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 pensez avoir besoin d'explications complémentaires, c'est l'occasion de découvrir, à travers un format court, les principaux risques numériques et les bonnes pratiques à adopter au quotidien.

Une version longue est disponible sur le site de l'URPS ML HDF.

Vous trouverez ci-après le lien vers le replay du webinaire de sensibilisation :

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

Si vous souhaitez bénéficier d'une sensibilisation, c'est l'occasion de découvrir, à travers un format court, les principaux risques numériques et les bonnes pratiques à adopter au quotidien.

Bonne lecture !

Sommaire

Le phishing

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

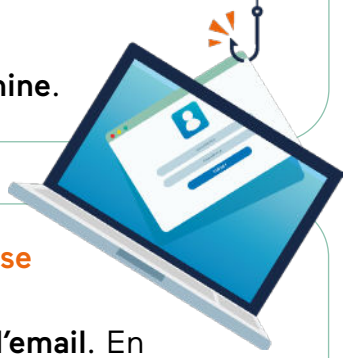
Peut-on être piraté en ouvrant simplement un mail de phishing, sans cliquer sur aucun de ses liens ?

Non. Le seul moyen de se faire pirater par e-mail est d'**interagir avec son contenu**.

Est-ce que des informations personnelles peuvent être récupérées en cliquant sur le lien contenu dans l'email ?

Oui, c'est **possible d'être infecté suite au clic sur le lien de l'email**.

En cas de doute, pensez à **lancer une analyse par l'antivirus de votre machine**.



Faut-il lire attentivement tous nos mails avant de les ouvrir, afin de se prémunir du phishing ?

Oui, il est recommandé d'**être vigilant et de vérifier les informations de l'email**. En cas de doute, pensez à aller directement sur le site qui serait à l'origine de l'email.

Plusieurs recommandations : contrôler la véracité du nom de domaine utilisé, la qualité de l'orthographe et de la syntaxe, ainsi que la qualité des liens de redirection.

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

Non, ce n'est pas possible.

Néanmoins, **le nom de domaine peut avoir une orthographe proche de celle d'un organisme de confiance**. 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.

La sauvegarde

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 fréquence de vos sauvegardes doit **s'adapter à vos besoins**.

Sélectionnez les données à protéger (celles qui ne pourront pas être récupérées en cas de perte / les données consultées régulièrement).

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**.

Il est recommandé d'effectuer des sauvegardes **à intervalles réguliers**.

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

Oui, il est recommandé de **sauvegarder toutes données utiles**, y compris celles stockées sur un logiciel métier en ligne. Une solution fiable consiste à créer une sauvegarde à distance des logiciels métier sur des serveurs sécurisés.

Il est conseillé de vous rapprocher de l'hébergeur de votre solution en ligne.

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

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.

Un redémarrage complet est possible avec une sauvegarde directe.

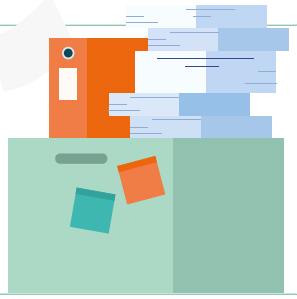
Règles de nommage : A minima, ces règles reprennent des impératifs sur :

1. La déclinaison analytique de l'Union ;
2. Le format des fichiers ;
3. Les caractères et symboles utilisés ;
4. La longueur des noms ;
5. Le format de date si utilisée dans le nom du fichier ;
6. Le statut (la version) du document enregistré.

Les espaces, caractères diacritiques (accent, tréma…), symboles (@…), signes de ponctuation (.,;), …, bien qu'acceptés par certains systèmes, sont à proscrire dans les noms de fichier ou de dossier.

TIPS

La donnée est trop importante : il est toujours bien de savoir réaliser une sauvegarde même lorsqu'un prestataire se charge de la sauvegarde.



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

Des comparatifs et tests accessibles sur internet, 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.*

Les anti-virus

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 » et même sur Mac !

Quel anti-virus choisir ?

Les 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)

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

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 ?

Oui, il est recommandé de **sécuriser ses serveurs professionnels**, en disposant notamment d'un **anti-virus**. La Commission Nationale de l'Information et des Libertés (CNIL) fournit de précieux conseils sur la façon la plus adéquate de sécuriser ses serveurs :
www.cnil.fr/fr/securite-securiser-les-serveurs

Les rançongiciels

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 ?

Non !

Si vous êtes victime :

- Conservez les preuves
- Déposez plainte auprès d'un commissariat (dépôt de plainte en ligne possible)
- Notifiez l'incident à la CNIL
- Faites-vous assister par un professionnel qualifié : www.cybermalveillance.gouv.fr

Les gestionnaires de mots de passe

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

Oui il peut tout à fait être sécurisé. Soyez attentif au sérieux de la solution et de l'éditeur.

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.

Un gestionnaire de mot de passe comporte plusieurs avantages. En effet, celui-ci permet de stocker tous vos mots de passes et les protège en les chiffrant.
De plus, le gestionnaire de mot de passe permet de générer des mots de passe « fort ». Grâce au gestionnaire de mots de passe, plus besoin de retenir des dizaines de mots de passe.

L'utilisation d'un gestionnaire de mot de passe permet de ne retenir qu'un seul mot de passe complexe et robuste.

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

Oui c'est possible.

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

Le site étatique Cybermalveillance.gouv.fr fait référence au gestionnaire de mots de passe sécurisé et gratuit, **KeePass**. Ce petit logiciel libre, **certifié par l'Agence Nationale de la Sécurité des Systèmes d'information (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 ?

Non, les cyberattaques peuvent avoir lieu à tout moment de la journée et provenir de différents pays.

Doctolib est-il protégé d'une attaque ?

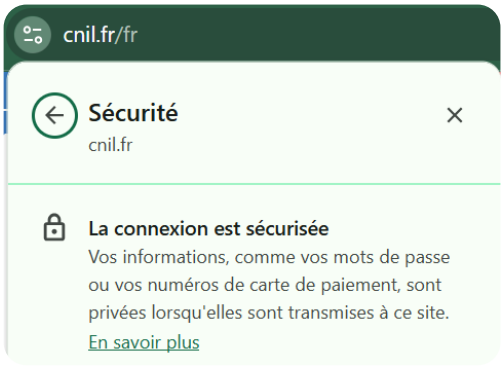
Doctolib déploie certains moyens afin de sécuriser ses services. Sa politique de sécurité est détaillée au lien suivant : https://info.doctolib.fr/securite/

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.

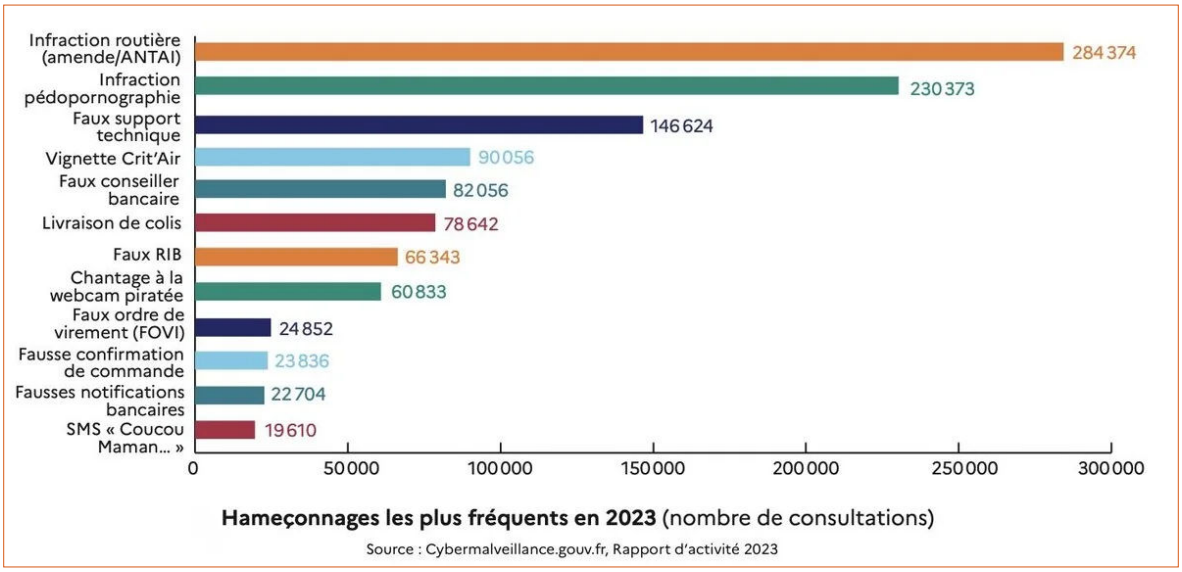


Je reçois énormément de mail d'hameçonnage sur le thème de la livraison de colis. Comment cela se fait ?

Cette méthode est souvent utilisée pour l'hameçonnage via l'envoi d'un SMS pour « une livraison de colis » par exemple.

L'hameçonnage peut être réalisé par mail ou même par SMS (smishing).

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

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 de manière sécurisée autant que possible les informations qui y sont contenues.** Envisagez également de protéger l'accès au disque dur via un mot de passe, afin d'éviter toute fuite.

Qui contacter pour avoir de l'aide en cas d'incident cyber ?

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/

Pour informer les médecins : numerique@urps-hdf.fr
Pour informer les pharmaciens : 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 consultant leur site internet, afin de vérifier avec lui si ce message est valable, ou si c'est une tentative de phishing.
Pour informer les pharmaciens : urgence@urps-pharmaciens-hdf.fr

TIPS **Bloc tel : la meilleure protection contre les appels non sollicités !**

Comment savoir quand un site est légitime ou non ?

- 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 transparente.
- **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.

Qu'est-ce qu'un VPN ?

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 service est fourni sur abonnement via un fournisseur de service VPN (installation de l'outil sur l'ordinateur, tablette, smartphone).

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.

Toutefois, un **VPN n'est pas une solution infaillible, il 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. Il est essentiel d'utiliser un réseau Wi-Fi sécurisé (WPA3 si possible), de mettre en place un pare-feu.
- **Performances** : L'accès en Wi-Fi peut être moins performant qu'une connexion filaire (Ethernet) en termes de vitesse et de stabilité.

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.

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 (masques très élaborés).

À 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.
Il peut être installé à votre insu via un mail phishing par exemple.

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. Néanmoins, les assurances professionnelles proposent de plus en plus des protections en matière de cyber.

Rappel sur l'utilisation des clés USB :
La clé USB est un système de stockage très répandu mais elle peut constituer un véritable danger pour la sécurité informatique. En effet, en passant d'un ordinateur à l'autre, les clés USB peuvent transmettre des malwares ou des virus facilement.
Conseils :

- Ne jamais utiliser une clé USB que l'on ne connait pas,
- N'utilisez que les clés USB fournies par l'employeur,
- Changez régulièrement de clé USB pour éviter l'usure et les pertes de données,
- Éjectez toujours correctement la clé avant de la débrancher,
- Nettoyez régulièrement la clé USB afin de détecter si elle est infectée par un virus.