Cybersécurité

Toutes les réponses à vos questions !

L'Union vous accompagne au quotidien dans l'utilisation des outils numériques. Cependant, cette pratique s'accompagne de nombreux risques et défis, notamment en matière de cybersécurité. Afin de répondre aux interrogations issues de votre expérience terrain, l'Union des URPS a regroupé vos principales questions et y a apporté des réponses claires et concrètes. Ce document vise à vous fournir des clés pour naviguer sereinement dans votre environnement numérique.

Si vous souhaitez bénéficier d'une sensibilisation

www.youtube.com/watch?v=KL4DyZ5rEfc&t=1121s

Bonne lecture !

Sommaire

Sur le phishing

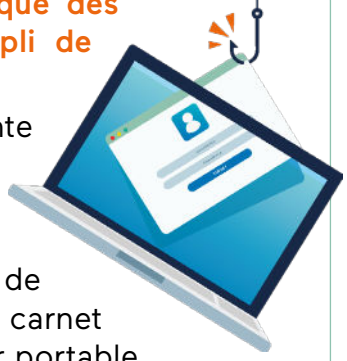
Le phishing est une forme d'escroquerie sur internet. Le fraudeur se fait passer pour un organisme que vous connaissez en vous demandant généralement de « mettre à jour » ou « confirmer vos informations », notamment vos coordonnées bancaires.

Un contenu généraliste et complet sur la thématique du phishing est accessible sur le site cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing

Peut-on être piraté en ouvrant simplement un mail de phishing, sans cliquer sur aucun de ses liens ?

Non, il n'est pas possible d'être piraté simplement en ouvrant un e-mail. **Le seul moyen de se faire pirater** par e-mail est **d'interagir avec son contenu**, par exemple en cliquant sur un lien ou une pièce jointe malveillante.

En cliquant sur un lien contenu dans un mail de phishing, est-ce que des informations peuvent être récupérées, sans pour autant avoir rempli de questionnaire ?



Si vous cliquez sur un **lien d'hameçonnage** ou ouvrez une pièce jointe dans l'un de ces messages, votre appareil peut être **infecté** par des **logiciels malveillants**, tels que des **virus**, des **logiciels espions** ou des **rançongiciels**. Une fois le logiciel malveillant installé à votre insu, **vos données personnelles pourraient être collectées**, d'autres courriels de phishing pourraient être envoyés aux personnes figurant dans votre carnet d'adresses, ou ouvrir un accès à distance à un pirate à votre ordinateur portable.

Vous pouvez vérifier si un virus a été installé sur votre machine en **lançant une analyse** par votre antivirus. Également, certains virus peuvent être détectés par **recherche manuelle**. Commencez par vous rendre dans votre outil de configuration système et observez le nom des programmes qui sont lancés au démarrage de votre machine. Si un programme inconnu s'y trouve, faites une recherche sur Internet pour déterminer s'il s'agit d'un programme légitime ou non. Le cas échéant désactivez-le et supprimez-le. Enfin, un **comportement anormal de votre machine** peut également être un symptôme qu'un virus s'est glissé sur votre machine.

Faut-il passer 2-3 minutes pour lire attentivement tous nos mails avant de les ouvrir, afin de se prémunir du phishing ?

Afin de se prémunir du hameçonnage, il est recommandé de prendre quelques secondes pour lire attentivement ses mails, en étant vigilants à plusieurs éléments, tels que la véracité du **nom de domaine** utilisé, **la qualité de l'orthographe** et de **la syntaxe**, ainsi que **la qualité des liens de redirection**. Un descriptif exhaustif de ces indices est disponible sur le site cybermalveillance.gouv.fr :

www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage

Est-il possible aux pirates informatiques de transmettre un mail écrit avec un faux nom de domaine, mais qui s'affiche comme étant le nom de domaine officiel ?

Non, ce n'est pas possible, à moins que la boite mail du site en question ait été piratée. Pour autant, les pirates informatiques peuvent mettre en œuvre plusieurs techniques, afin laisser croire à la fiabilité des mails frauduleux qu'ils envoient.

Il leur est par exemple possible de réserver **un nom de domaine dont l'orthographe est proche** de celle d'un organisme de confiance. Les cybercriminels utilisent ensuite ce nom de domaine pour tenter de tromper les destinataires. Pour augmenter le risque de confusion avec le nom de domaine légitime, ils peuvent **changer son extension (« .fr » en « .com » par exemple), ajouter ou supprimer des traits d'union ou des lettres**, ou encore utiliser des **caractères spéciaux** issus d'autres langues.

Il est également **possible d'usurper uniquement le nom de l'expéditeur**. Afin d'éviter cet écueil, il est recommandé de vérifier l'adresse mail associée, pour s'assurer qu'elle est bien valable.

Sur la sauvegarde

Une sauvegarde est l'opération qui consiste à dupliquer et à mettre en sécurité les données contenues dans un système informatique.

Un contenu généraliste et complet sur la thématique de la sauvegarde des données est accessible sur le site cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes

Doit-on sauvegarder tous les soirs nos données ?

La sauvegarde doit vous permettre de récupérer toute donnée utile. **La fréquence de vos sauvegardes doit donc s'adapter à vos besoins**.

Il n'est pas toujours possible ni nécessaire de sauvegarder la totalité de ses données. **Sélectionnez donc les données à protéger**, notamment celles qui sont stockées sur vos appareils. Pour savoir si des données doivent être sauvegardées ou non, posez-vous les questions suivantes : « quelles données ne peuvent pas être récupérées par ailleurs en cas de perte ? », « quelles données je consulte régulièrement ou celles qui me sont le plus souvent demandées ? ».

Si on effectue une sauvegarde chaque soir, doit-on appliquer le principe de « sauvegarde 3-2-1 » chaque soir ?

La méthode 3-2-1 consiste à réaliser **3 copies sur 2 supports différents, dont 1 externe**. Elle vise à la diversification des types de supports et environnements, mais aussi des lieux de stockage, le but étant que les duplications ne soient pas toutes connectées au même réseau physique. En cas de cyberattaque par exemple, ce principe de précaution évitera que la perte des données s'étende à toutes les copies.

Il est recommandé d'effectuer des sauvegardes à intervalles réguliers, afin de récupérer toute donnée qui vous serait utile. La fréquence et la manière d'y procéder seront à adapter à votre contexte.

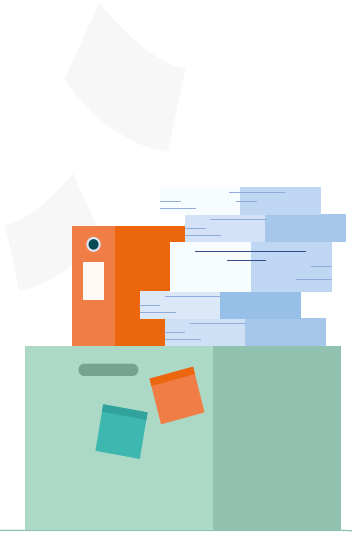
Doit-on sauvegarder les données qui sont stockées sur un logiciel métier en ligne ?

Si cela est possible, il est **recommandé de sauvegarder toutes données utiles**, y compris celles stockées sur un logiciel métier en ligne. En effet, il n'est pas impossible que ce logiciel soit lui-même la cible de hackers, et que vos données se retrouvent inaccessibles. En détenir une copie permet de parer efficacement à la disparition de vos documents. Une solution fiable consiste à créer **une sauvegarde à distance des logiciels métier sur des serveurs sécurisés**.

Si la sauvegarde des données stockées sur un logiciel métier en ligne n'était pas possible, il est recommandé de **vérifier que l'éditeur héberge les données sur plusieurs sites** afin d'assurer une continuité de service en cas de problème sur le site d'hébergement principal.

Nos sauvegardes régulières nous permettent-elles de récupérer les données ?

Une sauvegarde bien effectuée doit vous permettre de récupérer vos données. De ce fait, il est recommandé d'effectuer des **sauvegardes fréquentes**, à **intervalles réguliers**, afin de récupérer autant d'informations que possible. Également, il est recommandé de **sécuriser et tester les sauvegardes effectuées**, afin de s'assurer que les données y ont bien été copiées.



Quel outil utiliser pour la sauvegarde iso* des postes de travail ?

Il est difficile de répondre à cette question, car les performances et fonctionnalités des outils varient selon les besoins et les environnements technologiques utilisés (Apple, Windows, Linux...). Des **comparatifs et tests accessibles en ligne**, ou **la recommandation de confrères**, peuvent vous aiguiller dans votre recherche.

* *La sauvegarde ISO consiste en une représentation autonome et parfaite des données contenues sur un outil de stockage, tel un disque dur.*

Sur les anti-virus

Un logiciel anti-virus aide à protéger votre ordinateur contre les malwares et les attaques de cybercriminels. Un logiciel anti-virus analyse les données, pages web, fichiers, logiciels et applications qui transitent par le réseau vers vos appareils.

Un contenu généraliste et complet sur la thématique des anti-virus est accessible sur le site cybermalveillance.gouv.fr : www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/antivirus

Faut-il installer un antivirus sur sa machine ?

La réponse est **« oui ».** Même si aucun antivirus ne permet une protection absolue contre les virus, ils contribuent **à être protégé** des principaux virus connus. L'utilisation d'un antivirus est **une des principales mesures** à appliquer pour assurer votre cybersécurité. (Source Cybermalveillance.gouv.fr)

Quel anti-virus choisir ?

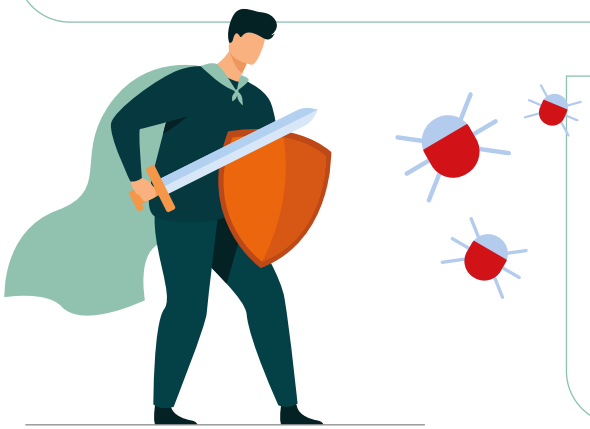
Il est difficile de répondre à cette question, car les performances et fonctionnalités des **principaux antivirus du marché sont assez similaires** et aucun ne peut se prévaloir d'apporter une protection à 100% efficace. Leur classement de performance varie d'un test à l'autre en fonction des critères utilisés pour leur évaluation. (Source Cybermalveillance.gouv.fr)

Un anti-virus est-il utile sur Mac ?

Oui. Si certains systèmes sont plus vulnérables que d'autres, **tous les équipements informatiques peuvent être infectés par un virus** et devraient donc être protégés.

Est-ce que Windows Defender suffit comme anti-virus ?

Chaque anti-virus dispose de spécificités et d'options qui lui sont propres. Windows Defender est un outil efficace et suffisant en soi.



Le serveur professionnel, tel le serveur d'une officine, doit-il nécessairement disposer d'un anti-virus ?

Il est recommandé de **sécuriser ses serveurs professionnels**, en disposant notamment d'un anti-virus. La CNIL fournit de précieux conseils sur la façon la plus adéquate de sécuriser ses serveurs :
www.cnil.fr/fr/securite-securiser-les-serveurs

Sur les rançongiciels

Un rançongiciel est un code malveillant qui bloque l'accès à votre appareil ou à des fichiers en les chiffrant et qui vous réclame le paiement d'une rançon pour obtenir le déchiffrement de vos données.

Un contenu généraliste et complet est accessible sur le site cybermalveillance.gouv.fr, sur la thématique des rançongiciels : www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Si on est victime d'un rançongiciel, doit-on payer la rançon ?

Il est recommandé de **ne pas payer pas la rançon** réclamée car vous n'êtes pas certain de récupérer vos données. Payer la rançon contribue également à alimenter ce système de cyberattaques.

Sur les gestionnaires de mots de passe

Il s'agit d'une solution numérique avec laquelle l'utilisateur peut gérer ses mots de passe en centralisant l'ensemble de ses identifiants et mots de passe dans une base de données (dit portefeuille).

Conseillez-vous l'utilisation d'un outil de gestionnaire de mot de passe ?

Un gestionnaire de mot de passe est une solution numérique par laquelle un utilisateur peut gérer ses mots de passe en **centralisant l'ensemble de ses identifiants et mots de passe dans une base de données** (dit portefeuille). Le gestionnaire de **mots de passe est protégé par un mot de passe unique, afin de n'en avoir plus qu'un seul à retenir**.

Utiliser un gestionnaire de mot de passe dédié est une bonne solution pour générer des mots de passe forts et uniques pour chacun de vos comptes.

L'utilisation d'un gestionnaire de mot de passe présente **plusieurs avantages** : Un bon gestionnaire de mots de passe est un **logiciel qui stocke tous vos mots de passe** et les **protège en les chiffrant**. Il vous **évite de retenir des dizaines de mots de passe** ou de les noter en clair dans un fichier texte ou un post-it.

L'utilisation d'un gestionnaire de mot de passe permet de ne retenir qu'un seul mot de passe complexe et robuste. La saisie du mot de passe maitre ouvre le « coffre-fort » contenant tous vos mots de passe. Il devra **être solide**, c'est-à-dire comporter **au moins 12 caractères** dont des chiffres et des caractères spéciaux.

En plus de stocker vos mots de passe, **certains gestionnaires vous proposent d'en générer des nouveaux**. Vous n'avez plus à réfléchir pour savoir si le mot de passe que vous concevez est suffisamment solide, le logiciel le fait selon vos propres critères.

Enfin, la plupart des gestionnaires proposent une **version mobile** à emporter sur votre smartphone, votre tablette ou votre ordinateur portable. Renseignez-vous sur le site de l'éditeur.

Un gestionnaire de mot de passe dédié est un outil spécifique et sécurisé, à distinguer du **gestionnaire de mot de passe navigateur, qui est peu sécurisé**.

Un gestionnaire de mot de passe gratuit est-il sécurisé ?

Un gestionnaire de mot de passe gratuit **peut tout à fait être sécurisé**, selon les technologies utilisées et le sérieux de la solution.

Un gestionnaire de mots de passe peut-il être piraté ?

Les gestionnaires de mots de passe sont sûrs, mais **leur efficacité dépend pour partie des actions de l'utilisateur**. Afin de conserver un niveau de sécurité élevé, il est recommandé de choisir un gestionnaire de mot de passe complet et fiable, d'utiliser un **mot de passe unique fort** et d'activer l'authentification multi-facteurs.

Pour autant, malgré toutes ces précautions, il se peut que le logiciel utilisé se fasse pirater, bien que les risques soient faibles.

Avez-vous des gestionnaires de mots de passe à conseiller ?

Le site Cybermalveillance.gouv.fr fait référence au gestionnaire de mots de passe sécurisé et gratuit, **KeePass**. Ce petit logiciel libre, certifié par l'**ANSSI**, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. KeePass dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires. Bien entendu, d'autres solutions sont accessibles et des comparatifs existent sur internet.

Questions généralistes

Est-il vrai que les attaques ont lieu principalement la nuit, quelle que soit la nature de l'attaque ?

Les cyberattaques peuvent **avoir lieu à tout moment de la journée**. Pour autant, les pirates informatiques initient régulièrement leurs attaques en dehors des heures de travail, la nuit ou le week-end. Le temps de réponse à incident est ainsi plus long, les équipes informatiques pouvant être moins mobilisées à ces horaires.

Doctolib est-il protégé d'une attaque ?

Doctolib déploie certains moyens afin de sécuriser ses services. Sa politique de sécurité est détaillée au lien suivant :
https://info.doctolib.fr/securite/

La présence du cadenas indique forcément la fiabilité du site internet ?

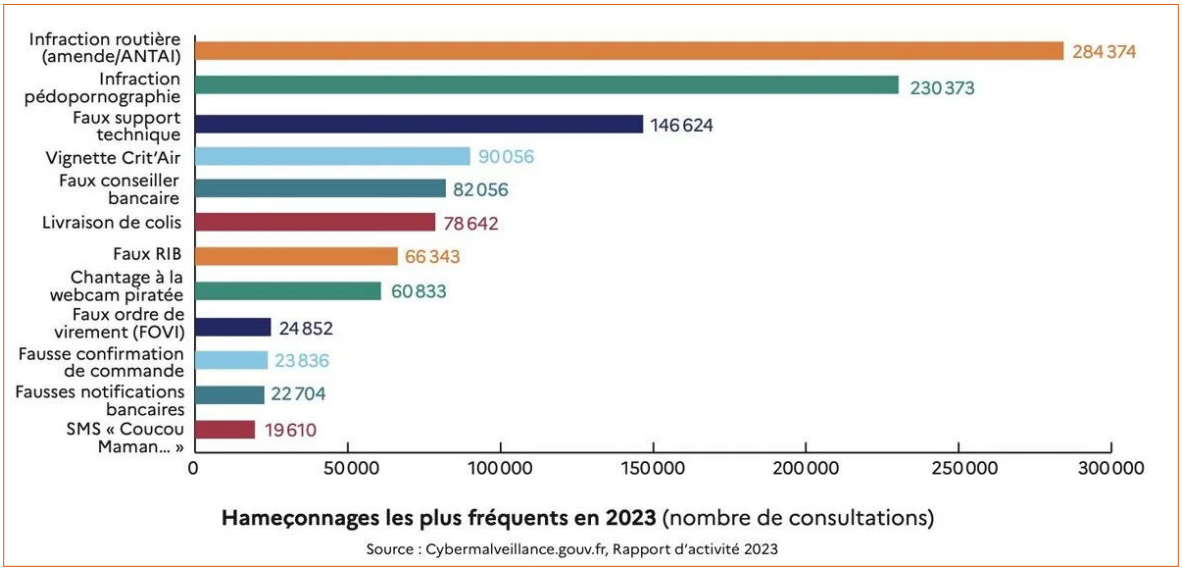
Non. La présence du petit cadenas indique une seule chose : la communication entre vous et le site internet concerné est sécurisée.

Au contraire, l'absence de cadenas indique que la communication s'effectue en clair sur le réseau, elle n'est pas sécurisée.

Pour autant, **ce cadenas sécurise seulement les transferts d'information**, il ne garantit pas que le site sur lequel vous vous trouvez est fiable et la seule présence de ce cadenas ne doit pas conduire à une perte de vigilance de votre part.

Je reçois énormément de mail d'hameçonnage sur le thème de la livraison de colis. Comment cela se fait ?

Ce type d'hameçonnage est malheureusement assez fréquent. Cybermalveillance.gouv.fr a recensé **les thématiques les plus utilisées** par les pirates informatiques en matière d'hameçonnage. La livraison de colis y figure en bonne position.



Hameçonnages les plus fréquents en 2023 (nombre de consultations)

Source : Cybermalveillance.gouv.fr, Rapport d'activité 2023

Le détail ici :
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/hameconnage-phishing-menace-predominante-tous-publics

Un contenu généraliste et complet sur la thématique du smishing est accessible sur le site cybermalveillance.gouv.fr :
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/smishing-hameconnage-sms

Est-il possible d'avoir des fiches pratiques simples et accessibles à tous ?

Le site Cybermalveillance.gouv.fr est une source d'informations fiable et exhaustive, qui apporte mises en garde, conseils et bonnes pratiques en matière de cybersécurité sous forme d'articles, de fiches thématiques et de mémos : www.cybermalveillance.gouv.fr/

Que faire du matériel informatique dont on souhaite se débarrasser ?

Si vous envisagez de vous débarrasser du matériel informatique que vous n'utilisez plus, que ce soit en le donnant, en le revendant ou en le détruisant, veillez auparavant à **sauvegarder vos données, à supprimer autant que possible les informations qui y sont contenues**. Envisagez également **de chiffrer le disque dur**, afin d'éviter toute fuite. Les procédures varieront selon l'outil concerné.

Nos fournisseurs de logiciel métier ont-ils des obligations de résultats dans notre protection contre la cybercriminalité ?

La réponse dépendra des logiciels-métiers utilisés. Il est plus probable que ces opérateurs aient une obligation de moyens que de résultats. L'Agence du Numérique en Santé a créé différents **questionnaires vous permettant d'évaluer la capacité de vos fournisseurs de service informatique à garantir un service** dont les modalités vous permettent de respecter vos obligations en matière de sécurité des systèmes d'information et de protection des données à caractère personnel, notamment en ce qui concerne la disponibilité de vos outils et services informatiques, ainsi que la confidentialité, l'intégrité et la disponibilité des données à caractère personnel, de santé ou autre. Ces questionnaires sont accessibles ici : https://esante.gouv.fr/sites/default/files/media_entity/documents/PGSSI_S-Guide_Orga-Memento_PS_Exercice_Liberal-Annexe_1-Questionnaires_fournisseurs-V2.0.pdf

Comment et à quel moment chiffrer ses données ?

La **CNIL** fournit explications et conseils exhaustifs sur le chiffrement des données et répertoires :

www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires

CNIL. COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Qu'est-ce que la DNS ?

La délégation au numérique en santé (**DNS**) est rattachée directement aux ministères chargés de la santé, de l'action sociale et de la sécurité sociale afin d'assurer le pilotage de l'ensemble des chantiers de transformation du numérique en santé.

MINISTÈRE DU TRAVAIL DE LA SANTÉ ET DES SOLIDARITÉS
Liberté Égalité Fraternité
Délégation au numérique en santé

Plus d'informations dédiées ici :

https://gnius.esante.gouv.fr/fr/acteurs/fiches-acteur/delegation-au-numerique-en-sante-dns

Qu'est-ce que l'ANS ?

L'Agence du Numérique en Santé (**ANS**) accompagne la transformation numérique du système de santé aux côtés de tous les acteurs concernés des secteurs sanitaire, social et médico-social, privés comme publics, professionnels ou usagers.

AGENCE DU NUMÉRIQUE EN SANTÉ

Plus d'informations dédiées ici :

https://gnius.esante.gouv.fr/fr/acteurs/fiches-acteur/agence-du-numerique-en-sante-ans

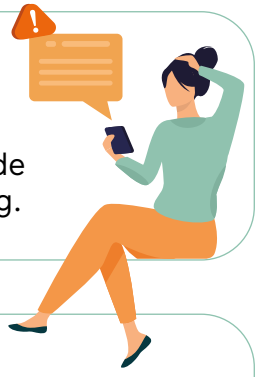
Qui contacter pour avoir de l'aide ?

Pour obtenir un diagnostic en ligne d'évaluation de la nature de l'incident cyber auquel vous faites face, vous pouvez utiliser l'outil de diagnostic en ligne de cybermalveillance.gouv.fr : Outils de diagnostic - Assistance aux victimes de cybermalveillance

Pour effectuer une déclaration :

- D'un incident cyber : CERT Santé - https://signalement.social-sante.gouv.fr/
- D'une attaque cyber en Hauts de France : ARS-HDF-SIGNAL@ars.sante.fr
- D'un vol avéré de données : CNIL - https://notifications.cnil.fr/notifications/
- D'un incident cyber, pour informer l'assurance maladie : abuse@assurance-maladie.fr
- D'un incident cyber, pour informer les pharmaciens : URPS - urgence@urps-pharmaciens-hdf.fr

Je reçois régulièrement des notifications sur mon téléphone professionnel indiquant que mon compte a été piraté. Dois-je m'en inquiéter ?



Il s'agira de vérifier qui est à l'origine de ces messages. Il est recommandé de **contacter l'éditeur du service concerné** en passant par leur site internet, afin de vérifier avec lui si ce message est valable, ou si c'est une tentative de phishing.

Comment faire quand on a des logiciels uniquement en ligne qui ont leur propre cloud ?

Différentes mesures doivent être mises en place pour limiter au maximum les risques inhérents à l'hébergement de vos données et applications dans le cloud. Gardez à l'esprit que, à l'image des accès sur un serveur central ou sur un micro-ordinateur, l'**erreur humaine demeure l'une des plus grandes menaces pour la sécurité du cloud.**

Une réponse exhaustive à cette question est apportée ici :
www.francenum.gouv.fr/guides-et-conseils/pilotage-de-lentreprise/stockage-des-donnees-en-ligne-cloud/securite-dans-le

Comment savoir quand un site est légitime ou non ?

Il n'existe pas de méthode infaillible pour déterminer la légitimité d'un site web, mais plusieurs mesures simples peuvent aider à réduire les risques, en voici quelques-unes :

Assurez-vous que **l'URL commence par « https:// »** et que le cadenas dans la barre d'adresse est fermé, ce qui indique une connexion sécurisée grâce à un certificat SSL/TLS valide.

- **Méfiez-vous des variations subtiles** ou des fautes d'orthographe dans le nom de domaine, qui peuvent signaler des tentatives de phishing ou des sites frauduleux.
- **Recherchez des coordonnées claires**, telles qu'une adresse physique ou un numéro de téléphone. Les sites légitimes fournissent généralement ces informations de manière Vérifiez la réputation du site en consultant des avis et des évaluations sur des plateformes fiables. Les retours d'autres utilisateurs peuvent révéler des signes de fraude.
- **Analysez le contenu** du site pour détecter d'éventuelles erreurs grammaticales, des informations incohérentes ou du contenu de faible qualité, qui sont souvent révélateurs d'un site frauduleux.

Sécuriser le wifi veut bien dire utiliser un mot de passe ou parlez-vous de restreindre l'accès uniquement aux personnes sélectionnées ?

Pour sécuriser un réseau Wi-Fi, il est **recommandé de prendre certaines mesures** qui vont au-delà de simplement utiliser un mot de passe. En voici quelques-unes :

- Activer le Wi-Fi uniquement quand nécessaire
- Utiliser un protocole de chiffrement robuste
- Choisir un mot de passe complexe.
- Limiter l'accès aux seuls utilisateurs autorisés
- Isoler le réseau Wi-Fi du réseau filaire
- Mettre en place des équipements de filtrage
- Activer la supervision des événements pour détecter toute activité suspecte.
- S'assurer que les systèmes et les points d'accès sont toujours à jour avec les derniers correctifs de sécurité

Pour plus de détails, nous vous recommandons vivement le guide de l'ANSSI sur la sécurisation des accès Wi-Fi : https://cyber.gouv.fr/publications/securiser-les-acces-wi-fi

Quand j'ai un doute sur un lien dans courriel sur mon iPhone je fais un clic prolongé sur le lien pour ouvrir une mini fenêtre « Aperçu ». Est-ce que ce geste est sécurisé ?

Il est difficile de répondre de manière catégorique à cette question car Apple fournit peu d'informations à ce sujet.

Faire un clic prolongé sur un lien pour afficher l'aperçu sur iPhone permet de **vérifier l'URL complète sans cliquer directement sur le lien**, ce qui aide à repérer les liens suspects ou de phishing. Cela peut également **permettre de détecter des incohérences évidentes** sur la page affichée.

Cependant, il est important de noter que cette pratique n'est pas infaillible. Bien que l'aperçu vous aide à détecter des problèmes évidents, il **ne garantit pas à 100 % la sécurité du lien**. Il est donc essentiel de **rester vigilant** et de compléter cette pratique par d'autres mesures de sécurité pour garantir une protection maximale.

Le VPN est-il utile ?

Un VPN (Virtual Private Network, ou réseau privé virtuel) est un outil qui permet de sécuriser la connexion Internet en créant un **tunnel chiffré entre votre appareil et un serveur distant**. Ce tunnel protège vos données en les rendant illisibles pour les tiers, comme les hackers ou même votre fournisseur d'accès Internet.

Un VPN peut s'avérer particulièrement **utile pour sécuriser des communications à distance**, par exemple lorsque des employés travaillent depuis chez eux ou lors de déplacements. Il permet aussi d'**accéder à des ressources internes** d'une entreprise, comme des bases de données ou des fichiers partagés, **sans exposer ces données sensibles à des risques externes**.

Toutefois, un **VPN n'est pas une solution infaillible** : il peut ralentir la connexion Internet, et s'il est mal configuré ou si le fournisseur de VPN est peu fiable, les données peuvent rester vulnérables. De plus, un VPN **ne protège pas contre toutes les menaces en ligne**, comme les logiciels malveillants ou les attaques de phishing.

Conseillez-vous l'utilisation d'une station NAS accessible en Wi-Fi ?

L'utilisation d'une station NAS (Network Attached Storage) accessible en Wi-Fi est une option pratique, mais **elle nécessite certaines précautions** :

Sécurité : Un NAS accessible en Wi-Fi peut être **vulnérable aux attaques** si les mesures de sécurité ne sont pas strictement appliquées. Il est essentiel d'utiliser un réseau Wi-Fi sécurisé (WPA3 si possible), de mettre en place un pare-feu, de sécuriser l'accès par des mots de passe forts, et d'activer le chiffrement des données.

Performances : L'accès en **Wi-Fi peut être moins performant** qu'une connexion filaire (Ethernet) en termes de vitesse et de stabilité, surtout lors de transferts de gros fichiers. Le Wi-Fi 6 peut atténuer ces problèmes, mais il n'égale pas toujours la fiabilité d'une connexion filaire.

En somme, un NAS en Wi-Fi est recommandé pour une utilisation non critique, mais pour des applications nécessitant des performances élevées et une sécurité renforcée, une connexion filaire reste préférable.

Quelle est l'efficacité de FaceID et de l'empreinte digitale ?

Face ID et l'empreinte digitale sont des technologies de reconnaissance biométrique largement utilisées pour sécuriser l'accès aux systèmes d'informations. Ces technologies offrent plusieurs avantages, mais comme toutes les technologies, elles présentent également certaines limites :

Avantages :

- Confort d'utilisation : Ces technologies sont très pratiques et rapides, ce qui peut encourager leur adoption et réduire les risques liés à l'utilisation de mots de passe faibles ou réutilisés.
- Authentification forte : Face ID et les empreintes digitales fournissent un niveau d'authentification élevé, car elles reposent sur des caractéristiques uniques à chaque individu.

Limites :

- Vulnérabilités potentielles : Bien que difficile, il est toujours possible de tromper ces systèmes. Par exemple, des chercheurs ont déjà réussi à contourner Face ID avec des masques très élaborés, et certaines empreintes digitales peuvent être reproduites à partir de traces laissées sur des surfaces.

A quoi sert le « key logger » de mon logiciel métier ?

Un "key logger" est un **outil de surveillance qui enregistre chaque frappe effectuée sur un clavier**. Son utilisation peut être légitime ou malveillante, selon le contexte.

Dans un logiciel métier, il **peut servir à des fins de sécurité et de suivi**, par exemple pour surveiller les activités des utilisateurs, vérifier la saisie correcte des données ou détecter des comportements suspects. Il peut également **être employé pour des audits de conformité ou pour améliorer l'interface utilisateur** en analysant les interactions.

L'utilisation d'un key logger doit être encadrée par des pratiques rigoureuses pour respecter la législation et éviter les cyberattaques. Il est impératif d'informer clairement les utilisateurs de la présence et de la fonction du key logger, obtenant ainsi leur consentement éclairé pour la collecte de données. Il est également crucial de mettre en œuvre des mesures de sécurité robustes, telles que le cryptage des données, pour prévenir toute vulnérabilité qui pourrait être exploitée par des attaquants. La collecte doit être limitée aux informations nécessaires pour atteindre les objectifs du logiciel, réduisant ainsi le risque de violations de la vie privée. Enfin, des audits réguliers permettent de vérifier que l'outil est utilisé conformément aux règlements et d'identifier toute faille de sécurité potentielle.

Y-a-t-il une aide de l'assurance maladie pour l'installation de matériels de sécurité type « filtre anti-intrusion » pour protéger le réseau internet , et l'installation de logiciels « coffre-fort» de mots de passe ?

Aucune aide est proposée à ce jour par l'assurance maladie.

Il existe des sociétés d'audit en termes de cybersécurité avec tout et n'importe quoi comme sérieux. Y a-t-il la possibilité de référencer par nos instances et notamment l'URPS, une ou plusieurs sociétés d'audit avec une expertise adaptée à notre profession, une garantie de qualité d'intervention, et une approche tarifaire adaptée ?

Nous allons travailler sur une fiche pratique présentant les éléments clés à vérifier lors du choix d'une société d'audit spécialisée en cybersécurité.