100
QUESTIONS/RÉPONSES

POUR VOUS METTRE EN CYBERSÉCURITÉ

Préface de Guillaume Poupard

Pierre Dal Zotto
Olivier Laurelli
William WebWolker

ellipses

INTRODUCTION

Dans un monde de plus en plus numérisé, les enjeux liés à la sécurité numérique nous concernent toutes et tous, que l'on soit un utilisateur occasionnel ou une personne hyperconnectée. Comprendre les bases de la cybersécurité est essentiel pour protéger nos données personnelles, nos transactions en ligne et notre identité numérique. Cette section aborde quelques questions fondamentales pour poser les bases de la compréhension des risques. Elle a pour but de vous aider à prendre conscience de l'importance de la sécurité dans le monde numérique d'aujourd'hui et vous montrera que, peu importe notre niveau de connexion, la cybersécurité nous touche au quotidien.

1 Suis-je concerné(e) par la cybersécurité ?

Permettez-nous de commencer par une histoire. Banale. Un matin comme un autre…

« 6 h 45. Le réveil sonne. Encore dans le lit, je consulte mes comptes Instagram et Twitter (on dit vraiment X ?). Je like quelques publications, je transfère trois posts.

Aux toilettes – moment d'intimité moderne – je jette un œil à mes mails pros et persos. Je repère un message d'une collègue en déplacement à l'étranger, avec un lien à consulter. Je clique. Le site me demande mes identifiants Office 365 – ceux de mon entreprise. J'essaie, mais ça ne marche pas. Le mot de passe enregistré sur mon téléphone doit être obsolète. Pas grave, je verrai ça au bureau.

Une fois prêt, je lance ma playlist. Une pub surgit : la veille, j'ai cherché des billets de concert à 80 €. Ce matin, une « vente flash » à 65 €. Je fonce. Le site ne me dit rien, mais je n'y prête pas attention : bonne affaire.

Petit dej' en main, je scrolle WhatsApp, Insta… Quelques « j'aime » plus tard, je suis en retard. Je file. Le bus est bondé. Mon téléphone redémarre – mise à jour. Je rentre le code PIN, puis mon mot de passe à l'aveugle, secoué par les virages. Une ou deux vidéos YouTube plus tard, j'arrive au bureau.

Mon responsable m'attend accompagné d'une autre que je ne connais pas. Visage fermé. Mon compte a été piraté. L'entreprise est victime d'une cyberattaque. Accès bloqué. Je suis dans le noir numérique.

Je tente d'ouvrir mon appli bancaire : trois débits suspects. 300 €, 200 €, 100 €. La panique monte. Je vérifie Instagram : bloqué. Twitter : bloqué. Gmail : inaccessible. Plus rien ne fonctionne. Ni mails, ni calendrier, ni photos, ni réservations. Ma vie numérique s'est arrêtée. »

Tout est inspiré de faits réels. Et cela illustre un point essentiel : en quelques clics, vous pouvez exposer non seulement votre vie – au revoir le cadeau pour votre ami(e), mais aussi celle de votre entourage ou de votre entreprise. Vous devenez, sans le vouloir, le point d'entrée d'une attaque…

Pour illustrer que vous n'êtes pas seul, voici quelques éléments publiés par le COMCYBER (Commandement de la cybersécurité du ministère de l'Intérieur)[1], le 30 juillet 2024, dans son premier rapport sur la cybercriminalité. Ces statistiques sont frappantes :

- 9 Français sur 10 ont déjà fait face à une malveillance informatique.
- 70 % ont été victimes de tentatives d'hameçonnage.
- Le quishing, basé sur de faux QR codes, explose.
- En 2023, 278 703 infractions numériques ont été enregistrées (+9 % vs 2022).
- 47 % des victimes ont moins de 44 ans.

Si les cyberattaques à grande échelle sont de plus en plus fréquentes, elles ne sont que la partie immergée de l'iceberg. On se souvient de l'attaque par ransomware WannaCry en 2017, qui a paralysé plus de 30 000 entreprises et de nombreux hôpitaux dans 150 pays. Plus insidieux encore, le scandale Cambridge Analytica, où les données personnelles de millions d'utilisateurs Facebook ont été exploitées à des fins politiques. Les cybercriminels vont plus vite, frappent plus fort et vont plus loin grâce à des outils accessibles et sans réelles compétences techniques. Personne n'est à l'abri. Pas besoin d'être un hacker pour nuire. Pas besoin d'être un expert pour se protéger.

Avant de continuer de chercher des réponses aux questions dans ce livre, nous vous suggérons d'effectuer une vérification rapide : consultez un site comme *Have I Been Pwned* (https://haveibeenpwned.com/) pour savoir si vos adresses courriels ou mots de passes ont déjà été compromis dans des fuites de données.

Ainsi, vous l'avez compris, se mettre en cybersécurité est crucial et cela nous concerne tous. Vous protégerez vos données, votre vie privée, votre réputation, et bien plus encore. Le périmètre à sécuriser grandit chaque jour, à mesure que nos vies s'entrelacent avec des appareils connectés et des services numériques.

Heureusement, des ressources existent pour vous aider à comprendre et renforcer votre protection. L'ANSSI - Agence Nationale à la Sécurité des Systèmes d'information, Cybermalveillance.fr vous offre des techniques

1. https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024

de défense et la DGSI – Direction Générale de la Sécurité Intérieur communique sur les risques actuels et émergeants, et ce livre, nous espérons, répondra à certaines de vos questions.

Bref, tout comme il n'est pas nécessaire d'être médecin pour maintenir une bonne hygiène de vie, il n'est pas indispensable d'être informaticien pour avoir une bonne hygiène numérique. Dans cet ouvrage, nous explorons une centaine de questions sur la cybersécurité et partageons des conseils concrets pour protéger ce qui compte le plus : nous, nos données et nos proches.

2 J'ai un problème de virement étrange, de harcèlement, etc., que faire ?

En cas de virement étrange, il faut contacter immédiatement la banque pour bloquer l'opération si possible ou les prochaines et déposez plainte si nécessaire. Pour un cas de harcèlement en ligne, il faut conserver les preuves (captures d'écran, messages, dates), bloquer la ou les personnes concernées, signaler les faits aux plateformes concernées, et aux autorités : rappelons que le harcèlement est puni par la loi (jusqu'à 2 ans d'emprisonnement et 30 000 € d'amende, voire davantage si les faits sont aggravés). Pour d'autres incidents (compte piraté, arnaque, usurpation d'identité...), le site officiel 17cyber.gouv.fr propose des aides concrètes, des conseils et un accompagnement vers les bons interlocuteurs.

Ce livre n'est pas un guide d'urgence ni un manuel juridique. Son objectif est de transmettre les connaissances nécessaires pour comprendre les enjeux numériques liés à la cybersécurité, pas de les guérir. Face à une situation critique, ne restez pas seul : cherchez rapidement de l'aide auprès de professionnels, d'autorités compétentes ou de services spécialisés.

3 Je ne suis personne, pourquoi serai-je menacé(e) ?

Il n'est pas nécessaire d'être une personne influente pour être exposé aux risques numériques. Même si vous n'êtes ni célèbre ni riche, vos données personnelles ont une valeur aux yeux des cybercriminels :

Certes, nous ne sommes pas tous des cibles aussi intéressantes que ce joueur de LOTO ayant gagné un montant record de 23 millions d'euros en 2024 en Girondes... Cependant, en 2023, la justice française a enregistré 164 434 victimes d'escroqueries en ligne. Ainsi, si l'on considère un prix de revente moyen de 144 € des données piratées en 2022[1], cela fait un chiffre d'affaires (144 € x 164 434 victimes) supérieur à ces 23 millions d'euros : c'est un ensemble de petits larcins qui nourrit le milieu de la cybercriminalité !

La cybersécurité joue donc un rôle crucial et nous concerne toute et tous. Elle va agir comme un bouclier, protégeant non seulement nos biens numériques et financiers, mais aussi nos droits fondamentaux. Qu'il s'agisse de droits individuels (vie privée, liberté d'opinion, de culte, d'expression ou de pensée) ou de droits collectifs (sécurité, démocratie, accès à l'information). Leur préservation dépend en partie de cette protection. Compromettre notre sécurité numérique revient à risquer de perdre ces libertés au profit de ceux qui exploitent nos vulnérabilités.

Les données personnelles englobent toutes les informations permettant d'identifier, directement ou non, une personne : nom, adresse, numéro de téléphone, courriels, données bancaires, historiques de navigation, préférences personnelles, et bien plus encore. Nous conseillons aux lecteurs une visite sur le site de la CNIL (Commission Nationale de l'Informatique et des Libertés) à l'adresse https://www.cnil.fr pour approfondir vos connaissances sur ce sujet et mieux comprendre les termes du RGPD (Règlement Général sur la Protection des Données). Cela étant, l'économie numérique moderne repose largement sur la collecte, l'analyse et l'exploitation de ces données[2]. Voici pourquoi elles sont si précieuses :

1. https://www.ndnm.fr/statistiques-cybersecurite-2022
2. La personne curieuse peut aussi consulté l'ouvrage de la même collection « La protection des données personnelles en 100 Questions/Réponses » https://www.editions-ellipses.fr/accueil/15002-la-protection-des-donnees-personnelles-en-100-questions-reponses-2e-edition-9782340082373.html

- Les géants du numérique s'appuient sur les données des utilisateurs pour perfectionner leurs services, proposer des publicités ciblées ou entraîner leurs modèles d'intelligence artificielle.
- Les données personnelles peuvent être vendues à des tiers ou utilisées pour construire des profils détaillés permettant d'anticiper les comportements des consommateurs. Ces pratiques ont donné naissance à un marché utilisé par des **data brokers** légitimes ou non.
- Dans un contexte géopolitique sous tension, les données personnelles deviennent des ressources stratégiques pour surveiller, prédire et influencer les comportements à grande échelle.
- Les données personnelles peuvent être exploitées pour extorquer de l'argent, pirater des comptes bancaires ou même usurper une identité.

Ainsi, chaque individu représente un point d'entrée potentiel pour des cyberattaques. Or, comme nous sommes tous connectés par moins de quatre degrés de séparation avec n'importe qui sur la planète[1], le facteur humain reste l'un des maillons les plus vulnérables de la chaîne de cybersécurité. Voici pourquoi :

- Les individus commettent fréquemment des erreurs, telles que cliquer sur des liens malveillants ou utiliser des mots de passe faibles. Ces failles sont exploitées par des techniques d'ingénierie sociale comme le phishing.
- Nous sous-estimons beaucoup la valeur de nos données personnelles et les conséquences d'un vol d'informations. Cette méconnaissance nous expose davantage et fait de nous des cibles plus faciles pour les cybercriminels.
- Avec l'essor du télétravail et l'utilisation hybride des appareils (professionnels et personnels), les cybercriminels disposent d'un éventail élargi de points d'accès. Ces appareils deviennent des cibles privilégiées, souvent moins bien protégées que les systèmes professionnels.
- L'expansion des maisons intelligentes et des objets connectés (caméras, thermostats, assistants vocaux) ouvre de nouvelles opportunités d'attaque. La faible sécurité de nombreux appareils, souvent conçus sans réelle préoccupation de sécurité (malgré des discours), facilite l'accès aux réseaux.

1. https://research.facebook.com/three-and-a-half-degrees-of-separation/

En somme, tout le monde peut être une cible potentielle des cybercriminels[1]. C'est pourquoi il est important de prendre des mesures pour protéger notre sécurité en ligne, quel que soit notre niveau de risque perçu. C'est ce que nous regroupons dans cet ouvrage (et qui souvent l'est sous les termes d'hygiène numérique).

1. La personne curieuse pourra voir l'étendue de l'ensemble des fuites de données en suivant ce lien : https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks

4 N'est-ce pas trop compliqué car je ne suis pas très fort(e) en informatique ?

Oui et non… Un peu comme il ne faut pas être serrurier pour protéger son domicile, il ne faut pas être informaticien pour mettre en place un minimum de cybersécurité.

Notre objectif devrait être de devenir une cible suffisamment difficile à atteindre pour décourager la plupart des cybercriminels, qui cherchent généralement des proies faciles. La bonne nouvelle c'est que cela nécessite une quantité raisonnable de connaissances et de compétences, accessibles à toutes et à tous.

En effet, d'après l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), de simples gestes comme l'utilisation de mots de passe robustes, la mise à jour régulière de ses logiciels ou la méfiance envers les courriels suspects, permettent déjà de réduire considérablement les risques. Cette petite dizaine de bonnes pratiques supprime la plupart des risques liés aux cyberattaques[1]. Devenir une cible plus difficile n'est pas une mission impossible, mais plutôt une question de discipline. Ce livre a été conçu pour vous accompagner dans cette démarche.

La deuxième section vous fournira des connaissances essentielles sur les cybermenaces et leurs mécanismes. Quant aux compétences nécessaires, il s'agit principalement de mettre en pratique des mesures simples que vous pourrez appliquer immédiatement. Vous n'avez pas besoin de maîtriser le jargon technique ou de devenir une personne experte en informatique. Ce qui compte, c'est d'adopter des habitudes qui protègent votre vie numérique au quotidien. Les voici détaillées[2] :

1. Protégez vos accès avec des mots de passe solides ;
2. Sauvegardez vos données régulièrement ;
3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées ;
4. Utilisez un antivirus ;

1. https://cyber.gouv.fr/bonnes-pratiques-protegez-vous
2. https://www.cybermalveillance.gouv.fr/medias/2021/01/FichePratique_SecuriteNumerique.pdf

5. Téléchargez vos applications uniquement sur les sites officiels ;
6. Méfiez-vous des messages inattendus ;
7. Vérifiez les sites sur lesquels vous faites des achats ;
8. Maîtrisez l'accès à vos réseaux sociaux ;
9. Séparez vos usages personnels et professionnels ;
10. Évitez les réseaux WiFi publics ou inconnus.

Dans cet ouvrage, nous allons vous guider à travers les bases de la cybersécurité, en vous expliquant les concepts clés et en vous donnant des conseils pratiques. Nous allons vous montrer comment être conscient des menaces en ligne et comment les éviter, comment choisir des mots de passe forts et comment les protéger, comment utiliser des logiciels de sécurité, et bien plus encore. Nous sommes convaincus que tout le monde peut contribuer à sa propre sécurité, et c'est pourquoi nous avons écrit ce livre pour vous aider à comprendre les enjeux de la cybersécurité et à adopter les bonnes pratiques pour vous protéger.

5 Est-ce réellement simple de se mettre en cybersécurité ?

Tout comme vous ne serez pas ceinture noire de judo en trois leçons, vous ne deviendrez pas avec la seule lecture de ce livre une personne experte en cybersécurité. Toutefois, les fondamentaux n'auront plus de secret pour vous, pour peu d'avoir conscience de leur importance et d'automatiser certains comportements. Se mettre en cybersécurité c'est simplement faire preuve d'anticipation et de préparation, pour faire simple il s'agit pour vous d'anticiper les scénarios désagréables et de se préparer à les traverser pour revenir à un état le plus normal possible. La liste de la question 3 est là pour nous rappeler que quelques actions simples mais systématiques, que nous détaillerons tout au long du livre, permettent de :

1. Limiter notre fragilité face à des attaques basiques ;
2. Augmenter la difficulté pour d'éventuelles attaques plus ciblées ;
3. Retrouver plus rapidement une situation supportable ;
4. Protéger nos proches et les aider à progresser.

Se protéger des attaques informatiques est quelque chose d'accessible sans compétence technique particulière. La clé réside dans l'adoption de bonnes pratiques, simples, et gratuites, qui réduisent drastiquement les risques. Nous allons en exposer la plupart succinctement ici, ainsi, il s'agit d'une réponse longue, mais nécessaire.

Commencez par activer les mises à jour automatiques de votre système d'exploitation, de votre navigateur web (comme Chrome ou Firefox) et de vos applications. Ces mises à jour corrigent des failles régulièrement exploitées par les pirates. Parallèlement, utilisez un antivirus de base mais évitez cependant de les empiler, un seul est suffisant pour bloquer la majorité des menaces courantes.

La gestion des mots de passe est un pilier essentiel. Évitez la réutilisation de vos mots de passe sur plusieurs sites : une seule fuite de données pourrait compromettre tous vos comptes. Pour simplifier cette tâche, des gestionnaires comme KeePass (gratuit et certifié par l'ANSSI) génèrent et stockent des mots de passe complexes de manière sécurisée. Complétez cette protection en activant la double authentification (2FA) partout où c'est possible (cf. question 32). Cette étape bloque 99 % des tentatives de piratage, même si votre mot de passe est volé.

Face au phishing, ces courriels ou SMS frauduleux imitant des organismes officiels, la vigilance est votre meilleure alliée. Méfiez-vous des liens ou pièces jointes inattendus, même s'ils semblent provenir d'une source fiable. Par exemple, un SMS de « La Poste » vous invitant à cliquer sur un lien pour suivre un colis est souvent une arnaque. Vérifiez directement sur le site officiel plutôt que de cliquer. Sur votre fournisseur de messagerie, utilisez le bouton « Signaler un spam » pour alerter les filtres automatiques.

Sécurisez votre réseau Wi-Fi domestique en modifiant le mot de passe par défaut de votre box (Livebox, Freebox…) et en choisissant le protocole de chiffrement WPA3 (ou WPA2). Désactivez si possible le WPS, une fonctionnalité pratique mais vulnérable aux intrusions. Pour protéger vos données contre les ransomwares, effectuez des sauvegardes régulières sur un disque dur externe et/ou un cloud (Google Drive, iCloud), en suivant dans la mesure du possible de la redondance, nous suggérons une « règle des 3 copies » : une sur l'appareil, une externe, une en ligne.

Optimisez votre navigation internet avec des extensions comme uBlock Origin (gratuite), qui bloque publicités et suivis malveillants. Privilégiez les sites en HTTPS (symbolisé par un cadenas dans la barre d'adresse) et évitez les téléchargements illégaux (logiciels crackés, films…), souvent porteurs de virus. Si vous avez un doute, utilisez VirusTotal, un outil gratuit analysant les fichiers avec 70 antivirus simultanément.

Enfin, sécurisez vos objets connectés (caméras, enceintes intelligentes, et de plus en plus d'électroménager) en changeant leurs mots de passe par défaut, souvent connus des pirates. Mettez à jour leur logiciel via l'application du fabricant. Enfin, l'utilisation d'un VPN, bien que souvent proposés par vos personnalités YouTube préférées n'est que très peu utile en termes de cybersécurité (cf. question 41). Cela étant, des outils comme ProtonVPN (gratuit) chiffrent votre connexion et protège votre vie privée.

Selon l'ANSSI, 9 attaques sur 10 ciblent des négligences évitables, en combinant ces mesures – mises à jour, gestion des mots de passe, vigilance anti-phishing et sauvegardes –, vous devenez une cible trop complexe pour la majorité des cybercriminels, qui préfèrent les proies faciles. Aucune compétence technique avancée n'est requise, juste une routine disciplinée. La cybersécurité commence par ces gestes simples, mais vitaux.

MAIS QU'EST-CE DONC ?

Dans cette section, nous abordons des questions de vocabulaire indispensables pour naviguer dans le monde numérique. Avec le développement rapide des technologies, les outils et techniques se multiplient et évoluent à un rythme effréné. Pour se mettre en cybersécurité et, plus généralement, pour comprendre le monde dans lequel nous évoluons, il est essentiel de disposer d'une base de connaissances solide. Nous avons ainsi regroupé dans cette partie une série de questions fréquemment posées, ainsi que d'autres moins courantes mais tout aussi essentielles. Vous pourrez puiser, au gré de vos interrogations, les réponses qui vous aideront à mieux appréhender les enjeux et le vocabulaire de l'univers numérique.

6 Qu'est-ce qu'une vulnérabilité ou être vulnérable dans le contexte de la cybersécurité ?

Pour expliciter la notion de vulnérabilité, l'exemple du château fort est fréquemment utilisé. Un château fort remplit plusieurs fonctions essentielles : il délimite un périmètre, filtre les accès, renforce ses points faibles et protège ce qui se trouve à l'intérieur. Une vulnérabilité se manifeste partout où un ennemi peut s'infiltrer : une brèche dans la muraille, des rondes mal assurées, une absence d'éclairage, des forces défensives insuffisantes, etc. Bien qu'elle soit aujourd'hui dépassée (en termes de sécurité, comme de cybersécurité), car trop rigide et massive, cette approche en comparaison reste pertinente.

Si l'on prend l'exemple, plus simple à appréhender, de la maison d'Alice et Bob[1], cela est plus parlant. Bob, passionné de technologie, installe une caméra de surveillance connectée pour sécuriser la maison. Il la configure rapidement, sans changer le mot de passe par défaut. Un jour, il découvre que des images de leur salon ont été diffusées en ligne. La caméra, laissée vulnérable, a été piratée.

Alice quant à elle, joue à des jeux en ligne et reçoit un message lui promettant des récompenses si elle clique sur un lien. Curieuse, elle vérifie et clique pour voir le formulaire de participation. Sans le savoir, elle a téléchargé un logiciel malveillant qui envoie des informations sensibles à des inconnus. Encore une fois, une vulnérabilité exploitée par la ruse.

À chaque fois une vulnérabilité - un oubli, un manque de vigilance, bref, une petite fissure - a permis une intrusion dans leur intimité. Concrètement il s'agit d'une faille, un point d'entrée que des individus malveillants peuvent exploiter pour accéder à nos informations personnelles, à nos appareils ou à notre vie privée. Ces failles peuvent être techniques, comme un logiciel non mis à jour, ou humaines, comme l'utilisation d'un mot de passe trop simple.

1. Lorsque l'on parle de cybersécurité, il est normal et commun de faire référence à Alice et Bob pour parler des personnes utilisant un système, voir https://fr.wikipedia.org/wiki/Alice_et_Bob si vous êtes une personne curieuse.

Mais alors, doit-on chercher à être invulnérable ? La réponse est simple, au-delà du fait que le statut d'invulnérabilité est quasiment impossible à atteindre, et encore plus impossible à garder, NON. Être vulnérable, ce n'est pas être faible ou incompétent. C'est être humain. Nous avons tous des moments d'inattention, de fatigue, ou de confiance excessive. Être vulnérable, c'est ignorer ses faiblesses, et, lorsqu'on les connaît, c'est ignorer les solutions possibles. Il faut chercher à être conscient de ses vulnérabilités, et en réduire leurs conséquences pour devenir résilient. C'est-à-dire revenir à une situation au plus près de la norme après un problème.

Mon pare-feu est en panne ? Je coupe les connexions sortantes ou je contrôle plus strictement les entrées. Je n'ai pas de système de gestion des sauvegardes automatiques ? Je compense avec une sauvegarde manuelle sur plusieurs supports (cf. question 68). Mon antivirus n'est pas à jour ? Je fais cela manuellement.

Vous l'aurez compris : il s'agit d'une posture, à la fois intellectuelle et comportementale. Alors, vous sentez-vous vulnérable ? Quelles données souhaitez-vous protéger ? Et à quel coût ? Le chemin de la résilience est parfois sinueux et escarpé. Mais en l'empruntant, vous prendrez conscience qu'au-delà de votre propre sécurité, c'est aussi celle de votre entourage que vous renforcez.

7 Qu'est-ce que l'ANSSI ?

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est un organisme public français, créé en 2009, dont la mission principale est d'assurer la cybersécurité des systèmes d'information (SI) stratégiques du pays. Placée sous l'autorité du Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN), l'ANSSI joue un rôle central dans la protection des infrastructures numériques de l'État, des entreprises et donc des citoyens.

Cette agence interministérielle a pour but de construire et d'organiser la protection de la nation face aux cyberattaques. Voici le détail de ces missions (en 2025)[1] :

1. Défendre :

- les systèmes d'information critiques de la nation en concevant et opérant le déploiement de capacités de détection des cyberattaques ;
- les victimes de cyberattaques d'ampleur ;
- la nation en structurant au niveau national l'assistance aux victimes de cyberattaques.

2. Connaître :

- l'état de l'art en sécurité des technologies et des systèmes d'information et en être des experts ;
- les menaces et les risques dans le cyberespace et développer des méthodes et des outils pour y faire face ;
- les tendances du monde de la cybersécurité, en France, en Europe et à l'international, pour s'y inscrire pleinement en défendant une vision singulière de la sécurité et de la stabilité du cyberespace.

3. Partager :

- des recommandations de cybersécurité, des solutions et des outils aux acteurs de la cybersécurité et de la transformation numérique pour démultiplier l'action de l'agence et renforcer la cybersécurité collective ;

1. https://cyber.gouv.fr/nos-missions

- sur la réponse à la menace au sein des réseaux de coopération techniques, opérationnels et stratégiques français, européens et internationaux ;
- l'expertise de l'agence dans le domaine de la cybersécurité pour former les agents de l'État et des opérateurs régulés à la cybersécurité ;
- largement les connaissances en matière de cybersécurité et encourager le développement de la filière et des formations en cybersécurité ;
- en lien avec ses partenaires, pour informer et sensibiliser les citoyens aux risques cyber.

4. Accompagner :

- le développement d'une doctrine française de cybersécurité et la conception des dispositifs normatifs et réglementaires aux niveaux national et européen ;
- le Gouvernement dans le déploiement d'une politique publique en matière de cybersécurité ;
- les plus hautes autorités dans leur appréhension du fait cyber ;
- les opérateurs régulés dans l'application des mesures de sécurisation de leurs systèmes d'information et leurs réponses aux incidents ;
- le développement d'un écosystème de prestataires de produits et de services de confiance dans le domaine de la cybersécurité.

8 Se préoccuper de cybersécurité est-il utile car la NSA sait absolument tout non ?

Les révélations d'Edward Snowden[1] sur la surveillance de masse du gouvernement américain et de ses alliés ont profondément bouleversé notre compréhension de la surveillance étatique. Les documents divulgués ont mis en lumière des programmes tels que PRISM, qui permettaient à la NSA de collecter en masse des données sur des millions d'individus à travers le monde. Ces programmes ne se contentaient pas de surveiller des suspects isolés, mais interceptaient des communications ordinaires, depuis les courriels jusqu'aux messages instantanés, démontrant ainsi l'ampleur d'un système de surveillance généralisée et intrusive.

On entend souvent : « *je me moque d'être surveillé car je n'ai rien à cacher* ». Ce raisonnement est non seulement naïf, mais aussi dangereux. Comme le rappelle Edward Snowden, dire que l'on se moque de la surveillance parce que l'on n'a rien à cacher, c'est comme dire que l'on se moque de la liberté d'expression parce que l'on n'a rien à dire. Ce n'est pas parce que vous n'êtes pas personnellement inquiété aujourd'hui que ces pratiques sont acceptables ou sans conséquence. Au-delà du fait qu'il est démontré que l'on change nos comportements lorsque l'on se sait surveillé, nous avons tous des informations sensibles (des opinions politiques, des préférences personnelles, des données financières) et nous avons tous quelque chose à cacher à quelqu'un, ne serait-ce que notre carte bancaire et son code. Accepter la surveillance de masse revient à renoncer à la confidentialité de ces informations sous prétexte qu'elles ne nous semblent pas compromettantes, dans l'immédiat.

Les lanceurs d'alertes tels qu'Edward Snowden ou encore Julian Assange[2] ont joué un rôle crucial en exposant ces pratiques. Dans le cas de Julian Assange, à travers Wikileaks, il a révélé des documents prouvant que la surveillance et la censure sont aussi des outils de contrôle politique, mettant en lumière les dérives potentielles des gouvernements et des institutions. Ces révélations nous rappellent

1. Voir une présentation courte sur YouTube proposée par Arte de Snowden https://www.youtube.com/watch?v=7epZcOJ9c-M
2. Voir une présentation d'Assange sur YouTube par LeParisien : https://www.youtube.com/watch?v=Zu5jNejhtrQ

que la surveillance ne concerne pas uniquement les criminels ou les terroristes, mais nous toutes et tous, citoyennes et citoyens dont les droits et libertés fondamentales peuvent être, et étaient alors, remis en cause.

La véritable leçon à tirer est qu'il est essentiel de comprendre les enjeux et d'adapter son usage des technologies numériques. Des questions pratiques telles que « comment envoyer un courriel sécurisé ? » (cf. questions 38 et 85) ou « comment chiffrer ses données ? » (cf. question 67) ne sont pas anodines. Elles sont des moyens concrets de reprendre le contrôle de nos vies numériques et de montrer que non, la cybersécurité n'est pas une lubie, mais une nécessité face à un système, de menaces et de surveillances, omniprésent.

En intégrant des techniques de chiffrement et en adoptant des pratiques de sécurité renforcées, nous affirmons que la surveillance de masse n'est pas une fatalité, mais bien une menace contre laquelle il est possible et nécessaire de se protéger. Cette démarche n'a rien à voir avec la paranoïa : il s'agit simplement d'un engagement éclairé pour préserver nos droits et notre liberté dans un monde où les technologies de surveillance continuent de s'étendre.

9 Qui sont les attaquants/hackers/pirates informatiques ?

Le profil d'un attaquant (qui n'a pas forcément volonté de vous attaquer d'ailleurs) qui va nous toucher est lié inévitablement à notre profil : la cybersécurité c'est un truc que l'on ignore ? Dans ce cas, on sera la cible des escrocs les moins compétents. On a des données à forte valeur, alors les meilleurs seront à nos trousses.

Pour les services officiels, il existe sept grandes catégories d'acteurs malveillants, c'est-à-dire de personnes qui nous veulent du mal. Le monde est ainsi fait. Il existe des personnes agressives, méchantes, désireuses d'obtenir vos biens ou de détruire nos vies. Qu'ils soient escrocs ou pédophiles, ils veulent ce que nous avons. Et entre nous et ces personnes malveillantes il y a tout une échelle de personnes qui, sans directement vouloir nous nuire, vont, par leur ignorance ou leur inattention, nous créer des problèmes.

- Nos proches

  Encore une fois malheureusement, nos proches (amis, famille) sont parfois la source de nos atteintes numériques. Un petit piège sur le téléphone de son conjoint / conjointe, une destruction d'un appareil ou un détournement d'argent sont des choses maintes fois constatées par la Police ou la Gendarmerie.

- Les attaquants numériques isolés

  Appelés les « *scripts kiddies* », les attaquants cyber isolés sont des amateurs sans grande expertise technique. Ils utilisent des outils ou des scripts déjà développés par d'autres hackers pour mener des atteintes hors de leur contrôle. Leur objectif est souvent de s'amuser ou de se faire remarquer mais aussi de mettre en œuvre des escroqueries faciles.

- Les cybers terroristes

  Un cyberterroriste est un individu ou un groupe qui utilise les technologies numériques pour mener des actes de terreur. Ces actions visent à provoquer la peur, à perturber les infrastructures essentielles, à infliger des dégâts économiques, ou encore à promouvoir une idéologie politique, religieuse ou sociale.

Contrairement aux cybercriminels motivés par des gains financiers, les cyberterroristes cherchent principalement à atteindre des objectifs idéologiques ou destructeurs.

- Les cyber hacktivistes

  Les hacktivistes sont des pirates motivés par des convictions politiques, sociales ou idéologiques. Ils mènent des cyberattaques pour dénoncer des injustices, soutenir des causes ou critiquer des institutions. Ils mettent en œuvre principalement des défigurations de sites web (affichage de messages militants) et des fuites de documents sensibles pour dénoncer des scandales.

- Les États-nation et groupes sponsorisés par des gouvernements

  Certains cyberattaquants sont directement affiliés aux États ou agissent sous leur commandement. Ces groupes mènent des cyberattaques pour des raisons géopolitiques, économiques ou militaires.

- Les cyber criminels

  Les cybercriminels cherchent principalement à obtenir un gain financier par des activités illégales en ligne. Souvent organisés en réseaux, ils opèrent à grande échelle et exploitent des techniques avancées. Ils sont organisés, éparpillés sur toute la surface du globe et détiennent des connaissances avancées voire supérieures à la plupart des experts.

Les finalités de ces groupes sont nombreuses car elles sont les mêmes que dans la vie prénumérique : gains financiers, idéologie, espionnage, sabotage, notoriété, diffamation, etc. Dans tous les cas, mis à part vos proches, on catégorise souvent les « pirates informatiques » dans deux catégories, les *black hat* et les *white hat,* ou chapeau noir et chapeau blanc. La plupart des criminels ci-dessus appartiennent à la catégorie des *black hat* qui regroupe les personnes cherchent à exploiter les faiblesses des systèmes informatiques dans des buts illégaux. À l'opposé de ces *black hat* il existe les *white hat* qui regroupent les hackers dits éthiques, qui agissent pour prévenir les cyberattaques. Ils collaborent avec les organisations ou les états afin d'identifier les failles de sécurité avant qu'elles ne soient exploitées par des individus malveillants.