à vivre dangereusement ! Mais au moins, vous le saurez et l'assumerez !

III. MOTS DE LA FIN : CE N'EST QUE LE DÉBUT !

Tout d'abord merci d'avoir téléchargé ce bonus et d'avoir tout lu !

A ce stade, vous avez un choix à faire. Continuer à vivre en oubliant toutes ces questions et adienne ce qu'il adviendra, ou bien vous avez envie de prendre ces questions à bras le corps et d'apporter des réponses à chacune d'entre elles.



C'est dans cet objectif que j'ai créé ce blog et que je l'alimenterai avec des contenus qui vous aideront à comprendre les enjeux, à vous protéger et à prendre des décisions.

IV. COPYRIGHT

Ce guide a été transmis gratuitement suite à votre inscription à la newsletter du blog <https://defense-numerique.com>. Le simple fait de lire le présent e-book vous donne le droit de le partager à qui vous le souhaitez.

Si vous avez reçu ce guide autrement qu'en vous inscrivant à la newsletter de « Défense Numérique », je vous propose de vous y inscrire, c'est totalement gratuit ! Vous recevrez régulièrement des astuces, des réflexions et des propositions pour vous aider à vous protéger des nuisances du monde numérique.

Je vous autorise à l'utiliser commercialement selon les mêmes conditions que sur mon blog, c'est à dire à l'offrir sur votre blog, sur votre site web, à l'intégrer dans des packages et à l'offrir en bonus avec des produits, mais PAS à le vendre directement, ni à l'intégrer à des offres punies par la loi dans votre pays.

Vous êtes donc libre de le distribuer à qui vous le souhaitez, à condition de ne pas le modifier, de toujours citer Charles du site « Défense Numérique » comme l'auteur de ce guide, de prévenir l'auteur grâce à la page « contact » du blog, et d'inclure un lien vers <https://defense-numerique.com>.

Le e-book « Les 13 questions auxquelles vous devez répondre pour votre sécurité numérique » par Charles du blog <https://defense-numerique.com> est mis à disposition selon les termes de la licence « Attribution - Pas d'Utilisation Commerciale - Pas de Modification »

Les autorisations au-delà du champ de cette licence peuvent être obtenues auprès de charles@defense-numerique.com.

<https://defense-numerique.com>