Manuel de cybersécurité

pour les

parlements

Un guide pour les parlements qui souhaitent se lancer dans un programme de cybersécurité

Manuel de cybersécurité

pour les

parlements

Un guide pour les parlements qui souhaitent se lancer dans un programme de cybersécurité

Table des matières

Légende visuelle

Tout au long du manuel, vous trouverez quelques éléments récurrents et mis en évidence en plus du texte principal. Voici une courte « légende » pour vous aider à comprendre les éléments de base :

Étude de cas

Indique des études de cas qui mettent en évidence l'impact réel d'un certain sujet sur les parlements à l'échelle mondiale ou dans un pays spécifique.

Conseils supplémentaires

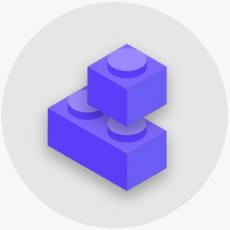
Souligne quelques conseils et informations supplémentaires auxquels prêter attention lorsque vous lisez le manuel.

Le monde réel

Cite des exemples courants d'outils tactiques de cybersécurité utilisés dans le « monde réel », à la fois pour le meilleur et pour le pire.

Avancé

Indique un sujet avancé - des informations importantes à prendre en compte par votre parlement, mais qui peuvent être un peu plus techniques ou compliquées.



Éléments constitutifs du programme de sécurité

Indique les « Éléments constitutifs du programme de sécurité », qui sont les principaux éléments à retenir de chaque section du manuel.

Le Top 10

Ces 10 éléments sont essentiels au programme de sécurité de votre parlement. Si vous cherchez un point de départ, jetez d'abord un coup d'œil ici.

1. **Organisez régulièrement des formations sur la sécurité au sein de votre parlement**
2. **Soyez attentif au hameçonnage et ayez un système de signalement**
3. **Utilisez le chiffrement pour toutes les communications - de bout en bout, si possible**
4. **Exigez des mots de passe forts et mettez en place un gestionnaire de mots de passe dans votre parlement**
5. **Exigez une authentification à deux facteurs dans la mesure du possible**
6. **Veillez à ce que tous les appareils et logiciels du personnel soient à jour**
7. **Utiliser un stockage en nuage sécurisé**
8. **Utilisez HTTPS et, le cas échéant, un VPN, pour accéder à Internet**
9. **Protégez les actifs physiques de votre parlement**
10. **Élaborez un programme de réponse aux incidents de l'organisation**

1

Instaurer une culture de la sécurité

2

Une base solide : Sécurisation des comptes et des appareils

3

Communiquer et Stocker des données en toute sécurité

4

Rester en sécurité sur Internet

5

Protection de la sécurité physique Sécurité

6

Que faire quand les choses tournent mal

Auteurs et remerciements

Ce guide a été produit par le National Democratic Institute (NDI) et le House Democracy Partnership (HDP).

Auteur principal : **Evan Summers (NDI)**
Auteurs collaborateurs : **Sarah Moulton (NDI); Chris Doten (NDI)**

Lors de l'élaboration de ce manuel, nous tenons à remercier tout particulièrement les experts externes qui nous ont fait part de leurs précieux commentaires, révisions et suggestions :

Fiona Krakenburger, Fonds technologique ouvert ; Bill Budington et Shirin Mori, Electronic Frontier Foundation ; Jocelyne Woolbright, Cloudflare ; Martin Shelton, Fondation pour la liberté de la presse ; Dave Leichtman, Microsoft ; Stephen Boyce, Fondation internationale pour les systèmes électoraux ; Amy Studdart, Institut républicain international ; Emma Hollingsworth, Global Cyber Alliance ; Caroline Sinders, Convocation Design + Research ; Dhyta Caturani; Sandra Pepera, NDI ; Aaron Azelton, NDI ; Frieda Arenos, NDI ; Anthony DeAngelo, NDI ; Whitney Pfeifer, NDI ; et Derek Luyten, House Democracy Partnership. Nous tenons également à remercier Paul Kollie des Services d'information législative au Libéria, Nihad Bahram et Fuad Ahmed au parlement du Kurdistan en Irak, Diana Plata au Sénat de Colombie ; Ayad Abbas et Majid Khudhur au Conseil irakien des représentants, et Tanja Danailovska à l'Assemblée de la Macédoine du Nord pour leurs précieuses idées et contributions.

Nous tenons également à mentionner tous les manuels, guides, cahiers d'exercices, modules de formation et autres documents remarquables développés et gérés par la communauté d'Organizational Security (OrgSec). Ce manuel est conçu pour compléter ces documents plus approfondis, en combinant les leçons clés en une ressource unique et facile à lire pour les parlements qui cherchent à se lancer dans le développement d'un programme de cybersécurité.

En plus de nous inspirer indirectement de nombreuses ressources remarquables compilées par la communauté, nous avons directement copié le langage utile d'une poignée de ressources disponibles également tout au long de ce manuel, en particulier le Surveillance Self Defense Guide de la Electronic Frontier Foundation, le Holistic Security Manual de Tactical Tech et une série d'explications du Center for Democracy and Technology et de la Freedom of the Press Foundation. Vous trouverez des citations spécifiques à ces ressources tout au long des sections ci-dessous, ainsi que des liens complets, des informations sur les auteurs et les licences au sein de l'Annexe A.

Qui sommes nous?

L'Institut Démocratique National pour les Affaires Internationales (National Democratic Institute for International Affairs - NDI) est une organisation à but non lucratif et non partisane, basée à Washington D.C., qui travaille en partenariat dans le monde entier pour renforcer et sauvegarder les institutions, les processus, les normes et les valeurs démocratiques afin de garantir une meilleure qualité de vie pour tous.

NDI estime que tous les individus ont le droit de vivre dans un monde qui respecte leur dignité, leur sécurité et leurs droits politiques, et que le monde numérique ne fait pas exception.

Au sein du NDI, l'équipe Démocratie et Technologie cherche à favoriser un écosystème numérique mondial où les valeurs démocratiques sont protégées, promues et peuvent s'épanouir ; les gouvernements sont plus transparents et inclusifs ; et tous les citoyens sont habilités à demander des comptes à leur gouvernement. Nous faisons ce travail en soutenant un réseau mondial d'activistes engagés dans la résilience numérique, et en collaborant avec des partenaires sur des outils et des ressources comme ce manuel. Vous pouvez en savoir plus sur notre travail sur notre site web, en nous suivant sur Twitter ou en vous adressant directement à cyberhandbook@ndi.org. Nous sommes toujours enchantés de vous écouter et de répondre à vos questions sur notre équipe et notre travail sur la cybersécurité, la technologie et la démocratie.

Le House Democracy Partnership (HDP) travaille avec les législatures du monde entier pour promouvoir un gouvernement réactif et efficace et renforcer les institutions démocratiques. Au cœur de notre travail se trouve la coopération entre pairs pour développer une expertise technique dans les législatures partenaires qui améliorera la responsabilité, la transparence, l'indépendance législative, l'accès à l'information et la surveillance gouvernementale. HDP a actuellement des partenariats avec plus de 20 législatures nationales à travers le monde. Les domaines de coopération avec les parlements partenaires du HDP comprennent la résolution des problèmes budgétaires, la garantie d'un fonctionnement plus efficace des commissions, l'amélioration des services aux électeurs, la fourniture d'outils pour un contrôle renforcé, le renforcement de l'éthique législative et l'amélioration de l'informatique, de la bibliothèque et de la recherche, ainsi que des processus et procédures législatifs. Les programmes du HDP sont mis en œuvre par le National Democratic Institute (NDI) et l'International Republican Institute (IRI) dans le cadre d'un accord de financement coopératif avec l'Agence pour le développement international (USAID).

Qui gère la cybersécurité parlementaire ?

Un parlement efficace et sûr nécessite un personnel doté des compétences et de l'autorité nécessaires pour mettre en œuvre les recommandations comprises dans ce manuel. Cela dit, les personnes responsables de la cybersécurité au sein des parlements peuvent varier considérablement et il n'existe pas de modèle « correct » pour déterminer qui devrait gérer la cybersécurité. Dans certains cas, il peut s'agir d'une équipe dédiée à la cybersécurité au sein de votre unité informatique, et dans d'autres, d'un groupe de différents membres du personnel administratif ou autres. Quoi qu'il en soit, gardez à l'esprit que s'il est important d'avoir une bonne équipe en charge de la cybersécurité de votre parlement, il est également de la responsabilité de chacun au sein et autour du parlement de suivre les politiques et procédures nécessaires pour assurer la sécurité du parlement. Vous trouverez ci-dessous quelques exemples de différents modèles de dotation en personnel pour la gestion de la cybersécurité parlementaire :

Chambre des députés des États-Unis
À la **Chambre des députés des États-Unis**, certains bureaux membres individuels embauchent un **administrateur système** responsable de la gestion de l'ensemble du matériel informatique et des systèmes logiciels utilisés par le bureau - y compris la gestion des considérations de cybersécurité - et forme les membres du personnel aux meilleures pratiques. Au niveau institutionnel, le directeur général de la Chambre des députés abrite une équipe des ressources informatiques, qui comprend un **département dédié à la sécurité de l'information.**

Assemblée nationale de Zambie
L'**Assemblée nationale de Zambie** compte sur son département des technologies de l'information et de la communication (TIC) pour diverses fonctions, notamment la gestion des logiciels, du matériel et de l'infrastructure d'information du parlement, la formation des membres ou du parlement et du personnel sur les systèmes technologiques et la sécurisation de l'infrastructure d'information du parlement. contre les menaces de cybersécurité internes et externes.

Parlement de Malaisie
Le **parlement de Malaisie** abrite sa division des technologies de l'information sous l'administrateur en chef du parlement, ce qui lui permet de servir les deux chambres du parlement. Cette division comprend un poste spécifique pour la sécurité du réseau, qui lui permet de s'assurer que les systèmes de réseau, les centres de données et l'infrastructure TIC sont à jour et aussi sécurisés que possible.

À qui s'adresse ce manuel ?

Ce manuel a été rédigé dans un but simple : aider votre parlement à élaborer un programme de cybersécurité compréhensible et réalisable.

Alors que le monde avance de plus en plus en ligne, la cybersécurité n'est pas seulement un mot à la mode mais un concept essentiel pour le succès des parlements, et la sécurité de l'information (à la fois en ligne et hors ligne) est un défi qui nécessite concentration, investissement et vigilance.

Votre parlement est susceptible de devenir, si ce n'est déjà le cas, la cible d'une attaque de cybersécurité. Ce constat ne se veut pas alarmiste ; c'est la réalité même pour les parlements qui ne se considèrent pas comme des cibles particulières.

Au cours d'une année moyenne, le Center for Strategic and International Studies, qui tient une **liste ouverte** de ce qu'il appelle des « cyberincidents significatifs », répertorie des centaines de cyberattaques graves, dont beaucoup visent des dizaines, voire des centaines d'organisations à la fois. En plus de ces attaques signalées, il y a probablement des centaines d'autres attaques plus légères chaque année qui passent inaperçues ou ne sont pas signalées, beaucoup visant des institutions gouvernementales, des organes législatifs et des organisations politiques.

Les cyberattaques de ce type ont des conséquences importantes. Que leur objectif soit de perturber les opérations parlementaires, de nuire à votre réputation ou même de voler des informations pouvant entraîner des dommages psychologiques ou physiques à vos membres ou à votre personnel, ces menaces doivent être prises au sérieux.

La bonne nouvelle est que vous n'avez pas besoin de devenir un codeur ou un technologue pour vous défendre, vous et votre parlement, contre les menaces courantes. Cependant, vous devez être prêt à investir des efforts, de l'énergie et du temps pour élaborer et mettre en œuvre un programme de sécurité parlementaire solide.

Si vous n'avez jamais envisagé de renforcer la cybersécurité au sein de votre parlement, si vous n'avez pas eu le temps de vous y consacrer, ou si vous connaissez quelques notions de base sur le sujet mais pensez que votre parlement pourrait améliorer sa cybersécurité, ce manuel est fait pour vous. **Peu importe d'où vous venez, ce manuel vise à donner à votre parlement les informations essentielles dont il a besoin pour mettre en place un programme de sécurité solide - un programme qui va au-delà de la simple mise sur papier et vous permet de mettre les meilleures pratiques en action.**

Qu'est-ce qu'un programme de sécurité et pourquoi mon parlement devrait-il en avoir un ?

Un programme de sécurité regroupe l'ensemble des politiques, procédures et instructions écrites sur lesquelles votre parlement s'est accordée pour atteindre le niveau de sécurité que vous et votre équipe jugez approprié pour assurer la sécurité de votre personnel, de vos partenaires et de vos informations.

Un programme de sécurité parlementaire bien conçu et mis à jour peut à la fois vous protéger et vous rendre plus efficace en vous apportant la tranquillité d'esprit nécessaire afin de vous concentrer sur le travail quotidien important de votre parlement. En l'absence d'un programme complet, il est très facile de ne pas percevoir certains types de menaces, de se focaliser sur un seul risque ou d'ignorer la cybersécurité jusqu'à ce qu'une crise survienne. Lorsque vous commencez à élaborer un programme de sécurité, vous devez vous poser certaines questions importantes qui forment un processus appelé **évaluation des risques.** En répondant à ces questions, votre parlement peut appréhender les menaces uniques auxquelles elle est confrontée et prendre du recul afin de réfléchir de manière globale à ce que vous devez protéger et contre qui vous devez le faire. Des évaluateurs formés, aidés par des systèmes comme le cadre d'audit **SAFETAG** d'Internews, peuvent aider votre parlement à mener à bien un tel processus. Si vous pouvez avoir accès à ce niveau d'expertise professionnelle, cela en vaut la peine, mais même si vous ne pouvez pas vous soumettre à une évaluation complète, vous devriez vous réunir avec vos parties prenantes dans tout le parlement afin de réfléchir à ces questions clés :

1 Quels sont les actifs dont dispose votre parlement et que voulez-vous protéger ?

Vous pouvez commencer à répondre à ces questions en créant un catalogue de tous les actifs de votre parlement. Les informations telles que les messages, les courriels, les contacts, les documents, les calendriers et les lieux sont autant d'actifs potentiels. Les téléphones, ordinateurs et autres appareils peuvent être des actifs. Les personnes, les relations et les liens peuvent aussi être des actifs. Faites une liste de vos actifs et essayez de les cataloguer en fonction de leur importance pour l'organisation, de l'endroit où vous les conservez (peut-être plusieurs endroits numériques ou physiques), et de ce qui empêche les autres d'y accéder, de les endommager ou de les perturber. N'oubliez pas que tout n'a pas la même importance. Si certaines des données de le parlement relèvent du domaine public, ou si vous publiez déjà des informations, il ne s'agit pas de secrets que vous devez protéger.

2 Qui sont vos adversaires et quelles sont leurs capacités et leurs motivations ?

« Adversaire » est un terme couramment utilisé dans le domaine de la sécurité organisationnelle. En termes simples, les adversaires sont les acteurs (individus ou groupes) qui souhaitent cibler votre parlement, perturber votre travail et accéder à vos informations ou les détruire : les méchants. Les adversaires potentiels peuvent être, par exemple, des escrocs financiers, des gouvernements locaux ou nationaux adversaires, ou des pirates informatiques à motivation idéologique ou politique. Il est important de dresser une liste de vos adversaires et de réfléchir de manière critique à qui pourrait vouloir avoir un impact négatif sur votre parlement et votre personnel. S'il est facile de percevoir des acteurs externes (comme un gouvernement étranger ou un groupe politique particulier) comme des adversaires, il ne faut pas oublier que les adversaires peuvent être des personnes que vous connaissez, comme des employés mécontents, d'anciens membres du personnel, des membres de votre famille ou des partenaires qui ne vous soutiennent pas. Des adversaires différents représentent des menaces différentes et disposent de ressources et de capacités différentes pour perturber vos opérations et accéder à vos informations ou les détruire.

Par exemple, les gouvernements disposent souvent de beaucoup d'argent et de moyens puissants, notamment pour couper l'internet ou utiliser des technologies de surveillance coûteuses ; les réseaux mobiles et les fournisseurs d'accès à l'internet ont probablement accès aux relevés d'appels et aux historiques de navigation ; des pirates informatiques qualifiés sur les réseaux Wi-Fi publics sont capables d'intercepter des communications ou des transactions financières peu sécurisées. Vous pouvez même devenir votre propre adversaire, par exemple en supprimant accidentellement des fichiers importants ou en envoyant des messages privés à la mauvaise personne.

Les motivations des adversaires sont susceptibles de varier, tout comme leurs capacités, leurs intérêts et leurs stratégies. La discréditation de votre parlement est-elle dans leur intérêt ? Peut-être ont-ils l'intention de faire passer votre message sous silence ou de perturber le travail du parlement ? Il est important de comprendre la motivation d'un adversaire, car cela peut aider votre parlement à mieux évaluer les menaces qu'il peut engendrer.

3 À quelles menaces votre parlement est-il confronté ? Et dans quelle mesure celles-ci peuvent-elles survenir et avoir un impact important ?

Au fur et à mesure que vous identifiez les menaces possibles, vous risquez de vous retrouver avec une longue liste qui peut être déroutante. Vous pouvez avoir l'impression que tout effort serait inutile, ou ne pas savoir par où commencer. Pour aider votre parlement à prendre des mesures productives, il est utile d'analyser chaque menace en fonction de deux facteurs : la probabilité que la menace se concrétise et l'impact si elle se concrétise.

Pour mesurer la probabilité d'une menace (peut-être « faible, moyenne ou élevée », selon qu'un événement donné a peu de chances de se produire, pourrait se produire ou se produit fréquemment), vous pouvez utiliser les informations que vous connaissez sur la capacité et la motivation de vos adversaires, l'analyse des incidents de sécurité passés, les expériences d'autres parlements similaires et, bien sûr, la présence de toute stratégie d'atténuation existante mise en place par votre parlement.

Pour mesurer l'impact d'une menace, réfléchissez à quoi ressemblerait votre environnement si la menace se concrétisait. Posez des questions telles que « Comment la menace nous a-t-elle nui en tant que parlement et en tant que personnes, physiquement et mentalement ? », « Quelle est la durée de l'effet ? », « Est-ce que cela engendre d'autres situations nuisibles ? » et « Comment cela entrave-t-il notre capacité à atteindre nos objectifs maintenant et à l'avenir ? ». En répondant à ces questions, déterminez si la menace a un impact faible, moyen ou élevé.

Une fois que vous avez classé vos menaces en fonction de leur probabilité et de leur impact, vous pouvez commencer à élaborer un plan d'action plus éclairé. En vous focalisant sur les menaces qui sont les plus susceptibles de se produire ET qui auront des impacts négatifs importants, vous canaliserez vos ressources limitées de la manière la plus efficace possible.

Votre objectif est toujours d'atténuer autant que possible les risques, mais personne, pas même le gouvernement ou l'entreprise la mieux dotée en ressources de la planète, ne pourra jamais éliminer totalement les risques. Et ce n'est pas grave car vous pouvez faire beaucoup de choses pour vous protéger vous, vos collègues et votre parlement en vous attaquant aux plus grandes menaces.

Pour vous aider à gérer ce processus d'évaluation des risques, envisagez d'utiliser une feuille de travail, comme **celle-ci** développée par l'Electronic Frontier Foundation. Gardez à l'esprit que les informations que vous développez dans le cadre de ce processus (comme la liste de vos adversaires et les menaces qu'ils représentent) peuvent elles-mêmes être sensibles, il est donc important d'en assurer la sécurité.

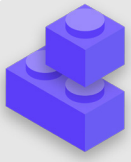
Créer le programme de cybersécurité de votre parlement

Bien que le programme de sécurité de chaque parlement soit légèrement différent en fonction de l'évaluation des risques et de la dynamique parlementaire, certains concepts de base sont presque universels.

Ce manuel aborde ces concepts essentiels de manière à aider votre parlement à élaborer un programme de sécurité concret basé sur des solutions pratiques et des applications concrètes.

Ce manuel s'efforce de fournir des options et des suggestions gratuites ou à très faible coût. N'oubliez pas que le coût le plus important associé à la mise en œuvre d'un programme de sécurité efficace sera le temps dont vous et le personnel, les membres, et les équipes du parlement aurez besoin pour discuter, vous familiariser et mettre en œuvre votre nouveau programme. Toutefois, compte tenu des risques auxquels votre parlement est susceptible d'être confronté, cet investissement sera plus que rentable.

Dans chaque section, vous trouverez une explication d'un sujet clé que votre parlement et son personnel doivent connaître, ce qu'il est et pourquoi il est important. Chaque sujet est associé à des stratégies essentielles, des approches et des outils recommandés pour limiter votre risque, ainsi qu'à des conseils et des liens renvoyant à des ressources supplémentaires qui peuvent vous aider à mettre en œuvre ces recommandations au sein de votre parlement.



Kit de démarrage du programme de sécurité

Pour aider votre parlement à assimiler les leçons du manuel et à les transformer en un véritable programme, servez-vous de ce kit de démarrage. Vous pouvez soit imprimer le kit, soit le remplir numériquement pendant que vous lisez le manuel en ligne. Lorsque vous prenez des notes et que vous commencez à mettre à jour ou à élaborer votre programme de sécurité, veillez à vous référer aux « éléments constitutifs du programme de sécurité » détaillés dans chaque section. Aucun programme de sécurité n'est complet sans qu'au moins ces éléments essentiels ne soient pris en compte.

Profitez également d'autres ressources qui peuvent vous aider à élaborer et à mettre en œuvre votre programme. Utilisez des ressources de formation gratuites comme le Security Planner de Consumer Reports, l'Umbrella app de Security First, le Totem Project de Free Press Unlimited et Greenhost et le Global Cyber Alliance Cybersecurity Toolkit for Mission-Based Organizations, qui comprend des ressources sur de nombreuses bonnes pratiques mentionnées dans ce manuel et des liens vers des dizaines d'outils de formation pour vous aider à mettre en œuvre de nombreux éléments fondamentaux.

Instaurer une culture de la sécurité

La sécurité concerne les personnes, et pour protéger votre parlement, vous devez vous assurer que toutes les personnes impliquées - y compris les députés, le personnel de soutien législatif et le personnel des services de recherche, et le personnel administratif des finances, des ressources humaines et de l'informatique, entre autres - prennent la cybersécurité au sérieux. Le changement de culture n'est pas chose facile, mais quelques mesures simples et des conversations importantes peuvent contribuer à créer une atmosphère qui renforcera la résilience de votre personnel et de votre parlement face aux menaces de sécurité. L'une des mesures les plus simples, mais aussi les plus importantes, à prendre pour instaurer cette culture de la sécurité parlementaire est de communiquer à ce sujet au sein de l'ensemble du parlement,et à faire en sorte que les dirigeants donnent toujours l'exemple et s'investissent dans un bon comportement.

Instaurer une culture de la sécurité au sein des parlements

En février 2019, l'Australie a subi une cyberattaque qui a compromis les réseaux du parlement national australien et de trois principaux partis politiques. Les attaquants ont pu accéder aux documents politiques et à la correspondance privée par courrier électronique entre les députés, leur personnel et leurs électeurs. L'attaque a eu lieu trois mois seulement avant la tenue des élections, soulignant la vulnérabilité des réseaux non sécurisés pendant les élections.

En réponse à cette attaque importante et réussie, le parlement a entrepris des efforts pour améliorer sa préparation à la cybersécurité. Ces investissements comprenaient l'enquête du Comité mixte des comptes publics et des audits sur la cyber-résilience du Commonwealth. L'enquête **s'est appuyée sur les conclusions d'audits** menés sur plusieurs années qui ont révélé que des processus d'atténuation des risques de cybersécurité faisaient défaut au sein du parlement et d'autres agences gouvernementales. Par exemple, le National Audit Office australien a souligné l'incapacité du parlement à se concentrer sur des objectifs stratégiques à long terme et à développer une approche basée sur les risques en matière de cybersécurité. Et bien que l'enquête et les audits n'aient pas été flatteurs, la volonté du parlement d'identifier les problèmes de cybersécurité et d'investir pour les résoudre est un exemple d'instauration d'une culture propice à une cybersécurité parlementaire efficace. Une culture qui commence par reconnaître les problèmes et investir dans des solutions techniques et humaines, où la sécurité n'est pas évitée mais plutôt priorisée. Par exemple, grâce au recrutement d'une équipe de « renforcement de la cybersécurité » et à un investissement budgétaire pour un **« Fonds de réponse à la cybersécurité »**, le parlement (et d'autres entités gouvernementales) devrait être mieux équipé pour atténuer les futures attaques si ces ressources sont correctement déployées, soutenues et si l'accent reste mis sur la cybersécurité en tant qu'élément régulier des opérations parlementaires. Cela dit, il est bien sûr préférable de renforcer cet engagement envers la sécurité au sein de votre parlement *avant* qu'une violation de sécurité importante ne se produise.

Intégrer la sécurité dans votre structure opérationnelle courante

Comme cela est décrit en détail dans le Holistic Security Guide de Tactical Tech, il est essentiel de créer des espaces réguliers et sûrs pour parler des différents aspects de la sécurité.

Ainsi, si le personnel et les membres ont des préoccupations en matière de sécurité, ils auront moins peur de paraître paranoïaques ou de faire perdre du temps aux autres. **Le fait de prévoir des conversations régulières sur la sécurité** normalise également la fréquence de l'interaction et de la réflexion sur les questions relatives à la sécurité, de sorte que les problèmes ne sont pas oubliés et que le personnel de toutes les équipes soit plus susceptible de faire preuve ne serait-ce que d'une sensibilisation passive en matière de sécurité dans leur travail en cours. Il n'est pas nécessaire de le faire chaque semaine, mais faites-en un rappel récurrent. Ces discussions ne doivent pas seulement laisser de la place aux sujets de sécurité technique, mais aussi aux questions qui ont un impact sur le confort et la sécurité du personnel, comme le harcèlement en ligne (et hors ligne) ou les problèmes liés à l'utilisation et à la mise en place d'outils numériques au sein des bureaux parlementaires. Les conversations peuvent même porter sur des sujets tels que les habitudes de partage des informations hors ligne et la manière dont le personnel sécurise ou non les informations en dehors du parlement. Après tout, il est important de se rappeler que la sécurité d'un parlement est aussi forte que son maillon le plus faible. Il est possible d'obtenir un engagement constant en ajoutant la sécurité à l'ordre du jour d'une réunion régulière. Vous pouvez également faire tourner la responsabilité de l'organisation et de l'animation d'une discussion sur la sécurité entre différents membres du personnel, ce qui peut contribuer à développer l'idée que la sécurité est la responsabilité de tous et pas seulement celle de quelques privilégiés ou de « l'équipe informatique ». Lorsque vous commencerez à formaliser les discussions sur la sécurité, les membres du personnel se sentiront probablement plus à l'aise pour discuter de ces questions importantes entre eux, ainsi que dans des cadres moins formels.

Il est également important d'intégrer des éléments de sécurité dans le fonctionnement normal du parlement, par exemple lors de l'intégration des membres et du personnel, et de penser à couper l'accès aux systèmes lors des départs d'employés. La sécurité ne doit pas être considérée comme une préoccupation supplémentaire, mais plutôt comme une ***partie intégrante de votre stratégie et de vos opérations.***

N'oubliez pas que tous les programmes de sécurité doivent être considérés comme des documents vivants et doivent être réévalués et rediscutés régulièrement, notamment lorsque le contexte de sécurité évolue.

Prévoyez de revoir votre stratégie et de la mettre à jour chaque année, ou en cas de changements majeurs au niveau de la stratégie, des outils ou des menaces auxquelles vous êtes confronté.

Obtenir l'adhésion de l'organisation

Une culture de la sécurité qui a du succès repose également sur l'adhésion de l'ensemble de votre parlement à votre programme de sécurité.

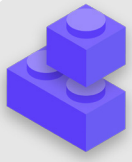
Il est essentiel d'obtenir le soutien et les conseils de la direction qui, dans de nombreux cas, prendra la décision finale d'allouer du temps, des ressources et de l'énergie au développement et à la mise en œuvre d'un programme de sécurité efficace. S'ils ne le prennent pas au sérieux, personne d'autre ne le fera. Pour obtenir cette adhésion réfléchissez bien au moment et à la manière de présenter votre programme, faites-le de manière claire, assurez-vous que la direction confirme les messages et guidez tout le monde à travers les éléments et les étapes du programme afin qu'il n'y ait pas de mystère ou de confusion sur ce que vous essayez d'atteindre. Assurez-vous également de prévoir un budget approprié pour la cybersécurité dans l'ensemble du parlement. Même si les moyens financiers sont limités, il est essentiel d'investir de manière appropriée dans la cybersécurité, faute de quoi d'autres investissements risquent d'être mis en péril. Lorsque vous parlez de sécurité, évitez les discours alarmistes. Parfois, les menaces auxquelles votre parlement et votre personnel sont confrontés peuvent être alarmantes, mais essayez de vous concentrer sur le partage des faits et de créer un espace de tranquillité pour les questions et les préoccupations. Si vous rendez les dangers trop menaçants, les gens risquent de considérer que vous faites du sensationnalisme ou vont tout simplement laisser tomber, pensant que rien de ce qu'ils font n'a d'importance, et rien n'est plus faux.

Établir un programme de formation

Une fois que vous avez élaboré un programme et que vous vous y êtes engagé, réfléchissez à la manière dont vous allez former tout les membres, le personnel et les bénévoles à ces nouvelles bonnes pratiques.

Exiger une formation régulière et rendre la participation à la formation obligatoire peut être une tactique efficace. Évitez de faire supporter des conséquences sévères et négatives au personnel qui a du mal à comprendre les concepts de sécurité. N'oubliez pas que certains membres du personnel peuvent s'adapter et apprendre la technologie différemment des autres, en fonction de leur niveau de familiarité avec les outils numériques et l'internet. La peur de l'échec ne fait que dissuader davantage le personnel de signaler les problèmes ou de demander de l'aide. Cependant, en instaurant une responsabilité positive et en récompensant les formations réussies et l'adoption des politiques, il est possible de favoriser l'amélioration au sein de le parlement. Vous pouvez obtenir un soutien supplémentaire précieux par le biais de réseaux locaux ou internationaux de formation à la sécurité numérique et de ressources de formation gratuites telles que l'application Umbrella de Security First, le Totem Project de Free Press Unlimited et Greenhost, et le Global Cyber Alliance Learning Portal.

Réfléchissez à la manière dont votre programme de formation peut atteindre les députés, le personnel parlementaire et l'administration parlementaire. Gardez à l'esprit que les membres éminents nécessitent souvent encore plus de formation et d'attention en matière de sécurité en raison de leur profil élevé. Assurez-vous que votre programme de formation et votre programme de sécurité s'appliquent à tous ces différents types d'individus et à tous les actifs qu'ils peuvent avoir à l'intérieur et à l'extérieur. du parlement.



Instaurer une culture de la sécurité

- **Prévoyez des conversations et des formations régulières sur la sécurité et votre programme de sécurité.**
- **Faites participer tout le monde : répartissez la responsabilité de la mise en œuvre de votre programme de sécurité au sein de tout le parlement.**
- **Veillez à ce que les dirigeants adoptent un bon comportement en matière de sécurité et s'engagent à respecter votre programme.**
- **Évitez les tactiques de crainte ou les punitions : récompensez les avancées et créez un espace confortable pour que le personnel puisse signaler les problèmes et demander de l'aide.**
- **Mettez à jour votre programme de sécurité chaque année ou après des changements majeurs dans le personnel parlementaire, la structure ou l'environnement opérationnel.**

Une base solide : Sécurisation des comptes et des appareils

Pourquoi se concentrer sur les comptes et les appareils ? Parce qu'ils constituent la base de tout ce que votre parlement fait sur le plan numérique.

Il est presque certain que vous accédez à des informations sensibles, que vous communiquez en interne et en externe et que vous sauvegardez des informations privées avec ces appareils et comptes. Il suffit de considérer la participation des membres aux sessions plénières, au vote (y compris virtuel), aux processus de rédaction législative et à la communication avec les membres du personnel et le grand public. En l'absence de comptes et d'appareils sécurisés, ces opérations parlementaires cruciales et bien d'autres encore peuvent être mises en péril. Par exemple, si des pirates surveillent vos frappes au clavier ou écoutent votre micro, les conversations privées avec vos collègues seront capturées, quel que soit le niveau de sécurité de vos applications de messagerie. Ou, si un adversaire accède aux comptes de réseaux sociaux de votre parlement, il pourrait facilement porter atteinte à votre réputation et à votre crédibilité, compromettant ainsi la confiance du public. Il est donc essentiel, en tant que parlement, de veiller à ce que chacun prenne des mesures simples mais efficaces pour sécuriser ses appareils et ses comptes. Il est important de noter que ces recommandations concernent également les comptes et les appareils personnels, qui sont souvent des cibles faciles pour les adversaires. Les pirates s'attaqueront volontiers à la cible la plus facile et pénétreront dans un compte personnel ou un ordinateur personnel si les membres et le personnel les utilisent pour communiquer et accéder à des informations importantes.

Comptes sécurisés et parlements

Le piratage largement médiatisé de SolarWinds révélé fin 2020, qui a compromis plus de 250 organisations, dont la plupart des départements du gouvernement des États-Unis, des fournisseurs de technologie comme Microsoft et Cisco, et des ONG, était en partie le résultat de pirates devinant des mots de passe faibles qui étaient utilisés sur des comptes administrateurs importants. Globalement, environ 80 % de toutes les violations liées au piratage informatique sont dues à des mots de passe faibles ou réutilisés.

Compte tenu de la prévalence croissante des violations de mots de passe de ce type et de l'accès plus facile de toutes sortes d'adversaires à des outils sophistiqués de piratage de mots de passe, les meilleures pratiques en matière de mots de passe et une authentification à deux facteurs sont des impératifs de sécurité pour toutes les organisations, notamment les parlements. Aucun incident n'illustre plus clairement cela que l'attaque de 2017 contre le système de messagerie électronique du Parlement britannique. Dans cet incident, les mauvaises pratiques en matière de mots de passe d'un nombre restreint mais significatif de députés ont conduit à l'exposition de comptes de messagerie et de conversations, à la fuite de milliers d'informations d'identification et à une perturbation considérable des activités parlementaires. Selon le service de presse du parlement britannique, les comptes piratés ont été « compromis en raison de mots de passe faibles qui n'étaient pas conformes aux directives émises par le service numérique parlementaire ».

Sécurité des comptes : Mots de passe et authentification à deux facteurs

De nos jours, il est probable que votre parlement et son personnel disposent de dizaines, voire de centaines de comptes qui, en cas de violation, pourraient exposer des informations sensibles ou même porter préjudice à des personnes à risque.

Pensez aux différents comptes dont disposent les membres du personnel et le parlement dans son ensemble : courriel, applications de chat, réseaux sociaux, banque en ligne, stockage de données dans le nuage, ainsi que les boutiques de vêtements, les restaurants locaux, les journaux et de nombreux autres sites Web ou applications auxquels vous vous connectez. Aujourd'hui, pour assurer une bonne sécurité, il faut adopter une approche diligente afin de protéger tous ces comptes contre des attaques. Cela commence par une bonne gestion des mots de passe et l'utilisation par tous d'une authentification à deux facteurs.

QU'EST-CE QUI FAIT UN BON MOT DE PASSE ?

Il y a trois clés pour un bon mot de passe fort : la longueur, le caractère aléatoire et l'unicité.

LONGUEUR	Plus le mot de passe est long, plus il est difficile pour un adversaire de le deviner. La plupart des piratages de mots de passe sont désormais effectués par des programmes informatiques et il ne faut pas longtemps à ces programmes malveillants pour craquer un mot de passe court. Par conséquent, il est essentiel que vos mots de passe comportent au moins 16 caractères, ou au moins cinq mots, et qu'ils soient de préférence plus longs.
CARACTÈRE ALÉATOIRE	Même si un mot de passe est long, il n'est pas très efficace s'il s'agit de quelque chose qu'un adversaire peut facilement deviner à votre sujet. Évitez d'inclure des informations telles que votre date de naissance, votre ville natale, vos activités préférées ou d'autres faits que quelqu'un pourrait découvrir à votre sujet en effectuant une recherche rapide sur Internet.
UNICITÉ	La mauvaise pratique la plus courante en matière de mot de passe consiste à utiliser le même mot de passe pour plusieurs sites. La répétition des mots de passe est un gros problème car cela signifie que lorsqu'un seul de ces comptes est compromis, tous les autres comptes utilisant ce même mot de passe sont également vulnérables. Si vous utilisez la même phrase de passe sur plusieurs sites, cela peut augmenter considérablement l'impact d'une erreur ou d'une violation de données. Vous ne vous souciez peut-être pas du mot de passe que vous utilisez pour accéder à la bibliothèque locale, mais si celui-ci est piraté et que vous utilisez le même mot de passe sur un compte plus sensible, des informations importantes pourraient être volées.

Un moyen facile d'atteindre ces objectifs de longueur, de caractère aléatoire et d'unicité est de choisir trois ou quatre mots communs mais aléatoires. Par exemple, votre mot de passe pourrait être « fleur lampe vert ours », qui est facile à retenir mais difficile à deviner. Vous pouvez consulter ce site de Better Buys pour voir une estimation de la vitesse à laquelle les mots de passe faibles peuvent être piratés.

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE POUR VOUS AIDER

Vous savez donc qu'il est important que chaque membre du parlement utilise un mot de passe long, aléatoire et différent pour chacun de ses comptes personnels et parlementaires, mais comment faire concrètement ? Il est impossible de mémoriser un mot de passe efficace pour des dizaines (voire des centaines) de comptes, ce qui oblige tout le monde à tricher. La mauvaise chose à faire est de réutiliser les mots de passe. Heureusement, nous pouvons nous tourner vers les gestionnaires de mots de passe numériques pour nous faciliter la vie (et rendre nos pratiques en matière de mots de passe beaucoup plus sûres). Ces applications, dont beaucoup sont accessibles via un ordinateur ou un appareil mobile, peuvent créer, stocker et gérer des mots de passe pour vous et toute votre organisation. L'adoption d'un gestionnaire de mots de passe sécurisé signifie que vous n'aurez jamais à vous souvenir que d'un seul mot de passe très fort et long, appelé mot de passe principal (historiquement appelé mot de passe « maître »), tout en bénéficiant des avantages de sécurité liés à l'utilisation de mots de passe forts uniques pour tous vos comptes. Vous utiliserez ce mot de passe principal (et idéalement un deuxième facteur d'authentification (2FA), qui sera abordé dans la section suivante) pour ouvrir votre gestionnaire de mots de passe et débloquer l'accès à tous vos autres mots de passe. Les gestionnaires de mots de passe peuvent également être partagés entre plusieurs comptes afin de faciliter le partage sécurisé des mots de passe au sein de votre parlement.

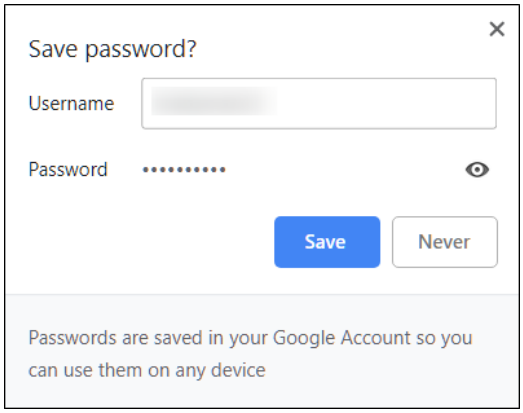
Pourquoi devons-nous utiliser quelque chose de nouveau ? Ne pouvons-nous pas simplement les écrire sur papier ou dans une feuille de calcul sur notre ordinateur ?

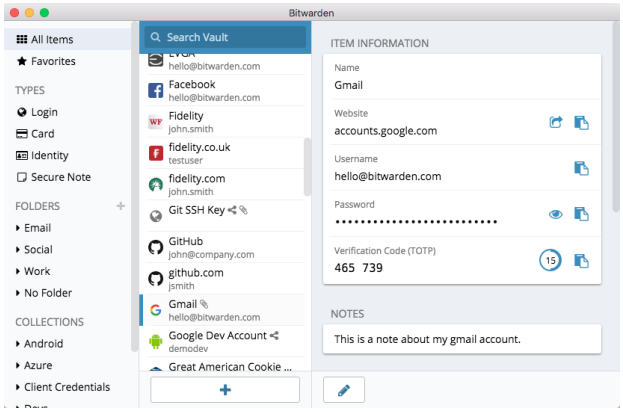
Malheureusement, de nombreuses approches courantes de la gestion des mots de passe ne sont pas sûres. Le stockage des mots de passe sur des feuilles de papier (à moins que vous ne les gardiez enfermés dans un coffre-fort) peut les exposer au vol physique, aux regards indiscrets, à la perte et à des dommages faciles. Si vous enregistrez vos mots de passe dans un document sur votre ordinateur, il est beaucoup plus facile pour un pirate d'y accéder (ou pour une personne qui vole votre ordinateur d'avoir non seulement votre appareil mais aussi l'accès à tous vos comptes). L'utilisation d'un bon gestionnaire de mots de passe est tout aussi simple, mais beaucoup plus sûre.

Pourquoi faire confiance à un gestionnaire de mots de passe ?

Les gestionnaires de mots de passe de qualité déploient des efforts considérables (et emploient d'excellentes équipes de sécurité) afin de garantir la sécurité de leurs systèmes. Les bonnes applications de gestion des mots de passe (nous en recommandons quelques-unes ci-dessous) sont également configurées de manière à ce qu'elles ne puissent pas « déverrouiller » vos comptes. Cela signifie que, dans la plupart des cas, même s'ils étaient piratés ou contraints légalement de transmettre des informations, ils ne pourraient pas perdre ou donner vos mots de passe. Il est également important de se rappeler qu'il est infiniment plus probable qu'un adversaire devine l'un de vos mots de passe faibles ou répétés, ou en trouve un via une violation de données à caractère publique, plutôt que de voir un bon gestionnaire de mots de passe voir ses systèmes de sécurité violés. Il est important d'être sceptique et de ne pas faire aveuglément confiance à tous les logiciels et applications, mais les gestionnaires de mots de passe réputés ont toutes les raisons de faire les choses correctement.

Au lieu d'utiliser votre navigateur (comme Chrome, affiché à gauche) pour enregistrer vos mots de passe, utilisez un gestionnaire de mots de passe dédié (comme Bitwarden, affiché à droite). Les gestionnaires de mots de passe ont des fonctions qui rendent la vie à la fois plus sûre et plus pratique pour votre parlement.





Qu'en est-il du stockage des mots de passe via un navigateur ?

Enregistrer des mots de passe dans votre navigateur ne revient pas à utiliser un gestionnaire de mots de passe sécurisé. En bref, vous ne devez pas utiliser Chrome, Firefox, Safari ou tout autre navigateur comme gestionnaire de mots de passe. Bien qu'il s'agisse d'un progrès certain par rapport à l'écriture sur papier ou à l'enregistrement dans une feuille de calcul, les fonctions de base de sauvegarde des mots de passe de votre navigateur web laissent à désirer du point de vue de la sécurité. Ces inconvénients vous privent également d'une grande partie des avantages qu'apporte un bon gestionnaire de mots de passe. En perdant cette commodité, il est plus probable que les parlementaires continueront à avoir des pratiques médiocres en matière de création et de partage de mots de passe.

Par exemple, contrairement aux gestionnaires de mots de passe spécialisés, les fonctions intégrées des navigateurs « Enregistrer ce mot de passe » ou « Se souvenir de ce mot de passe » n'offrent pas de compatibilité mobile simple, de fonctionnalité inter-navigateurs, ni d'outils puissants de génération et d'audit de mots de passe. Ces fonctionnalités sont en grande partie à l'origine de l'utilité d'un gestionnaire de mots de passe dédié et de son intérêt pour la sécurité de votre parlement. Les gestionnaires de mots de passe comprennent également des fonctions spécifiques à le parlement (telles que le partage de mots de passe) qui apportent non seulement une valeur de sécurité individuelle, mais aussi une valeur pour votre parlement dans son ensemble. Si vous avez enregistré des mots de passe avec votre navigateur (intentionnellement ou non), prenez un moment pour les supprimer.

Quel gestionnaire de mots de passe faut-il utiliser ?

Il existe de nombreux bons outils de gestion des mots de passe qui peuvent être configurés en moins de 30 minutes. Si vous recherchez une option en ligne fiable pour votre parlement, à laquelle les personnes peuvent accéder à partir de plusieurs appareils et à tout moment, 1Password (à partir de $2,99 USD par utilisateur et par mois) ou le logiciel à code source ouvert Bitwarden sont tous deux solutions bien prises en charge et recommandées. Une option en ligne comme Bitwarden peut s'avérer très utile en termes de sécurité et de praticité. Bitwarden, par exemple, vous aidera à créer des mots de passe uniques et forts et à accéder à vos mots de passe depuis plusieurs appareils grâce à des extensions de navigateur et une application mobile.

Avec la version payante ($10 USD pour une année complète), Bitwarden fournit également des rapports sur les mots de passe réutilisés, faibles et éventuellement violés pour vous aider à ne pas perdre le contrôle sur vos mots de passe. Une fois que vous avez configuré votre mot de passe principal (appelé mot de passe maître), vous devez également activer l'authentification à deux facteurs pour que le coffre-fort de votre gestionnaire de mots de passe soit aussi sécurisé que possible.

Il est essentiel de **suivre certaines règles de sécurité lors de l'utilisation de votre gestionnaire de mots de passe.** Par exemple, si vous utilisez l'extension de navigateur de votre gestionnaire de mots de passe ou si vous vous connectez à Bitwarden (ou à tout autre gestionnaire de mots de passe) sur un appareil, n'oubliez pas de vous déconnecter après utilisation si vous partagez cet appareil ou si vous pensez être exposé à un risque élevé quant au vol de votre appareil. Cela inclut la déconnexion de votre gestionnaire de mots de passe si vous laissez un ordinateur ou un appareil mobile sans surveillance. Si vous partagez des mots de passe au sein de vos équipes et de votre parlement, veillez également à révoquer l'accès aux mots de passe (et à modifier les mots de passe eux-mêmes) lorsque des personnes quittent le parlement. Vous ne voulez pas qu'un ancien membre du personnel conserve l'accès au mot de passe Facebook de votre parlement, par exemple.

Que faire si quelqu'un oublie son mot de passe principal ?

Il est essentiel de se souvenir de votre mot de passe principal. Les bons systèmes de gestion des mots de passe, comme ceux recommandés ci-dessus, ne mémoriseront pas votre mot de passe principal pour vous et ne vous permettront pas de le réinitialiser directement par courriel, comme c'est le cas pour les sites web. Il s'agit d'un bon dispositif de sécurité, mais il est également essentiel de mémoriser votre mot de passe principal lorsque vous configurez votre gestionnaire de mots de passe pour la première fois. Pour vous aider, pensez à mettre en place un rappel quotidien pour vous rappeler votre mot de passe principal lorsque vous créez pour la première fois un compte de gestion de mots de passe.

Utilisation d'un gestionnaire de mots de passe pour votre parlement

Vous pouvez renforcer les pratiques de votre parlement en matière de mots de passe et vous assurer que tous les membres du personnel ont accès à un gestionnaire de mots de passe (et l'utilisent) en en mettant un en place au sein de toute le parlement. Au lieu de demander à chaque membre du personnel de créer son propre programme, envisagez d'investir dans un programme pour équipes ou pour entreprises. Par exemple, le programme « organisation d'équipes » de Bitwarden coûte 3 $ par utilisateur et par mois. Avec ce programme (ou d'autres programmes d'équipe de gestionnaires de mots de passe comme 1Password), vous avez la possibilité de gérer tous les mots de passe partagés au sein de l'« organisation ». Les fonctionnalités d'un gestionnaire de mots de passe à l'échelle du parlement ou de l'équipe offrent non seulement une plus grande sécurité, mais aussi une plus grande praticité pour le personnel. Vous pouvez partager en toute sécurité des informations d'identification au sein du gestionnaire de mots de passe lui-même, vers différents comptes d'utilisateurs. Bitwarden, par exemple, propose également une fonction pratique de partage de fichiers et de textes chiffrés de bout en bout, appelée « Bitwarden Send », dans le cadre de son programme pour équipes. Ces deux fonctionnalités permettent à votre parlement de mieux contrôler qui peut voir et partager quels mots de passe, et offrent une option plus sûre pour le partage des informations d'identification pour les comptes d'équipes ou de groupes. Si vous mettez en place un gestionnaire de mots de passe à l'échelle de votre parlement, veillez à ce qu'une personne soit spécifiquement chargée de supprimer les comptes du personnel et de modifier les mots de passe partagés lorsqu'une personne quitte l'équipe.

QU'EST-CE QUE L'AUTHENTIFICATION À DEUX FACTEURS ?

Quelle que soit la qualité de votre politique en matière de mots de passe, il n'est que trop fréquent que les pirates informatiques contournent les mots de passe. Une autre couche de protection est nécessaire pour protéger vos comptes contre certaines menaces courantes du monde moderne. C'est là qu'intervient l'authentification multifactorielle ou bifactorielle, appelée MFA ou A2F.

Il existe de nombreux guides et ressources intéressantes qui vous renseignent sur l'authentification à deux facteurs, notamment l'article **Authentification à deux facteurs pour les débutants** de Martin Shelton et le **guide pratique de cybersécurité électorale 101** du Center for Democracy & Technology. Cette section s'inspire largement de ces deux ressources pour expliquer pourquoi il est si important de mettre en place une authentification à deux facteurs au sein du parlement.

En bref, le système A2F renforce la sécurité des comptes en exigeant une deuxième information (quelque chose de plus qu'un simple mot de passe) pour obtenir l'accès. Le deuxième élément d'information est généralement quelque chose que vous possédez, comme un code provenant d'une application sur votre téléphone ou un jeton ou une clé physique.

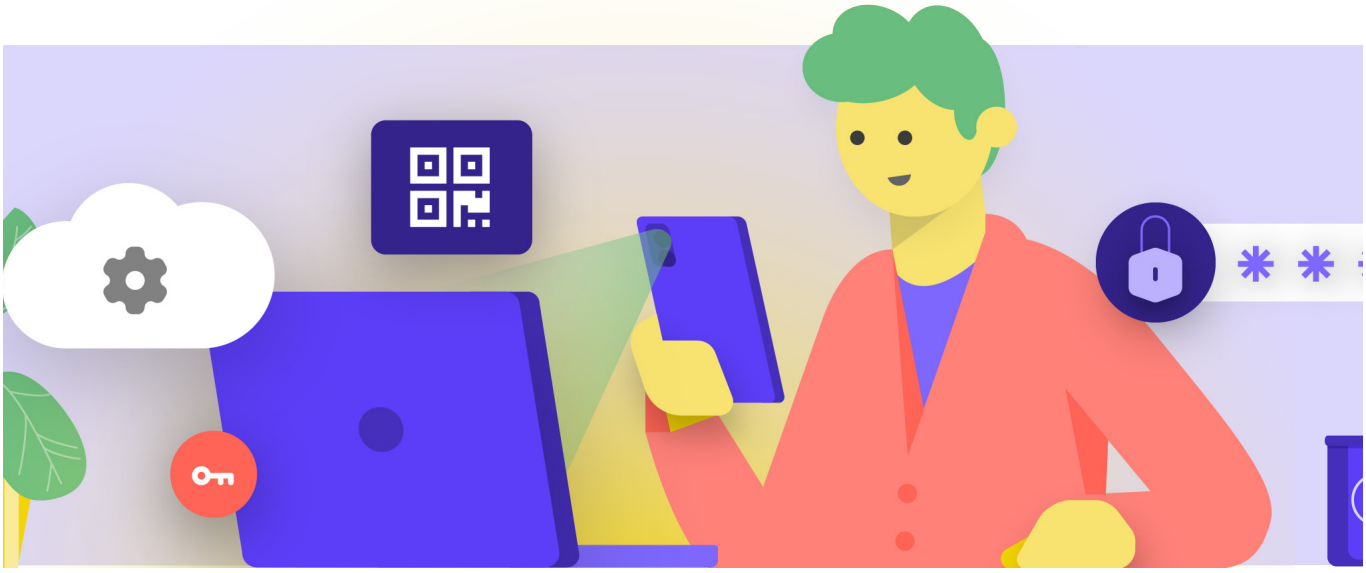
Ce deuxième élément d'information agit comme une deuxième couche de protection. Si un pirate informatique vole votre mot de passe ou y accède via une fuite de mots de passe provenant d'une importante violation de données, un système 2FA efficace peut l'empêcher d'accéder à votre compte (et donc à des informations privées et sensibles). Il est essentiel de veiller à ce que chaque membre du parlement mette en place le système A2F sur ses comptes.

COMMENT CONFIGURER 2FA ?

Il existe trois méthodes courantes pour le A2F : les clés de sécurité, les applications d'authentification et les codes SMS à usage unique.

Clés de sécurité

Les clés de sécurité sont la meilleure option, en partie parce qu'elles sont presque totalement à l'abri du hameçonnage. Ces « clés » sont des jetons matériels (de type mini clé USB) qui peuvent être attachés à votre trousseau de clés (ou rester dans votre ordinateur) pour être facilement accessibles et conservés. Lorsque le moment est venu d'utiliser la clé pour déverrouiller un compte donné, il suffit de l'insérer dans votre appareil et de la toucher physiquement lorsque vous y êtes invité lors de la connexion. Il existe un large éventail de modèles que vous pouvez acheter en ligne (20-50 USD), notamment les très réputés **YubiKeys**. Le Wirecutter du New York Times propose un **guide utile** avec quelques recommandations sur les clés à acheter. N'oubliez pas que la même clé de sécurité peut être utilisée pour autant de comptes que vous le souhaitez.



Applications d'authentification

Les **applications d'authentification constituent la deuxième meilleure option pour le A2F.** Ces services vous permettent de recevoir un code de connexion temporaire à deux facteurs par le biais d'une application mobile ou d'une notification push sur votre smartphone. Parmi les options populaires et fiables figurent Google Authenticator, Authy et Duo Mobile. Les applications d'authentification sont également excellentes car elles fonctionnent lorsque vous n'avez pas accès à votre réseau cellulaire et sont gratuites pour les particuliers. Toutefois, les applications d'authentification sont plus exposées à l'hameçonnage que les clés de sécurité, car les utilisateurs peuvent être incités à saisir les codes de sécurité d'une application d'authentification sur un faux site web. Veillez à ne saisir les codes de connexion que sur des sites Web légitimes. Et n'acceptez pas les notifications push de connexion si vous n'êtes pas sûr d'être l'auteur de la demande de connexion. Il est également essentiel, lorsque vous utilisez une application d'authentification, de disposer de codes de sauvegarde (voir ci-dessous) en cas de perte ou de vol de votre téléphone.

Codes par SMS

SMS Les codes envoyés par SMS sont la forme la moins sûre, mais malheureusement encore la plus courante, du système A2F. Étant donné que les SMS peuvent être interceptés et que les numéros de téléphone peuvent être usurpés ou piratés via votre opérateur mobile, les SMS laissent beaucoup à désirer comme méthode de demande de codes 2FA. C'est mieux que d'utiliser uniquement un mot de passe, mais les applications d'authentification ou une clé de sécurité physique sont recommandées dans la mesure du possible. Un adversaire déterminé peut avoir accès aux codes SMS A2F, généralement en appelant la compagnie de téléphone et en échangeant votre carte SIM. Lorsque vous êtes prêt à commencer à activer le A2F pour tous les différents comptes de votre parlement, utilisez ce site web (https://2fa.directory/) pour rechercher rapidement des informations et des instructions pour des services spécifiques (comme Gmail, Office 365, Facebook, Twitter, etc.) et pour voir quels services autorisent quels types de A2F.

2FA et parlements

Selon des rapports de l'année 2020, des pirates ont infiltré le système de messagerie parlementaire norvégien, compromettant les comptes de messagerie appartenant à plusieurs responsables parlementaires et téléchargeant même certaines informations des systèmes parlementaires. Bien que tous les détails du piratage n'aient pas été rendus publics, la Norvège a attribué l'intrusion à APT28, un groupe de piratage affilié aux services de sécurité russes. Bien que très sophistiqués, APT28 et d'autres pirates utilisent souvent des tactiques moins complexes telles que les « attaques par force brute » (dans lesquelles l'attaquant utilise des outils pour essayer de nombreux mots de passe dans l'espoir de deviner éventuellement le bon) pour accéder au compte. Cette tactique permet aux pirates de deviner même des mots de passe solides, comme cela a été supposé être le cas en Norvège. La bonne nouvelle? Ces types d'attaques ont beaucoup moins de chances de réussir si l'on dispose d'une clé appropriée ou d'un système d'authentification à deux facteurs basé sur une application !

Les clés de sécurité dans le monde réel

En fournissant des clés de sécurité physique pour l'authentification à deux facteurs à plus de 85 000 de ses employés, Google (une organisation à très haut risque et très ciblée) a effectivement neutralisé toute attaque de hameçonnage réussie contre l'organisation. Ce cas montre à quel point les clés de sécurité peuvent être efficaces, même pour les organisations les plus à risque.

QUE SE PASSE-T-IL SI QUELQU'UN PERD UN DISPOSITIF A2F ?

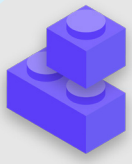
Si vous utilisez une clé de sécurité, traitez-la de la même manière que la clé de votre maison ou de votre appartement, si vous en avez un/une. En bref, ne la perdez pas. Comme pour les clés de votre maison, il est toujours bon d'avoir une clé de secours enregistrée sur votre compte, qui reste enfermée dans un endroit sûr (comme un coffre-fort à la maison ou une boîte de dépôt sécurisée), juste en cas de perte ou de vol. Sinon, vous devriez créer des codes de sauvegarde pour les comptes qui le permettent. Vous devez conserver ces codes dans un endroit très sûr, comme votre gestionnaire de mots de passe ou un coffre-fort physique. Ces codes de sauvegarde peuvent être générés à partir des paramètres A2F de la plupart des sites (au même endroit où vous activez le A2F en premier lieu), et peuvent servir de clé de secours en cas d'urgence. Le problème le plus courant avec le système A2F se produit lorsque les gens remplacent ou perdent les téléphones qu'ils utilisent pour les applications d'authentification. Si vous utilisez Google Authenticator, vous êtes condamné si votre téléphone est volé, à moins que vous ne sauvegardiez les codes de sauvegarde générés au moment où vous connectez un compte à Google Authenticator. Par conséquent, si vous utilisez Google Authenticator comme application A2F, veillez à enregistrer les codes de sauvegarde de tous les comptes que vous connectez dans un endroit sûr. Si vous utilisez Authy ou Duo, ces deux applications ont des fonctions de sauvegarde intégrées avec des paramètres de sécurité forts que vous pouvez activer. Si vous choisissez l'une ou l'autre de ces applications, vous pouvez configurer ces options de sauvegarde en cas de bris, de perte ou de vol de votre appareil. Consultez les instructions d'Authy ici et celles de Duo ici. Veillez à ce que chacun connaisse ces étapes lorsqu'il commencera à activer le 2FA sur l'ensemble de ses comptes.

Mettre en place le 2FA au sein de votre parlement

Si votre parlement fournit des comptes e-mail à l'ensemble du personnel par l'intermédiaire de Google Workspace (anciennement connu sous le nom de GSuite) ou de Microsoft 365 en utilisant votre propre domaine (par exemple, @ndi.org), vous pouvez appliquer le A2F et des paramètres de sécurité forts pour tous les comptes. Cette mise en application permet non seulement de protéger ces comptes, mais aussi d'introduire et de normaliser le 2FA auprès de vos membres et de votre personnel afin qu'il soit plus à l'aise pour l'adopter également pour ses comptes personnels.

En tant qu'administrateur de Google Workspace, vous pouvez suivre ces instructions pour appliquer le 2FA pour votre domaine. Vous pouvez faire quelque chose de similaire avec Microsoft 365 en suivant ces étapes en tant qu'administrateur de domaine.

Envisagez également d'inscrire les comptes de votre parlement au Programme Protection Avancée (Google) ou AccountGuard (Microsoft) pour appliquer des contrôles de sécurité supplémentaires et exiger des clés de sécurité physiques pour l'authentification à deux facteurs.



Sécurité des comptes

- **Exigez des mots de passe forts pour tous les comptes du parlement ; encouragez les membres, les employés et les bénévoles à faire de même pour leurs comptes personnels.**
- **Mettez en place un gestionnaire de mots de passe de confiance pour votre parlement (et encouragez son utilisation dans le cadre de la vie privée du personnel également).**
  - Exigez un mot de passe principal fort et un système A2F pour tous les comptes du gestionnaire de mots de passe.
  - Rappelez à chacun de se déconnecter du gestionnaire de mots de passe sur les appareils partagés ou lorsqu'il y a un risque élevé de vol ou de confiscation de l'appareil.
- **Modifiez les mots de passe partagés lorsque le personnel et les députés quittent le parlement.**
- **Ne partagez les mots de passe qu'en toute sécurité, par exemple via le gestionnaire de mots de passe de votre parlement ou des applications chiffrées de bout en bout.**
- **Exigez le A2F sur tous les comptes du parlement et encouragez le personnel à mettre en place le A2F sur tous les comptes personnels également.**
  - Si possible, fournissez des clés de sécurité physique à tout les membres et au personnel.
  - Si votre budget ne prévoit pas de clés de sécurité, encouragez l'utilisation d'applications d'authentification au lieu de SMS ou d'appels téléphoniques pour le A2F.
- **Organisez régulièrement des formations pour vous assurer que tout le monde connaisse les meilleures pratiques en matière de mot de passe et de A2F, notamment en ce qui concerne les caractéristiques d'un mot de passe fort et l'importance de ne jamais réutiliser les mots de passe, de n'accepter que les demandes A2F légitimes et de générer des codes A2F de secours.**

Sécurité des dispositifs

Outre les comptes, il est essentiel de garder tous les appareils (ordinateurs, téléphones, clés USB, disques durs externes, etc.) bien protégés.

Cette protection commence par une vigilance quant au type d'appareils que votre parlement et votre personnel achètent et utilisent. Les vendeurs ou fabricants auxquels vous faites confiance doivent justifier du respect des normes mondiales en matière de développement sécurisé de dispositifs matériels (téléphones et ordinateurs, par exemple). Tous les appareils que vous achetez doivent être fabriqués par des entreprises de confiance qui n'ont pas intérêt à remettre des données et des informations à un adversaire potentiel. Il est important de noter que le gouvernement chinois exige des entreprises chinoises qu'elles fournissent des données au gouvernement central. Par conséquent, malgré l'omniprésence et la présence à bas prix de smartphones comme le Huawei ou le ZTE, il convient de les éviter. Bien que le coût du matériel bon marché puisse être très attractif, les risques de sécurité potentiels pour les parlements devraient vous orienter vers d'autres options d'appareils et d'équipements.

Vos adversaires peuvent compromettre la sécurité de vos appareils (et de tout ce que vous faites à partir de ces appareils) en obtenant un accès physique ou un accès « à distance » à votre appareil.

Sécurité des appareils et parlements

Certains des logiciels malveillants les plus avancés au monde ont été développés et déployés dans le monde entier pour **cibler** les députés, d'autres responsables gouvernementaux et leur personnel. En Inde, par exemple, un consortium de journalistes **a révélé** que plusieurs députés et ministres du gouvernement étaient ciblés par le logiciel espion Pegasus, un type de logiciel malveillant qui a fait la une des journaux en 2020.

Pegasus est tristement célèbre pour sa capacité à infecter les appareils mobiles et à donner à l'agresseur la possibilité d'enregistrer de l'audio, d'intercepter les frappes et les messages et, en fait, de mettre la victime sous surveillance totale. sans nécessiter l'interaction de la victime. Cependant, la grande majorité des logiciels espions réussissent à compromettre leurs victimes.

ACCÈS PHYSIQUE À L'APPAREIL PAR PERTE OU VOL

Pour éviter toute compromission physique, il est essentiel de sécuriser physiquement vos appareils. En bref, ne facilitez pas la tâche d'un adversaire qui pourrait vous voler ou même vous enlever temporairement votre appareil. Gardez les appareils sous clé s'ils sont laissés à la maison ou au bureau. Gardez-les sur vous si vous pensez que c'est plus sûr. Cela signifie bien sûr que la sécurité des appareils passe en partie par la sécurité physique de vos espaces de travail (que ce soit dans un bureau ou à la maison). Vous devrez installer des serrures solides, des caméras de sécurité ou d'autres systèmes de surveillance. Rappelez au personnel qu'il doit traiter les appareils de la même manière qu'il traiterait une grosse pile d'argent, sans les laisser traîner sans surveillance ou sans protection.

Que se passe-t-il si un appareil est volé ?

Afin de limiter l'impact si quelqu'un parvenait à voler un appareil, ou même s'il n'y accédait que pour une courte période, veillez à **obliger l'utilisation de mots de passe ou de codes d'accès forts sur les ordinateurs et les téléphones de chacun.** Les mêmes conseils de mot de passe que ceux de la section Mots de passe de ce manuel s'appliquent à un mot de passe fort pour un ordinateur ou un portable. Lorsqu'il s'agit de verrouiller votre téléphone, utilisez des codes d'au moins six à huit chiffres et évitez d'utiliser des « combinaisons de glissement » pour déverrouiller l'écran. Pour obtenir des conseils supplémentaires sur les verrouillages d'écran, consultez le Data Detox Kit de Tactical Tech. En utilisant de bons mots de passe pour votre appareil, il est beaucoup plus difficile pour un adversaire d'accéder rapidement aux informations qu'il contient en cas de vol ou de confiscation. Assurez-vous que les appareils délivrés par le parlement sont également enregistrés dans un **système de gestion des appareils mobiles ou des points d'extrémité.** Bien qu'ils ne soient pas peu coûteux, ces systèmes permettent à votre parlement d'appliquer des politiques de sécurité sur tous les appareils, d'en localiser un et d'effacer son contenu potentiellement sensible en cas de vol, de perte ou de confiscation. Bien qu'il existe de nombreuses solutions différentes pour la gestion des appareils mobiles, quelques options fiables qui fonctionnent sur toutes les plates-formes (iPhone, Android, Mac et Windows) incluent Hexnode, Meraki Systems Manager de Cisco, IBMs MDM et la fonctionnalité intégrée de gestion des appareils mobiles de Google Workspace. Si le coût est un facteur limitant, il faut au moins encourager les députés et les membres du personnel à utiliser les fonctions intégrées « Trouver mon appareil » sur leurs smartphones personnels et ceux fournis par le parlement, comme Find My iPhone d'iPhone et Find My Device d'Android.

Qu'en est-il du chiffrement des appareils ?

Il est important d'utiliser le chiffrement, qui consiste à brouiller les données pour les rendre illisibles et inutilisables, sur tous les appareils, notamment les ordinateurs et les smartphones. Si possible, vous devez configurer tous les appareils de votre parlement avec un procédé appelé **chiffrement intégral du disque**. Le chiffrement intégral du disque permet de chiffrer l'intégralité d'un appareil, de sorte qu'un adversaire, s'il devait le voler physiquement, serait incapable d'en extraire le contenu sans connaître le mot de passe ou la clé que vous avez utilisés pour le chiffrer. De nombreux smartphones et ordinateurs modernes permettent de réaliser un chiffrement intégral de leur disque. Les appareils Apple tels que les iPhones et les iPads, de manière assez pratique, activent le chiffrement intégral du disque lorsque vous définissez un code d'accès normal pour l'appareil. Les ordinateurs Apple utilisant macOS sont dotés d'une fonction appelée FileVault que vous pouvez activer pour un chiffrement intégral du disque. Les ordinateurs Windows dotés de licences pro, entreprise ou éducation disposent d'une fonction appelée BitLocker que vous pouvez activer pour un chiffrement intégral du disque. Vous pouvez activer BitLocker en suivant ces instructions de Microsoft, qui peuvent devoir être préalablement activées par l'administrateur de votre organisation. Si le personnel ne dispose que d'une licence domestique pour ses ordinateurs Windows, BitLocker n'est pas disponible. Toutefois, il est toujours possible d'activer le chiffrement intégral du disque en allant dans « Mise à jour et sécurité » > « Chiffrement du périphérique » dans les paramètres du système d'exploitation Windows.

Sur les appareils Android, à partir de la version 9.0, le chiffrement des fichiers est activé par défaut. Le chiffrement basé sur les fichiers d'Android fonctionne différemment du chiffrement intégral du disque, mais offre néanmoins une sécurité solide. Si vous utilisez un téléphone Android relativement récent et que vous avez défini un code d'accès, le chiffrement basé sur les fichiers devrait être activé. Cependant, il est bon de vérifier vos paramètres pour en être sûr, surtout si votre téléphone a plus de deux ans. Pour vérifier, allez dans Paramètres > Sécurité sur votre appareil Android. Dans les paramètres de sécurité, vous devriez voir une sous-section intitulée « Chiffrement » ou « Chiffrement et informations d'identification », qui indiquera si votre téléphone est chiffré et, dans le cas contraire, vous permettra d'activer le chiffrement.

Pour les ordinateurs (qu'il s'agisse de Windows ou de Mac), il est particulièrement important de conserver les clés de chiffrement (appelées clés de récupération) dans un endroit sûr. Ces « clés de récupération » sont dans la plupart des cas essentiellement des mots de passe longs ou des phrases de passe. Si vous oubliez le mot de passe de votre appareil habituel ou si un événement inattendu se produit (comme une panne de l'appareil), les clés de récupération sont le seul moyen pour récupérer vos données chiffrées et, si nécessaire, les déplacer vers un nouvel appareil. Par conséquent, lorsque vous activez le chiffrement intégral du disque, veillez à enregistrer ces clés ou mots de passe dans un endroit sûr, comme un compte en nuage sécurisé ou le gestionnaire de mots de passe de votre parlement.

ACCÈS À DISTANCE AUX APPAREILS (ÉGALEMENT CONNU SOUS LE NOM DE PIRATAGE)

Outre la sécurité physique des appareils, il est important de les préserver des logiciels malveillants. **Security-in-a-Box** de Tactical Tech donne une description utile de ce qu'est un logiciel malveillant et pourquoi il est important de les éviter, qui est légèrement adaptée dans le reste de cette section.

Comprendre et éviter les logiciels malveillants

Il existe de nombreuses méthodes de classification des malwares (terme désignant un logiciel malveillant). Les virus, les logiciels espions, les vers, les chevaux de Troie, les rootkits, les rançongiciels et les cryptojackers sont tous des types de logiciels malveillants. Certains types de logiciels malveillants se propagent sur l'internet par le biais de courriels, de messages texte, de pages web malveillantes et d'autres moyens. Certains se propagent par le biais de dispositifs tels que des clés USB qui sont utilisées pour échanger et voler des données. Et, alors que certains logiciels malveillants exigent qu'une cible peu méfiante commette une erreur, d'autres peuvent infecter silencieusement des systèmes vulnérables sans que vous fassiez quoi que ce soit de mal.

Outre les logiciels malveillants classiques, qui sont diffusés à grande échelle et visent le grand public, les logiciels malveillants ciblés sont généralement utilisés pour interférer avec un individu, une organisation ou un réseau particulier ou l'espionner. Les criminels ordinaires utilisent ces techniques, mais aussi les services militaires et de renseignement, les terroristes, les harceleurs en ligne, les conjoints violents et les acteurs politiques véreux.

Quel que soit leur nom, quelle que soit la manière dont ils sont distribués, les logiciels malveillants peuvent ruiner les ordinateurs, voler et détruire des données, perturber les opérations parlementaires, porter atteinte à la vie privée et mettre les utilisateurs en danger. En bref, les logiciels malveillants sont vraiment dangereux. Cependant, il existe quelques mesures simples que votre parlement peut prendre pour se protéger contre cette menace courante.

Un outil anti-malware peut-il nous protéger ?

Les outils anti-malware ne sont malheureusement pas une solution complète. Cependant, c'est une très bonne idée d'utiliser quelques outils de base gratuits comme point de départ. Les logiciels malveillants évoluent si rapidement et les nouveaux risques sont si fréquents dans le monde réel que le recours à un tel outil ne peut suffire à vous défendre.

Si vous utilisez Windows vous devriez jeter un coup d'œil à la version intégrée de Windows Defender. Les ordinateurs Mac et Linux ne sont pas équipés d'un logiciel anti-malware intégré, pas plus que les appareils Android et iOS. Vous pouvez installer un outil réputé et gratuit comme **Bitdefender** ou **Malwarebytes** pour ces appareils (ainsi que pour les ordinateurs Windows). **Mais ne vous appuyez pas là-dessus comme seule ligne de défense** car ils passeront certainement à côté de certaines des nouvelles attaques les plus ciblées et les plus dangereuses.

En outre, veillez à ne télécharger que des outils anti-malware ou anti-virus bien réputés provenant de sources légitimes (telles que les sites Web mentionnés ci-dessus). Malheureusement, il existe de nombreuses versions falsifiées ou compromises d'outils anti-malware qui font beaucoup plus de mal que de bien.

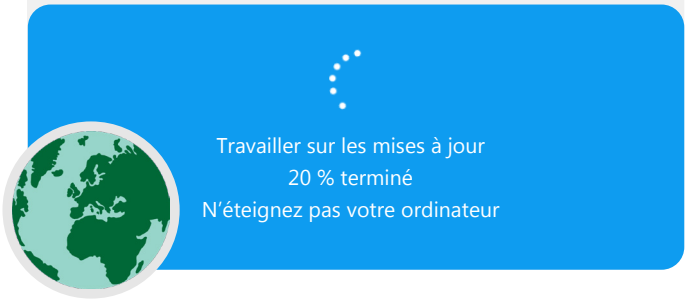
Si vous utilisez Bitdefender ou un autre outil anti-malware au sein de votre parlement, veillez à ne pas exécuter deux de ces outils en même temps. Beaucoup d'entre eux identifient le comportement d'un autre programme anti-malware comme suspect et l'empêchent de s'exécuter, ce qui entraîne un dysfonctionnement des deux programmes. Bitdefender ou d'autres programmes anti logiciels malveillants réputés peuvent être mis à jour gratuitement et le programme intégré Windows Defender reçoit les mises à jour en même temps que votre ordinateur. Veillez à ce que votre logiciel anti-malware se mette à jour régulièrement (certaines versions d'essai de logiciels commerciaux livrés avec un ordinateur sont désactivées après l'expiration de la période d'essai, ce qui les rend plus dangereux qu'utiles). De nouveaux logiciels malveillants sont créés et diffusés chaque jour, et votre ordinateur deviendra rapidement encore plus vulnérable si vous ne vous tenez pas au courant des nouvelles techniques de lutte contre les logiciels malveillants et de leurs évolutions. Si possible, vous devez configurer votre logiciel pour qu'il installe automatiquement les mises à jour. Si votre outil anti logiciels malveillants dispose d'une fonction optionnelle « Toujours actif », vous devriez l'activer et envisager d'analyser occasionnellement tous les fichiers de votre ordinateur.

Maintenir les appareils à jour

Les mises à jour sont essentielles. Utilisez la dernière version du système d'exploitation de votre appareil (Windows, Mac, Android, iOS, etc.) et maintenez-le à jour. Maintenez également à jour les autres logiciels, votre navigateur et ses éventuels plugins. Installez les mises à jour dès qu'elles sont disponibles, idéalement en **activant les mises à jour automatiques.** Plus le système d'exploitation d'un appareil est à jour, moins il est vulnérable. Considérez les mises à jour comme un pansement sur une plaie ouverte : elles permettent de colmater une brèche et réduisent considérablement les risques d'infection. Désinstallez également les logiciels que vous n'utilisez plus. Les logiciels obsolètes présentent souvent des problèmes de sécurité.Vous avez peut-être installé un outil qui n'est plus mis à jour par le développeur, ce qui le rend plus vulnérable aux pirates.

Les logiciels malveillants dans le monde réel : Les mises à jour sont essentielles

En 2017, les attaques via le ransomware WannaCry ont infecté des millions d'appareils dans le monde entier, mettant hors service des hôpitaux, des entités gouvernementales, de grandes et petites organisations et des entreprises dans des dizaines de pays. Pourquoi l'attaque a-t-elle été si efficace ? En raison de systèmes d'exploitation Windows obsolètes et non corrigés, dont beaucoup étaient initialement piratés. Une grande partie des dommages (humains et financiers) aurait pu être évitée grâce à de meilleures pratiques de mise à jour automatisée et à l'utilisation de systèmes d'exploitation légitimes.



Faites attention aux clés USB

Soyez prudent lorsque vous ouvrez des fichiers qui vous sont envoyés en pièces jointes, par des liens de téléchargement ou par tout autre moyen. Réfléchissez également **à deux fois avant d'insérer des supports amovibles comme des clés USB**, des cartes mémoire flash, des DVD et des CD dans votre ordinateur, car ils peuvent être un vecteur de logiciels malveillants. Les clés USB qui ont été partagées un certain temps sont très susceptibles de contenir des virus. Pour connaître les autres options permettant de partager des fichiers en toute sécurité au sein de votre parlement, consultez la section Partage de fichiers du manuel.

Soyez également prudent quant aux autres appareils auxquels vous vous connectez via Bluetooth. Vous pouvez synchroniser votre téléphone ou votre ordinateur avec une enceinte Bluetooth reconnue et fiable pour écouter votre musique préférée, mais faites attention à ne pas établir de connexion avec des appareils que vous ne reconnaissez pas ou à ne pas accepter de requêtes de ces appareils. N'autorisez les connexions qu'avec des appareils de confiance et n'oubliez pas de désactiver la fonction Bluetooth lorsqu'elle n'est pas utilisée.

Soyez intelligent lorsque vous naviguez

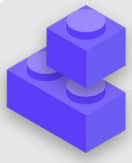
N'acceptez et n'exécutez jamais d'applications provenant de sites Web que vous ne connaissez pas et auxquels vous ne faites pas confiance. Plutôt que d'accepter une « mise à jour » proposée dans une fenêtre contextuelle du navigateur, par exemple, vérifiez les mises à jour sur le site web officiel de l'application concernée. Comme évoqué dans la section Hameçonnage du manuel, il est essentiel de rester vigilant lorsque vous naviguez sur des sites web. Vérifiez la destination d'un lien (en le survolant) avant de cliquer et jetez un coup d'œil à l'adresse du site web après avoir suivi un lien et assurez-vous qu'elle semble appropriée avant de saisir des informations sensibles comme votre mot de passe. Ne cliquez pas sur les messages d'erreur ou les avertissements et faites attention aux fenêtres du navigateur qui s'affichent automatiquement et lisez-les attentivement au lieu de cliquer simplement sur Oui ou OK.

Les logiciels malveillants dans le monde réel : Applications mobiles malveillantes

Depuis des années, des pirates de différents pays utilisent de fausses applications dans la boutique Google Play pour diffuser des logiciels malveillants. Un cas particulier visant des utilisateurs au Vietnam a été révélé en avril 2020. Cette campagne d'espionnage utilisait de fausses applications, censées aider les utilisateurs à trouver les bars à proximité ou à rechercher des informations sur les églises locales. Une fois installées par des utilisateurs Android non informés, les applications malveillantes collectent des journaux d'appels, des données de localisation et des informations sur les contacts et les messages texte. Ce n'est qu'une des nombreuses raisons pour lesquelles il faut faire attention aux applications que vous téléchargez sur vos appareils.

Qu'en est-il des smartphones ?

Comme pour les ordinateurs, maintenez le système d'exploitation et les applications de votre téléphone à jour, et activez les mises à jour automatiques. Installez uniquement des logiciels provenant de sources officielles ou de confiance, comme le Play Store de Google et l'App Store d'Apple (ou F-droid, une boutique d'applications à code source ouvert pour Android). Les applications peuvent contenir des logiciels malveillants tout en semblant fonctionner normalement. Vous ne saurez donc pas toujours si l'une d'entre elles est affectée par un logiciel malveillant. Assurez-vous également que vous téléchargez la version légitime d'une application. En particulier sur les appareils Android, il existe des versions « fausses » d'applications populaires. Assurez-vous donc qu'une application est créée par la bonne société ou le bon développeur, qu'elle a de bonnes évaluations et qu'elle a le nombre de téléchargements attendus (par exemple, une fausse version de WhatsApp pourrait n'avoir que quelques milliers de téléchargements, mais la vraie version en compte plus de cinq milliards). Faites attention aux autorisations que vos applications demandent. Si elles vous semblent excessives (comme une calculatrice demandant l'accès à votre appareil photo ou Angry Birds demandant l'accès à votre localisation, par exemple), refusez la demande ou désinstallez l'application. Désinstaller les applications que vous n'utilisez plus peut également contribuer à protéger votre smartphone ou votre tablette. Les développeurs vendent parfois la propriété de leurs applications à d'autres personnes. Ces nouveaux propriétaires peuvent essayer de gagner de l'argent en ajoutant un code malveillant.



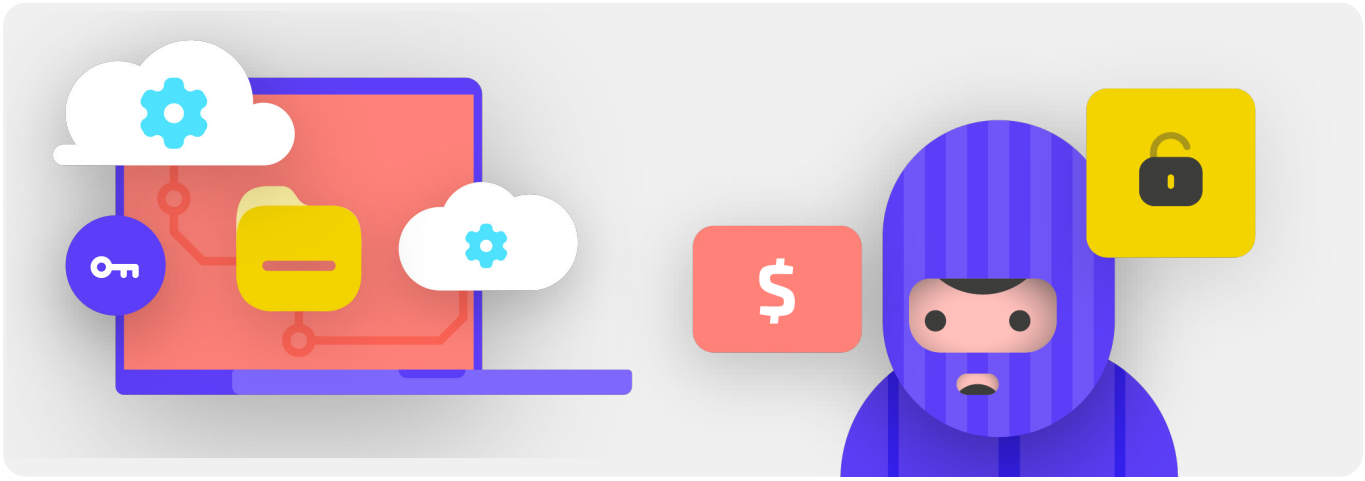
Assurer la sécurité des appareils

- **Formez les membres et le personnel aux risques liés aux logiciels malveillants et aux meilleures pratiques pour les éviter.**
  - Prévoyez des directives concernant la connexion de périphériques externes, le clic sur des liens, le téléchargement de fichiers et d'applications, et la vérification des autorisations des logiciels et des applications.
- **Exigez que les appareils, les logiciels et les applications soient constamment mis à jour.**
  - Activez les mises à jour automatiques lorsque cela est possible.
- **Inscrivez tous les appareils parlementaires dans un système de gestion des appareils mobiles ou des points d'extrémité.**
- **Assurez-vous que tous les appareils utilisent des logiciels sous licence.**
- **Exigez la protection par mot de passe de tous les appareils parlementaires, y compris les appareils mobiles personnels qui sont utilisés pour des communications liées au parlement.**
- **Activez le chiffrement intégral du disque sur les périphériques.**
- **Rappelez fréquemment aux membres et au personnel de sécuriser physiquement leurs appareils et gérez la sécurité de votre bureau avec des serrures appropriées ainsi que des moyens de sécuriser les ordinateurs.**
- **Ne partagez pas de fichiers à l'aide de clés USB et ne branchez pas de clés USB sur vos ordinateurs.**
  - Utilisez plutôt d'autres options de partage de fichiers sécurisés.

Hameçonnage : Une menace courante pour les appareils et les comptes

L'hameçonnage est l'attaque la plus courante et la plus efficace contre les organisations du monde entier, y compris les parlements. Cette technique est utilisée par les armées des États-nations les plus sophistiqués ainsi que par les petits fraudeurs.

L'hameçonnage, en termes simples, consiste pour un adversaire à tenter de vous inciter à partager des informations qui pourraient être utilisées contre vous ou votre organisation. L'hameçonnage peut se faire par courriel, par SMS (souvent appelé hameçonnage par SMS ou « smishing »), par des applications de messagerie comme WhatsApp, par des messages ou des messages sur les médias sociaux ou par des appels téléphoniques (souvent appelé hameçonnage vocal ou « vishing »). Les messages d'hameçonnage peuvent vous inciter à saisir des informations sensibles (comme des mots de passe) sur un faux site web afin d'accéder à un compte, vous demander de partager des informations privées (comme un numéro de carte de crédit) par la voix ou le texte, ou vous convaincre de télécharger un malware (logiciel malveillant) qui peut infecter votre appareil. Pour donner un exemple non technique, chaque jour, des millions de personnes reçoivent de faux appels téléphoniques automatisés leur disant que leur compte bancaire a été compromis ou que leur identité a été volée.Tous ces appels sont conçus pour inciter les personnes non averties à partager des informations sensibles.



COMMENT IDENTIFIER LE HAMEÇONNAGE ?

Le hameçonnage peut sembler inquiétant et impossible à détecter, mais il existe des mesures simples que chacun dans le parlement peut prendre pour se protéger contre la majorité des attaques. Les conseils de défense contre le hameçonnage suivants sont modifiés et étendus à partir du guide approfondi sur le hameçonnage élaboré par la Freedom of the Press Foundation, et doivent être partagés avec toutes les personnes qui intègrent le parlement de quelque façon que ce soit et intégrés dans votre programme de sécurité :

Parfois, le champ « de » vous ment

Sachez que le champ « de » dans vos e-mails peut être falsifié ou contrefait pour vous tromper. Il est fréquent que les hameçonneurs créent une adresse courriel qui ressemble beaucoup à une adresse légitime que vous connaissez bien, avec quelques petites erreurs d'orthographe pour vous tromper. Par exemple, vous pouvez recevoir un courriel d'une personne dont l'adresse est « john@goooogle.com » et non « john@google.com ». Remarquez les O supplémentaires dans Google. Vous pouvez également connaître quelqu'un qui a une adresse de courriel « john@gmail.com », mais qui reçoit un e-mail de hameçonnage d'un usurpateur qui a créé « johm@gmail.com », la seule différence étant un changement subtil de lettres à la fin. Vérifiez toujours que vous connaissez l'adresse d'envoi d'un courriel avant de poursuivre. Un concept similaire s'applique à l'hameçonnage par le biais de textes, d'appels ou d'applications de messagerie. Si vous recevez un message d'un numéro inconnu, réfléchissez-y à deux fois avant de répondre ou d'interagir avec le message.

Hameçonnage et parlements

Thu 4/8/2021 8:48 AM

<redacted> <<redacted>@aop.gov.af>

Kindlty mention this email Most Urgent.

To <redacted>@nsc.gov.af

Message | NSC Press conference.rar (38 KB)

Yesterday I called your office and no one answered it. We have received your file and modified it. There is an error in the third line of the second page. Please confirm whether the error exists.
File Pass: nsc2021
Press conference by 5:00PM.

Regards | <redacted>

Press office | Spokesman
Presidential Palace (ARG) | Islamic Republic of Afghanistan
Mobile: <redacted> | ocs.gov.af
Mail: <redacted>

Des attaques de hameçonnage sophistiquées et personnalisées ciblent régulièrement les parlements et d'autres acteurs gouvernementaux du monde entier.

Des responsables parlementaires fédéraux et locaux en Allemagne ont été la cible d'e-mails de hameçonnage à l'approche des élections de l'automne 2021. Quelques mois auparavant, en Afghanistan, un groupe de piratage **avait utilisé des techniques de hameçonnage pour infiltrer avec succès** l'ancien Conseil de sécurité nationale en prenant l'identité du porte-parole de l'ancien président afghan Ashraf Ghani. Les pirates ont envoyé des e-mails de hameçonnage (illustrés ci-dessus) demandant aux victimes d'ouvrir un fichier joint qui, selon le « porte-parole », contenait une erreur. Lorsque les victimes ont téléchargé et ouvert le fichier pour « confirmer l'erreur », la pièce jointe malveillante a déployé un logiciel malveillant qui a accordé aux pirates un accès durable aux ordinateurs. Un tel accès a permis aux pirates de télécharger des fichiers, d'exécuter des commandes sur les appareils à volonté et de voler des données gouvernementales très sensibles.

Méfiez-vous des pièces jointes

Les pièces jointes peuvent contenir des logiciels malveillants et des virus, et accompagnent souvent les e-mails de hameçonnage. **La meilleure façon d'éviter les logiciels malveillants contenus dans les pièces jointes est de ne jamais les télécharger.** En règle générale, n'ouvrez pas immédiatement les pièces jointes, surtout si elles proviennent de personnes que vous ne connaissez pas. Si possible, demandez à la personne qui vous a envoyé le document de copier-coller le texte dans un courriel ou de partager le document via un service comme Google Drive ou Microsoft OneDrive, qui disposent d'une analyse antivirus intégrée pour la plupart des documents téléchargés sur leurs plateformes. Instaurez une culture organisationnelle où l'ouverture de pièces jointes est découragée.

Si vous devez absolument ouvrir la pièce jointe, elle ne doit être ouverte que dans un environnement sûr (voir la section « Avancées » ci-dessous) où les logiciels malveillants potentiels ne peuvent pas être déployés sur votre appareil.

Si vous utilisez Gmail et que vous recevez une pièce jointe dans un courriel, au lieu de la télécharger et de l'ouvrir sur votre ordinateur, cliquez simplement sur le fichier joint et lisez-le via la fonction « Aperçu » de votre navigateur. Cette étape vous permet de visualiser le texte et le contenu d'un fichier sans le télécharger ni lui permettre de charger d'éventuels logiciels malveillants sur votre ordinateur. Cela fonctionne bien pour les documents Word, les PDF et même les présentations de diapositives. Si vous devez modifier le document, envisagez d'ouvrir le fichier dans un programme en nuage comme Google Drive et de le convertir en Google Doc ou Google Slides.

Si vous utilisez Outlook, vous pouvez également prévisualiser les pièces jointes sans les télécharger à partir du client web d'Outlook. Si vous devez modifier la pièce jointe, envisagez de l'ouvrir avec OneDrive, si vous y avez accès. Si vous utilisez Yahoo Mail, le même concept s'applique. Ne téléchargez pas les pièces jointes, mais visualisez-les plutôt à partir du navigateur web.

Quels que soient les outils dont vous disposez, la meilleure approche consiste simplement à ne jamais télécharger de pièces jointes que vous ne connaissez pas ou auxquelles vous ne faites pas confiance, et quelle que soit l'importance d'une pièce jointe, ne jamais ouvrir quelque chose dont le type de fichier n'est pas reconnu ou que vous n'avez pas l'intention d'utiliser.

Défense contre le hameçonnage au sein de votre Parlement

Si votre parlement utilise Microsoft 365 pour les courriels et d'autres applications, votre administrateur de domaine doit définir la politique de sécurité en matière de pièces jointes afin de se protéger contre les pièces jointes dangereuses. Si vous utilisez Google Workspace (anciennement connue sous le nom de GSuite), il existe une option tout aussi efficace que votre administrateur doit configurer, appelée Google Security Sandbox. Les utilisateurs particuliers plus avancés peuvent envisager de configurer des programmes sandbox sophistiqués, tels que Dangerzone ou, pour ceux qui disposent de la version Pro ou Enterprise de Windows 10, Windows Sandbox. Une autre option avancée à envisager de mettre en place dans l'ensemble du parlement est un service de filtrage sécurisé du système de nom de domaine (DNS).

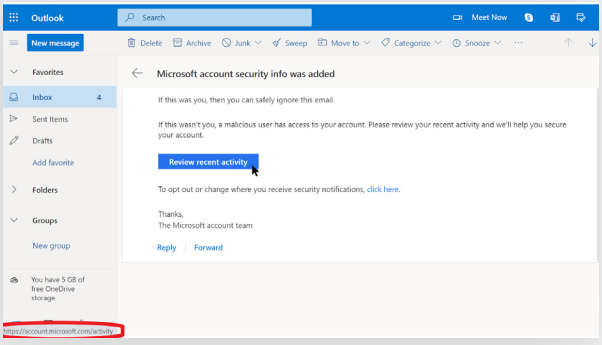
Les parlements peuvent utiliser cette technologie pour empêcher le personnel d'accéder accidentellement à des contenus malveillants ou d'interagir avec eux, ce qui constitue un niveau de protection supplémentaire contre l'hameçonnage. De nouveaux services comme Cloudflare Gateway offrent de telles capacités aux organisations sans être trop coûteux. D'autres outils gratuits, notamment Quad9 de Global Cyber Alliance Toolkit, vous aideront à bloquer l'accès à des sites connus contenant des virus ou d'autres logiciels malveillants et peuvent être mis en place en moins de cinq minutes.

Faites attention à où vous cliquez

Méfiez-vous des liens présents dans les courriels ou autres messages textuels. Des liens peuvent être détournés pour télécharger des fichiers malveillants ou vous conduire vers de faux sites qui peuvent vous demander de fournir des mots de passe ou d'autres informations sensibles. Sur un ordinateur, il existe une astuce simple pour s'assurer qu'un lien dans un courriel ou un message vous enverra là où il est censé vous mener : Utilisez votre souris pour survoler un lien avant de cliquer dessus et regardez en bas de la fenêtre de votre navigateur pour voir quelle est l'URL réelle (voir l'image ci-dessous).

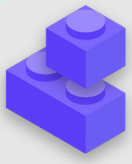
Il est plus difficile de vérifier les liens dans un courriel sur un appareil mobile sans cliquer accidentellement dessus. Soyez donc prudent.Vous pouvez vérifier la destination d'un lien sur la plupart des smartphones en appuyant longuement sur le lien jusqu'à ce que l'URL complète apparaisse. Dans le cadre du hameçonnage par SMS et applications de messagerie, les liens raccourcis sont une pratique très courante utilisée pour masquer la destination d'une URL. Si vous voyez un lien court (par exemple, bit.ly ou tinyurl.com) au lieu de l'URL complète, ne cliquez pas dessus. Si le lien est important, copiez-le dans un expandeur d'URL, tel que https://www.expandurl.net/, pour voir la destination réelle d'une URL raccourcie. En outre, ne cliquez pas sur les liens menant à des sites web qui ne vous sont pas familiers. En cas de doute, effectuez une recherche sur le site, avec le nom du site entre guillemets (par ex : « www.mauvaissiteweb.com ») pour vérifier s'il s'agit d'un site web légitime. Vous pouvez également faire passer les liens potentiellement suspects par l'analyseur d'URL de VirusTotal. Ce n'est pas précis à 100 %, mais c'est une bonne mesure de précaution à prendre.

Enfin, si vous cliquez sur un lien dans un message et qu'on vous demande de vous connecter à quelque chose, ne le faites pas à moins d'être sûr à 100 % que l'e-mail est légitime et qu'il vous amène sur le site approprié. De nombreuses attaques d'hameçonnage fournissent des liens qui vous renvoient à de fausses pages de connexion pour Gmail, Facebook ou d'autres sites populaires. Ne tombez pas dans le panneau. Vous pouvez toujours ouvrir un nouveau navigateur et vous rendre directement sur un site connu comme Gmail.com, Facebook.com, etc. si vous voulez ou devez vous y connecter. Cela vous permettra également d'accéder en toute sécurité au contenu, s'il était légitime au départ.



Que devons-nous faire lorsque nous recevons un message de hameçonnage ?

Si quelqu'un au sein du parlement reçoit une pièce jointe, un lien ou une image non sollicités, ou un message ou un appel suspect, il est important qu'il le signale immédiatement au responsable ou aux équipes de la sécurité informatique. Si vous ne disposez pas d'une telle personne ou d'une telle équipe, vous devez en désigner une dans le cadre de l'élaboration de votre programme de sécurité. Le personnel et les membres peut également signaler le courriel comme spam ou hameçonnage directement via Gmail ou Outlook. Il est essentiel de mettre en place un programme indiquant ce que le personnel, les membres ou les volontaires doivent faire s'ils reçoivent un message de hameçonnage. En outre, nous vous recommandons d'adopter les meilleures pratiques en matière d'hameçonnage (ne pas cliquer sur les liens suspects, éviter les pièces jointes et vérifier l'adresse « de ») et de les partager avec les personnes avec lesquelles vous travaillez, de préférence par le biais d'un canal de communication largement utilisé. Cela montre que vous vous préoccupez des personnes avec lesquelles vous communiquez et contribue à instaurer une culture d'alerte et de sensibilisation aux dangers de l'hameçonnage au sein de vos réseaux. Votre sécurité dépend des organisations auxquelles vous faites confiance, et vice versa. De meilleures pratiques permettent de protéger tout le monde. En plus de partager les conseils ci-dessus avec tout le monde, vous pouvez également vous entraîner à identifier le hameçonnage avec le Questionnaire sur le hameçonnage de Google. Nous vous recommandons également de mettre en place des formations régulières sur l'hameçonnage avec le personnel afin de tester la sensibilisation et de maintenir la vigilance. Cette formation peut être formalisée dans le cadre de réunions d'équipe et parlementaires régulières ou se dérouler de manière plus informelle. L'important est que tous les membres participant aux opérations parlementaires se sentent à l'aise pour poser des questions sur l'hameçonnage, pour le signaler (même s'ils pensent avoir fait une erreur, par exemple en cliquant sur un lien) et pour contribuer à la défense de votre parlement contre cette menace à fort impact et à forte probabilité.



Hameçonnage

- **Formez régulièrement les membres et le personnel sur ce qu'est l'hameçonnage et sur la manière de le repérer et de s'en protéger, y compris l'hameçonnage par messages texte, applications de messagerie et appels téléphoniques, et pas seulement par courriel.**
- **Rappelez fréquemment aux membres et au personnel les meilleures pratiques telles que :**
  - Ne téléchargez pas de pièces jointes inconnues ou potentiellement suspectes.
  - Vérifiez l'URL d'un lien avant de cliquer dessus. Ne cliquez pas sur des liens inconnus ou potentiellement suspects.
  - Ne fournissez pas d'informations sensibles ou privées par courriel, SMS ou appel téléphonique à des adresses ou des personnes inconnues ou non confirmées.
- **Encouragez le signalement des cas d'hameçonnage.**
  - Mettez en place un mécanisme de signalement et un responsable en matière d'hameçonnage au sein du parlement.
  - Récompensez les signalements et ne punissez pas les erreurs.

Communiquer et stocker des données en toute sécurité

Communications et partage des données

Afin de prendre les meilleures décisions pour votre parlement sur la manière de communiquer, il est essentiel de comprendre les différents types de protection que nos communications peuvent avoir, et pourquoi cette protection est importante.

L'un des éléments les plus importants de la sécurité des communications consiste à préserver la confidentialité des communications privées, ce qui, à l'ère moderne, est largement assuré par le chiffrement. Sans un chiffrement approprié, les communications parlementaires internes peuvent être interceptées par un grand nombre d'adversaires.

Les communications non sécurisées peuvent exposer des informations et des messages sensibles ou embarrassants, révéler des mots de passe ou d'autres données privées, et éventuellement mettre votre personnel et vos membres ou votre personnel en danger, selon la nature de vos communications et du contenu que vous partagez. En tant que parlement, il est également important de veiller à ce que les communications officielles des membres et du personnel du gouvernement respectent toutes les obligations de transparence (telles que les demandes de liberté d'information) et les engagements en matière de sécurité des données. Par conséquent, lors de la conception et de la mise en œuvre de systèmes et de politiques de communication sécurisés au sein du parlement, veillez à garder ces facteurs à l'esprit afin que les messages pertinents puissent à la fois être correctement sécurisés et, si la loi l'exige, préservés.

Communications sécurisées et parlements

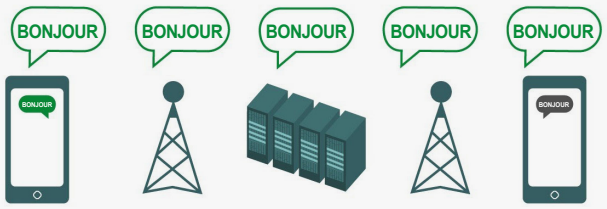
Ces dernières années, de nombreux incidents ont compromis les systèmes de communication des parlements et les comptes des députés et de leur personnel, entraînant une perturbation des activités parlementaires et, dans certains cas, le vol de communications sensibles. En juillet 2021, par exemple, les autorités polonaises ont annoncé que les comptes de messagerie de près d'une douzaine de députés locaux avaient été piratés, y compris un compte personnel du principal assistant du Premier ministre et des comptes de membres de presque tous les groupes d'opposition parlementaire. Ce rapport a été publié quelques mois seulement après que des informations similaires ont été révélées concernant une cyberattaque contre les systèmes d'information et de communication du parlement finlandais. Les autorités finlandaises ont qualifié cette attaque d'« espionnage aggravé et d'interception de messages » visant son parlement.

QU'EST-CE QUE LE CHIFFREMENT ET POURQUOI EST-IL IMPORTANT ?

Le chiffrement est un processus mathématique utilisé pour brouiller un message ou un fichier afin que seule une personne ou une entité possédant la clé puisse le « déchiffrer » et le lire. Le guide Surveillance Self Defense de l'Electronic Frontier Foundation fournit une explication pratique (avec des graphiques) de ce que représente le chiffrement :

Messagerie non chiffrée

Sans chiffrement, nos messages peuvent être lus par des adversaires potentiels, notamment des gouvernements étrangers hostiles ou des pirates informatiques. Ce type de chiffrement est important non seulement pour les communications parlementaires internes, mais aussi pour les communications externes dans lesquelles la vie privée et l'intégrité doivent être protégées.

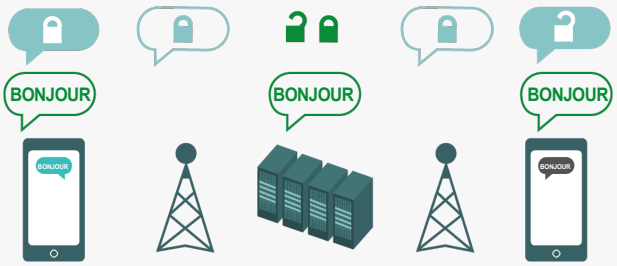


Comme vous pouvez le voir sur l'image ci-dessus, un smartphone envoie un message texte vert et non chiffré (« hello ») à un autre smartphone situé à l'extrême droite. En cours de route, une tour de téléphonie mobile (ou, dans le cas d'un message envoyé par internet, votre fournisseur d'accès à internet, appelé FAI) transmet le message aux serveurs de l'entreprise. De là, il traverse le réseau jusqu'à une autre tour de téléphonie mobile, qui peut voir le message « hello » non chiffré, et est finalement acheminé vers sa destination. Il est important de noter que sans aucun chiffrement, toutes les personnes impliquées dans la transmission du message, ainsi que toute personne qui peut jeter un coup d'œil au moment où il passe peuvent lire son contenu. Cela n'a peut-être pas beaucoup d'importance si vous ne faites que dire « bonjour », mais cela peut être un problème si vous communiquez quelque chose de plus privé ou de plus sensible que vous ne voulez pas que votre télécom, votre FAI, un gouvernement hostile ou tout autre adversaire voie. Pour cette raison, il est essentiel d'éviter d'utiliser des outils non chiffrés pour envoyer des messages sensibles (et idéalement tout message). N'oubliez pas que certaines des méthodes de communication les plus populaires (comme les SMS et les appels téléphoniques) fonctionnent pratiquement sans aucun chiffrement (comme sur l'image ci-dessus).

Il existe deux manières de chiffrer des données lors de leur déplacement : le ***chiffrement de la couche de transport*** et le ***chiffrement de bout en bout***. Il est important de connaître le type de chiffrement pris en charge par un fournisseur de services lorsque votre parlement fait des choix pour adopter des pratiques et des systèmes de communication plus sûrs. De telles différences sont bien décrites par le guide Surveillance Self-Defense , qui est à nouveau adapté ici :

Chiffrement de la couche de transport

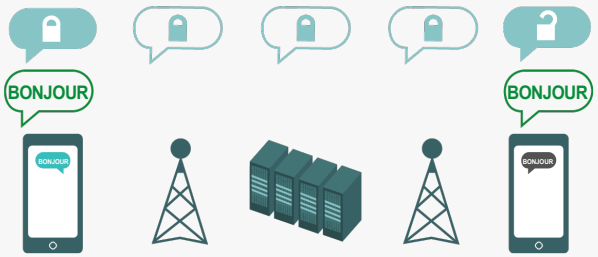
Le chiffrement de la couche de transport, également connu sous le nom de Sécurité de la couche de transport (TLS), protège les messages lorsqu'ils transitent de votre appareil vers les serveurs de l'application ou du service de messagerie et, de là, vers l'appareil de votre destinataire. Ils sont ainsi protégés des regards indiscrets des pirates informatiques qui se trouvent sur votre réseau ou chez vos fournisseurs de services Internet ou de télécommunications. Cependant, entre les deux, votre fournisseur de services de messagerie ou de courriel, le site web sur lequel vous naviguez ou l'application que vous utilisez peuvent voir des copies non chiffrées de vos messages. Étant donné que vos messages peuvent être consultés par les serveurs de l'entreprise (et sont souvent stockés sur ces derniers), ils peuvent être vulnérables aux demandes des forces de l'ordre ou au vol si les serveurs de l'entreprise sont compromis.



L'image ci-dessus montre un exemple de chiffrement de la couche de transport. Sur la gauche, un smartphone envoie un message vert, non chiffré : « Hello. » Ce message est chiffré et ensuite transmis à une tour de téléphonie mobile. Au milieu, les serveurs de l'entreprise sont en mesure de déchiffrer le message, de lire son contenu, de décider où l'envoyer, de le rechiffrer et de l'envoyer à la prochaine tour de téléphonie mobile vers sa destination. A la fin, l'autre smartphone reçoit le message chiffré et le déchiffre pour lire « Hello. »

Chiffrement de bout en bout

Le chiffrement de bout en bout protège les messages en transit, de l'expéditeur au destinataire. Il garantit que l'information est transformée en un message secret par son expéditeur initial (le premier « bout ») et décodée uniquement par son destinataire final (le second « bout »). Personne, y compris l'application ou le service que vous utilisez, ne peut « écouter » et mettre sur écoute votre activité.



L'image ci-dessus montre un exemple de chiffrement de bout en bout. Sur la gauche, un smartphone envoie un message vert, non chiffré : « Hello. » Ce message est chiffré, puis transmis à une tour de téléphonie mobile, puis aux serveurs de l'application ou du service, qui ne peuvent pas lire le contenu, mais transmettent le message secret à sa destination. A la fin, l'autre smartphone reçoit le message chiffré et le déchiffre pour lire « hello ». Contrairement au chiffrement de la couche de transport, votre FAI ou votre hôte de messagerie n'est pas en mesure de déchiffrer le message. Seuls les points d'extrémité (les dispositifs d'origine qui envoient et reçoivent les messages chiffrés) disposent des clés pour déchiffrer et lire le message.

DE QUEL TYPE DE CHIFFREMENT AVONS-NOUS BESOIN ?

Lorsque vous déterminez si votre parlement a besoin d'un chiffrement de la couche transport ou d'un chiffrement de bout en bout pour vos communications (ou d'une combinaison des deux pour différents systèmes et activités), les grandes questions que vous devez poser portent sur la confiance. Par exemple, faites-vous confiance à l'application ou au service que vous utilisez ? Faites-vous confiance à son infrastructure technique ? Êtes-vous préoccupé par la possibilité qu'un gouvernement étranger hostile puisse forcer l'entreprise à remettre vos messages et, si c'est le cas, faites-vous confiance aux politiques de l'entreprise pour se protéger contre les demandes des forces de l'ordre étrangères ?

Si vous répondez « non » à l'une de ces questions, vous avez besoin d'un chiffrement de bout en bout. Si vous répondez « oui » à ces questions, un service qui ne prend en charge que le chiffrement de la couche de transport peut suffire, mais il est généralement préférable d'opter pour des services qui prennent en charge le chiffrement de bout en bout lorsque cela est possible.

Une autre série de questions à se poser est de savoir si, en tant que parlement, vous êtes tenu par la loi de maintenir un accès unique à toutes les communications parlementaires, s'il existe des exigences en matière de localisation des données dans votre pays, et/ou si certaines communications doivent être conservées (par exemple, ne pas être supprimées définitivement par le personnel) afin de respecter les lois et les engagements en matière de transparence gouvernementale. Si c'est le cas, vous pourriez envisager un système de communication d'entreprise avec chiffrement de bout en bout dans lequel vous, en tant que parlement, pouvez contrôler vous-même les clés de chiffrement. De tels systèmes (qui seront abordés plus en détail dans la section **« Stocker les données en toute sécurité »** du manuel) peuvent être puissants, mais leur mise en œuvre nécessite des compétences techniques avancées.

Par ailleurs, lorsque vous envoyez des messages à des groupes, gardez à l'esprit que la sécurité de vos messages est fonction de la sécurité effective de tous ceux qui les reçoivent. En plus de choisir soigneusement des applications et des systèmes sécurisés, il est important que tous les membres du groupe suivent d'autres bonnes pratiques concernant la sécurité des comptes et des appareils. Il suffit d'un seul mauvais intervenant ou d'un seul appareil infecté pour que le contenu d'une conversation ou d'un appel de groupe entier soit divulgué.

QUE DEVONS-NOUS FAIRE À PROPOS DES E-MAILS ?

En général, le courrier électronique n'est pas la meilleure option en matière de sécurité. Même les meilleures options de chiffrement de bout en bout des courriels laissent généralement à désirer du point de vue de la sécurité, par exemple en ne chiffrant pas les lignes d'objet des courriels et en ne protégeant pas les métadonnées (un concept important qui sera décrit ci-dessous). Si vous devez communiquer des informations très sensibles qui ne doivent pas être conservées dans les archives publiques, gardez à l'esprit qu'il est préférable d'éviter le courrier électronique (à la fois le système du parlement et surtout le compte personnel de quelqu'un) au profit d'options de messagerie sécurisée (qui seront mises en évidence dans la section suivante).

Cependant, en tant que parlement, il se peut que vous souhaitiez ou ayez besoin que les membres et le personnel communiquent des contenus sensibles ou privés par le biais d'un système géré de manière centralisée dans le cadre de leurs activités quotidiennes. Un système de messagerie électronique à l'échelle du parlement, avec des contrôles de compte appropriés bien sûr, peut être utile dans ce cas. Si, d'après votre analyse ci-dessus, le chiffrement de la couche de transport suffit, les offres professionnelles standard des fournisseurs de messagerie tels que Google Workspace (Gmail) et Microsoft 365 (Outlook) pourraient constituer des options solides pour votre parlement. Cependant, si vous craignez que votre fournisseur de courriel ne soit légalement tenu de fournir des informations sur vos communications à un gouvernement étranger ou à un autre adversaire, ou si les exigences locales en matière de résidence des données peuvent poser problème, vous devriez envisager d'utiliser une option de courriel chiffré de bout en bout. Parmi ces options, citons l'ajout de votre propre gestion des clés de chiffrement à Google Workspace ou Microsoft 365 (comme décrit dans la section **« Stocker les données en toute sécurité »** du présent manuel), ou l'adoption de services de messagerie chiffrés de bout en bout conçus pour les grandes organisations, tels que **ProtonMail** Business ou **Tutanota** Business.

QU'EST-CE QUE LES MÉTADONNÉES ET DEVONS-NOUS NOUS EN PRÉOCCUPER ?

Les personnes à qui vous, vos membres et votre personnel parlez et quand et où vous leur parlez, tout cela peut souvent être aussi problématique que ce dont vous parlez. Il est important de se rappeler que le chiffrement de bout en bout ne protège que le contenu (le « quoi ») de vos communications. C'est là que les métadonnées entrent en jeu. Le guide Surveillance Self-Defense de l'EFF donne une présentation des métadonnées et explique pourquoi elles sont importantes (en incluant une illustration de ce à quoi ressemblent les métadonnées) :

Les métadonnées sont souvent décrites comme étant tout sauf le contenu de vos communications. Vous pouvez considérer les métadonnées comme l'équivalent numérique d'une enveloppe. Tout comme une enveloppe contient des informations sur l'expéditeur, le destinataire et la destination d'un message, il en va de même pour les métadonnées. Les métadonnées sont des informations sur les communications numériques que vous envoyez et recevez.

Voici quelques exemples de métadonnées :
- avec qui vous communiquez
- la ligne d'objet de vos courriels
- la durée de vos conversations
- l'heure à laquelle une conversation a eu lieu
- votre localisation lors de la communication

Si la transparence des opérations parlementaires applicables est essentielle, il est également important de limiter l'accès non autorisé aux métadonnées (en plus de protéger le contenu des communications). Après tout, les métadonnées peuvent révéler des informations sensibles à des pirates informatiques, à des gouvernements étrangers, à des entreprises ou à d'autres personnes dont l'accès n'est pas souhaité. Voici quelques exemples de la façon dont les métadonnées peuvent être révélatrices :

Ils savent qu'un député ou un membre du personnel a appelé un journaliste et parlé avec lui pendant une heure avant que ce dernier ne publie un article avec une citation anonyme. Cependant, ils ne savent pas de quoi vous avez parlé.

Ils savent que vous avez reçu un e-mail d'un service de test de COVID, puis que vous avez appelé votre médecin, puis que vous avez visité le site web de l'Organisation mondiale de la santé dans la même heure. Cependant, ils ne savent pas ce que contenait l'e-mail ni ce dont vous avez parlé au téléphone.

Outils recommandés pour les communications chiffrées de bout en bout

MESSAGERIE TEXTE (INDIVIDUELLE OU COLLECTIVE)	• **Signal** • **WhatsApp (uniquement avec les configurations de paramètres spécifiques détaillées ci-dessous)**
APPELS AUDIO ET VIDÉO	• **Signal (jusqu'à 40 personnes)** • **WhatsApp (jusqu'à 32 personnes en audio, huit en vidéo)**
PARTAGE DE FICHIERS	• **Signal** • **Keybase / Équipes Keybase** • **Tresorit**

QUELS OUTILS DE MESSAGERIE CHIFFRÉE DE BOUT EN BOUT DEVRIONS-NOUS UTILISER (À PARTIR DE 2022) ?

Si vous devez utiliser le chiffrement de bout en bout, ou si vous souhaitez simplement adopter la meilleure pratique quel que soit le contexte de menace de votre parlement, voici quelques exemples fiables de services qui, **à partir de 2022**, offrent une messagerie et des appels chiffrés de bout en bout. Cette section du manuel sera régulièrement mise à jour en ligne, mais veuillez noter que les choses évoluent rapidement dans le monde de la messagerie sécurisée, de sorte que ces recommandations peuvent ne pas être à jour au moment où vous lisez cette section. Gardez à l'esprit que la sécurité de vos communications dépend de celle de votre appareil. Ainsi, en plus d'adopter des pratiques de messagerie sécurisée, il est essentiel de mettre en œuvre les meilleures pratiques décrites dans la section **« Sécurité des dispositifs »** de ce manuel.

Les métadonnées ne sont pas protégées par le chiffrement fourni par la plupart des services de messagerie. Si vous envoyez un message sur WhatsApp, par exemple, n'oubliez pas que, même si le contenu de votre message est chiffré de bout en bout, il est toujours possible pour d'autres personnes de savoir à qui vous envoyez des messages, à quelle fréquence et, dans le cas des appels téléphoniques, pendant combien de temps. Par conséquent, vous devez garder à l'esprit les risques qui existent (le cas échéant) si certains adversaires sont en mesure de savoir à qui vous parlez, quand vous leur avez parlé et (dans le cas des e-mails) les lignes d'objet générales des communications de votre parlement.

L'une des raisons pour lesquelles **Signal** est si fortement recommandé est que, en plus de fournir un chiffrement de bout en bout, il a **introduit des fonctionnalités et pris des engagements afin de réduire la quantité de métadonnées qu'il enregistre et stocke.** Par exemple, la fonction « Expéditeur scellé » de Signal chiffre les métadonnées relatives à la personne qui parle à un autre, de sorte que Signal ne connaît que le destinataire d'un message, mais pas l'expéditeur. Par défaut, cette fonction ne fonctionne que lorsque vous communiquez avec des contacts ou des profils existants (personnes) avec lesquels vous avez déjà communiqué ou que vous avez enregistrés dans votre liste de contacts. Cependant, vous pouvez activer ce paramètre « Expéditeur scellé » pour « Autoriser de n'importe qui » s'il est important pour vous d'éliminer ces métadonnées dans toutes les conversations Signal, même celles avec des personnes qui vous sont inconnues.

Cela n'est peut-être pas essentiel pour la majorité des communications parlementaires, mais il est important d'être conscient des risques posés par les métadonnées et de choisir en conséquence les outils et les politiques de communication appropriés.

PEUT-ON VRAIMENT FAIRE CONFIANCE À WHATSAPP ?

WhatsApp est un choix populaire en matière de messagerie sécurisée et peut constituer une bonne option compte tenu de son omniprésence. Certains s'inquiètent du fait qu'il est détenu et contrôlé par Facebook, qui s'est efforcé de l'intégrer à ses autres systèmes. D'autres sont également préoccupées par la quantité de métadonnées (c'est-à-dire des informations sur les personnes avec qui vous communiquez et quand) que WhatsApp collecte. Si vous choisissez d'utiliser WhatsApp comme option de messagerie sécurisée, veillez à lire la section ci-dessus sur les métadonnées. Il y a également quelques paramètres dont il est nécessaire de s'assurer qu'ils soient correctement configurés. Plus important encore, assurez-vous de désactiver les sauvegardes dans le nuage ou, à tout le moins, d'activer la nouvelle fonctionnalité de sauvegardes chiffrées de bout en bout de WhatsApp en utilisant une clé de chiffrement à 64 chiffres ou un code de passe long, aléatoire et unique enregistré dans un endroit sûr (comme votre gestionnaire de mots de passe). Veillez également à afficher les notifications de sécurité et à vérifier les codes de sécurité. Vous pouvez trouver des guides pratiques simples pour configurer ces paramètres sur les téléphones Android ici et les iPhones ici. **Si votre personnel *et ceux avec qui vous communiquez tous* ne configurent pas correctement ces options, alors il ne faut pas considérer WhatsApp comme une bonne option pour les communications sensibles qui nécessitent un chiffrement de bout en bout.** Signal reste la meilleure option pour ces besoins de messagerie chiffrée de bout en bout, compte tenu de ses paramètres par défaut sécurisés ainsi que de ses mesures de protection des métadonnées.

ET LES TEXTOS ?

Les messages texte de base ne sont pas du tout sécurisés (les SMS standard sont effectivement non chiffrés) et doivent être évités pour tout ce qui n'est pas destiné à être connu du public. Bien que les messages entre iPhone d'Apple (connus sous le nom d'iMessages) soient chiffrés de bout en bout, s'il n'y a pas d'iPhone dans la conversation, les messages ne sont pas sécurisés. Il vaut mieux être prudent et **éviter les SMS pour tout ce qui est de loin sensible, privé ou confidentiel.**

POURQUOI TELEGRAM, FACEBOOK MESSENGER OU VIBER NE SONT-ILS PAS RECOMMANDÉS POUR LES DISCUSSIONS SÉCURISÉES ?

Certains services, comme Facebook Messenger et Telegram, n'offrent un chiffrement de bout en bout que si vous l'activez délibérément (et uniquement pour les discussions en tête-à-tête), ce ne sont donc pas de bonnes options pour les messages sensibles ou privés, en particulier pour les équipes. Ce ne sont donc pas de bonnes options pour les communications sensibles ou privées, surtout pour une organisation. Ne vous fiez pas à ces outils si vous devez utiliser le chiffrement de bout en bout, car il est assez facile d'oublier de modifier les paramètres par défaut, qui sont moins sûrs. Viber affirme offrir un chiffrement de bout en bout, mais n'a pas mis son code à la disposition des chercheurs en sécurité externes afin qu'ils puissent l'examiner. Le code de Telegram n'a pas non plus été mis à disposition pour un audit public.Par conséquent, de nombreux experts craignent que le chiffrement de Viber (ou les « discussions secrètes » de Telegram) ne soit pas conforme aux normes et ne convienne donc pas aux communications qui nécessitent un véritable chiffrement de bout en bout.

NOS COLLÈGUES PARLEMENTAIRES ET NOS ÉLECTEURS UTILISENT D'AUTRES APPLICATIONS ET SYSTÈMES DE MESSAGERIE POUR COMMUNIQUER - COMMENT LES CONVAINCRE DE TÉLÉCHARGER UNE NOUVELLE APPLICATION POUR COMMUNIQUER AVEC NOUS ?

Il faut parfois faire un compromis entre sécurité et praticité, mais un petit effort supplémentaire en vaut la peine afin de garantir la sécurité des communications sensibles. Montrez l'exemple à vos contacts, qu'il s'agisse d'autres agences gouvernementales, d'institutions, de parlementaires ou d'électeurs externes. Si vous devez utiliser d'autres systèmes moins sûrs, faites très attention à ce que vous dites. Évitez de discuter de sujets sensibles. Certains parlements peuvent avoir des protocoles différents pour les conversations générales ou les communications avec le public par rapport aux discussions confidentielles avec les dirigeants, par exemple. Classez vos communications parlementaires (internes et externes) en fonction de leur sensibilité et assurez-vous que les membres et le personnel utilisent les mécanismes de communication appropriés ! Bien sûr, le plus simple est que tout soit automatiquement chiffré en permanence, car ainsi il n'y a rien à oublier ou à penser.

Heureusement, les applications chiffrées de bout en bout comme Signal sont de plus en plus populaires et conviviales ; sans compter qu'elles ont été adaptées dans des dizaines de langues afin de pouvoir être utilisées dans le monde entier. Si vos partenaires ou autres contacts ont besoin d'aide pour passer à une option de chiffrement de bout en bout comme Signal, prenez le temps de leur expliquer pourquoi il est si important de protéger correctement vos communications. Lorsque tout le monde en comprendra l'importance, les quelques minutes nécessaires au téléchargement d'une nouvelle application et les quelques jours qu'il faudra peut-être pour s'habituer à l'utiliser ne sembleront pas être de trop.

EXISTE-T-IL D'AUTRES PARAMÈTRES POUR LES APPLICATIONS CHIFFRÉES DE BOUT EN BOUT QUE NOUS DEVRIONS CONNAÎTRE ?

Avec l'application Signal, la vérification des codes de sécurité (qu'ils appellent numéros de sécurité) est également importante. Pour afficher un numéro de sécurité et le vérifier avec Signal, vous pouvez ouvrir votre discussion avec un contact, appuyer sur son nom en haut de votre écran, puis faire défiler l'écran vers le bas pour appuyer sur « Afficher le numéro de sécurité ». Si votre numéro de sécurité correspond à celui de votre contact, vous pouvez le marquer comme « vérifié » à partir de ce même écran. Il est particulièrement important de prêter attention à ces numéros de sécurité et de vérifier vos contacts si vous recevez une notification dans une discussion indiquant que votre numéro de sécurité avec un contact donné a changé. Si vous ou d'autres membres du personnel ont besoin d'aide pour configurer ces paramètres, Signal lui-même **fournit des instructions pratiques.** Si vous utilisez Signal, qui est largement considéré comme la meilleure option conviviale en matière de messagerie sécurisée et d'appels individuels, veillez à **définir un code pin fort.** Utilisez au moins six chiffres sans utiliser quelque chose de facile à deviner comme votre date de naissance. Pour plus de conseils sur la façon de configurer correctement **Signal** et **WhatsApp**, vous pouvez consulter les **guides d'outils** élaborés par l'EFF pour ces deux produits dans son guide **Surveillance Self-Defense.**

QU'EN EST-IL DES APPELS VIDÉO DE GROUPES PLUS IMPORTANTS ? EXISTE-T-IL DES OPTIONS DE CHIFFREMENT DE BOUT EN BOUT ?

Avec l'augmentation du travail à distance, il est important de disposer d'une option sécurisée pour les appels vidéo de grands groupes ou les assemblées générales virtuelles des députés. Malheureusement, il n'existe pas actuellement de grandes options qui remplissent toutes les conditions : convivialité, prise en charge d'un grand nombre de participants et de fonctions de collaboration, et chiffrement de bout en bout par défaut.

Les besoins spécifiques des sessions plénières et des réunions de commissions seront abordés plus loin dans ce manuel, mais pour vos autres réunions plus générales qui ne nécessitent pas de fonctions de collaboration telles que le partage d'écran ou des salles de réunion, il existe quelques options. Pour les groupes jusqu'à huit personnes, Signal est fortement recommandé. Les appels vidéo de groupe sur Signal peuvent être rejoints soit à partir d'un smartphone, soit à partir de l'application de bureau Signal sur un ordinateur. N'oubliez pas, cependant, que seuls vos contacts qui utilisent déjà Signal peuvent être ajoutés à un groupe Signal.

Si vous recherchez d'autres options, **Jitsi Meet** est une plateforme qui a récemment intégré une option de chiffrement de bout en bout. Jitsi Meet est une solution d'audioconférence et de vidéoconférence basée sur le web qui peut fonctionner pour de grands publics (jusqu'à 100 personnes) et ne nécessite aucun téléchargement d'application ou de logiciel spécial. Notez que si vous utilisez cette fonction avec des groupes importants (plus de 15-20 personnes), la qualité de l'appel peut baisser. Pour organiser une réunion sur Jitsi Meet, vous pouvez vous rendre sur **meet.jit.si**, saisir un code de réunion et partager ce lien (via un canal sécurisé tel que Signal) avec les participants souhaités. Pour utiliser le chiffrement de bout en bout, jetez un coup d'œil à ces **instructions** décrites par Jitsi. Notez que tous les utilisateurs individuels devront eux-mêmes activer le chiffrement de bout en bout pour que cela fonctionne. Lorsque vous utilisez Jitsi, veillez à créer des noms de salle de réunion aléatoires et à utiliser des codes d'accès forts pour protéger vos appels.

Si cette option ne convient pas à vos équipes, vous pouvez envisager d'utiliser une option commerciale populaire comme Webex ou Zoom avec un chiffrement de bout en bout activé. Webex offre un chiffrement de bout en bout depuis longtemps. Toutefois, cette option n'est pas activée par défaut et les participants doivent télécharger Webex pour rejoindre votre réunion. Afin de bénéficier de l'option de chiffrement de bout en bout pour votre compte Webex, vous devez ouvrir un cas d'assistance Webex et suivre **ces instructions** pour vous assurer que le chiffrement de bout en bout est configuré. Seul l'hôte de la réunion doit activer le chiffrement de bout en bout. De cette manière, la réunion entière sera chiffrée de bout en bout. Si vous utilisez Webex pour des réunions de groupe et des ateliers sécurisés, veillez à activer également des codes d'accès forts pour vos appels.

Après des mois de publicité négative, Zoom a développé une **option de chiffrement de bout en bout** pour ses appels. Cependant, cette option n'est pas activée par défaut, exige que l'hôte de l'appel associe son compte à un numéro de téléphone et ne fonctionne que si tous les participants se joignent via l'application de bureau ou mobile Zoom au lieu de composer un numéro. Comme il est facile de mal configurer ces paramètres par accident, il n'est pas idéal de se fier à Zoom comme option de chiffrement de bout en bout. Toutefois, si vous avez besoin d'un chiffrement de bout en bout et que Zoom est votre seule option, vous pouvez suivre les **instructions** de Zoom afin de le configurer. N'oubliez pas de vérifier avant le début de l'appel qu'il est bien chiffré de bout en bout en cliquant sur le cadenas vert dans le coin supérieur gauche de l'écran Zoom et en voyant la mention « bout en bout » à côté du paramètre de chiffrement. Vous devez également définir un code d'accès fort pour chaque réunion Zoom.
Il convient toutefois de noter que certaines fonctions populaires des outils ci-dessus ne fonctionnent qu'avec le chiffrement de la couche de transport. Par exemple, l'activation du chiffrement de bout en bout de Zoom désactive les salles de réunion, les fonctions de sondage et l'enregistrement dans le nuage. Avec Jitsi Meet, les salles de pause peuvent désactiver la fonction de chiffrement de bout en bout, ce qui réduit involontairement la sécurité.

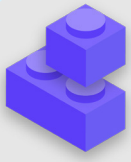
UNE NOTE SUR LE PARTAGE DE FICHIERS

Outre le partage sécurisé des messages, le partage sécurisé des fichiers est probablement un élément important du programme de sécurité de votre parlement. La plupart des options de partage de fichiers sont intégrées aux applications ou services de messagerie que vous utilisez peut-être déjà. Par exemple, le partage de fichiers via Signal est une excellente option si vous avez besoin d'un chiffrement de bout en bout. Si le chiffrement de la couche de transport est suffisant, l'utilisation de Google Drive ou de Microsoft SharePoint peut être une bonne option pour votre parlement. Veillez simplement à configurer correctement les paramètres de partage afin que seules les personnes autorisées aient accès à un document ou à un dossier donné, et assurez-vous que ces services sont connectés aux comptes courriel de l'organisation (et non aux comptes personnels du personnel). Si vous le pouvez, interdisez le partage de fichiers sensibles via des pièces jointes de courriel ou le partage physique avec des clés USB. L'utilisation de dispositifs tels que des clés USB au sein de votre parlement augmente considérablement la probabilité de voir se manifester des logiciels malveillants ou des vols, et le fait de s'appuyer sur des courriels ou d'autres formes de pièces jointes affaiblit les défenses de votre parlement contre les attaques de hameçonnage.

ET SI NOUS N'AVIONS VRAIMENT PAS BESOIN D'UN CHIFFREMENT DE BOUT EN BOUT POUR TOUTES NOS COMMUNICATIONS ?

Si un chiffrement de bout en bout n'est pas nécessaire pour toutes les communications de votre parlement en fonction de votre évaluation des risques, vous pouvez envisager d'utiliser des applications protégées par le chiffrement de la couche de transport. N'oubliez pas que ce type de chiffrement exige que vous fassiez confiance au fournisseur de services, tel que Google pour Gmail, Microsoft pour Outlook/Exchange ou Facebook pour Messenger, car il peut consulter/entendre vos communications (ainsi que toute personne avec laquelle il pourrait être contraint de partager des informations). Une fois encore, les meilleures options dépendront de votre profil de menace (par exemple, si vous ne faites pas confiance à Google ou si le gouvernement américain est votre adversaire, Gmail n'est pas une bonne option), mais voici quelques options populaires et généralement fiables :

COURRIEL	• **Gmail (via Google Workspace)** • **Outlook (via Office 365)** • N'hébergez pas votre propre serveur Microsoft Exchange pour le courrier électronique de votre parlement. Si vous le faites actuellement, vous devez migrer vers Office 365.
MESSAGERIE TEXTE (INDIVIDUELLE OU COLLECTIVE)	• **Google Hangouts** • **Slack** • **Microsoft Teams** • **Mattermost** • **Line** • **KaKao Talk** • **Telegram**
CONFÉRENCES DE GROUPE, APPELS AUDIO ET VIDÉO	• **Jitsi Meet** • **Google Meet** • **Microsoft Teams** • **Webex** • **GotoMeeting** • **Zoom**
PARTAGE DE FICHIERS	• **Google Drive** • **Microsoft Sharepoint** • **Dropbox** • **Slack** • **Microsoft Teams**



Communiquer des données en toute sécurité

- **Classez les communications en fonction de leur sensibilité.**
  - Déterminez les systèmes et les outils de communication appropriés en conséquence.
  - Définissez une politique sur la durée de conservation des messages, en gardant à l'esprit la sécurité et les engagements en matière de transparence parlementaire.
- **Exigez l'utilisation de services de messagerie de confiance chiffrés de bout en bout pour les communications sensibles de votre parlement.**
  - Prenez le temps d'expliquer au personnel et aux partenaires externes pourquoi les communications sécurisées sont si importantes ; cela renforcera les chances de succès de votre programme.
- **Assurez-vous que les paramètres appropriés sont configurés pour les applications de communication sécurisées, notamment :**
  - Assurez-vous que tous les membres du personnel sont attentifs aux notifications de sécurité et, s'ils utilisent WhatsApp, qu'ils ne sauvegardent pas les conversations.
  - Si vous utilisez une application où le chiffrement de bout en bout n'est pas activé par défaut (par exemple Zoom ou Webex), assurez-vous que les utilisateurs concernés ont activé les paramètres appropriés au début de tout appel ou réunion.
- **N'essayez pas d'héberger votre propre serveur de messagerie - utilisez des services de messagerie basés sur le nuage tels qu'Office 365 ou Google Workspace.**
  - N'autorisez pas le personnel à utiliser des comptes de messagerie électronique personnels dans le cadre de son travail.
- **Rappelez fréquemment au personnel et aux membres les meilleures pratiques de sécurité liées à la messagerie de groupe et aux métadonnées.**
  - Faites attention à qui est inclus dans les messages de groupe, les discussions en ligne et les fils de discussion par courriel.

Parlements numériques (e-Parlement)

En tant que parlement, il est important d'accorder une attention particulière aux politiques de communication et de sécurité opérationnelle de vos fonctions les plus essentielles, y compris celles qui se déroulent en ligne et dans l'espace numérique.

Que votre parlement envisage de se doter d'un système complet de « e-Parliament » capable de tout numériser, de la rédaction des projets de loi au débat et au vote électronique (comme Nextsense, Propylon ou Granicus, pour ne citer que quelques exemples), ou que vous utilisiez des outils plus simples et moins coûteux pour faciliter vos opérations parlementaires, il est essentiel d'examiner comment tout le ou les outils et processus tiennent compte de la sécurité, de l'intégrité et de la disponibilité de l'information.

Sécurité et parlements numériques

Comme l'a montré une série d'incidents en Afrique du Sud, la transition des opérations parlementaires vers le monde numérique nécessite de prêter attention à la cybersécurité afin d'éviter non seulement la perte ou le vol de données sensibles, mais aussi l'embarras, l'insulte et le préjudice potentiels pour les membres et le personnel. En mai 2020, des images pornographiques sont apparues quelques minutes avant le début d'une réunion virtuelle de l'Assemblée nationale du pays.

Après l'affichage des images offensantes, le « hacker » ou « zoom bomber » a proféré des insultes sexistes et raciales à l'encontre du président de l'assemblée qui animait la session, forçant l'ajournement de la réunion. Un incident similaire s'était produit un mois auparavant, lorsqu'une réunion présidée par le ministre des femmes, de la jeunesse et des personnes handicapées avait été perturbée par des images pornographiques.

SESSIONS PLÉNIÈRES ET RÉUNIONS DE COMMISSIONS À DISTANCE

Les sessions plénières et les réunions des commissions sont au premier rang de ces processus. Ces sessions et les conversations, décisions et votes qui s'y déroulent sont au cœur d'une grande partie du travail de votre parlement et peuvent donc constituer une cible particulière pour les adversaires. Dans un monde moderne touché par une pandémie, ces sessions et réunions se déroulent de manière de plus en plus diversifiée selon le contexte de votre pays, à la fois en personne, entièrement en ligne et de manière « hybride ».

Comme le souligne le récent guide **Parliaments Responding to a Pandemic** du House Democracy Partnership, la structure typique d'un débat parlementaire est différente d'une conférence-discussion normale ou d'une réunion organisationnelle standard. Les besoins en matière de vote à distance, de soumission de propositions officielles et d'amendements, de débat structuré et même d'interprétation simultanée pour garantir l'inclusion de toutes les circonscriptions nécessitent souvent des fonctions supplémentaires que l'on ne trouve pas dans la plupart des solutions technologiques standard. Par conséquent, lors de l'organisation d'une session virtuelle ou hybride, il est probable que votre parlement doive développer (ou ait déjà développé) un logiciel personnalisé, ou acheter des solutions d'entreprise coûteuses (telles que **Webex Legislate** de Cisco) conçues spécifiquement pour gérer les sessions parlementaires à distance. Quelle que soit l'option choisie par votre parlement, il est important de réfléchir, comme le souligne le guide **Parliaments Responding to a Pandemic**, à la manière dont tous les membres et le personnel pourront accéder à un tel système. Il est également essentiel de veiller à ce que ce système soit correctement sécurisé.

Lors de l'élaboration et de la mise en œuvre de solutions techniques pour les sessions parlementaires, il est important de veiller à ce que les principes de base de la sécurité soient en place. Il s'agit notamment de veiller à ce que les données soient sécurisées « au repos » dans le système lui-même, qu'elles soient correctement chiffrées lorsqu'elles sont en transit et que seuls les utilisateurs autorisés soient en mesure d'accéder au système. De nombreuses approches peuvent être adoptées pour garantir cette sécurité, y compris un grand nombre des principes fondamentaux décrits dans le reste du présent manuel. Le chiffrement de bout en bout de tous les systèmes de partage de données et de communication utilisés, les exigences en matière de mot de passe fort et d'authentification à deux facteurs et/ou la restriction de l'adresse IP pour les utilisateurs qui accèdent à ces systèmes (à moins qu'ils ne soient destinés à être ouverts au public), l'exigence de réseaux privés virtuels (qui seront examinés plus loin dans le manuel) et la limitation de l'accès aux seuls dispositifs propres et de confiance sont autant de mesures utiles.

VOTE À DISTANCE

La nécessité d'une sécurité solide est peut-être particulièrement critique lorsqu'il s'agit de vote à distance. Comme le souligne le guide **Parliaments Responding to a Pandemic** susmentionné, les députés sont élus au parlement dans le but précis de voter au nom de leurs électeurs. La capacité à faire confiance et à vérifier ces votes est cruciale non seulement pour le fonctionnement de votre parlement, mais aussi pour le système démocratique dans son ensemble. Ces votes sont relativement faciles à vérifier lorsqu'un député vote en personne, mais lorsqu'il participe virtuellement, l'authentification technique devient un défi plus important qui nécessite beaucoup de soin et d'attention. Comme le souligne le **témoignage** d'un expert présenté au Comité permanent de la procédure et des affaires de la Chambre des communes du Canada, les parlements choisissent généralement l'une des quatre options suivantes pour le vote à distance :

- Le vote par courrier électronique : les membres reçoivent un formulaire de vote par voie électronique et soumettent leur vote par courrier électronique. Cette option est généralement considérée comme peu sûre, notamment en raison de l'absence de chiffrement de bout en bout, et devrait être évitée.
- Le vote par Internet : les membres accèdent et votent par l'intermédiaire d'un site web sur un ordinateur ou un téléphone portable. Cette approche nécessite un investissement dans une infrastructure sécurisée, y compris des dispositifs sécurisés avec des contrôles d'authentification forts, comme mentionné ci-dessus.
- Le vote par application : les membres téléchargent une application pour accéder aux bulletins de vote et les déposer. Semblable au vote par Internet, il utilise une application spécifique qui peut être téléchargée sur un téléphone ou une tablette, au lieu d'être accessible via un navigateur.
- Le vote par vidéo : les membres votent à l'écran à main levée ou par voix. Pour le vote non anonyme, il peut s'agir de la méthode la moins compliquée techniquement et la moins sophistiquée à mettre en place et à sécuriser. Elle nécessite toutefois des systèmes de chiffrement et d'authentification robustes pour éviter l'usurpation d'identité ou l'interruption des sessions de vote.

Quelle que soit l'option choisie par votre parlement pour le vote à distance - si tant est qu'il utilise le vote à distance - il est important d'aborder les bases de la cybersécurité tout au long du processus de vote. Il faut notamment s'assurer que les appareils utilisés par les députés pour voter sont correctement sécurisés physiquement et exempts de logiciels malveillants, que l'accès à Internet des députés est correctement sécurisé lorsqu'ils votent (et lorsqu'ils mènent d'autres activités parlementaires), et que les députés disposent de connexions Internet stables et sont en mesure de voter lorsqu'ils sont appelés à le faire. Comme le souligne le guide **Parliaments Responding to a Pandemic**,

lors de l'adoption du vote à distance, il est nécessaire de tester le système de manière approfondie avant sa mise en service et de fournir un soutien et une formation aux députés afin de s'assurer qu'ils peuvent utiliser le système de manière efficace. Il est important de se rappeler qu'une partie de la sécurité est la *disponibilité*. Il est également nécessaire de s'assurer que les femmes parlementaires et le personnel sont en mesure d'utiliser les systèmes en ligne en toute sécurité, y compris le vote à distance, et qu'elles ont accès à la technologie nécessaire pour le faire. Lorsque les femmes, en particulier les femmes élues, se connectent à Internet, elles sont davantage confrontées à l'intimidation et au harcèlement, et ce facteur doit être pris en compte lors du développement et de l'utilisation de technologies telles que le vote à distance, afin de s'assurer que tous les députés sont en mesure de remplir leurs fonctions de manière efficace. En outre, il est essentiel de garantir un accès multilingue à distance adéquat dans les pays où les membres et le personnel parlent plusieurs langues officielles.

SÉCURITÉ DES FOURNISSEURS ET DES LOGICIELS DU PARLEMENT NUMÉRIQUE

Tout logiciel que vous achetez - qu'il soit utilisé pour le vote à distance ou pour un éventail plus large de besoins parlementaires - **devrait provenir d'une source sûre et accréditée, faire l'objet d'un audit de sécurité par des équipes indépendantes et recevoir les certifications appropriées.** Il est important de se rappeler que les développeurs de logiciels, ceux que vous engagez pour créer une application ou un outil, ne sont pas toujours eux-mêmes des experts en sécurité. C'est pourquoi il est essentiel de faire appel à des experts en sécurité pour tester l'application afin de déceler d'éventuelles failles de sécurité par le biais d'un audit, afin de réduire le risque de piratage ou de compromission de votre plateforme, outil ou application. Même les meilleurs développeurs de logiciels commettent des erreurs sans une deuxième (ou une troisième) paire d'yeux d'experts qui vérifient leur travail !

Le vote à distance dans le monde réel

Plusieurs parlements ont mis en place des systèmes de vote à distance et, ce faisant, ont pris des mesures considérables pour garantir la sécurité et l'intégrité des votes des membres. L'un des éléments de ce processus, parmi d'autres mentionnés ci-dessus, consiste à garantir une authentification appropriée. Parmi les exemples, on peut citer la Chambre des communes du Royaume-Uni, où les membres utilisent un processus d'authentification unique pour se connecter à leurs comptes parlementaires avant de voter, ce qui nécessite l'utilisation d'un mot de passe sur un appareil spécifique et assigné. En Espagne, les députés se voient attribuer des codes personnels qui doivent être saisis via une application pour smartphone avant qu'un vote puisse être enregistré à distance. Au Chili, les sénateurs qui votent à distance via l'application de vote à distance soigneusement conçue par la chambre doivent être visibles à l'écran pour pouvoir voter.

Stocker des données en toute sécurité

Pour la plupart des parlements, l'une des décisions les plus importantes à prendre est de savoir où stocker leurs données.

Est-il « plus sûr » de stocker des données sur les ordinateurs du personnel, sur un serveur local, sur des appareils de stockage externes ou dans le nuage ? Dans 99 % des cas, l'option la plus simple et la plus sûre consiste à conserver les données stockées au sein de services de stockage en nuage fiables. Les exemples les plus courants sont sans doute Microsoft 365 et Google Drive. Sans un programme de stockage en nuage intégré, il est probable que les données de votre parlement soient stockées à divers endroits, notamment sur les ordinateurs du personnel et des députés, sur des disques durs externes, voire sur des serveurs locaux. S'il est possible de sécuriser les données sur tous ces appareils, il est très difficile de le faire de manière satisfaisante sans dépenser beaucoup d'argent et sans engager une équipe informatique assez conséquente.

Stockage des données et parlements

L'avènement du stockage de données dans le nuage à un prix abordable (parfois gratuit) a rendu la vie plus facile (et plus sûre) pour de nombreux parlements et autres organisations. Malheureusement, nombreux sont ceux qui tentent encore d'héberger leurs propres serveurs avec un budget, un personnel et un support informatique relativement limités. En mars 2021, la menace d'une telle infrastructure organisationnelle est devenue réelle pour des dizaines de milliers d'organisations à travers le monde, notamment des parlements, lorsqu'un acteur malveillant affilié au gouvernement chinois, appelé Hafnium, a déclenché une catastrophe mondiale en matière de cybersécurité avec une attaque sophistiquée sur des serveurs Microsoft Exchange auto-hébergés. L'attaque a compromis les serveurs locaux, notamment celui du parlement norvégien, permettant aux pirates d'accéder aux comptes e-mail du parlement, d'installer des logiciels malveillants supplémentaires sur les serveurs de la victime et les systèmes connectés, et finalement **d'extraire des données sensibles.** Bien que Microsoft ait rapidement publié une mise à jour et des instructions afin d'identifier et de supprimer les intrus potentiels une fois les piratages rendus publics, de nombreuses organisations n'avaient pas la capacité informatique d'appliquer rapidement ces mises à jour, ce qui les a laissées exposées pendant de longues périodes. L'ampleur et l'impact de ce piratage mondial révèlent le danger que courent les parlements et autres organisations qui choisissent d'héberger elles-mêmes leurs serveurs de messagerie électronique et d'autres types de données sensibles, en particulier sans investir massivement dans du personnel spécialisé en cybersécurité.

AVANTAGES DU STOCKAGE EN NUAGE

Même si vous prenez toutes les mesures nécessaires pour protéger vos ordinateurs contre les logiciels malveillants et le vol physique, il est toujours possible pour un adversaire déterminé de pirater votre ordinateur ou votre serveur parlementaire local. Il leur est beaucoup plus difficile de déjouer les défenses de sécurité de Google ou de Microsoft, par exemple. Les entreprises de stockage en nuage fiables disposent de ressources de sécurité inégalées et ont tout intérêt à offrir une sécurité maximale à leurs utilisateurs. En bref, une stratégie de stockage en nuage fiable sera beaucoup plus facile à mettre en œuvre et à protéger au fil du temps. Ainsi, au lieu d'essayer d'identifier (et de retenir) le nombre d'employés spécialisés et hautement qualifiés en cybersécurité requis pour protéger les serveurs locaux de votre parlement, concentrez votre énergie sur une poignée de tâches plus simples. Il s'agit notamment de choisir l'option de stockage en nuage qui convient à vos besoins en matière de confidentialité des données et de localisation, de mettre en place une bonne sécurité des comptes, de former le personnel à partager (et à ne pas partager) correctement les dossiers et les documents (en général, vous devriez créer des dossiers dans votre unité de stockage en nuage qui limitent l'accès aux seuls membres du personnel qui en ont besoin pour des fichiers donnés), et d'auditer régulièrement votre système pour vous assurer que le personnel et les membres ne partagent pas trop de fichiers (par exemple en activant le partage universel de liens pour des fichiers qui devraient plutôt être limités à quelques personnes seulement). Le fait de conserver l'essentiel de vos informations dans le nuage permet de faire face à toute une série de risques courants. L'ordinateur de quelqu'un a été oublié dans un restaurant ou son téléphone dans le bus ? Votre enfant a renversé un verre de jus sur votre clavier, ce qui rend votre appareil inutilisable ? Avez-vous besoin de séparer les données qui appartiennent à une députée elle-même des informations qu'elle génère pour le parlement lui-même ? Un membre du personnel a-t-il été infecté par un logiciel malveillant et doit-il réinitialiser son ordinateur ? Si la plupart des documents et des données se trouvent dans le nuage, il est facile de les resynchroniser et de repartir à zéro sur un ordinateur nettoyé ou entièrement neuf. De même, si un logiciel malveillant s'introduit dans un ordinateur ou si un voleur scanne un disque dur, il n'y a rien à voler si la plupart des documents sont accessibles via le navigateur web.

POUVONS-NOUS VRAIMENT FAIRE CONFIANCE AU STOCKAGE EN NUAGE ?

En bref, il n'y a rien d'intrinsèquement indigne de confiance dans le stockage en nuage. Comme indiqué plus haut, la plupart des grands fournisseurs de services de stockage en nuage disposent d'équipes composées des meilleurs ingénieurs en sécurité au monde qui travaillent chaque jour à la protection de leurs produits et offrent à leurs clients une assistance en matière de sécurité qui va au-delà de ce que la plupart des petits services informatiques pourraient être en mesure d'offrir par eux-mêmes. Il faut toutefois garder à l'esprit que les services traditionnels de stockage en nuage nécessitent généralement d'accorder l'accès aux données sensibles à une société tierce qui fournit le service. **Cela dit, chaque parlement devra tenir compte de ses propres considérations politiques et exigences légales (telles que les mandats de localisation des données) pour décider s'il peut faire confiance à un fournisseur de stockage en nuage donné et l'utiliser.**

QUEL FOURNISSEUR DE STOCKAGE EN NUAGE CHOISIR ?

Si votre parlement n'a pas à tenir compte d'exigences en matière de localisation des données et n'a aucun problème avec le partage de l'accès aux données par une entreprise tierce de confiance, les deux options de stockage en nuage les plus populaires sont Google Workspace (anciennement connu sous le nom de GSuite) et Microsoft 365. Si votre parlement utilise déjà Gmail, l'inscription à Google Workspace et le stockage des données dans Google Drive avec ses applications intégrées Google Docs, Sheets et Slides pour le traitement de texte, les feuilles de calcul et les présentations sont très utiles. De même, si votre parlement dépend d'Excel et de Word, le choix le plus simple est de s'inscrire à Microsoft 365, qui lui donne accès à Outlook pour le courriel et aux versions sous licence de Microsoft Word, Excel, Powerpoint et Teams.

QUE SE PASSE-T-IL SI NOUS DEVONS CONTRÔLER NOS PROPRES DONNÉES OU NOUS CONFORMER AUX LOIS SUR LA LOCALISATION DES DONNÉES ?

Pour de nombreux parlements, une option aussi simple n'est peut-être pas réalisable en raison des exigences en matière de localisation des données ou des attentes spécifiques qui requièrent un contrôle exclusif du parlement sur ses propres données. La bonne nouvelle, c'est que les fournisseurs de stockage en nuage sécurisé ont récemment développé des options qui permettent aux entreprises clientes de choisir l'emplacement de leurs données (notez que cela est principalement limité aux clients européens pour l'instant), ou de contrôler leurs propres clés de chiffrement. **En pratique, cela signifie que votre parlement a la possibilité de contrôler ses propres données tout en bénéficiant de l'infrastructure et de la sécurité du stockage en nuage.**

Si votre entreprise utilise actuellement ou souhaite utiliser Google Workspace pour le stockage et le partage de données dans le nuage, Google a introduit une fonctionnalité permettant le **Cryptage côté client** pour les organisations Enterprise Plus. Bien qu'elle soit actuellement en phase de test et qu'elle ne soit disponible que pour les plans Google Workspace les plus chers, cette fonctionnalité permet de profiter de l'ensemble des fonctions de stockage et de partage de données de Google Drive, ainsi que des fonctions de sécurité qui y sont intégrées, tout en limitant la capacité de Google à accéder aux informations sensibles ou privées de votre parlement. Avec le chiffrement côté client, vous pouvez choisir d'intégrer un service supplémentaire de gestion des clés, tel que Virtru, et permettre aux utilisateurs de gérer leurs propres clés de chiffrement sans autoriser l'accès à Google lui-même. Un tel service exige que chacun prenne soin de protéger ces clés afin de protéger correctement l'accès au système de gestion des clés que vous avez choisi d'intégrer à l'espace de travail Google. Les administrateurs de compte peuvent en savoir plus sur l'activation du chiffrement côté client sur la **page d'assistance** de Google Workspace.

Si votre parlement utilise actuellement ou s'intéresse à Microsoft 365 pour le stockage et le partage de données dans le nuage, il propose une option légèrement plus complexe mais bien établie pour gérer vos propres clés de chiffrement, connue sous le nom de **Microsoft 365 Double Key Encryption.** Cette option de sécurité nécessite **Microsoft 365 E5**, mais vous permet de garder le contrôle de toutes les données parlementaires sensibles ou privées et d'en limiter l'accès même à Microsoft elle-même.

Tresorit est une autre option plus simple à mettre en œuvre si votre parlement craint de permettre à un tiers d'accéder à vos informations internes. Tresorit fournit un chiffrement de bout en bout pour le stockage en nuage et le partage de fichiers, et offre une gamme d'options de résidence des données.

QUE SE PASSE-T-IL SI NOUS NE POUVONS FAIRE CONFIANCE À AUCUNE SOLUTION DE STOCKAGE EN NUAGE ?

Si vous choisissez de faire cavalier seul et de vous appuyer sur des serveurs locaux pour stocker les données de votre parlement, il est essentiel que vous investissiez beaucoup de temps et de ressources dans le renforcement des défenses numériques des appareils de votre parlement et que vous veilliez à ce que ces serveurs soient correctement configurés, chiffrés et physiquement sécurisés. Comme indiqué ci-dessus, une telle approche nécessite d'identifier, d'embaucher et de conserver un certain nombre de personnes dévouées et hautement qualifiées dans le domaine de la cybersécurité afin de maintenir la sécurité de votre infrastructure de serveurs locaux.

Renforcer la sécurité des comptes en nuage parlementaires

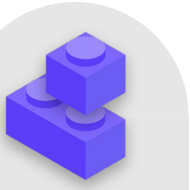
Si votre parlement choisit de configurer un domaine dans Google Workspace ou Microsoft 365, sachez que ces deux sociétés offrent des niveaux de sécurité plus élevés pour les comptes à risque. **Le Programme Protection Avancée de Google** et **Microsoft's AccountGuard** offrent une sécurité encore plus solide à tous les comptes en nuage des organisations éligibles et vous aident à réduire considérablement la probabilité de hameçonnage efficace et de compromission des comptes. Si vous pensez que votre parlement satisfait aux conditions requises et que vous souhaitez faire adhérer vos membres et votre personnel à l'un ou l'autre de ces programmes, visitez les sites Web indiqués ci-dessus ou contactez **cyberhandbook@ndi.org** pour obtenir une assistance supplémentaire.

SAUVEGARDE DES DONNÉES

Que votre parlement stocke des données sur des dispositifs physiques ou des serveurs dans le nuage, il est important de disposer d'une sauvegarde. Gardez à l'esprit que si vous dépendez d'un dispositif de stockage physique, il est assez facile de perdre l'accès à vos données. Vous pourriez renverser du café sur votre ordinateur et en détruire le disque dur. Les ordinateurs du personnel pourraient être piratés et tous les fichiers locaux verrouillés par un ransomware. Quelqu'un pourrait perdre un appareil dans un train ou se le faire voler avec sa mallette. Comme mentionné ci-dessus, c'est une autre raison pour laquelle l'utilisation du stockage en nuage peut être un avantage, car ce dernier n'est pas lié à un appareil spécifique qui peut être infecté, perdu ou volé. Les Macs sont dotés d'un logiciel de sauvegarde intégré appelé **Time Machine** qui s'utilise avec un périphérique de stockage externe ; pour les appareils Windows, **Historique des fichiers** offre une fonctionnalité similaire.Les appareil iPhone et Android peuvent sauvegarder automatiquement leurs contenus les plus importants dans le nuage si cette option est

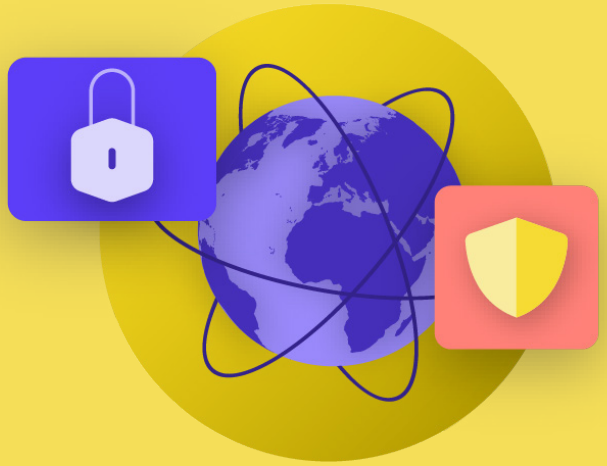
activée dans les paramètres de votre téléphone.
Si votre parlement utilise un stockage en nuage (comme Google Drive), le risque que Google soit mis hors service ou que vos données soient effacées en cas de catastrophe est assez faible, mais l'erreur humaine (comme la suppression accidentelle de fichiers importants) reste possible. Il peut être intéressant de se tourner vers une solution de sauvegarde en nuage comme Backupify ou SpinOne Backup.

Si les données sont stockées sur un serveur local et/ou des dispositifs locaux, une sauvegarde sécurisée devient encore plus indispensable. Vous pouvez sauvegarder les données de votre parlement sur un disque dur externe ou une série de disques, mais veillez à chiffrer ces disques avec un mot de passe fort. Time Machine peut chiffrer les disques durs pour vous. Vous pouvez également utiliser des outils de chiffrement fiables pour l'ensemble de vos disques durs, comme VeraCrypt ou BitLocker. Veillez à conserver vos dispositifs de sauvegarde dans un endroit distinct de vos autres dispositifs et fichiers. N'oubliez pas qu'un incendie qui détruit à la fois vos ordinateurs et leurs sauvegardes vous prive de toute sauvegarde.Pensez à conserver une copie dans un endroit très sûr, comme un coffre-fort.



Stocker des données en toute sécurité

- **Stockez vos données sensibles exclusivement dans un service de stockage en nuage de confiance.**
  - Veillez à ce que tous les comptes connectés utilisés pour accéder à un tel service soient dotés de mots de passe forts et d'un système 2FA.
- **Définissez et appliquez une politique afin de limiter les paramètres de partage au sein du nuage.**
  - Formez l'ensemble des membres et du personnel sur la manière de partager correctement (et non de surpartager) les documents.
- **Si votre parlement opte pour le stockage local des données, investissez dans un personnel informatique qualifié.**
- **Assurez la sécurité de vos sauvegardes de données en chiffrant les disques durs ou autres dispositifs de sauvegarde.**



Rester en sécurité sur Internet

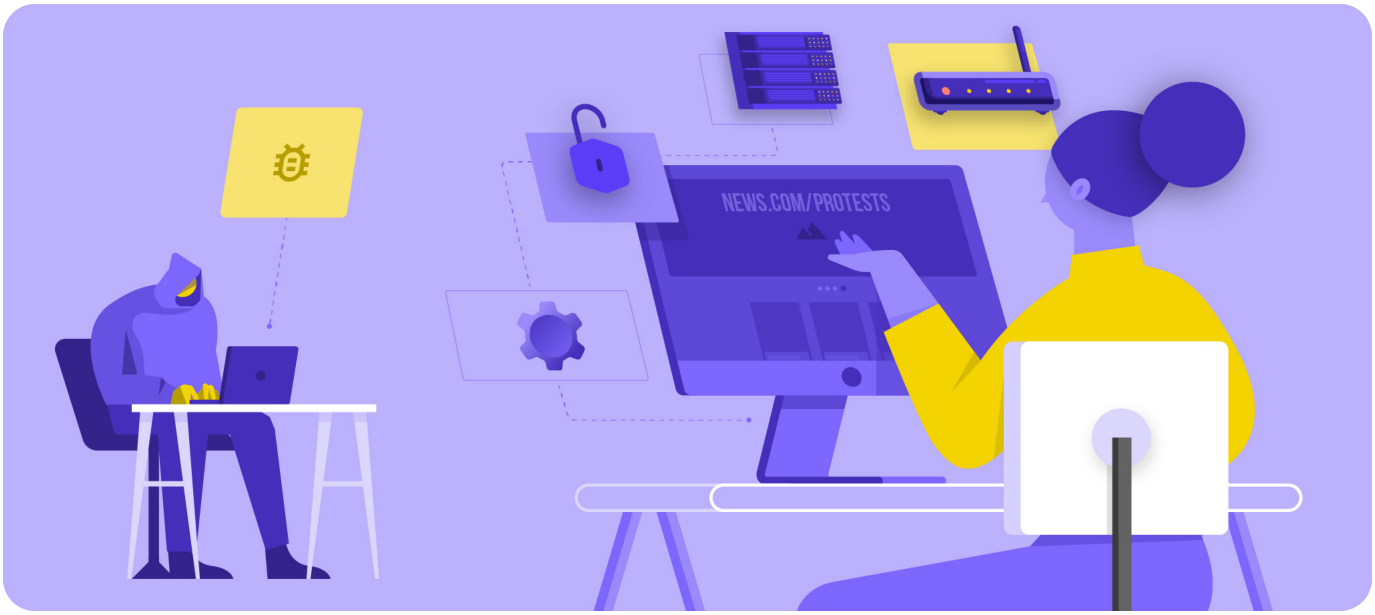
Lorsque vous utilisez Internet sur votre téléphone ou votre ordinateur, votre activité peut en dire long sur vous et votre organisation.

Il est important de conserver les informations sensibles, comme les noms d'utilisateur et les mots de passe que vous saisissez sur un site web, vos publications sur les médias sociaux ou, dans certains contextes, même les noms des sites web que vous visitez, à l'abri des regards indiscrets. Le blocage ou la restriction de votre accès à certains sites ou applications constitue également une préoccupation courante. Ces deux problèmes (surveillance d'Internet et censure d'Internet) vont de pair et les stratégies visant à réduire leurs impacts sont similaires.

Naviguer en toute sécurité

UTILISATION DE HTTPS

L'étape la plus importante pour limiter la capacité d'un adversaire à surveiller votre parlement en ligne consiste à minimiser la quantité d'informations disponibles sur votre activité sur Internet et celle de vos collègues. Vérifiez toujours que vous vous connectez à des sites web en toute sécurité : assurez-vous que l'URL (emplacement) commence par « https » et affiche une petite icône de cadenas dans la barre d'adresse de votre navigateur. Lorsque vous naviguez sur Internet **sans chiffrement,** les informations que vous saisissez sur un site (comme les mots de passe, les numéros de compte ou les messages), ainsi que les détails du site et des pages que vous visitez sont tous exposés. Cela signifie que (1) les pirates présents sur votre réseau, (2) votre administrateur réseau, (3) votre fournisseur d'accès à Internet et toute entité avec laquelle ils pourraient partager des données (comme les autorités gouvernementales), (4) le fournisseur d'accès à Internet du site que vous visitez et toute entité avec laquelle ils pourraient partager des données, et bien sûr (5) le site que vous visitez lui-même ont tous accès à un certain nombre d'informations potentiellement sensibles.



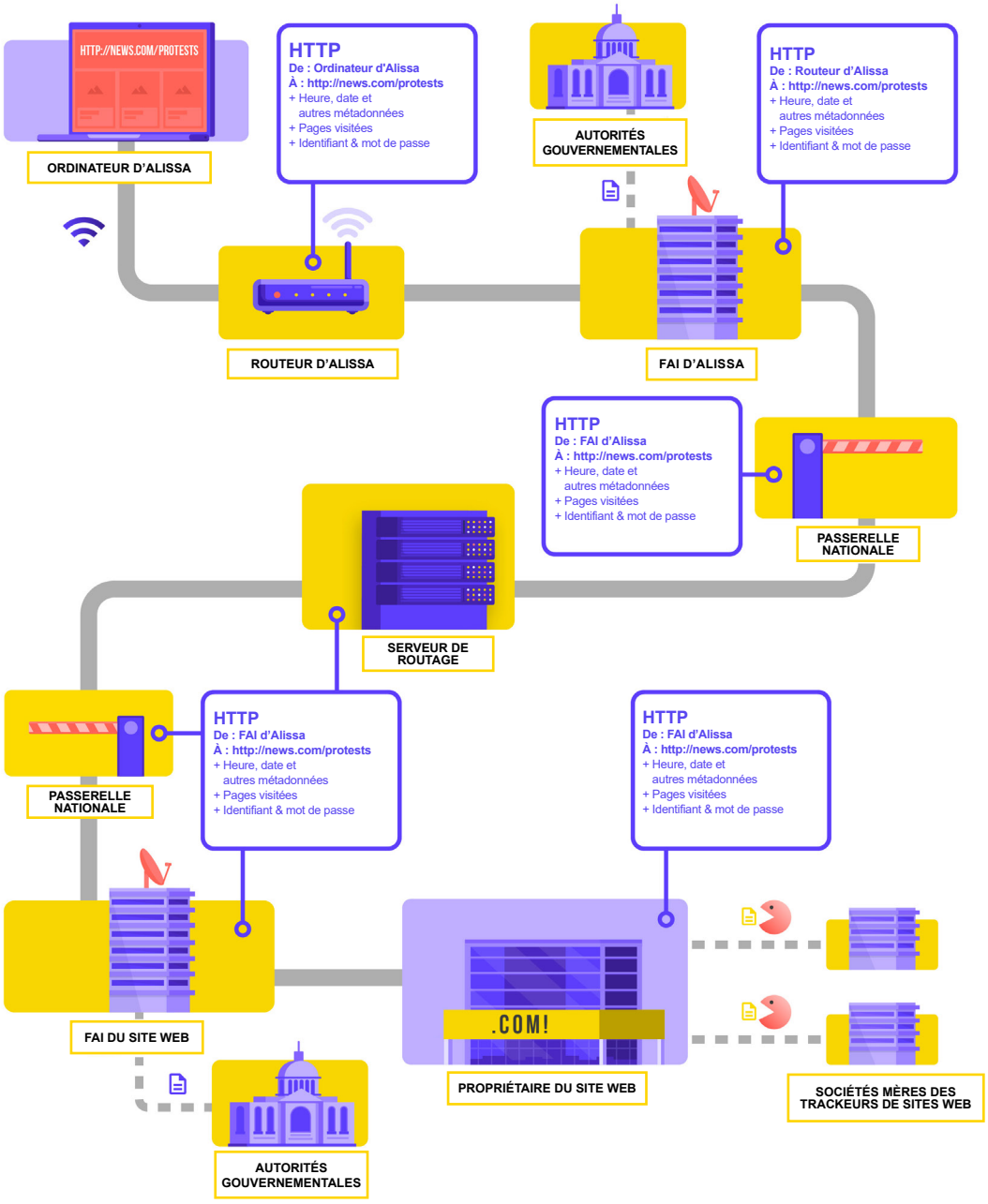
Surveillance, censure et parlements

Des gouvernements hostiles et d'autres acteurs menaçants du monde entier utilisent des technologies de surveillance de plus en plus accessibles et, dans certains cas, un simple piratage du réseau Wi-Fi, pour surveiller l'activité en ligne des députés et d'autres personnes travaillant au Parlement. Par exemple, en 2013, des pirates ont volé des données au personnel et aux visiteurs du Parlement européen en **usurpant le réseau Wi-Fi public du Parlement**. Un avant-goût d'attaques beaucoup plus sophistiquées dans les années à venir.

Outre le détournement du trafic Internet et le vol de données, les adversaires perturbent également les opérations parlementaires critiques en bloquant l'accès à Internet et aux systèmes. À Bruxelles, le parlement belge a été mis hors service par une **attaque massive par déni de service** en mai 2021. L'attaque a forcé le report de certains débats et réunions de commissions, car les utilisateurs ne pouvaient pas accéder aux services virtuels nécessaires pour participer à la session.

La fréquence croissante de ces attaques contre l'accès et la liberté d'information en ligne montre à quel point il est essentiel pour les parlements de comprendre les risques liés à l'utilisation d'Internet et de développer des programmes pour se connecter lorsque la connectivité est affectée.

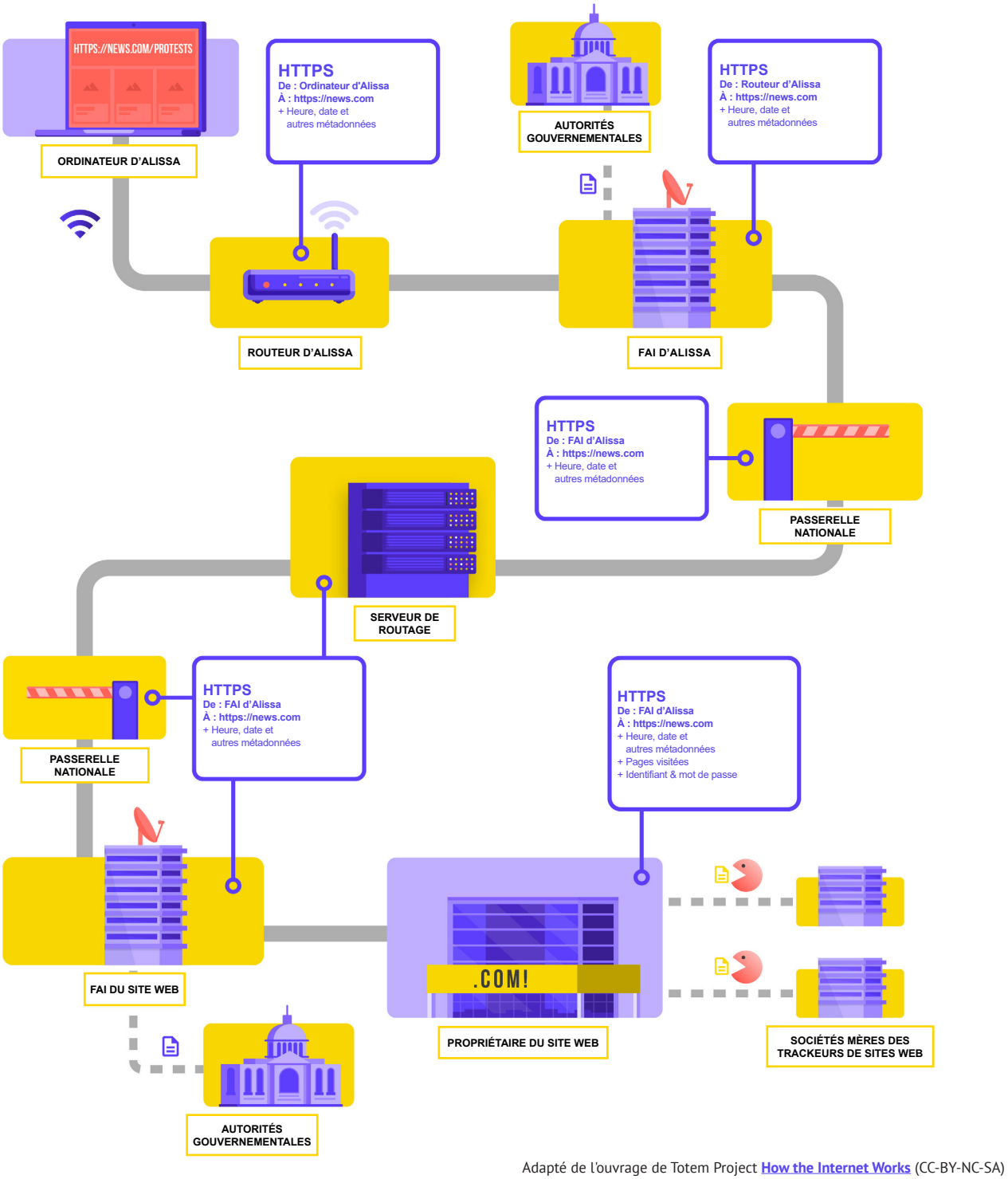
Prenons un exemple concret de ce à quoi ressemble la navigation sans chiffrement :



Adapté de l'ouvrage de Totem Project How the Internet Works (CC-BY-NC-SA)

Lorsque vous naviguez sans chiffrement, toutes vos données sont exposées. Comme illustré ci-dessus, un adversaire peut voir où vous êtes, que vous allez sur news.com, que vous regardez spécifiquement la page sur les manifestations dans votre pays,et peut-être le plus important en tant que député ou membre du personnel parlementaire, voir le mot de passe que vous partagez pour vous connecter au site lui-même. Si ces informations tombent entre de mauvaises mains, elles exposent non seulement votre compte, mais donnent également à des adversaires potentiels, où qu'ils se trouvent dans le monde, une bonne idée de ce que vous faites ou pensez.

L'utilisation de **HTTPS (le « s » signifie sécurisé) signifie qu'un chiffrement est en place.** Cela vous offre beaucoup plus de protection. Voyons à quoi ressemble la navigation avec le HTTPS (c'est-à-dire avec un chiffrement) :



Adapté de l'ouvrage de Totem Project How the Internet Works (CC-BY-NC-SA)

Avec le HTTPS, un adversaire potentiel ne peut plus voir votre mot de passe ou d'autres informations sensibles que vous pourriez partager avec un site web. Ils peuvent cependant toujours voir quels domaines (par exemple, news.com) vous visitez. Et bien que le protocole HTTPS chiffre également les informations relatives aux différentes pages d'un site (par exemple, website.com/protests) que vous visitez, des adversaires rusés peuvent toujours voir ces informations en inspectant votre trafic internet. Avec le protocole HTTPS, un adversaire pourrait savoir que vous allez sur news.com, mais il ne pourrait pas voir votre mot de passe, et il lui serait plus difficile (mais pas impossible) de voir que vous cherchez des informations sur les protestations (pour utiliser ce seul exemple). Il s'agit là d'une différence importante. Vérifiez toujours que le protocole HTTPS est en place avant de naviguer sur un site web ou de saisir des informations sensibles. Vous pouvez également utiliser **l'extension de navigateur HTTPS Everywhere** afin de vous assurer que vous utilisez le HTTPS à tout moment, ou si vous utilisez Firefox, activez le mode **HTTPS uniquement** à partir du navigateur.

Si votre navigateur vous avertit qu'un site web n'est peut-être pas sûr, ne l'ignorez pas. Il y a un problème. Il peut s'agir d'un problème bénin, comme l'expiration du certificat de sécurité d'un site ou d'une usurpation d'identité malveillante. Dans tous les cas, il est important de tenir compte de l'avertissement et de ne pas se rendre sur le site. Le protocole HTTPS est essentiel et les DNS chiffrés offrent une protection supplémentaire contre l'espionnage et le blocage de sites, mais si votre parlement s'inquiète d'une surveillance très ciblée de vos activités en ligne et est confrontée à une censure sophistiquée en ligne (blocage de sites Web et d'applications, par exemple), il est préférable d'utiliser un réseau privé virtuel (en anglais « virtual private network, VPN ») de confiance.

Utilisation de DNS chiffrés

Si vous voulez qu'il soit plus difficile (mais pas impossible) pour un FAI de connaître les informations sur les sites Web que vous visitez, vous pouvez utiliser des DNS chiffrés.

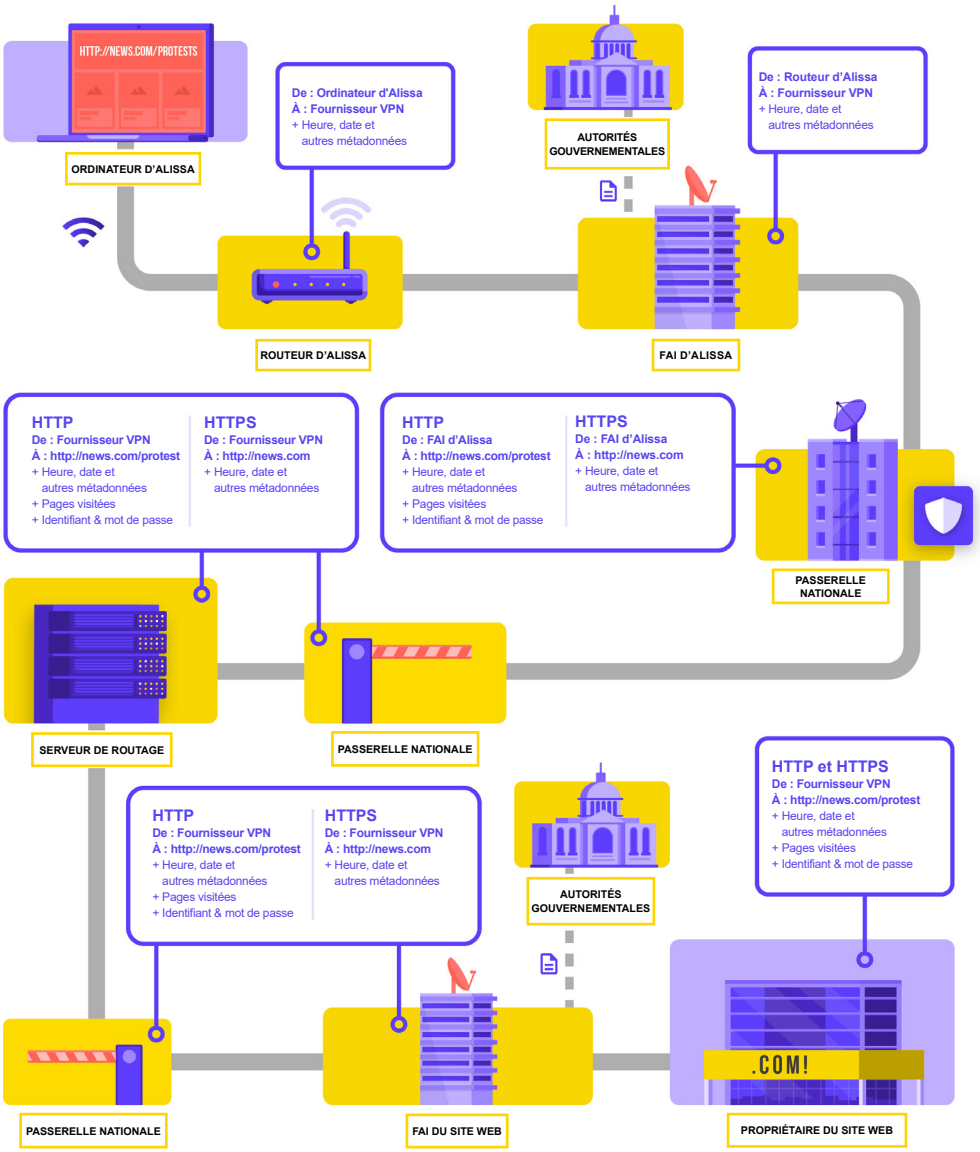
Si vous vous **posez la question**, DNS est l'abréviation de Domain Name System. Il s'agit essentiellement du répertoire téléphonique d'Internet, qui traduit les noms de domaine adaptés aux humains (comme ndi.org) en adresses de protocole Internet (IP) adaptées au web. Cela permet aux gens d'utiliser des navigateurs web pour rechercher et charger facilement des ressources Internet et visiter des sites web. Par défaut, cependant, le DNS n'est pas chiffré.

Pour utiliser des DNS chiffrés et ajouter un peu de protection à votre trafic Internet en même temps, une option facile consiste à télécharger et à activer **l'application 1.1.1.1 de Cloudflare** sur votre ordinateur et votre appareil mobile. D'autres options de chiffrement des DNS, dont le 8.8.8.8 de Google, sont disponibles mais nécessitent **plus d'étapes techniques** pour être configurées. Si vous utilisez le navigateur Firefox, le chiffrement des DNS est désormais activé par défaut. Les utilisateurs des navigateurs Chrome ou Edge **peuvent activer les DNS** chiffrés via les paramètres de sécurité avancés du navigateur en activant « Utiliser un DNS sécurisé » et en sélectionnant « Avec : Cloudflare (1.1.1.1) » ou le fournisseur de leur choix.

La solution 1.1.1.1 de Cloudflare avec WARP permet de chiffrer vos DNS et de crypter vos données de navigation, offrant ainsi un service similaire à un VPN traditionnel. Bien que WARP ne protège pas entièrement votre emplacement contre tous les sites Web que vous visitez, il s'agit d'une fonction facile à utiliser qui peut aider le personnel de votre parlement à profiter d'un DNS chiffré et d'une protection supplémentaire de la part de votre FAI dans les situations où un VPN complet n'est pas fonctionnel ou est nécessaire compte tenu du contexte lié aux menaces. Dans les paramètres DNS avancés 1.1.1.1 avec WARP, le personnel peut également activer 1.1.1.1 pour les familles afin de fournir une protection supplémentaire contre les logiciels malveillants lors de l'accès à Internet.

QU'EST-CE QU'UN VPN ?

Un VPN est essentiellement un tunnel qui protège contre la surveillance et le blocage de votre trafic Internet par les pirates de votre réseau, votre administrateur réseau, votre fournisseur d'accès Internet et toute personne avec laquelle ils pourraient partager des données. Dans une grande organisation - comme un parlement - les VPN « professionnel » ou « d'entreprise » sont souvent utilisés pour aider à protéger l'intégrité de l'accès aux systèmes et applications internes (tels que ceux utilisés pour le vote à distance). Qu'il s'agisse d'un VPN personnel ou d'un VPN conçu à des fins professionnelles, le concept de protection de votre trafic internet contre l'espionnage fonctionne généralement de la même manière, et il reste essentiel de continuer à utiliser HTTPS (même avec le VPN en place). Il est également essentiel de s'assurer que vous faites confiance au VPN utilisé par votre parlement. Voici un exemple de ce à quoi ressemble la navigation avec un VPN :



Adapté de l'ouvrage de Totem Project [How the Internet Works](#) (CC-BY-NC-SA)

Pour décrire les VPN de manière plus approfondie, cette section fait référence au **guide Surveillance Self-Defense** de l'EFF :

Les VPN traditionnels sont conçus pour masquer votre adresse IP réelle et créer un tunnel chiffré pour le trafic Internet entre votre ordinateur (ou votre téléphone ou tout autre appareil « intelligent » en réseau) et le serveur du VPN. Étant donné que le trafic dans le tunnel est chiffré et envoyé à votre VPN, il est beaucoup plus difficile pour des tiers, comme les fournisseurs d'accès à Internet ou les pirates sur les réseaux Wi-Fi publics, de surveiller, modifier ou bloquer votre trafic. Après avoir traversé le tunnel entre vous et le VPN, votre trafic quitte ensuite le VPN vers sa destination finale, en masquant votre adresse IP d'origine. Cela permet de dissimuler votre emplacement physique pour quiconque examine le trafic après qu'il a quitté le VPN. Cela vous offre plus de confidentialité et de sécurité, mais l'utilisation d'un VPN ne vous rend pas complètement anonyme en ligne : votre trafic est toujours visible pour l'opérateur du VPN. Votre FAI saura également que vous utilisez un VPN, ce qui pourrait augmenter votre profil de risque.

Cela signifie qu'il **est essentiel de choisir un fournisseur de VPN digne de confiance.** Dans certains pays, comme l'Iran, des gouvernements hostiles ont mis en place leurs propres VPN afin de pouvoir suivre les activités des citoyens. Pour trouver le VPN qui convient à votre parlement et à son personnel, vous pouvez évaluer les VPN en fonction de leur modèle économique et de leur réputation, des données qu'ils collectent ou non, et bien sûr de la sécurité de l'outil lui-même.

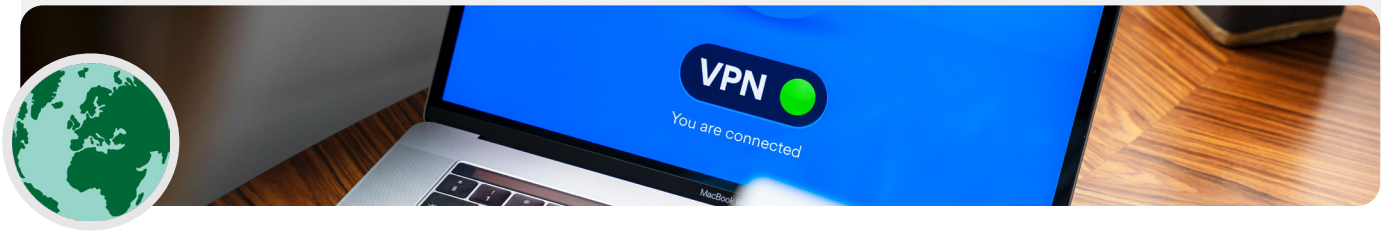
Pourquoi ne pas simplement utiliser un VPN gratuit ? La réponse courte est que la plupart des VPN gratuits, y compris ceux qui sont préinstallés sur certains smartphones, sont assortis de contreparties importantes. Comme toutes les entreprises et tous les fournisseurs de services, les VPN doivent subsister d'une manière ou d'une autre. Si le VPN ne vend pas son service, comment peut-il maintenir son activité à flot ? Sollicite-t-il des dons ? Les services premium sont-ils payants ? Est-il soutenu par des organisations caritatives ou des bailleurs de fonds ? Malheureusement, de nombreux VPN gratuits gagnent leur argent en collectant puis en vendant vos données.

Un fournisseur de VPN qui ne collecte pas de données en premier lieu constitue une meilleure option. Si les données ne sont pas collectées, elles ne peuvent être vendues ou remises à un gouvernement étranger si celui-ci le demande. Lorsque vous consultez la politique de confidentialité d'un fournisseur de VPN, vérifiez si le VPN collecte effectivement les données des utilisateurs. S'il n'est pas explicitement indiqué que les données de connexion de l'utilisateur ne sont pas enregistrées, il y a de fortes chances pour qu'elles le soient. Même si une entreprise prétend ne pas enregistrer les données de connexion, ce n'est pas toujours le cas et cela ne garantit pas une bonne conduite.

Cela vaut la peine d'effectuer une recherche sur l'entreprise qui est derrière le VPN. Est-elle approuvée par des professionnels indépendants de la sécurité ? Le VPN fait-il l'objet d'articles de presse ? L'entreprise a-t-elle déjà été surprise en train de tromper ou de mentir à ses clients ? Si le VPN a été établi par des personnes connues au sein de la communauté de la sécurité de l'information, il est plus probable qu'il soit digne de confiance. Soyez sceptique à l'égard d'un VPN qui offre un service sur lequel personne ne veut miser sa réputation ou qui est géré par une société que personne ne connaît.

Les faux VPN dans le monde réel

Fin 2017, à la suite d'une recrudescence des manifestations dans le pays, **les Iraniens ont commencé à découvrir une version « gratuite » (mais fausse) d'un VPN populaire partagée par SMS**. Le VPN gratuit (qui n'a pas réellement fonctionné) promettait de donner accès à Telegram, qui était alors bloqué localement. Malheureusement, la fausse application n'était rien d'autre qu'un logiciel malveillant qui permettait aux autorités de suivre les déplacements et de surveiller les communications de ceux qui l'avaient téléchargée.



Alors quel VPN utiliser ?

Si, en plus d'assurer la sécurité du trafic Internet parlementaire, vous avez également besoin d'une solution pour limiter en toute sécurité l'accès aux systèmes et applications parlementaires internes aux seules personnes de votre réseau parlementaire (même lorsqu'elles travaillent à distance), vous pouvez mettre en œuvre un VPN « professionnel » ou « d'entreprise ». Il existe une gamme d'options utilisant diverses technologies que vous pouvez envisager, notamment **AnyConnect** de Cisco, **Global Protect** de PaloAlto ou **Access** de Cloudflare (techniquement un système d'accès Zero Trust, et non un VPN), pour n'en citer que quelques-uns. Quoi qu'il en soit, la mise en œuvre et la gestion efficace de ces systèmes nécessitent un personnel informatique qualifié.

Si un système VPN « d'entreprise » avancé est hors budget ou inutilement compliqué pour votre parlement, vous pouvez également envisager d'utiliser des options VPN personnelles comme **ProtonVPN** ou **TunnelBear** (qui offre également un plan Teams pour simplifier la gestion des comptes) pour tous les membres et le personnel du parlement. Une autre option fiable consiste à configurer votre propre serveur en utilisant **Outline** de Jigsaw, pour lequel il n'y a pas d'entreprise qui gère votre compte, mais en contrepartie vous devez configurer votre propre serveur.

Bien que la plupart des VPN modernes se soient améliorés en termes de performances et de vitesse, il convient de garder à l'esprit que l'utilisation d'un VPN peut ralentir votre vitesse de navigation si vous êtes sur un réseau à très faible bande passante, souffrez d'une forte latence ou de retards réseau, ou subissez des coupures internet intermittentes. Si vous êtes sur un réseau plus rapide, vous devriez utiliser par défaut un VPN en permanence.

Si vous recommandez au personnel d'utiliser un VPN, il est également important de veiller à ce qu'il reste activé. Cela peut sembler évident, mais un VPN qui est installé mais ne fonctionne pas n'offre aucune protection.

Anonymat grâce à Tor

Outre les VPN, vous avez peut-être entendu parler de Tor comme d'un autre outil permettant d'utiliser Internet de manière plus sûre. Il est important de comprendre leur nature, et les raisons pour lesquelles vous pouvez utiliser l'un ou l'autre.

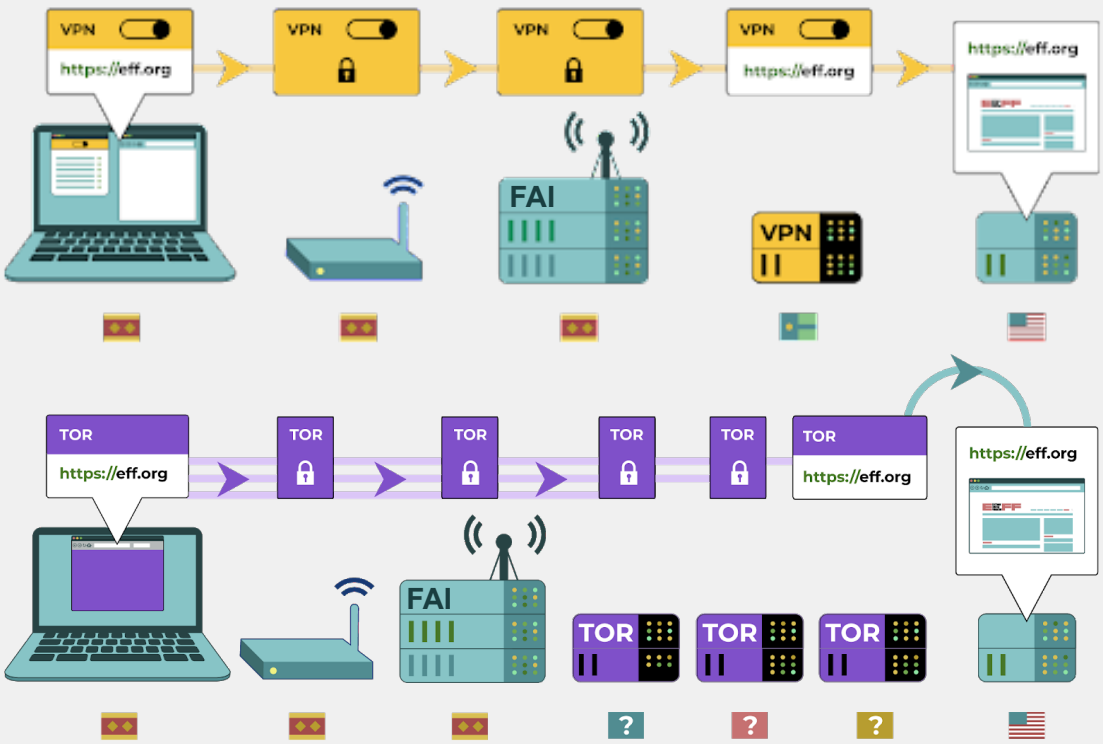
Tor est un protocole qui permet de transmettre des données de manière anonyme sur Internet en acheminant des messages ou des données à travers un réseau décentralisé. Vous pouvez en savoir plus sur le fonctionnement de Tor **ici**, mais en bref, il achemine votre trafic à travers plusieurs points sur le chemin de sa destination, de sorte qu'aucun point ne dispose d'assez d'informations pour exposer qui vous êtes et ce que vous faites en ligne au même moment.

Tor est différent d'un VPN à plusieurs égards. Plus fondamentalement, il diffère parce qu'il ne repose pas sur la confiance d'un point spécifique (comme un fournisseur de VPN).

Ce graphique, élaboré par l'EFF, montre la différence entre un VPN traditionnel et Tor.

La façon la plus simple d'utiliser Tor est à travers le **navigateur web de Tor**. Il fonctionne comme n'importe quel navigateur normal, sauf qu'il fait transiter votre trafic par le réseau Tor. Vous pouvez télécharger le navigateur Tor sur Windows, Mac, Linux ou les appareils Android. Gardez à l'esprit que lorsque vous utilisez le navigateur Tor, vous ne protégez que les informations auxquelles vous accédez **pendant que vous utilisez le navigateur.** Il n'offre aucune protection aux autres applications ou aux fichiers téléchargés que vous pourriez ouvrir séparément sur votre appareil. Gardez également à l'esprit que Tor ne chiffre pas votre trafic, donc (comme pour l'utilisation d'un VPN) il est toujours essentiel de recourir aux meilleures pratiques comme le protocole HTTPS lors de la navigation.

Si vous souhaitez étendre les protections de l'anonymat de Tor à l'ensemble de votre ordinateur, les utilisateurs les



plus avertis peuvent installer Tor comme une connexion internet à l'échelle du système, ou envisager d'utiliser le système d'exploitation Tails, qui route tout le trafic à travers Tor par défaut. Les utilisateurs d'Android peuvent également utiliser l'application Orbot pour exécuter Tor pour la totalité du trafic internet et des applications sur leur appareil. Indépendamment de la façon dont vous utilisez Tor, il est important de savoir que lorsque vous l'utilisez, votre fournisseur d'accès à Internet ne peut pas voir quels sites vous visitez, mais il peut voir que vous utilisez Tor. Comme dans le cas de l'utilisation d'un VPN, cela pourrait augmenter considérablement votre profil de risque, car Tor n'est pas un outil très courant et se distingue donc pour les adversaires qui pourraient surveiller votre trafic Internet.

Ainsi, bien qu'il y ait très peu de cas où il serait nécessaire d'utiliser Tor dans un contexte parlementaire, si vous ne pouvez pas vous permettre un VPN de confiance ou si votre parlement fonctionne dans un environnement où les VPN sont régulièrement bloqués, Tor peut être une bonne option, si elle est légale, pour limiter l'impact de la surveillance et éviter la censure en ligne.

Y a-t-il des raisons pour lesquelles nous ne devrions pas utiliser un VPN ou Tor ?

Outre les inquiétudes concernant les services VPN non réputés, le plus important est de savoir si l'utilisation d'un VPN ou de Tor peut attirer une attention non désirée ou, localement, être contraire à la loi. Bien que votre FAI ne connaisse pas les sites que vous visitez en utilisant ces services, il peut voir que vous êtes connecté à Tor ou à un VPN. Si c'est illégal là où votre parlement ou son personnel opèrent ou si cela risque d'attirer l'attention ou de présenter plus de risques que de simplement naviguer sur le web avec un protocole HTTPS standard et un DNS chiffré, peut-être qu'un VPN ou surtout Tor (qui est beaucoup moins utilisé et donc davantage sujet aux alertes) n'est pas le bon choix.

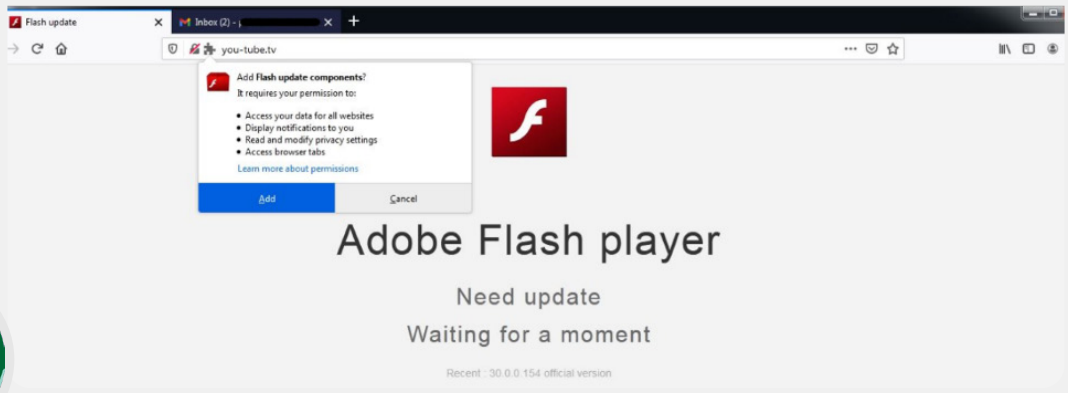
QUEL NAVIGATEUR DOIT-ON UTILISER ?

Utilisez un navigateur réputé tel que Chrome, Firefox, Brave, Safari, Edge ou Tor. Chrome et Firefox sont tous deux très largement utilisés et offrent un excellent niveau de sécurité. Certaines personnes préfèrent Firefox en raison de son orientation vers la protection de la vie privée. Quoi qu'il en soit, il est important que vous les redémarriez, ainsi que votre ordinateur, assez fréquemment pour que votre navigateur reste à jour. Si vous souhaitez comparer les caractéristiques des navigateurs, consultez cette **ressource** de la Freedom of the Press Foundation. Quel que soit le navigateur utilisé, il est également judicieux d'utiliser une extension ou un module complémentaire comme **Privacy Badger**, **uBlock Origin** ou **Privacy Essentials de DuckDuckGo** qui empêche les annonceurs et autres traceurs tiers de suivre vos déplacements et les sites que vous visitez. De plus, lorsque vous naviguez sur Internet, pensez à changer vos recherches web par défaut de Google pour **DuckDuckGo**, **Startpage**, ou un autre moteur de recherche protégeant la vie privée. Un tel changement permettra de limiter les annonceurs et les traceurs tiers également.

La sécurité des navigateurs dans le monde réel

Les attaques par extensions de navigateur ou modules complémentaires peuvent être tout aussi dommageables que les logiciels malveillants transmis directement par des téléchargements issus de hameçonnage ou d'autres logiciels. Par exemple, un **module complémentaire malveillant intelligemment conçu**, intitulé « Flash update components », a ciblé des organisations politiques tibétaines au début de l'année 2021. Le module complémentaire était présenté aux utilisateurs qui visitaient des sites web liés à des courriels d'hameçonnage et, une fois installé, il permettait aux pirates de voler des courriels et des données de navigation.

Les modules complémentaires de navigateur peuvent également être un vecteur d'infection des ressources parlementaires telles que les sites web, qui peuvent à leur tour diffuser des logiciels malveillants à un large éventail de visiteurs du site (y compris le grand public, le personnel parlementaire et les députés eux-mêmes). Prenons l'exemple de l'exploitation par des pirates du populaire module complémentaire de navigateur Browsealoud (aujourd'hui connu sous le nom de ReachDeck), un programme qui convertit le texte des sites web en audio pour les utilisateurs malvoyants. En 2018, des pirates ont inséré un code malveillant dans le module complémentaire du navigateur, qui avait été utilisé sur les sites web de diverses entités gouvernementales, y compris le **parlement de l'État de Victoria en Australie**. Le module complémentaire de navigateur infecté étant en place et mal configuré, les appareils des visiteurs du site web ont été infectés par des logiciels malveillants lors de la visite du site. Dans ce cas, le logiciel malveillant a été utilisé pour exploiter les appareils afin de miner de la crypto-monnaie, mais de telles tactiques pourraient également être utilisées par les pirates pour diffuser des logiciels malveillants à des fins de vol de données ou d'espionnage.



Sécurité des réseaux sociaux

Le personnel parlementaire et les députés peuvent révéler beaucoup de choses, et parfois plus qu'ils ne le souhaitent, en publiant et en commentant sur les réseaux sociaux.

Qu'il s'agisse de Facebook, Twitter, Instagram, YouTube ou de sites de réseaux sociaux spécifiques à une région, tels que VKontakte et Odnoklassniki, vous devez toujours bien réfléchir à ce que vous publiez et configurer correctement les paramètres de confidentialité qui existent. Cela vaut non seulement pour les pages officielles de votre parlement, mais aussi, dans certains cas, pour les comptes personnels des membres de son personnel et ceux de leur famille et de leurs amis.

Sécurité des réseaux sociaux et parlements

Même les organisations présentant un faible risque peuvent être ciblées et harcelées sur les réseaux sociaux si des politiques de sécurité adéquates ne sont pas mises en place. Dans cet exemple de 2018, un refuge pour animaux à but non lucratif a perdu des milliers de dollars et s'est mis à dos ses partisans après qu'un administrateur de compte non autorisé a mis en place une fausse collecte de fonds, et que de faux comptes se faisant passer pour des employés sont apparus sur la plateforme. Si des pirates sont prêts à tout pour gagner quelques milliers de dollars sur le dos d'un refuge pour animaux, vous pouvez imaginer les dommages que des adversaires rusés pourraient infliger s'ils parvenaient à accéder aux comptes de votre parlement ou à usurper l'identité d'un député ou d'un membre du personnel en ligne.

Outre le piratage des comptes de réseaux sociaux, les sites web des parlements sont également des cibles courantes en raison de leur visibilité publique et de l'importance de leur réputation. Dans un exemple datant de 2017, le site web du parlement autrichien a été détruit par un groupe de pirates informatiques qui était supposé être en colère contre les relations tendues du pays avec la Turquie à l'époque.

ÉLABORER UNE POLITIQUE PARLEMENTAIRE SUR LES RÉSEAUX SOCIAUX

Partez du principe que tout ce qui est publié sur les réseaux sociaux peut devenir public et élaborez une politique parlementaire en matière de réseaux sociaux en conséquence. Étant donné le caractère public de la plupart des travaux parlementaires, il est probable que vous souhaitiez partager publiquement la plupart des messages, mais il est tout de même essentiel de poser des questions et d'y répondre : Qui a accès à vos comptes de réseaux sociaux ? Qui est autorisé à publier des messages et qui doit les approuver ? Qu'en est-il des commentaires et des réponses ? Quelles informations doivent/ne doivent pas être partagées sur les réseaux sociaux ? Si vous publiez des photos, des informations de localisation ou d'autres informations permettant d'identifier votre personnel, vos membres ou vos partenaires avez-vous demandé leur permission et ont-ils envisagé les risques éventuels ? Ces questions sont particulièrement importantes si votre parlement s'engage publiquement avec les citoyens par le biais des réseaux sociaux ou de portails en ligne similaires pour l'engagement public. Outre l'élaboration de votre politique et sa clarification auprès du personnel, veillez à configurer correctement vos paramètres de confidentialité et de sécurité. Voici quelques questions clés à vous poser pour déterminer les paramètres de confidentialité et de sécurité les plus pertinents pour vos comptes personnels et parlementaires :

- Voulez-vous partager vos messages avec le public, ou seulement avec un groupe spécifique de personnes en interne ou en externe ?
- Est-ce que tout le monde doit pouvoir commenter, répondre ou interagir avec vos messages ou publications ?
- Les gens doivent-ils pouvoir vous trouver en utilisant votre adresse e-mail ou votre numéro de téléphone (personnel ou professionnel) ?
- Voulez-vous que votre localisation soit partagée automatiquement lorsque vous publiez un message ?
- Voulez-vous bloquer ou mettre en sourdine des comptes hostiles ?
- Voulez-vous bloquer des mots ou des hashtags spécifiques ?

Chaque site de réseaux sociaux a ses propres paramètres de confidentialité et de sécurité, mais ces concepts généraux s'appliquent universellement. Lorsque vous réfléchissez à ces questions, servez-vous des guides sur la confidentialité des principales plateformes : **Facebook**, **Twitter**, **Instagram**, et **YouTube**. Pour Facebook en particulier, soyez prudent quant à vos choix de confidentialité concernant les groupes. Les groupes Facebook sont très populaires pour l'engagement, la sensibilisation et le partage d'informations, mais les groupes non restreints peuvent être rejoints par n'importe qui. Il n'est pas rare que de « faux » comptes se fassent passer pour de vraies personnes dans le but d'infiltrer des groupes ou des pages de réseaux sociaux privés. Par conséquent, acceptez les demandes d'amis et d'abonnés avec précaution. N'oubliez pas que les comptes de réseaux sociaux de votre parlement ne sont aussi sûrs que les comptes qui y sont « liés ». Il est particulièrement important de s'en souvenir pour Facebook, dans la mesure où la page peut être gérée par le compte personnel d'une personne liée.

HARCÈLEMENT EN LIGNE

Malheureusement, de nombreux parlements et groupes affiliés font face à un harcèlement important en ligne, notamment sur les réseaux sociaux. Ce harcèlement est **souvent dirigé avec encore plus d'intensité vers les femmes et les populations marginalisées.** La violence en ligne contre les femmes, en particulier, peut créer un environnement hostile qui conduit à l'autocensure ou au retrait du dialogue politique ou civique. Comme l'identifie le rapport **Tweets qui donnent froid dans le dos** (Tweets that Chill) de l'équipe Genre, femmes et démocratie du NDI, lorsque les attaques contre les femmes politiquement actives sont relayées en ligne, la portée étendue des réseaux sociaux peut amplifier l'effet du harcèlement et de la violence psychologique, sapant le sentiment de sécurité personnelle des femmes d'une manière que les hommes ne subissent pas.

Lorsque votre parlement élabore sa politique en matière de réseaux sociaux, il est important d'être conscient de cette dynamique. Intégrez à votre programme de sécurité un soutien structuré pour les membres et le personnel qui sont confrontés à des messages négatifs, des insultes et des menaces sur les réseaux sociaux, tant dans le cadre de leur travail que dans leur vie personnelle. Développez une infrastructure de lutte contre le harcèlement au sein du parlement, notamment en interrogeant votre personnel afin de comprendre comment le harcèlement en ligne l'affecte et en créant une équipe réactive pour aider le personnel à faire face aux situations difficiles. Le **Online Harassment Field Manual** de PEN America fournit également des recommandations détaillées sur la manière dont vous pouvez soutenir le personnel confronté à ce type de harcèlement. Vous pourriez envisager, si votre personnel est à l'aise pour le faire, de **signaler les incidents** de harcèlement et/ou les comptes problématiques directement auprès des plateformes également.

Lorsqu'on s'adresse aux membres et au personnel qui ont été victimes de harcèlement en ligne (et dans le monde physique également), il est important de faire preuve de sensibilité. Comme le souligne le document **Take Back the Tech** du programme des droits des femmes de l'Association for Progressive Communications, comprenez qu'un survivant peut être confronté à un traumatisme et reconnaissez que la violence (en ligne ou hors ligne) n'est jamais la faute du survivant. Veillez à ce que ces questions puissent être soulevées et discutées (si le personnel est à l'aise pour le faire) dans un environnement confidentiel et sûr, avec une possibilité d'anonymat. Incluez dans le programme de sécurité de votre parlement une liste de professionnels, d'organisations et d'organismes d'application de la loi locaux auxquels vous pouvez adresser votre personnel pour obtenir une assistance juridique, médicale, psychologique et technique si nécessaire. Pour obtenir des idées supplémentaires, consultez le **guide Online Safety** de Feminist Frequency.

Maintenir vos sites web en ligne

Outre la protection de votre capacité à accéder à Internet en toute sécurité, il est également important de faire le nécessaire pour que les autres puissent accéder aux sites web ou aux ressources web de votre parlement.

Pour les pages de réseaux sociaux, cela signifie protéger ces comptes avec des mots de passe forts et uniques et une authentification à deux facteurs. Pour votre site web, cela signifie le protéger contre le piratage et les attaques par déni de service. Les attaques par déni de service distribué (DDoS) consistent à ce qu'un grand groupe d'ordinateurs noie simultanément votre serveur dans un trafic malveillant. Parmi les options de protection contre les attaques DDoS - qui font qu'il est beaucoup plus difficile pour un adversaire de faire tomber votre site web - figurent Cloudflare, AWS Shield d'Amazon, ou le service Deflect d'eQualitie.

Héberger le site Web de votre parlement en toute sécurité

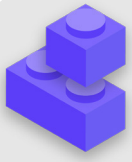
Les sites web sont hébergés sur des ordinateurs et ceux-ci sont vulnérables au piratage, tout comme vos propres appareils. Si possible, votre parlement devrait profiter des services d'hébergement existants comme WordPress, Wix ou d'autres qui gèrent toute la sécurité de vos sites pour vous. Si vos besoins en matière de site web sont plus complexes, et/ou si vous devez héberger votre site vous-même, veillez à maintenir votre système d'exploitation et votre logiciel d'hébergement à jour, comme vous le feriez pour votre ordinateur personnel. Pensez à utiliser des fournisseurs d'hébergement en nuage bien établis, tels que Amazon Web Services (AWS), Microsoft Azure ou eclips.is de Greenhost, qui offrent des options de sécurité renforcée pour les sites Web hébergés. Quels que soient les outils que vous utilisez pour héberger votre site web, assurez-vous que tous les comptes utilisés pour accéder aux paramètres d'édition et de configuration du contenu sont protégés par des mots de passe forts et une authentification à deux facteurs.

Si votre parlement dispose des connaissances techniques nécessaires pour héberger son propre site web, vous devriez envisager de choisir un site dit « statique » ou plat. Contrairement aux sites Web dynamiques, ces types de sites réduisent la surface d'attaque des pirates et rendent votre site Web plus résistant aux attaques.

Protéger votre réseau WiFi

Toutes ces mesures visant à protéger le trafic web contre la surveillance et la censure sont importantes, mais elles ne remplacent pas la sécurité de base du réseau au parlement et à la maison.

N'oubliez pas les éléments de base comme l'utilisation d'un mot de passe fort (pas le mot de passe par défaut) sur votre ou vos routeurs WiFi, la garantie que seuls les utilisateurs autorisés ont accès à votre réseau en changeant fréquemment le mot de passe, et l'activation du pare-feu intégré de vos routeurs sans fil. Envisagez également de créer un réseau invité dans les locaux parlementaires si vous avez des visiteurs qui entrent et sortent du bâtiment et qui utilisent Internet.



Rester en sécurité sur Internet

- **Organisez régulièrement des formations pour les membres et le personnel sur l'importance du respect des mesures de sécurité de base sur Internet.**
- **Rappelez au personnel de toujours naviguer avec le protocole HTTPS et un DNS chiffré.**
- **Demandez au personnel de redémarrer régulièrement son navigateur afin d'installer les mises à jour.**
- **Encouragez l'utilisation de navigateurs et d'extensions protégeant la vie privée.**
- **Si un VPN est approprié, choisissez-en un de bonne réputation, formez votre personnel à son utilisation et veillez à ce qu'il soit utilisé de manière cohérente.**
- **Élaborez et diffusez une politique parlementaire claire sur l'utilisation des réseaux sociaux.**
- **Activez les paramètres de confidentialité et de sécurité sur tous les comptes de réseaux sociaux.**
- **Comprenez les conséquences du harcèlement en ligne et préparez-vous à soutenir les membres et le personnel qui en est victime.**
- **Dressez une liste de professionnels, d'organisations et d'organismes d'application de la loi locaux auxquels vous pouvez adresser les membres et le personnel pour obtenir une assistance juridique, psychologique et technique en réponse au harcèlement en ligne.**
- **Souscrivez à une protection DDOS pour vos sites web.**
- **Utilisez un fournisseur d'hébergement web fiable et digne de confiance.**
- **Utilisez un mot de passe fort et un réseau invité pour le WiFi de vos locaux.**

Protéger la sécurité physique

Il est essentiel d'assurer la sécurité physique de vos appareils. N'oubliez pas que la sécurité physique ne se limite pas aux appareils et qu'elle doit inclure des stratégies visant à protéger tout ce qui se trouve au sein de votre environnement. Cela inclut les documents papier ; les bureaux du parlement ; les chambres ou les espaces de travail ; et bien sûr, vous-même, votre personnel et vos membres.

Sécurité physique et parlement

Malheureusement, les attaques physiques contre parlements et les autres organes législatifs ne sont pas rares et ont souvent des répercussions importantes sur la sécurité physique et la sécurité des informations. Le 6 janvier 2021, des insurgés ont pris d'assaut le Capitole des États-Unis - où siègent les deux chambres du Parlement américain - dans le but d'empêcher la certification des résultats de l'élection présidentielle. L'attaque physique a tragiquement fait cinq morts et a causé une détresse psychologique importante aux membres et aux personnel du Congrès. Mais ce n'est pas le seul impact négatif. Les attaquants ont également détruit des équipements informatiques, accédé à des documents sensibles dans les bureaux des membres et, ce qui est peut-être le plus dommageable, volé des ordinateurs et d'autres appareils contenant des informations potentiellement confidentielles du Congrès américain. des États-Unis.

Installations d'informations compartimentées sensibles (SCIF)

Pour tenir des conversations très sensibles, certains parlements disposent de salles physiques sécurisées appelées SCIF. Ces espaces sont créés pour que les informations sensibles, telles que les questions liées à la sécurité nationale ou au renseignement, puissent être vues et discutées par les députés et leur personnel sans crainte d'une surveillance extérieure ou d'un espionnage. En plus d'une construction physique correcte, un SCIF adéquat nécessite que les personnes laissent leurs appareils (tels que leurs téléphones portables) à l'extérieur de la pièce avant d'entrer pour la discussion.

Protection des actifs physiques

La sécurité physique de vos appareils est un élément essentiel de la sécurité des informations.

Outre les mesures visant à atténuer l'impact du vol d'un appareil en utilisant des écrans de verrouillage et des mots de passe, en mettant en œuvre un chiffrement complet du disque et en activant des fonctions d'effacement à distance, vous devez également réfléchir à des moyens d'empêcher le vol de ces appareils. Pour rendre le vol plus difficile, veillez à installer des serrures solides (et à les faire changer à chaque changement de personnel) dans les locaux parlementaires et/ou à la maison. En outre, envisagez d'acheter un coffre-fort pour ordinateurs portables ou une armoire verrouillable afin de protéger les appareils pendant la nuit. Les systèmes de caméras ou de détecteurs de mouvement autour des locaux peuvent détecter et, espérons-le, décourager les effractions et les vols. Recherchez une option **respectueuse de la vie privée** disponible dans votre pays et veillez à sélectionner des caméras et des systèmes de sécurité fournies par des entreprises de confiance qui n'ont pas intérêt à transmettre des données et des informations à un adversaire potentiel.

Si de vieux appareils contiennent encore des informations mais ne sont plus utilisés, pensez à les effacer. **Ce guide** de Wirecutter est une excellente ressource qui vous explique comment procéder pour la plupart des appareils modernes. S'il n'est pas possible d'effacer vos appareils, vous pouvez également les détruire physiquement. La méthode la plus simple, voire la plus respectueuse de l'environnement, consiste à détruire les appareils et leurs disques durs à l'aide d'un marteau. Parfois, les solutions les plus traditionnelles sont toujours les plus efficaces !

Avant même de passer à ces étapes techniques, prenez le temps de dresser un inventaire de tous les équipements du parlement. Si vous ne disposez pas d'une liste de tous vos appareils, il est plus difficile de savoir ce qui peut manquer en cas de vol.

QUE FAISONS-NOUS DE TOUT CE PAPIER ?

Il est probable que votre parlement dispose d'un grand nombre d'informations imprimées sur papier, écrites dans des carnets ou griffonnées sur des post-it. Certains de ces documents peuvent être très sensibles : impressions de budgets, listes de participants, lettres de donateurs et notes de réunions privées. Certains de ces documents peuvent être très sensibles, comme les notes prises lors de témoignages confidentiels ou de réunions privées. Si vous devez absolument conserver des copies papier d'informations sensibles, assurez-vous qu'elles sont stockées en toute sécurité dans une armoire verrouillée ou dans un autre endroit sûr. Ne gardez pas d'informations privées ou sensibles (y compris des mots de passe) sur votre bureau ou sur un tableau. Ne conservez aucune information privée ou sensible (y compris les mots de passe) sur un bureau ou sur un tableau. Conservez les informations très sensibles dans un endroit moins ciblé et bien protégé.

Dans la mesure du possible, essayez de détruire les informations sur papier qui ne sont pas nécessaires. N'oubliez pas que ce que vous n'avez pas ne peut pas être volé. Définissez une politique parlementaire en matière de propriété des notes sur papier et veillez à récupérer ces dernières auprès des membres du personnel s'ils décident de quitter l'organisation ou s'ils sont licenciés, tout comme vous récupéreriez un ordinateur ou un téléphone fourni par le parlement. Pour vous débarrasser des papiers sensibles, achetez une déchiqueteuse de qualité. Une activité amusante en fin de semaine peut consister à prendre une pause de 15 minutes avec vos équipes pour déchiqueter les impressions ou notes sensibles de la semaine précédente.

LA POLITIQUE PARLEMENTAIRE

Bien que, pour beaucoup, les réalités du bureau aient considérablement changé depuis le début de la pandémie de COVID-19, il est toujours important pour votre parlement de définir une politique claire en ce qui concerne l'accès aux locaux. Une telle politique doit aborder des questions clés, notamment qui est autorisé à entrer dans les locaux parlementaires (et quand), qui peut accéder à quelles ressources du bureau (comme le réseau WiFi) et que faire des invités.

Une question simple mais importante à laquelle il faut répondre est de savoir qui se voit attribuer une clé du bureau ou un badge d'accès. Seul le personnel de confiance doit être en possession des clés ou des badges et les serrures doivent être changées lors du départ du personnel et/ou sur une base semi-régulière. Pendant la journée, toute porte laissée déverrouillée doit être constamment visible par une personne de confiance et/ou d'un agent de sécurité. En outre, veillez à ce que votre parlement entretienne une relation de confiance avec les prestataires de services tels que le personnel de nettoyage et les techniciens externes qui ont accès aux locaux. Réfléchissez aux informations ou aux appareils auxquels ces personnes pourraient avoir accès et veillez à les protéger, en particulier si vous n'avez pas cette relation de confiance. Une personne de confiance doit toujours être désignée pour fermer les bureaux et les bâtiments à clé et s'assurer que les appareils sont correctement sécurisés avant de quitter le bureau à la fin de la journée.

Les électeurs sont-ils autorisés à pénétrer dans votre parlement ? Le public a-t-il le droit d'accéder à certaines parties des locaux parlementaires ? Si c'est le cas, assurez-vous qu'ils n'ont pas accès (ou au moins un accès sans surveillance) aux appareils ou aux données sensibles sur papier. S'il est obligatoire ou prévu que le public visiteur et les invités aient accès à Internet lors de leur visite, vous devez mettre en place un réseau « Invité » afin que ces derniers ne puissent pas surveiller votre trafic régulier. En général, seul le personnel de confiance doit pouvoir accéder au réseau et aux périphériques réseau tels que les imprimantes. Il est également judicieux d'exiger à ce que les invités s'inscrivent afin de disposer d'un registre des personnes qui ont visité le site.

Lorsque vous élaborez une politique de bureau, l'objectif doit être de n'autoriser que les personnes de confiance à accéder aux dispositifs, documents, espaces et systèmes sensibles.

SOUTIEN AU PERSONNEL ET AUX VOLONTAIRES

Les menaces relatives à la sécurité physique de votre parlement peuvent également toucher votre personnel. Comme le harcèlement sur les réseaux sociaux, ces menaces de sécurité physique ont souvent un impact disproportionné sur les femmes et les communautés marginalisées. Ce n'est pas seulement une question de fenêtres cassées et d'ordinateurs portables volés. L'intimidation, les menaces ou les cas de violence physique ou sexuelle, les abus domestiques et la peur d'être attaqué peuvent avoir un impact négatif profond sur la vie des membres et du personnel. L'outil de planification de la sécurité du NDI **#Think10** est une ressource utile à fournir aux femmes politiquement actives qui pourraient être exposées à un risque personnel élevé en raison de leur participation au parlement et à la politique en général.

Le bien-être du personnel est manifestement un atout important d'un point de vue individuel, mais il s'agit également d'un élément crucial pour la santé et le bon fonctionnement d'un parlement. À cette fin, réfléchissez aux ressources supplémentaires que vous pouvez fournir au personnel afin de le protéger et, en cas d'attaque physique ou numérique, de l'aider à surmonter les difficultés. Comme nous l'avons mentionné plus haut dans le manuel, cela signifie qu'il faut au minimum dresser une liste de ressources vers lesquelles le personnel peut se tourner pour obtenir une assistance juridique, médicale, psychologique et technique, si nécessaire. Une fois de plus, le **Manuel en ligne sur le harcèlement sur le terrain** de PEN America contient des idées sur la manière dont les organisations peuvent soutenir le personnel pendant et après les crises.

LA SÉCURITÉ LORS DES VOYAGES

Les voyages, que ce soit dans un autre pays ou dans une ville voisine, intensifient souvent les risques liés à la sécurité des informations physiques. On peut généralement supposer que vous et vos appareils n'avez aucun droit à la vie privée lorsque vous traversez les frontières. C'est pourquoi il est bon d'inclure dans votre programme de sécurité une politique de voyage parlementaire qui rappelle les meilleures pratiques en matière de sécurité. La politique de votre parlement en matière de voyages devrait inclure une grande partie des informations couvertes dans d'autres sections du manuel, notamment l'utilisation sécurisée d'Internet et la protection physique des appareils et des autres sources d'information, ainsi que leur présence à tout moment lors des déplacements. Dans la mesure du possible, laissez vos informations sensibles et utilisez simplement un ordinateur neuf, proprement effacé, accédez aux fichiers dont vous avez absolument besoin depuis le nuage, puis effacez-les en rentrant chez vous.

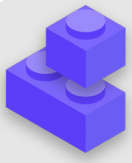
Outre la préparation des voyages et la réduction des données partagées lors des déplacements, il existe des conseils opérationnels essentiels auxquels vous devriez réfléchir et que vous devriez inclure dans votre politique de voyage parlementaire.

Envisagez d'utiliser des ordinateurs portables ou des téléphones adaptés aux voyages, sur lesquels ne sont stockées que peu ou pas de données sensibles. Si la plupart des travaux de votre parlement sont effectués dans le nuage, un Chromebook relativement bon marché peut être une bonne option. Réinitialisez ou « nettoyez » ces appareils à leur retour avant de vous connecter aux réseaux WiFi courants à la maison ou au bureau. Fournissez au personnel des informations de contact et un programme d'action indiquant ce qu'il doit faire si quelque chose ne se déroule pas comme prévu pendant le voyage. Il devrait notamment disposer d'informations sur les hôpitaux, les cliniques ou les pharmacies de la région en cas de besoin d'assistance médicale pendant au cours du voyage.

Les membres du personnel doivent également garder tous les appareils sur eux lorsqu'ils voyagent. Par exemple, gardez votre ordinateur portable à vos pieds (et non dans le compartiment supérieur ou dans un bagage enregistré) lorsque vous êtes dans un bus, un train ou un avion. Ne supposez pas qu'une chambre d'hôtel (ou même le coffre-fort de l'hôtel) est un « endroit sûr » pour conserver des appareils et des objets sensibles. Ne faites pas confiance aux ports de charge USB publics. Les ports de charge USB que l'on trouve dans les aéroports, les gares et les véhicules sont de plus en plus courants et constituent un moyen très pratique d'alimenter les appareils. Cependant, ils peuvent être un vecteur idéal pour attraper des logiciels malveillants. Veillez donc à recharger les appareils de la manière traditionnelle par le biais d'une prise murale, ou achetez des **bloqueurs de données USB** pour permettre au personnel en déplacement de recharger leurs appareils par USB en toute sécurité.

Réserver des voyages en toute sécurité pour votre parlement

Lorsque vous élaborez une politique en matière de voyages, gardez à l'esprit les informations qui pourraient être exposées lorsque vous organisez ou réservez un voyage. Cela peut être particulièrement important si vous organisez des événements ou des conférences de grande envergure pour lesquels vous traitez des informations sensibles provenant de divers membres du personnel, des membres ou des participants. Réfléchissez bien à la manière dont vous allez partager et stocker en toute sécurité (si nécessaire) des informations personnelles telles que des informations de passeport, des itinéraires de voyage et des dossiers médicaux.



Protéger votre sécurité physique

- **Rappelez aux membres et au personnel qu'ils doivent garder les appareils physiquement protégés à tout moment.**
- **Vérifiez et sécurisez tous les moyens par lesquels les gens peuvent entrer dans vos locaux.**
- **Mettez en place une politique d'accueil des invités et d'accès aux locaux.**
- **Utilisez des serrures solides, des systèmes d'identification/de badge et faites-les changer quand c'est nécessaire.**
- **Envisagez d'installer des caméras ou d'autres systèmes de sécurité sur place.**
- **Munissez-vous de déchiqueteuses.**
  - Prévoyez du temps pour que le personnel se débarrasse des documents sur papier qui contiennent des informations sensibles.
- **Dressez une liste de professionnels, d'organisations et d'organismes d'application de la loi locaux avec lesquels vous pouvez mettre les membres et le personnel en contact pour obtenir une assistance juridique, médicale et de santé mentale en réponse à des attaques ou des menaces physiques.**
- **Élaborez une politique de voyage parlementaire.**
- **Veillez à ce que le personnel sache ce qu'il faut faire en cas d'urgence lors d'un voyage.**
- **Tenez compte des données supplémentaires qui sont créées et partagées lors de l'organisation de voyages ou d'événements.**

Que faire quand les choses tournent mal

Vous savez maintenant ce qu'il faut faire. Vous avez mis en place les politiques et formé tous les membres du parlement aux meilleures pratiques. Même avec tout ce travail acharné, il est très probable que quelque chose finisse par mal tourner.

Tout peut arriver. Afin de vous prémunir contre toute éventualité, il est essentiel de mettre en place un programme de réponse aux incidents. C'est un élément crucial, et souvent sous-estimé, du programme de sécurité de votre parlement, car il peut faire la différence entre une attaque qui compromet la réputation de votre parlement et une simple perturbation. N'oubliez pas que vous ne pouvez réagir à un incident que si vous en êtes informé. Il est très important d'avoir une forte culture de la sécurité au sein du parle et d'encourager les membres et le personnel à signaler les problèmes. C'est pourquoi il est préférable de récompenser les bons comportements liés à la sécurité plutôt que de punir les manquements ou les erreurs en la matière. Il est également important d'exprimer de l'empathie et de s'assurer du bien-être du personnel lorsqu'il signale un incident. Vous voulez que le personnel signale immédiatement un clic sur un lien dans un message d'hameçonnage, un téléphone volé ou un compte de réseaux sociaux piraté, et ce, sans hésiter par crainte de représailles ou d'un manque de soutien. Après tout, la réponse aux incidents, tout comme les stratégies d'atténuation mentionnées dans d'autres sections du manuel, est un effort mené à l'échelle du parlement.

Que devez-vous programmer ? En bref, tout ce qui a une certaine probabilité de se produire. La situation sera différente pour chaque parlement, mais les questions courantes auxquelles un programme de réponse aux incidents permettra de répondre sont les suivantes :

- Que faire si nos comptes ou nos sites web sont piratés ?
- Que faire si quelqu'un clique sur un e-mail d'hameçonnage ou si un appareil a un comportement suspect ?
- Que faire si nos e-mails ou nos documents les plus sensibles sont volés et font l'objet d'une fuite ?
- Que faire si un membre de notre personnel est mis en danger physiquement ? Que faire s'ils sont en proie au stress et à l'anxiété à cause de ces menaces ?
- Que faire si notre bureau est endommagé par un incendie, une inondation ou une catastrophe naturelle ?
- Que faire en cas de perte ou de vol de l'ordinateur ou du téléphone d'un membre ?

Les réponses à ces questions et à d'autres varieront d'un parlement à l'autre, mais il est important d'y réfléchir ensemble et d'élaborer et de partager un programme clair afin que chacun soit prêt à agir immédiatement afin de limiter les dégâts. En se basant sur le guide Holistic Security de Tactical Tech, un bon point de départ pour un programme de réponse aux incidents est de **définir un incident ou une urgence** dans le contexte de votre parlement. Déterminez ce qu'est une « urgence » c'est-à-dire le moment à partir duquel nous devons commencer à mettre en œuvre les actions et les mesures d'urgence prévues. Si vous imaginez un scénario tel que la perte de contact avec un collègue en mission sur le terrain, combien de temps attendriez-vous avant de déclarer une urgence ? Il ne faut pas se précipiter, mais attendre trop longtemps peut, dans certaines circonstances, être désastreux. Il est également important de réfléchir à toutes les **étapes des opérations**. Attribuez à chaque personne un rôle clair qu'elle connaît et qu'elle a accepté à l'avance. Cela réduira la désorganisation et la panique en cas d'incident. Cette stratégie importante pour les situations d'urgence comprend l'activation d'un réseau de soutien - un vaste réseau d'alliés, qui peut inclure différentes branches de votre propre gouvernement, d'autres gouvernements amis, des entreprises technologiques, des fournisseurs de sécurité et des institutions multilatérales, pour n'en citer que quelques exemples. L'activation d'un réseau de soutien (un vaste réseau d'alliés, qui peut inclure les amis et la famille, la communauté, les alliés locaux, les ressources gouvernementales et les alliés nationaux ou internationaux comme les ONG et les journalistes) fait partie de cette importante stratégie d'urgence. Comment vos alliés peuvent-ils vous soutenir ?Devriez-vous les contacter à l'avance afin de vérifier s'ils sont prêts à vous aider en cas d'urgence et leur faire savoir ce que vous attendez d'eux ?

Lors de la réponse à un incident, il est de plus en plus important d'avoir des **communications efficaces**. Déterminez le moyen le plus sûr et le plus efficace de communiquer avec chaque acteur dans différents scénarios et identifiez un moyen de secours. Sachez qu'en cas d'urgence, il peut être utile d'avoir des directives claires sur ce qu'il faut (et ce qu'il ne faut pas) communiquer, quand il faut communiquer, quels canaux utiliser pour communiquer et avec qui il faut communiquer. Tenez également compte de l'impact d'un incident sur la réputation de votre parlement et soyez prêt à réagir en conséquence. Assurez-vous que le responsable de la communication du parlement est au courant de l'incident et qu'il peut surveiller les réseaux sociaux ou d'autres médias pour en évaluer l'impact potentiel. Ils doivent également être prêts à répondre aux éventuelles demandes de renseignements du public ou des médias concernant un incident, le cas échéant. C'est particulièrement important afin d'anticiper toute publicité négative potentielle ou toute atteinte à la réputation. Bien que chaque incident et chaque contexte soient différents, des communications sincères et transparentes permettent souvent d'instaurer la confiance à la suite d'un incident.

Création d'un système d'alerte et de réponse rapide

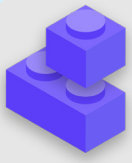
Envisagez de mettre en place un système d'alerte et de réponse rapide. Un tel système peut sembler complexe, mais il s'agit essentiellement d'un document centralisé (électronique ou autre) à ouvrir en cas d'urgence. Dans ce document, vous devez consigner tous les détails concernant les indicateurs de sécurité et les incidents qui se sont produits sur une base temporelle, fournir une description claire des actions et de la séquence relatives à la réponse prévue, et indiquer ce qui doit être réalisé pour signifier que le risque a de nouveau diminué. Il doit également comprendre les mesures à prendre après un incident afin de protéger les personnes concernées contre tout nouveau préjudice et de les aider à se rétablir physiquement et émotionnellement. Un système d'alerte précoce et de réponse peut fournir une documentation utile à partager avec les forces de l'ordre (le cas échéant), une analyse ultérieure de ce qui s'est passé et des conseils sur la manière d'améliorer vos tactiques de prévention et vos réponses aux menaces à l'avenir.

En plus de ces concepts importants de réponse aux incidents, votre parlement doit également se préparer à toute réponse **technique** spécifique. Dans certains cas, une réponse technique peut être gérée par le personnel informatique interne ou les administrateurs de système. Par exemple, si un compte courriel semble avoir été piraté, votre administrateur de compte doit être préparé et capable de fermer ou de désactiver le compte concerné. Certains incidents techniques peuvent toutefois nécessiter une expertise dont vous ne disposez pas au sein de votre parlement. Dans de telles situations, il est important d'identifier une liste de confiance d'experts techniques externes qui peuvent vous aider à répondre aux incidents. Dans certains cas, vous pouvez négocier au préalable les conditions avec les fournisseurs de services (tels que l'hébergeur de votre site web ou une entreprise de sécurité informatique) afin de vous assurer qu'ils sont disponibles (et qu'ils ne factureront pas de supplément) pour une telle réponse aux incidents techniques.

Enfin, et surtout, vous devez envisager de prendre des mesures **légales**. Il est important de comprendre les protections juridiques dont vous pouvez bénéficier, ainsi que les obligations ou conséquences juridiques auxquelles votre parlement pourrait être confronté à la suite d'une violation de données ou d'un autre incident de sécurité. En tant que parlement, vous occupez une position particulièrement importante et puissante lorsqu'il s'agit de comprendre et de respecter les réglementations locales en matière de sécurité des données et de protection de la vie privée.

Prenez le temps d'examiner les incidents possibles avec un conseiller juridique compétent, si nécessaire, et élaborez un programme afin de savoir ce que vous feriez en réponse. Il est bon de passer un accord avec ce conseiller de confiance pour qu'il vous représente et défende vos intérêts si nécessaire à la suite d'un incident. Dans le cadre de cette préparation juridique, assurez-vous que vous comprenez les obligations légales de tout vendeur ou partenaire. Sont-ils tenus de vous informer en cas de violation de leurs propres données ? Quel soutien (le cas échéant) sont-ils tenus de vous fournir en cas d'incident ? Lorsque vous élaborez des contrats et des accords avec des fournisseurs externes, gardez à l'esprit qu'une violation des données ou un autre incident pourrait survenir.

Bien qu'il n'existe pas d'approche unique pour la réponse aux incidents, il est essentiel de mettre en place des plans opérationnels, techniques, juridiques et de communication clairs. Lorsque vous élaborez votre programme de réponse aux incidents, nous vous encourageons vivement à utiliser d'excellentes ressources déjà existantes, conçues pour aider les organisations à s'orienter en matière de réponse aux incidents. Bien que ces ressources ne soient pas toutes conçues spécifiquement pour les parlements, leur contenu reste très pertinent. Ces ressources comprennent le **Digital First Aid Kit** développé par Rarenet et CiviCERT, le manuel **Online Harassment Field** de PEN America, le **Cybersecurity Campaign Playbook** et le **Cyber Incident Communications Plan Template** du Belfer Center, et le **Digital Security Helpline** d'Access Now.



Réponse aux incidents

- **Élaborez un programme de réponse aux incidents parlementaires et mettez-le en pratique.**
  - Réfléchissez aux incidents possibles et préparez votre réponse avant qu'ils ne se produisent.
- **Assurez-vous que tous les membres du parlement sont conscients de la manière dont vous communiquerez et des mesures techniques qui seront prises en cas d'incident.**
- **Prenez le temps de bien comprendre vos protections et obligations légales.**
- **Soyez prêt à fournir aux membres et au personnel du parlement le soutien émotionnel et social dont ils ont besoin à la suite d'un incident.**

Annexe A : Ressources recommandées

- Manuel de sécurité holistique de Tactical Tech ; Creative Commons Attribution-ShareAlike 4.0 International License
  - Chapter 2.4 - Understanding and Cataloguing Our Information
  - Chapter 1.5 - Communiquer sur les menaces au sein des équipes et des organisations
  - Chapter 3.4 - La sécurité au sein des groupes et des organisations
- Compagnon d'éducation à la sécurité de l'Electronic Frontier Foundation ; Creative Commons Attribution 3.0 US License
  - Threat Modeling Activity Handout
- Guide de prévention de l'hameçonnage et d'hygiène des courriers électroniques de la Freedom of the Press Foundation ; Creative Commons Attribution 4.0 International License
- Guide sur le signal de verrouillage de la Freedom of the Press Foundation ; Creative Commons Attribution 4.0 International License
- Guide d'autodéfense en matière de surveillance de l'Electronic Frontier Foundation ; Creative Commons Attribution 3.0 US License
  - What Should I Know About Encryption
  - Communicating with Others
  - Choisir le VPN qui vous convient le mieux
- Guide pour la sécurisation des outils de discussion de groupe et de conférence des Frontline Defenders
- Data Detox Kit du Tactical Tech
  - Let the Right One In: Make Your Passwords Stronger
  - Strengthen Your Screen Locks
- Guide de sécurité en matière de mots de passe dans un cadre électoral du Democracy and Technology ; Creative Commons Attribution 4.0 International License
- Guide de sécurité en matière d'authentification à deux facteurs dans un cadre électoral du Center for Democracy and Technology ; Creative Commons Attribution 4.0 International License
- Authentification à deux facteurs pour les débutants de Martin Shelton ; Creative Commons Attribution 4.0 International License
- Tactical Tech and Frontline Defender's Security in a Box ; Creative Commons Attribution-ShareAlike 3.0 Unported License
  - Protect your device from malware and phishing attacks
  - Protégez-vous contre les menaces physiques
- SANS' OUCH! Newsletter : Bloquez ce logiciel malveillant
- Accès aux appareils et aux données d'Apple lorsque la sécurité des personnes est en jeu
- Boîte à outils de cybersécurité pour les organisations basées sur une mission de la Global Cyber Alliance
- Outil d'évaluation de la cybersécurité de la Fondation Ford

Annexe B : Kit de démarrage du programme de sécurité

Utilisez le kit de démarrage suivant pour prendre des notes pendant que vous et votre parlement lisez le manuel et assimilez le matériel, et examinez les questions qui l'accompagnent avec vos collègues pour aider à générer des discussions productives.

Veillez à vous référer aux éléments clés de chaque section du manuel pour vous assurer que vous abordez les sujets importants lors de l'élaboration de votre plan de sécurité. À la fin du manuel, les éléments de base, les réponses aux questions de discussion et vos notes devraient constituer les fondements d'un plan de sécurité réussi.

Instaurer une culture de la sécurité

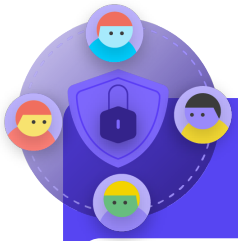
Une base solide : Sécurisation des comptes et des appareils

Communiquer des données en toute sécurité

Rester en sécurité sur Internet

Protéger la sécurité physique

Que faire quand les choses tournent mal



Instaurer une culture de la sécurité

QUESTIONS À ENVISAGER :

- Quand pouvez-vous programmer une conversation pour examiner votre programme de sécurité avec l'ensemble du parlement ?
- Quels jours ou heures conviennent le mieux au parlement pour programmer des conversations régulières et des formations sur la sécurité ?
- Quelles mesures les dirigeants peuvent-ils prendre pour donner l'exemple d'un bon comportement en matière de sécurité et d'un engagement à l'égard d'un programme de sécurité ? Comment les autres membres du parlement peuvent-ils jouer un rôle dans la sécurité ?

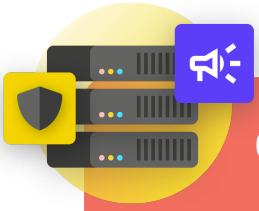
VOS REMARQUES ET IDÉES :

Une base solide : Sécurisation des comptes et des appareils

QUESTIONS À ENVISAGER :

- Comment allez-vous mettre en œuvre les mesures de sécurité des comptes - comme un gestionnaire de mots de passe et 2FA - dans l'ensemble du parlement ? Quels obstacles pourriez-vous rencontrer lors de la mise en œuvre ?
- Comment votre parlement veillera-t-il à ce que les appareils soient sécurisés et mis à jour ? Dans ce cadre, le parlement aura-t-il besoin d'un programme pour traiter les logiciels ou les ordinateurs sans licence ?
- Quel est le bon moment pour organiser une formation pour l'ensemble du personnel sur les dangers du hameçonnage, les logiciels malveillants et les meilleures pratiques en matière de sécurité des appareils ?

VOS REMARQUES ET IDÉES :

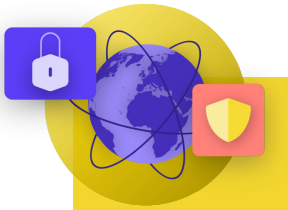


Communiquer et stocker des données en toute sécurité

QUESTIONS À ENVISAGER :

- Comment votre parlement va-t-il mettre en place une messagerie chiffrée de bout en bout pour une communication sécurisée ? Quels obstacles pourriez-vous rencontrer lors de la mise en œuvre ?
- Comment votre parlement mettra-t-il en œuvre une solution de partage de fichiers sécurisée à la fois en interne et en externe ? Quels obstacles pourriez-vous rencontrer lors de la mise en œuvre ?
- Comment votre parlement mettra-t-il en œuvre une solution de stockage et de sauvegarde des données sécurisée ? Quels obstacles pourriez-vous rencontrer lors de la mise en œuvre ?

VOS REMARQUES ET IDÉES :



Rester en sécurité sur Internet

QUESTIONS À ENVISAGER :

- Comment votre parlement mettra-t-il en œuvre des exigences de navigation sécurisée telles que HTTPS, un navigateur de confiance et, le cas échéant, un VPN pour le personnel ?
- Quels seront les éléments clés de la politique de votre parlement en matière de réseaux sociaux ? Comment sera-t-elle appliquée ?
- Comment votre parlement protégera-t-il ses sites web et ses propriétés web ?

VOS REMARQUES ET IDÉES :

Protéger la sécurité physique

QUESTIONS À ENVISAGER :

- Comment le parlement distribuera-t-il et appliquera-t-il sa politique d'accès et d'accueil des invités ?
- Qui est chargé de préparer le personnel aux problèmes de sécurité physique et numérique auxquels il pourrait être confronté lors de ses déplacements professionnels ?
- Quelles mesures le personnel peut-il prendre pour assurer la sécurité de ses appareils au bureau et lors de ses déplacements ?

VOS REMARQUES ET IDÉES :

Que faire lorsque les choses tournent mal

QUESTIONS À ENVISAGER :

- Comment le parlement distribuera-t-il et mettra-t-il en pratique sa politique de réponse aux incidents ?
- Existe-t-il des ressources disponibles pour le personnel qui pourrait avoir besoin d'un soutien émotionnel et social à la suite d'un incident ? Si ce n'est pas le cas, comment le parlement pourrait-il fournir ces ressources en cas d'incident ?

VOS REMARQUES ET IDÉES :

Annexe C : Citations d'images

Page 14 : New York Times, « Australian Parliament Reports Cyberattack on Its Computer Network », 2019, image numérique, Getty Images, https://www.nytimes.com/2019/02/07/world/australia/cyberattack-parliament-hack.html .
Page 18 : CNP Collection, « Security Protection Anti-Virus Software cms », 2014, image numérique, Alamy Stock Photo, https://www.alamyimages.fr/security-protection-anti-virus-software-cms-image67114038.html?irclickid=2oWTxrXnOxyIRKXzgq3HowdNUkDzCPSFpyViRI0&utm_source=77643&utm_campaign=Shop%20Royalty%20Free%20at%20Alamy&utm_medium=impact&irgwc=1.
Page 24 : Bleeping Computers, « Norway parliament data stolen in Microsoft Exchange attack », 2021, image numérique, https://www.bleepstatic.com/content/hl-images/2021/03/10/storting.jpg.
Page 25 : Cottonbro, « Person Holding Black and Silver Key », 2020, image numérique, Pexels, https://www.pexels.com/photo/person-holding-black-and-silver-key-5474292/?utm_content=attributionCopyText&utm_medium=referral&utm_source =pexels.
Page 27 : Blogtrepreneur, « Malware Infection », 2016, image numérique, Flickr, https://www.flickr.com/photos/143601516@N03/.
Page 30 : « Microsoft Loading Screen », image numérique, Kompass, 23 septembre 2019, https://asset.kompas.com/crops/kYVdzylbrYB5lIpuKDDwJLNFMV4=/164x49:679x393/750x500/data/photo/2018/07/02/4208974652.png .
Page 30 : Mateuz Dach, « Turned-on iPhone and Displaying Icons », 2017, image numérique, Pexels, https://www.pexels.com/photo/turned-on-iphone-and-displaying-icons-365194/.
Page 33 : ZDNet, « Chinese hacking group impersonates Afghan president to infiltrate government agencies », 2021, image numérique, https://www.zdnet.com/article/chinese-hacking-group-impersonates-afghan-president-to-infiltrate-government-agences/
Page 38 : Andrew Keymaster, « People Gathering on Street During Daytime Photo », 2020, image numérique, Unsplash, https://unsplash.com/photos/JXQ2bizu7kc.
Page 39 : Surveillance Self-Defense, « No Encryption in Transit », image numérique, Electronic Frontier Foundation, 17 janvier 2019. https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 40 : Surveillance Self-Defense, « 4.Transport-layer-alternate », image numérique, Electronic Frontier Foundation, 17 janvier 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/4.transport-layer-alternate.png. ; Surveillance Self-Defense, « 6. End-to-end Alternate », image numérique, Electronic Frontier Foundation, January 17, 2019, https://ssd.Surveillance Self-Defense.org/files/2018/11/26/6.end-to-end-alternate.png.
Page 42 : Surveillance Self-Defense, « 9._endtoendencryptionmetadata », 2019, image numérique, Electronic Frontier Foundation, https://ssd.eff.org/en/module/what-should-i-know-about-encryption.
Page 49 : Agence de presse africaine, « Parliament meeting falls victim to hacking as MPs greeted by pornographic images », 2020, image numérique, Reuters, https://www.iol.co.za/news/politics/parliament-meeting-falls-victim- au-piratage-en-tant-que-mps-accueilli-par-des-images-pornographiques-47657120
Page 51 : Parlement britannique, image numérique, Jessica Taylor, https://e3.365dm.com/20/04/768x432/skynews-parliament-house-of-commons_4974709.jpg?20200422191547
Page 52 : Brett Sayles, « Server Racks on Data Center », 2020, image numérique, Pexels, https://www.pexels.com/photo/server-racks-on-data-center-4508751/.
Page 58 : PhotoMIX Company, 2016, « White 2 Cctv Cameras Mounted on Black Post Under Clear Blue Sky », image numérique, Pexels, https://www.pexels.com/photo/white-2-cctv-camera-mounted-on-black -post-under-clear-blue-sky-96612/.
Page 63 : Stefan Coders, « laptop-screen-vpn-cyber-security », 2020, image numérique, Unsplash, https://pixabay.com/photos/laptop-screen-vpn-cyber-security-5534556/.
Page 65 : Autodéfense de surveillance, « Using the Tor Browser », image numérique, Electronic Frontier Foundation, 25 avril 2020. https://ssd.eff.org/files/2020/04/25/circumvention-tor_0.png
Page 67 : Nathan Dumlao, « White Samsung Android Smartphone on Brown Wooden Table », 2020, image numérique, Unsplash, https://unsplash.com/photos/kLmt1mpGJVg.
Page 72 : Matt Artz, « Two Broken 6-Pane On White Painted Wall Photo », image numérique, Unsplash, 1er octobre 2017, https://unsplash.com/photos/vT684iB7Ejg.


NDI
NATIONAL
DEMOCRATIC
INSTITUTE


HOUSE
DEMOCRACY
PARTNERSHIP


IRI
INTERNATIONAL
REPUBLICAN
INSTITUTE
Advancing Democracy Worldwide


USAID
FROM THE AMERICAN PEOPLE