POUR ÊTRE CYBER-SEREIN

Guide pratique de cybersécurité

HAUTE-GARONNE
NUMÉRIQUE

Soyons acteurs de la cybersécurité !

Depuis sa création en 2016, Haute-Garonne Numérique a relevé un défi majeur pour notre territoire : garantir à l'ensemble des habitants et des collectivités un accès au Très Haut Débit.

Désormais, notre mission ne s'arrête pas là. Nous nous tournons résolument vers l'avenir, avec un objectif clair : accompagner les communes et les intercommunalités dans le développement des usages numériques et la sécurisation de ces nouveaux outils.

Dans un monde où les cybermenaces sont en constante évolution, la sécurité des systèmes d'information devient une priorité incontournable. Nos collectivités, nos mairies et nos élus sont en première ligne pour protéger non seulement leurs infrastructures, mais aussi les données sensibles de leurs administrés.

C'est dans ce cadre que Haute-Garonne Numérique met à disposition son expertise pour vous accompagner dans cette transition. À l'occasion du Cybermois 2024, dont nous sommes partenaires, Haute-Garonne Numérique réaffirme son engagement pour renforcer la cybersécurité sur l'ensemble du territoire. Cette initiative nationale, dédiée à la sensibilisation et à la lutte contre les cyberattaques, est l'opportunité de promouvoir les bonnes pratiques et de fournir aux collectivités des outils indispensables à la protection de leurs systèmes.

Le guide que vous avez entre les mains a été conçu comme un outil de sensibilisation, spécifiquement destiné aux élus et responsables locaux. Il se veut à la fois pratique et opérationnel, afin que chacun puisse rapidement mettre en place de nouvelles habitudes et pratiques pour améliorer la sécurité de ses systèmes numériques.

La cybersécurité est un enjeu crucial pour nos territoires. Protéger vos systèmes, c'est protéger l'avenir de nos services publics, l'efficacité de nos administrations et la confiance des citoyens. Ensemble, agissons pour un numérique sûr, au service de nos collectivités et de leurs habitants. Soyons acteurs de la cybersécurité, ensemble.

Victor DENOUVION
Président du Syndicat Mixte Haute-Garonne Numérique

La cybersécurité, c'est quoi ?

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes.
On l'appelle également "sécurité informatique" ou "sécurité des systèmes d'information".

Haute-Garonne Numérique vous accompagne pour lutter contre la cybermalveillance.

A quelles cybermenaces ma collectivité peut-elle faire face ?

Piratage d'un système informatique professionnel :
L'intrusion dans un système informatique (serveur, réseau...) se définit comme l'accès illicite à ce système par un cybercriminel, ce qui peut entraîner le vol, voire la perte totale, des informations du système touché.

Virus informatique :
Un virus est un programme informatique malveillant qui a pour objectif de perturber le fonctionnement normal d'un appareil informatique voire de dérober des informations personnelles qu'il contient.

L'arnaque au faux ordre de virement ou FOVI :
L'arnaque au faux ordre de virement ou FOVI désigne un type d'escroquerie qui, par usurpation d'identité, vise à amener la victime à réaliser un virement de fonds sur un compte frauduleux.

La fraude à la carte bancaire :
La fraude à la carte bancaire désigne l'utilisation des coordonnées de la carte bancaire d'une personne pour réaliser des achats frauduleux à son insu.

Le spam téléphonique :
Le spam téléphonique désigne une communication non sollicitée à des fins publicitaires, commerciales ou malveillantes.
Il peut prendre différentes formes : SMS, MMS ou bien appel téléphonique. Dans bien des cas, il s'agit de messages publicitaires adressés à des fins de prospection commerciale.
Mais le spam téléphonique peut également revêtir un caractère malveillant : incitation à rappeler un numéro surtaxé, envoyer un SMS à un numéro payant ou encore tentatives d'hameçonnage (phishing en anglais) pour récupérer des données personnelles et/ou confidentielles.

Le spam électronique :
Le spam électronique, également appelé courrier indésirable ou pourriel, désigne une communication électronique non sollicitée à des fins publicitaires, commerciales ou malveillantes.
Dans la majorité des cas, il s'agit de messages de prospection commerciale ne respectant pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant : astuces pour gagner de l'argent, sollicitation pour transférer des fonds ou encore tentatives d'hameçonnage (phishing en anglais).

La défiguration de site web :
La défiguration de site web est l'altération par un pirate de l'apparence d'un site Internet, qui peut devenir uniformément noir, blanc ou comporter des messages, des images, des logos ou des vidéos sans rapport avec l'objet initial du site, voire une courte mention comme « owned » ou « hacked ».
La défiguration est le signe visible qu'un site Internet a été attaqué et que l'attaquant en a obtenu les droits lui permettant d'en modifier le contenu. La défiguration démontre que l'attaquant a pu prendre le contrôle du serveur, et donc, accéder potentiellement à des données sensibles (personnelles, bancaires, commerciales…).

Le piratage de compte :
Le piratage de compte désigne la prise de contrôle voire l'utilisation frauduleuse d'un compte au détriment de son propriétaire légitime.

Quelles bonnes pratiques ma collectivité peut-elle mettre en place pour lutter contre les cybermenaces ?

Que faire en cas de cyberattaque ?

Pour une collectivité, quelle qu'en soit la taille, une cyberattaque est une situation de crise dont les conséquences ne sont pas seulement techniques, mais également financières, de réputation, voire juridiques et peuvent impacter jusqu'à la survie des plus petites structures.
Une cyberattaque doit donc être gérée avec méthode et au plus haut niveau de l'organisation afin d'en limiter les impacts et permettre une reprise d'activité dans les meilleurs délais et conditions de sécurité pour éviter une récidive.

1. **Premiers réflexes**

- **Alertez immédiatement votre support informatique si vous en disposez** afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).
- **Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.
- **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…)
- **Tenez un registre des évènements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.
- **Préservez les preuves** de l'attaque : messages reçus, machines touchées, journaux de connexions…

2. Piloter la crise

- **Notifier l'incident de sécurité auprès de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI**) en contactant :
  Le référent ANSSI régional: occitanie@ssi.gouv.fr
  Le CERT-FR joignable 7J/7; 24h/24 au 32.18 ou au 09.70.83.32.18.
  Mail: cert-fr@ssi.gouv.fr
- **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.
- **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager, voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle
- **Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.
- **Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.
- **Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.
- **Notifiez l'incident à la CNIL** dans les 72 h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.
- **Gérez votre communication** pour informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias...

3. Sortir de la crise

- **Faites une remise en service progressive et contrôlée** après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.
- **Tirez les enseignements de l'attaque** et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

Comment piloter sa cybersécurité ?

1. Faites un état des lieux
Dans un premier temps, il convient de dresser un inventaire le plus exhaustif possible de l'ensemble de vos actifs numériques (réseaux internes, sites Internet, messageries, réseaux sociaux, applications et services externalisés…), et de leurs responsables (support informatique interne ou externe).

2. Prenez conscience du risque
Pour chaque système recensé, évaluez sa criticité pour le fonctionnement de votre organisation s'il venait à être piraté ou détruit, voire si les données qu'il contient étaient dérobées par des cybercriminels.

3. Évaluez votre niveau de protection
Interrogez votre support informatique interne et/ou externe sur la pertinence des mesures de sécurité techniques, organisationnelles voire contractuelles appliquées au regard des enjeux, telles les politiques
de mots de passe, de sauvegardes, de mises à jour ou encore de filtrage des accès externes.

4. Définissez un plan d'action
80 % des cyberattaques pourraient être évitées par l'application de mesures simples et à faible coût comme une bonne gestion des mots de passe, des sauvegardes, des mises à jour de sécurité ou des droits d'accès. Priorisez les actions à entreprendre en fonction du rapport criticité/coût/efficacité.

5. Faites-vous accompagner
Si aucun collaborateur n'est assigné à ce rôle, désignez une personne en charge de vous assister dans le pilotage du plan de cybersécurité de votre organisation. Pour l'évaluation technique du niveau de protection sur vos systèmes critiques, faites appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

(Pour une collectivité, quelle qu'en soit la taille, une cyberattaque est une situation de crise dont les conséquences ne sont pas seulement techniques, mais également financières, de réputation, voire juridiques et peuvent impacter jusqu'à la survie des plus petites structures.

Une cyberattaque doit donc être gérée avec méthode et au plus haut niveau de l'organisation afin d'en limiter les impacts et permettre une reprise d'activité dans les meilleurs délais et conditions de sécurité pour éviter une récidive.).

6. Sensibilisez vos collaborateurs
Vos collaborateurs sont un maillon essentiel de votre cybersécurité, qu'il s'agisse d'appliquer de bonnes pratiques de cybersécurité ou même de détecter voire de réagir à une tentative de cyberattaque. De nombreuses ressources gratuites de sensibilisation sont disponibles sur Cybermalveillance.gouv.fr.

7. Préparez-vous au pire
Il n'y a pas de cybersécurité absolue : le risque d'une cyberattaque réussie est malheureusement toujours possible. Il convient donc de préparer des plans de secours pour affronter une crise : annuaire de crise, fonctionnement dégradé, communication… et de réaliser des exercices pour s'assurer de leur efficacité.

8. Impliquez-vous
Pour vous assurer que le plan d'action cybersécurité est bien conduit, vous devez en tant que dirigeant vous impliquer, en le pilotant par
des points de situation et d'avancement réguliers à son niveau. Vous devez également montrer l'exemple et exiger de vos cadres et collaborateurs qu'ils ne dérogent ou ne contournent pas les mesures de sécurité décidées pour protéger leur organisation.

9. Contrôlez
Il est en effet important de vérifier que les mesures décidées ont bien été mises en place. Pour les systèmes les plus critiques, un audit technique et organisationnel peut s'avérer nécessaire : il est recommandé de faire appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

10. Itérez
Les services numériques des organisations évoluent en permanence, tout comme les moyens permettant de les attaquer. Pour intégrer cette évolution de la surface d'attaque des organisations, il est recommandé de réappliquer cette méthode de manière globale tous les deux à trois ans, en intégrant dans son plan de cybersécurité tout nouveau service numérique avant sa mise en œuvre. Réappliquer cette méthode de manière globale tous les deux à trois ans, en intégrant dans son plan de cybersécurité tout nouveau service numérique avant sa mise en œuvre.

Mon site Internet est-il sécurisé ?

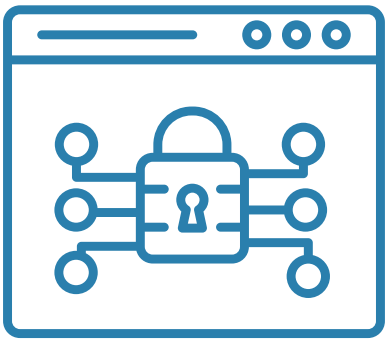
Une cyberattaque de votre site Internet peut avoir de multiples conséquences sur votre activité : arrêt de services, pertes financières, vol d'informations, pertes de confiance et de crédibilité, coût de remédiation, responsabilité juridique…

Voici 15 questions à poser à votre support informatique pour évaluer le niveau de sécurité de votre site Internet et définir les axes d'améliorations nécessaires.

1. Les accès à mon site internet sont-ils filtrés par un pare-feu ?
Un pare-feu est un équipement qui permet de limiter les accès aux seuls services et machines autorisées.

2. Mon site internet est-il protégé contre les attaques en déni de service ?
Votre opérateur et/ou votre hébergeur peuvent mettre en place des solutions pour absorber la surcharge de trafic de ce type de cyberattaque.

3. Mon site internet est-il protégé par un antivirus ?
Un antivirus peut détecter et bloquer des programmes malveillants qui pourraient être déposés ou stockés sur votre site.



4. Mon site internet est-il régulièrement mis à jour de tous les correctifs de sécurité matériels et logiciels ?
L'application des mises à jour de sécurité sur toutes les composantes de votre site permet de supprimer les failles de sécurité connues.

5. Mon site internet est-il régulièrement sauvegardé et ses sauvegardes testées ?
Une sauvegarde opérationnelle est indispensable pour pouvoir rétablir votre site internet dans l'état antérieur à un incident.

6. Les services ouverts sur mon site internet sont-ils limités au strict nécessaire ?
Chaque service ouvert sur votre site internet est une porte d'entrée possible pour un cybercriminel. Il convient donc de les limiter à l'indispensable.

7. L'accès en administration ou publication sur mon site internet est-il limité aux seules personnes et machines autorisées ?
Les accès permettant de gérer votre site internet ou de le modifier doivent être différenciés et faire l'objet d'un contrôle renforcé.

8. Les mots de passe d'accès à mon site internet sont-ils « solides » et « uniques » pour chaque personne autorisée ?
Une mauvaise gestion des mots de passe est l'une des premières causes des cyberattaques.

9. L'accès en administration ou publication sur mon site internet est-il protégé par une double authentification ?
L'authentification en deux étapes renforce la sécurité des mots de passe en demandant un code de confirmation à chaque nouvelle connexion.

10. Les communications avec mon site internet sont-elles sécurisées en HTTPS ?
Le protocole HTTPS permet de protéger d'une interception les informations échangées entre les postes utilisateurs et votre site Internet.

11. Le nom de domaine de mon site internet est-il protégé (dépôt INPI, utilisation d'un verrou de registre…) ?
Il est important d'utiliser les solutions disponibles pour éviter le vol ou le détournement du nom de votre site internet.

12. Les extensions logicielles utilisées sur mon site internet sont-elles indispensables et réputées sûres ?
Ces extensions peuvent améliorer les fonctionnalités de votre site, mais sont également des portes d'entrée possibles pour les cybercriminels.

13. Tous les accès à mon site internet sont-ils bien enregistrés ou journalisés ?
La journalisation des accès permet d'identifier des accès illégitimes et de retracer la chronologie d'une attaque.

14. L'activité de mon site internet est-elle régulièrement surveillée pour détecter un piratage ?
La surveillance des connexions et des modifications de votre site permet de détecter et de réagir au plus tôt aux tentatives de cyberattaque.

15. La sécurité de mon site internet est-elle régulièrement vérifiée ?
Votre site internet évolue sans cesse. Le maintien de son niveau de sécurité doit donc être régulièrement contrôlé (audit) par des spécialistes.

Comment bien gérer ses sauvegardes ?

Dans nos usages professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de vos données. Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme.

Voici 10 bonnes pratiques à adopter pour gérer efficacement vos sauvegardes.

1. Effectuez des sauvegardes régulières de vos données
En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports. Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.). Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.

2. Identifiez les appareils et supports qui contiennent des données
Dans notre vie quotidienne, nous utilisons un nombre croissant d'appareils et de supports qui enregistrent et stockent nos fichiers et nos données : ordinateurs, serveurs, tablettes, téléphones mobiles (smartphone), disques durs, clés USB, etc. Prenez le temps de les identifier.

3. Déterminez quelles données doivent être sauvegardées
Il n'est pas toujours possible ni nécessaire de sauvegarder la totalité de ses données. Sélectionnez les données à protéger, notamment celles qui sont stockées sur vos appareils (dans le disque dur de votre ordinateur ou dans la mémoire de votre téléphone mobile). Pour savoir si des données doivent être sauvegardées, posez-vous ces questions: « quelles données ne peuvent pas être récupérées ? », « quelles données je consulte régulièrement ou me sont le plus souvent demandées ? ».

4. Choisissez une solution de sauvegarde adaptée à vos besoins
Il existe des solutions gratuites ou payantes qui répondent à différents besoins. Identifiez-les et déterminez quelles sont les fonctionnalités attendues, l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe, une clé USB, etc.

5. Planifiez vos sauvegardes
Lorsqu'un fichier régulièrement mis à jour est perdu, sa restauration dans sa version la plus récente est nécessaire. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière. Vérifiez qu'elle est bien activée et que la fréquence de vos sauvegardes est adaptée à vos besoins.

6. Déconnectez votre support de sauvegarde après utilisation
Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait la détruire. Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique ou mettez-le hors ligne lorsque vous ne l'utilisez plus.

7. Protégez vos sauvegardes
Les risques de perte, de vol, de panne, de piratage ou de destruction peuvent également affecter vos sauvegardes. Protégez-les au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports. Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre.

8. Testez vos sauvegardes
Parfois, le processus de sauvegarde ne s'effectue pas correctement. Aussi, assurez-vous régulièrement que votre sauvegarde fonctionne,
par exemple, en la copiant dans le système original.

9. Vérifiez le support de sauvegarde
Tout comme les supports qui permettent de stocker les données originales, les supports sur lesquels sont réalisées les sauvegardes peuvent être endommagés. Vérifiez leur état, de manière à prévenir toute défaillance ou panne. Soyez également vigilant sur la durée de vie de votre support car certains conservent les données sur une durée plus ou moins longue. Par exemple, la durée de vie moyenne d'un DVD gravé est de 10 à 15 ans.

10. Sauvegardez les logiciels indispensables à l'exploitation de vos données [PRO]
La défaillance d'un appareil entraîne non seulement la perte des données produites par son utilisateur mais également du système d'exploitation de l'appareil comme Microsoft Windows, iOS, Android, et des logiciels qui y sont installés. Si les données sauvegardées sont dépendantes d'un système d'exploitation, d'un logiciel ou d'une configuration particulière, sauvegardez vos données ainsi que celles nécessaires à leur exploitation. Les systèmes d'exploitation récents proposent des fonctionnalités de sauvegarde du système qui permettent de le restaurer. Reportez-vous à sa documentation pour plus d'information.

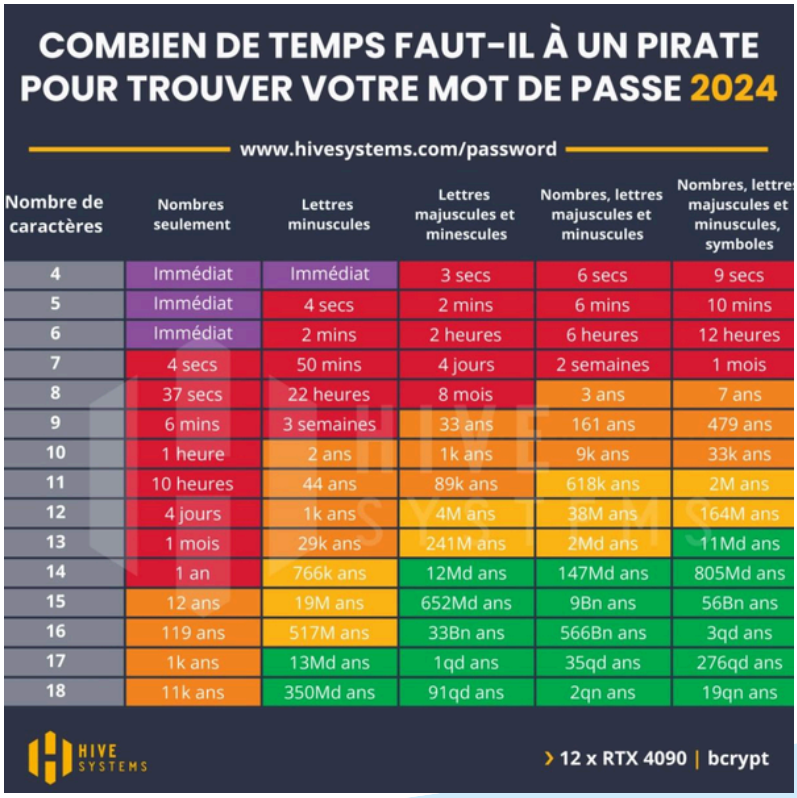
Comment bien gérer ses mots de passe ?

Messageries, réseaux sociaux, banques, administrations… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à leur profusion, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait les risques de compromettre la sécurité de vos accès.

Voici 10 bonnes pratiques à adopter pour mieux gérer vos mots de passe.

1. Utilisez un mot de passe différent pour chaque service
Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable.

2. Utilisez un mot de passe suffisamment long et complexe
Une technique d'attaque répandue consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de mots de passe.
Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 14 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.



Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minescules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans

HYVE SYSTEMS

3. Utilisez un mot de passe impossible à deviner
Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple).

4. Utilisez un gestionnaire de mots de passe
Il est impossible de retenir les dizaines de mots de passe longs et complexes. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé.

5. Changez votre mot de passe au moindre soupçon
Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné.

6. Ne communiquez jamais vos mots de passe à un tiers
Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe. Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

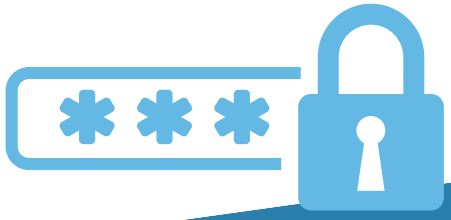
7. N'utilisez pas vos mots de passe sur un ordinateur partagé
Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels ou cybercafés peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée », veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur.

8. Activez la « double authentification »* lorsque c'est possible
Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option. En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. Pour en savoir plus, retrouvez notre article sur la double authentification.

9. Changez les mots de passe par défaut des différents services auxquels vous accédez
De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

10. Choisissez un mot de passe particulièrement robuste pour votre messagerie
Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle.

Votre mot de passe de messagerie est donc l'un des plus importants à protéger.



Comment bien gérer ses mises à jour ?

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (patch en anglais) visant à corriger ces failles.

1. Pensez à mettre à jour sans tarder l'ensemble de vos appareils et logiciels

Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

2. Téléchargez les mises à jour uniquement depuis les sites officiels

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3. Identifiez l'ensemble des appareils et logiciels utilisés
Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour. Certains Fournisseurs d'Accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique. Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabricant ou des éditeurs des applications installées.

4. Activez l'option de téléchargement et d'installation automatique des mises à jour
Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

5. Définissez les règles de réalisation des mises à jour
Pour assurer votre cybersécurité, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise. Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

6. Planifiez les mises à jour lors de périodes d'inactivité
Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel…), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises à jour (déjeuner, réunion, de nuit…).

7. Méfiez-vous des fausses mises à jour sur internet
En naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran : fausses publicités sur des sites Internet ou fenêtres malveillantes. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

8. Informez-vous sur la publication régulière des mises à jour de l'éditeur
L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques. Si les mises à jour ne sont plus proposées, ils sont plus vulnérables. Avant l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication des mises à jour de l'éditeur, ainsi que la date de fin de leur mise à disposition. Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils.

9. Testez les mises à jour lorsque cela est possible et faites des sauvegardes
Il arrive que la mise à jour d'un équipement entraîne des conséquences inattendues, comme de rendre incompatible la solution qui vient d'être mise à jour avec un autre équipement. Il convient donc de tester les mises à jour lorsque cela est possible. Par ailleurs, n'hésitez pas à réaliser une sauvegarde de vos données et de vos logiciels avant une opération de mise à jour pour pouvoir revenir en arrière si nécessaire.

10. Protégez autrement les appareils qui ne peuvent pas être mis à jour
Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément. Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

Comment protéger ses appareils mobiles ?

Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître
et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder.

Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles.

1. Mettez en place les codes d'accès
Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations.

2. Chiffrez les données de l'appareil
En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3. Appliquez les mises à jour de sécurité
Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4. Faites des sauvegardes
Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5. Utilisez une solution de sécurité contre les virus et autres attaques
De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (ransomware), l'hameçonnage (phishing)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

6. N'installez des applications que depuis les sites officiels
Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal: elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

7. Contrôler les autorisations de vos applications
Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages.

8. Ne laissez pas votre appareil sans surveillance
Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9. Évitez les réseaux publics Wifi publics ou inconnus
Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

10. Ne stockez pas d'informations confidentielles sans protection
Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

Les antivirus

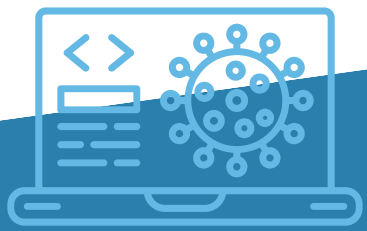
En naviguant sur Internet, en cliquant sur un lien ou en ouvrant la pièce-jointe d'un message, en branchant une clé USB… vous pouvez être infecté par un virus informatique. Les virus sont des programmes malveillants qui cherchent à perturber le fonctionnement normal d'un appareil à l'insu de son propriétaire ou à porter atteinte à ses données : vol ou destruction d'informations, espionnage ou chantage, utilisation de sa machine pour en attaquer d'autres… Les antivirus contribuent à vous protéger contre ces menaces.

Comment fonctionne un antivirus ?

Un antivirus se greffe sur le système d'exploitation de l'appareil. Il permet de rechercher les virus dans ce qui peut y être stocké, y entrer ou en sortir. Cela concerne leur(s) mémoire(s) ou leur(s) disque(s) dur(s), le contenu des messages (email), le chargement d'une page Internet, la lecture d'un média amovible (clés USB, DVD…). Pour cela, l'antivirus s'appuie sur des « bases de signatures » qui contiennent des définitions ou empreintes de virus régulièrement actualisées, et souvent aussi sur des analyses de comportements anormaux (dites « analyses heuristiques ») qui pourraient être liés à des virus.

Comment bien utiliser son antivirus ?

Pour bien utiliser votre antivirus, il faut vous assurer qu'il est bien installé, qu'il est activé, que la protection en « temps réel » pour analyser ce qui entre et sort est bien configurée, qu'il se met à jour régulièrement de son programme et de ses signatures. Pour cela, il faut vérifier les paramètres de l'antivirus et tester son bon fonctionnement (voir encadré).



Réalisez également régulièrement une analyse approfondie (scan) de votre matériel pour vous assurer qu'aucun virus initialement inconnu ne serait venu s'y implanter entre deux mises à jour.

Pourquoi faut-il mettre à jour son antivirus ?
Des milliers de nouveaux virus sont créés chaque jour. Pour permettre aux utilisateurs d'antivirus de rester protégés face à ces nouvelles menaces, les éditeurs réalisent des mises à jour régulières des bases de signatures, de leurs méthodes de détections heuristiques et de leurs produits. Ces mises à jour peuvent être diffusées jusqu'à plusieurs fois par jour. Il est donc primordial de s'assurer de leur installation automatique dès qu'elles sont disponibles.

Que faire si mon antivirus détecte un virus ?
Si votre antivirus vous alerte qu'il détecte un virus, il y a généralement trois cas de figure possibles. L'antivirus vous signale :

- qu'il a supprimé le virus ;
- qu'il a mis en quarantaine un fichier suspecté de contenir un virus ;
- qu'il a détecté un virus sans parvenir à le supprimer.

Dans tous les cas, suite à une alerte d'infection virale, il est vivement conseillé de déconnecter l'appareil d'Internet et d'en faire une analyse approfondie (scan) pour vous assurer qu'aucune trace du virus ne subsiste sur votre équipement. De même, il est fortement recommandé de ne sortir un fichier suspect de quarantaine que si vous êtes certain qu'il n'est pas infecté. Enfin, en cas d'impossibilité de supprimer un virus, une réinstallation complète de l'appareil et un changement de tous les mots de passe utilisés doivent être envisagés.

La sécurité sur les réseaux sociaux

Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux. Voici 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux.

1. Protégez l'accès à votre compte
Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels. Pour vous assurer que personne
ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l'accès à votre compte en utilisant des mots de passe différents et suffisamment robustes. Si le service le propose, activez également la double authentification.

2. Vérifiez vos paramètres de confidentialité
Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email…) et de vos publications sont souvent très ouverts. Vos données peuvent ainsi être partagées à tous les abonnés du réseau social. Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations
et de vos activités. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

3. Maîtrisez vos publications
Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser. Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez. Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire. Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise.

4. Faites attention à qui vous parlez
Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries. Soyez vigilants, car à leur insu, vos « amis » ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir. Quelques conseils supplémentaires : n'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable, n'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter et méfiez-vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries (hameçonnage).

5. Contrôlez les applications tierces
Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte. Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés… Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus. Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas. Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

6. Évitez les ordinateurs et les réseaux Wifi publics
Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel. Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte. Évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre. Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous.

7. Vérifiez régulièrement les connexions à votre compte
La plupart des réseaux sociaux offrent des fonctionnalités qui vous permettent de voir les connexions ou sessions actives sur votre compte depuis les différents appareils que vous utilisez pour y accéder. Consultez régulièrement ces informations. Si vous détectez une session ou une connexion inconnue ou que vous n'utilisez plus, déconnectez-la. Au moindre doute, considérez qu'il peut s'agir d'un piratage et changez immédiatement votre mot de passe.

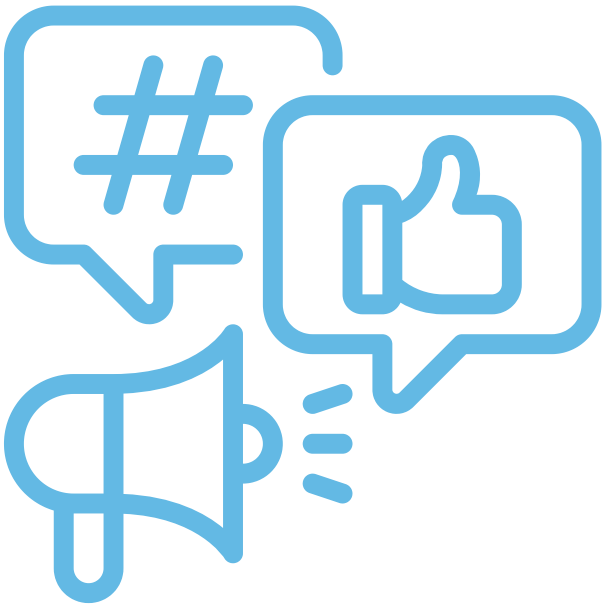
8. Faites preuve de discernement avec les informations publiées
Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification. Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément. Avec la puissance des réseaux sociaux, ces fausses informations (appelées « fake news » en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes. Aussi, avant de considérer ou relayer une information, efforcez-vous d'en vérifier la véracité.

9. Utilisez en conscience l'authentification avec votre compte de réseau social sur d'autres sites

Pour s'y connecter, certains sites Internet vous proposent d'utiliser votre compte de réseau social. Cette fonctionnalité peut sembler pratique car elle évite de créer un compte et un mot de passe supplémentaires, mais cela signifie que vous allez communiquer au réseau social des informations sur ce que vous faites sur le site concerné, et à l'inverse que vous allez peut-être donner au site des droits d'accès sur votre compte de réseau social. De plus, si votre compte de réseau social était un jour piraté, le cybercriminel pourrait automatiquement accéder à tous ces sites en usurpant votre identité. Aussi, avant d'utiliser cette fonctionnalité, ayez bien conscience des risques et vérifiez attentivement les autorisations que vous délivrez.

10. Supprimez votre compte si vous ne l'utilisez plus

Pour éviter que vos informations ne soient récupérées par des tiers ou que votre compte ne soit utilisé à votre insu, notamment pour usurper votre identité, supprimez-le si vous ne l'utilisez plus.



La sécurisation du télétravail

Le développement du télétravail présente de réelles opportunités tant pour les collaborateurs que pour les employeurs. Il nécessite toutefois généralement l'ouverture vers l'extérieur du système d'information
de l'organisation, ce qui peut engendrer de sérieux risques de sécurité susceptibles de mettre à mal votre organisation, voire d'engager sa survie
en cas de cyberattaque (rançongiciel, vol de données, faux ordres de virement…).

Voici quelques recommandations à mettre en œuvre pour limiter au mieux les risques.

Définissez et mettez en œuvre une politique d'équipement des télétravailleurs
Privilégiez autant que possible l'utilisation de moyens mis à disposition, sécurisés et maîtrisés par votre organisation. Lorsque ce n'est pas possible, donnez des directives d'utilisation et de sécurisation claires aux employés en ayant conscience que leurs équipements personnels ne pourront jamais avoir un niveau de sécurité vérifiable (voire sont peut-être déjà compromis par leur usage personnel).

Maîtrisez vos accès extérieurs
Limitez par un pare-feu l'ouverture de vos accès extérieurs ou distants (RDP par exemple) aux seules personnes et services indispensables, et filtrez strictement ces accès grâce à cet équipement de sécurité. Une attention toute particulière sera portée sur les éventuels accès de télémaintenance qui peuvent présenter une vulnérabilité importante s'ils sont compromis. Cloisonnez également les systèmes pour lesquels un accès à distance n'est pas nécessaire pour les préserver, surtout s'ils revêtent un caractère sensible pour l'activité de votre organisation (comme les réseaux de sauvegardes et les réseaux d'administration informatique par exemple).

Sécurisez vos accès extérieurs
Systématisez les connexions sécurisées à vos infrastructures par l'utilisation d'un « VPN » (Virtual Private Network ou « réseau privé virtuel » en français). Outre le chiffrement de vos connexions extérieures, ces dispositifs permettent également de renforcer la sécurité de vos accès distants en les limitant aux seuls équipements authentifiés. La mise en place d'une double authentification sur ces connexions VPN sera également à privilégier pour se prémunir de toute usurpation.

Renforcez votre politique de gestion des mots de passe
Qu'il s'agisse des mots de passe des utilisateurs en télétravail, mais aussi de ceux en charge du support informatique, les mots de passe doivent être suffisamment longs, complexes et uniques sur chaque équipement ou service utilisé. La majorité des attaques est due à des mots de passe trop simples ou réutilisés. Au moindre doute ou même régulièrement en prévention, changez-les et activez la double authentification chaque fois que cela est possible.

Durcissez la sauvegarde de vos données
Les sauvegardes seront parfois le seul moyen pour l'organisation de recouvrer ses données suite à une cyberattaque. Les sauvegardes doivent être réalisées et testées régulièrement pour s'assurer qu'elles fonctionnent.

Des sauvegardes déconnectées sont souvent indispensables pour faire face à une attaque destructrice par rançongiciel (ransomware). En outre, il convient également de s'assurer du niveau de sauvegarde des données des postes nomades des collaborateurs et de celles de ses hébergements externes (cloud, site Internet de l'organisation, service de messagerie…) pour vérifier que le service souscrit est bien en adéquation avec les risques encourus par votre organisation.

Mettez en place une journalisation de l'activité de tous vos équipements d'infrastructure
Ayez une journalisation systématique et d'une durée de rétention suffisamment longue de tous les accès et activités de vos équipements d'infrastructure (serveurs, pare-feu, proxy…), voire des postes de travail. Cette journalisation sera souvent le seul moyen de pouvoir comprendre comment a pu se produire une cyberattaque et donc de pouvoir y remédier, ainsi que d'évaluer l'étendue de l'attaque.

Supervisez l'activité de vos accès externes et systèmes sensibles
Cette supervision doit vous permettre de pouvoir détecter le plus rapidement possible toute activité anormale qui pourrait être le signe d'une cyberattaque, tels une connexion suspecte d'un utilisateur inconnu ou d'un utilisateur connu en dehors de ses horaires habituels, ou encore un volume inhabituel de téléchargement d'informations…

Sensibilisez et apportez un soutien réactif à vos collaborateurs en télétravail

Donnez aux télétravailleurs des consignes claires et formalisées sur ce qu'ils peuvent faire ou ne pas faire et sensibilisez-les aux risques de sécurité liés au télétravail. Cela, avec pédagogie pour vous assurer de leur adhésion et donc, de l'efficacité des consignes. Les utilisateurs sont souvent le premier rempart pour éviter, voire détecter les cyberattaques. Utilisez au besoin nos supports et notre kit de sensibilisation . Ces utilisateurs coupés de leur organisation ont également besoin d'un soutien de qualité et réactif pour éviter toute dérive.

Les 10 mesures essentielles pour assurer votre cybersécurité

1. Protégez vos accès avec des mots de passe solides
2. Sauvegardez vos données régulièrement
3. Appliquez les mises à jour de sécurité sur tous vos appareils (PC, tablettes, téléphones…), et ce, dès qu'elles vous sont proposées
4. Utilisez un antivirus
5. Téléchargez vos applications uniquement sur les sites officiels
6. Méfiez-vous des messages inattendus
7. Vérifiez les sites sur lesquels vous faites des achats
8. Maîtrisez vos réseaux sociaux
9. Séparez vos usages personnels et professionnels
10. Évitez les réseaux WiFi publics ou inconnus

Assistance et conseil informatique par Haute-Garonne Ingénierie

Parcours cybersécurité : Evaluer et optimiser son système d'information

DESCRIPTIF

Haute-Garonne Ingénierie propose un plan d'action en cybersécurité d'une durée de 4 à 6 mois, structuré en 3 phases distinctes et indépendantes.

- La première phase se concentre sur la sensibilisation des agents aux risques et aux bonnes pratique en matière de sécurité informatique.
- La deuxième phase comprend un audit complet de la sécurité et de la conformité du système d'information et des sites Internet, suivi de la mise en œuvre d'un plan d'actions et d'un suivi de développement.
- La troisième phase se consacre à l'intégration d'outils pour renforcer la sécurité et faciliter les usages quotidiens.

EXEMPLES

Je souhaite :

- Former les agents à reconnaître et à réagir face aux tentatives de phishing ;
- Identifier et corriger les vulnérabilités des infrastructures informatiques.

Bénéficiaires de l'accompagnement : Communes, EPCI, PETR

Modalités d'accompagnement

L'accompagnement de cette prestation de cybersécurité commence par un entretien préalable avec des experts, en présence des agents et des élus responsables de la sécurité du système d'information. Cet entretien a pour but de définir précisément les besoins et d'élaborer un plan d'actions adapté ainsi qu'un calendrier détaillé, en fonction des phases choisies. L'accompagnement se fera selon le choix initial des phases et pourra s'étendre sur une durée allant jusqu'à 6 mois. Haute-Garonne Ingénierie suivra rigoureusement les collectivités dans l'avancement des actions mises en place pour garantir leur efficacité et apporter les ajustements nécessaires.

Accompagnement et livrables possibles

- Formation et sensibilisation
- Conseil stratégique et approche globale de la sécurité du Système d'Information
- Scénarios de pistes d'actions, orientations possibles
- Réalisation et présentation d'un rapport d'audit
- Evaluation du projet

Prérequis et conditions de la réalisation de l'accompagnement

- Etre adhérent de Haute-Garonne Ingénierie
- Payant pour l'acquisition des outils de campagnes automatiques de sensibilisation et de tests automatiques de failles de sécurité de la phase 3
- Convenir d'un calendrier de présence à la mission/demande

Contact Expert : Haute-Garonne Ingénierie
Direction informatique et urbanisme
accueil@atd31.fr / 05.34.45.56.56

Ce guide a été élaboré à partir des éléments que vous pouvez retrouver sur https://www.cybermalveillance.gouv.fr/.

HAUTE-GARONNE NUMÉRIQUE

Agir avec vous !

HAUTE-GARONNE INGENIERIE
AGENCE TECHNIQUE DÉPARTEMENTALE