

Journée régionale

Le numérique en santé en Pays de la Loire

Cybersécurité en santé : tous concernés, les bonnes pratiques à adopter

Emilie Prioux, chef de projet cybersécurité, GRADeS Pays de la Loire

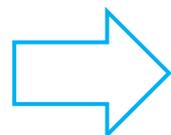
Cyber quiz – A vos smartphones

ETAPE 1 : CONNEXION

Accéder à l'adresse
<https://kahoot.it/>

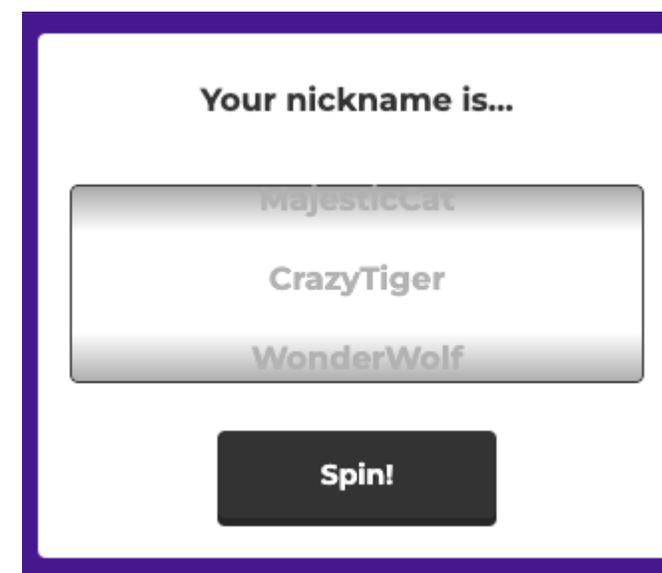


et rentrer le **code PIN**,
affiché à l'écran.



ETAPE 2 : INSCRIPTION

Faites tourner la
roulette et choisissez
votre pseudo
(**3 essais max**)



Cyber quiz – Présentation des questions

Chrono en secondes

Test : choisissez les réponses 2 et 4

Affichage de la question

22

11 réponses

Nbre de participants ayant répondu (temps réel)

▲ 1

◆ 2

● 3

■ 4

Quitter la prévisualisation < 1 sur 18 > L7

Affichage des propositions de réponses (2 ou 4)

Note : Cliquer sur « Envoyer » pour valider votre sélection de réponses sur les choix multiples.

A vous de jouer !



Mot de passe

- **1 mot de passe = 1 seul usage.**
- Utiliser un **mot de passe robuste** pour l'accès à la session utilisateur et **verrouiller** (Windows + L) cette dernière lorsque le terminal n'est plus sous surveillance.
- Définir un **mot de passe fort / robuste** :
 - *au moins 12 caractères,*
 - *ou phrase d'au moins 7 mots,*
 - *majuscules + minuscules + caractères spéciaux + chiffres.*
- Utiliser **l'authentification à plusieurs facteurs** dès qu'elle est disponible (PRO-SANTE CONNECT / eCPS, CPS, ...).
- Ne pas enregistrer les mots de passe dans les navigateurs web mais privilégier **l'utilisation d'un gestionnaire ou coffre-fort numérique de mots de passe** (exemples : KeePassXC, KeePass, Bitwarden, ...).
- Garder **secret le code PIN** de votre carte CPS ou e-CPS (idem pour les téléphones professionnels et tablette).

Info BONUS : pour savoir si votre adresse mail a été victime d'un ou plusieurs piratages avec fuite de mot de passe >> « **have I been pwned** »

UTILISERIEZ-VOUS
UN INSTRUMENT USAGÉ ?



Les mots de passe et les brosses à dents ont beaucoup de points communs !

Il faut les choisir avec soin, les changer régulièrement, ne pas les partager et surtout... les utiliser !



QUITTERIEZ-VOUS VOTRE MAISON
SANS FERMER LA PORTE À CLÉ ?

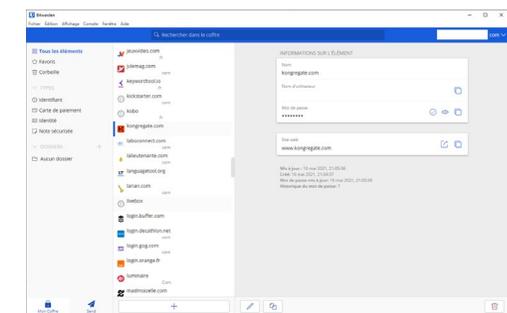
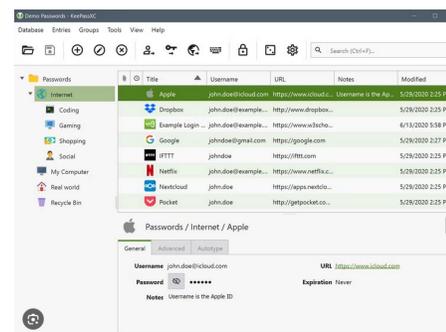


Nos comptes d'utilisateur donnent accès à des données sensibles. Verrouillons nos sessions !

A quoi bon assurer une protection technique forte, si nous laissons l'accès libre à notre poste de travail au risque de vol ou détérioration des données. Changeons nos habitudes !



Keepass XC



Bitwarden

A vous de jouer !



Renforcer la sécurité de mon SI

- Installer un **antivirus** et m'assurer de sa mise à jour régulièrement.
- Assurer la **sécurité physique** de mes équipements :
 - *prise parafoudre pour l'alimentation électrique,*
 - *accès restreints et contrôlés aux ordinateurs / smartphones / supports de stockage, ...*
- **Refuser** l'usage de **dispositifs amovibles** (clé USB, disque, carte SD, smartphone, gadget USB et même un simple câble...) **non maîtrisés**.
- **Limiter** les **comptes administrateurs** (à privilèges) sur les matériels et applicatifs sensibles.
- Ne laisser accéder aux données / documents / informations que les **personnes habilitées** à en prendre connaissance.

VOUS LAISSERIEZ-VOUS CONTAMINER ?



Les clés USB, disques durs et autres périphériques amovibles peuvent propager des virus informatiques.

Soyez conscients des risques ! Ne connectez pas de support USB de source inconnue ou personnelle aux équipements de l'établissement. Si cela est indispensable, réalisez une analyse antivirus avant toute utilisation.



VOUS JETTERIEZ-VOUS DANS LA GUEULE DU LOUP ?



La curiosité est un vilain défaut ! N'ouvrons pas les clés USB trouvées dans la rue, les parkings ou dans nos boîtes aux lettres.

Ces clés USB contiennent des virus sans discontinuer dans votre appareil. Ces clés apparaissent sèches ou avec des données inhabituelles mais cachent des programmes malveillants redoutables capables de se propager dans les systèmes. Ils éliminent vos données, compromettent vos données importantes. Ne branchez jamais de clé inconnue.



Exemple >



Accueil > Actualités et événements > Actualités > Campagne d'envoi de courriers alarmistes contenant une carte SD ou une clé USB

03/10/2023

Plusieurs établissements ont reçu récemment un courrier avec un message "alarmiste" et contenant des cartes SD ou des clés USB. Ces supports contiennent potentiellement un contenu malveillant.

L'auteur de ces courriers invite à prendre connaissance du contenu des supports pour avoir plus amples informations sur cette nouvelle menace sanitaire. Il s'agit donc potentiellement d'une forme de phishing par courrier.

Si un tel courrier vous parvient, nous vous recommandons de :

- Ne pas utiliser les supports ;
- Ne les connecter à aucun poste du SI, sous aucune raison ;
- Les isoler et les conserver pour traces (idéalement, sous coffre).

Renforcer la sécurité de mon SI

- Disposer d'un **inventaire** et/ou une **cartographie** complète de mon SI afin :
 - d'obtenir une vue d'ensemble de celui-ci (matériel, logiciel, ...),
 - d'identifier ses **composants les plus critiques et/ou exposés** pour mettre en place les mesures de protection adéquates.
 - de **réagir plus efficacement** en cas d'incident / cyberattaque,
 - de **qualifier les impacts** et **prévoir les conséquences** des **actions défensives** réalisées.
- Utiliser des **terminaux / systèmes / logiciels** dont le **maintien en conditions de sécurité est garanti** (durée de maintenance) et **appliquer les mises à jour de sécurité** dès qu'elles sont disponibles.
- **Vérifier les contrats avec les prestataires** (périmètre d'intervention, engagements de service, respect de la protection des données, ...).

« Tous les Hommes ne sont pas vulnérables de la même façon ; aussi faut-il connaître son point faible pour le protéger davantage. »
Sénèque

Il en est de même pour votre SI !



Sauvegardes

- **Sauvegarder régulièrement** les données :
 - Chez un prestataire spécialisé et certifié **Hébergeur de Données de Santé (HDS)** pour les données concernées,
 - Sur des supports amovibles, isolés du réseau, chiffrés, stockés dans un rangement sécurisé, protégés des vols et sinistres.
- **Tester** régulièrement la bonne exécution des **sauvegardes** et leurs **restaurations**.
- **Détruire les données devant être supprimées** (destruction physique et/ou effacement sécurisé des supports) dans le respect des délais de conservation définis (*Délibération CNIL n° 2020-081 en date du 18 juin 2020 et conformément au Code de la Santé Publique*).

EN CAS D'INCIDENT, AVEZ-VOUS UN PLAN B ?



Nos systèmes ne sont pas infailibles. Cependant la prise en charge des usagers ne doit être ni interrompue, ni dégradée.

Des procédures de secours décrivent les modalités à tenir en cas de défaillance du système ont été élaborées par la structure. Veillez à les connaître et suivre leurs mises à jour.



PARTAGEZ-VOUS DES DOCUMENTS VOLUMINEUX VIA LE CLOUD ?



En utilisant des espaces de partage sur internet, la sécurité des données de l'utilisateur n'est pas assurée.

Respectons la vie privée des usagers et le secret des informations les concernant en utilisant des services de partage sécurisés chez des hébergeurs certifiés de données de santé.



Exemples

Doctolib perd des milliers de données médicales sensibles

Accueil > Sécurité

Sécurité Par Amandine Joniaux le 05 mai 2023 à 10h00

4 commentaires

Doctolib a perdu plusieurs milliers de données liées à des consultations médicales, et vous êtes peut-être concernés.



A vous de jouer !



Messagerie

- Utiliser une **Messagerie Sécurisée de Santé (MSSanté)** pour échanger des données sensibles et/ou à caractère personnel entre professionnels de santé et avec les patients.

LA PLAGE

Salut Mamie et Papi,
On pense très fort à vous pendant les vacances avec papa et maman.

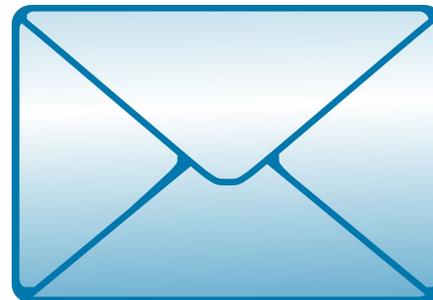
On retrouve nos copains au club Mickey tous les jours et le soir papa s'occupe du barbecue.
C'est trop bien les vacances!
On espère que vous pourrez venir nous voir très vite.



Thierry et Sylvie Adam
1 route de la vallée
14390 Houlgate

Messagerie Classique (Gmail, Outlook, ...)

MSSanté (messagerie sécurisée)



COMMENT ÉCHANGEZ-VOUS LES DONNÉES PERSONNELLES DE VOS PATIENTS ?



Les messageries non sécurisées ne respectent pas le secret professionnel. Passons à la MSSanté !

Nos messageries classiques d'établissement ou celles sur internet ne constituent pas un canal fiable et réglementaire pour la transmission des données patients. Échangeons entre professionnels habilités grâce à une Messagerie Sécurisée de Santé.



PARTAGEZ-VOUS DES DOCUMENTS VOLUMINEUX VIA LE CLOUD ?



En utilisant des espaces de partage sur internet, la sécurité des données de l'utilisateur n'est pas assurée.

Respectons la vie privée des usagers et le secret des informations les concernant en utilisant des services de partage sécurisés chez des hébergeurs certifiés de données de santé.



Messagerie

- Les éléments à vérifier en cas de réception d'un mail suspect :
 - **Le nom de l'expéditeur + l'adresse d'expédition.**
 - Augmentation des cas d'usurpation de noms de contacts ou services connus et d'attaque par ingénierie sociale.
 - Il est recommandé de contacter l'expéditeur (quand celui-ci est connu) par un autre canal pour confirmer l'origine de l'envoi du mail.
- Un objet de mail et/ou contenu trop **alarmiste** ou **alléchant**.
- Une **apparence suspecte**, un **horaire** en dehors des heures de travail habituel, etc.
- Une **demande inhabituelle**, potentiellement associée à une demande **d'infos confidentielles**, avec un **caractère d'urgence**.
- Une incitation à **cliquer sur un lien** (positionner le curseur de sa souris sur le lien, sans cliquer pour vérifier l'URL) ou à **télécharger une pièce jointe**.



En règle générale, méfiez-vous si vous observez des différences entre l'apparence de l'e-mail reçu et celle des mails habituels.



pimkles@dfyoxc.owler.com
Heure d'envoi = 02:10

Message du 20/10/21 02:10
De : "Group Service" <pimkles@dfyoxc.owler.com>
A : [redacted]
Copie à :
Objet : Assurance Maladie | Ameli.fr

« Nous vous demandons de mettre à jour vos données ... dans les plus brefs délais. »



Contenu alléchant = remboursement de frais d'environ 300€.

A vous de jouer !



Usages et nomadisme

- Disposer d'une **charte informatique** précisant les règles d'utilisation (s'il y a plusieurs utilisateurs du SI).
- **Eviter la mutualisation des usages professionnels et personnels** sur un même appareil.
- **Ne pas se connecter à des réseaux non maîtrisés et/ou non sécurisés** (Wi-Fi public, objet connecté inconnu, ...).
- **Protéger la confidentialité des données** en utilisant par exemple un **filtre de confidentialité** lorsque l'écran peut être observé par des tiers (déplacements, lieux publics, ...).
- Réaliser un **chiffrement complet du disque** (Bitlocker – outil natif Windows, Cryhod - recommandé par l'ANSSI, Veracrypt – recommandé par la CNIL.)
- **Limiter la liste des applications pouvant être installées** sur des terminaux nomades. Utiliser des logiciels, applications et produits de sécurité référencés (notamment en établissement) :
 - SESAM-VITALE
 - ANSSI : <https://www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf>

JO Paris 2024 04/03/2024 20:25 | Actualisé le 04/03/2024 21:53

JO Paris 2024 : vol d'un deuxième ordinateur contenant des « plans confidentiels » à Drancy, en Seine-Saint-Denis

Un ordinateur qui contenait un plan détaillé des JO de Paris 2024 a été dérobé à Drancy, en Seine-Saint-Denis. Il appartenait à un membre de la direction de l'hôpital Avicenne de Bobigny.

Exemple

JO PARIS 2024 - Deux vols en l'espace d'une semaine. Une nouvelle personne en possession d'informations confidentielles concernant l'organisation des JO de Paris 2024 a été victime d'un vol, ce vendredi 1er mars. Aux alentours de 20 heures, la voiture de la secrétaire générale de la direction de l'hôpital Avicenne de Bobigny a été cambriolée, alors qu'elle était garée sur un parking du centre commercial « Avenir » à Drancy, le temps que sa conductrice fasse une course.

Sans que cette dernière en soit témoin, le déflecteur arrière droit du véhicule a été brisé et son sac contenant son ordinateur de travail a été volé. Or l'appareil contenait des documents confidentiels, notamment les plans d'accès et les plans de circulation des JO. En effet, ces documents sont indispensables pour les secours qui devront intervenir pendant l'évènement.

https://www.huffingtonpost.fr/jo-paris-2024/article/jo-paris-2024-un-deuxieme-ordinateur-contenant-des-plans-confidentiels_230738.html

A vous de jouer !



Réagir en cas d'incident

- **Déconnecter du réseau/wifi** la machine sur laquelle l'incident est suspecté.
- **Maintenir l'appareil sous tension**, le brancher s'il est sur batterie.
- **Prévenir votre service informatique ou prestataire** pour obtenir une assistance.
- **Déclarer ou décrire l'incident** en cours sur votre système d'information :

Etablissements de santé, Organismes et services exerçant des activités de prévention, de diagnostic ou de soins et les établissements médico-sociaux	Autres structures, professionnels libéraux
<p>Déclarer l'incident (obligation réglementaire) : https://signalement.social-sante.gouv.fr/</p> <p>Doit être déclarée sur le portail, sans délai, toute action ou suspicion d'action malveillante sur le SI ayant un impact sur le fonctionnement normal de l'établissement.</p> <p>Les déclarations reçues sur le portail de signalement sont transmises à l'ARS, au GRADEs PdL et à l'Agence du Numérique en Santé (CERT Santé).</p>	<p>Décrire l'incident de sécurité sur le site www.cybermalveillance.gouv.fr et suivre les conseils donnés.</p> <p>Service gratuit. La description de l'incident permet d'obtenir un premier diagnostic avec des conseils adaptés à la situation rencontrée.</p> <p>Si besoin, les victimes sont mises en relation avec des prestataires de proximité spécialisés, référencés, susceptibles d'aider dans la résolution du problème.</p> <p>Vous pouvez également contacter le Centre régional de réponses aux incidents de sécurité informatique et cyberattaques (Pays de la Loire Cyber Assistance - CSIRT régional).</p>

- **Alerter** les autorités compétentes :
 - **CNIL** : en cas de violation de données suspectée ou avérée.
 - **Gendarmerie / police** : si l'incident est d'origine malveillante pour effectuer un dépôt de plainte.

Sécurité numérique
en santé

MÉMO – Dépôt de plainte suite à un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

POURQUOI DÉPOSER PLAINTE ?

- ✓ Être reconnu en tant que victime et ainsi faire valoir vos droits via l'ouverture d'une enquête pénale ;
- ✓ Être accompagné dans une situation complexe par des professionnels habilités et aguerris (expertise cyber, ...)
- ✓ Permettre le cas échéant, selon vos contrats d'assurance*, le déclenchement du processus de prise en charge de tout ou d'une partie des coûts financiers résultant de l'incident, à condition que la plainte soit déposée dans les 72h comme stipulé dans la Loi du 24/01/23 d'Orientation et de Programmation du ministère de l'Intérieur (LOPMI) ;
- ✓ Bénéficier des résultats de l'enquête (identité de l'auteur des faits, indemnisation, récupération des données (le cas échéant), déchiffrement, ...)
- ✓ Participer à la lutte contre la cybercriminalité en fournissant aux forces de l'ordre des informations précieuses permettant d'en apprendre davantage sur les méthodes des cybercriminels et permettre de leur arrestation potentielle.
- ✓ Limiter le risque d'engagement de votre responsabilité en cas d'utilisation non souhaitée de votre système d'information pour mener des attaques à l'encontre de tiers (partenaires, fournisseurs, usagers, ...).

À noter qu'en aucun cas, un dépôt de plainte ne se substitue à la déclaration sur le portail de signalement des événements sanitaires indésirables (<https://signalement.social-sante.gouv.fr/accueil>), qui est OBLIGATOIRE pour tous les établissements de santé (sanitaires et médico-sociaux) et une déclaration à la CNIL (dans les 72H) en cas de violation de données à caractère personnel.

COMMENT DÉPOSER PLAINTE ?

- Etape 1 :**
La structure victime d'un acte malveillant sur son système d'information réalise une analyse de la situation afin de caractériser les faits autant que possible (Cf. § Questions / Informations pour l'analyse de la situation).
- Etape 2 :**
À la suite de cette première analyse, le représentant légal de la structure peut aller déposer plainte :
 - Soit, en se **déplaçant physiquement** dans un commissariat de police ou une brigade de gendarmerie ;
 - Soit, sur le site internet : <https://www.pre-plainte-en-ligne.gouv.fr/> ;
 - Soit, en **transmettant un courrier papier au procureur de la République** de la ville de l'établissement.

Le dépôt de plainte doit intervenir avant la réinstallation des appareils touchés, de manière à conserver et collecter les preuves techniques de l'incident afin de les fournir aux enquêteurs. Cf. Fiche mémo – « Collecte des traces suite à une cyberattaque ».

ABSENCE REPRÉSENTANT LÉGAL

Dans le cas où le représentant légal de la structure ne peut se déplacer lui-même pour effectuer le dépôt de plainte, il lui est possible d'envoyer une autre personne de la structure ayant en sa possession :

- Une copie de la pièce d'identité du représentant légal,
- Un avis de situation SIRENE,
- Un mandat daté et signé par le représentant légal de la structure.

*ZOOM ASSURANCE « CYBER »

Les contrats d'assurance « cyber » sont constitués d'un ensemble de garanties ciblant principalement en tant que causes, les actes malveillants, et certaines erreurs, ayant pour conséquence des compromissions de données et des perturbations d'activité.

En réponse à l'émergence de risques récents, elles apportent donc une couverture de frais de gestion et dommages immatériels, aux Tiers ou aux Assurés, venant ainsi compléter respectivement les offres assurantielles en « Responsabilité Civile » et « Dommages aux Biens » qui ciblent historiquement d'autres types de sinistres.

À noter que leur contractualisation demande en prérequis la mise en œuvre d'un niveau minimal de sécurité informatique.



Sensibilisation à la cybersécurité

Pour aller plus loin

- S'informer régulièrement sur les cybermenaces : www.cybermalveillance.gouv.fr
- Partager, rappeler régulièrement les bonnes pratiques et conseils d'hygiène numérique avec ses confrères/consœurs/collaborateurs.
- Documentation liée à la **cybersécurité et au RGPD** pour les **professions libérales**



Référentiel CNIL relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux

https://www.cnil.fr/sites/cnil/files/atoms/files/refere-ntiel_-_cabinet.pdf



Mémento de sécurité informatique pour les professionnels de santé en exercice libéral - Annexe 1 Questionnaire fournisseurs

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



Guide CNIL et CNOM sur la protection des données personnelles

https://www.conseil-national.medecin.fr/sites/default/files/external-package/edition/17ss6et/guide_cnol_rgpd.pdf

« La sécurité informatique est comme une chaîne, elle ne peut être forte que si chaque maillon est solide. »

Robert Mueller,
ancien directeur du FBI



Sensibilisation à la cybersécurité

Pour aller plus loin

- Livret sur la cybersécurité « Tous cybervigilants ! » de l'URPS Masseurs-Kinésithérapeutes des Pays de la Loire :



<https://www.urps-mk-paysdelaloire.fr/livret-sur-la-cybersecurite-tous-cyber-vigilants/>

- Guide cybersécurité dédié aux ESMS : « La cybersécurité pour le social et le médicosocial en 13 questions ».



SYNTHÈSE

ACTIONS PRIORITAIRES À RÉALISER

<p>1. Constituez-vous efficacement votre parti informatique ?</p> <ul style="list-style-type: none"> - Appointer - Responsabilité et rôles - Logiciel utilisé - Données et traitement de données - Date de mise à jour - Maintenance 	<p>2. Appliquez-vous régulièrement les mises à jour ?</p> <ul style="list-style-type: none"> - Appliquez les mises à jour en logiciel, système, système d'exploitation, applications et des matériels. - Activez toutes les mises à jour de logiciels et des matériels. 	<p>3. Avez-vous implémenté une politique d'usage de mots de passe robustes ?</p> <ul style="list-style-type: none"> - Définir et mettre en œuvre des politiques de mots de passe. - Définir des règles de mots de passe en matière de complexité et de durée de validité. - Définir des règles de mots de passe en matière de confidentialité.
<p>4. Utilisez-vous un antivirus ?</p> <ul style="list-style-type: none"> - Identifier les logiciels à protéger. - Choisir un antivirus compatible avec votre système d'exploitation. - Choisir le ou les logiciels à protéger. - Éviter le partage de fichiers et de données. 	<p>5. Utilisez-vous un pare-feu ?</p> <ul style="list-style-type: none"> - Définir et mettre en œuvre des politiques de mots de passe. - Définir des règles de mots de passe en matière de complexité et de durée de validité. - Définir des règles de mots de passe en matière de confidentialité. 	<p>6. Avez-vous activé un pare-feu ?</p> <ul style="list-style-type: none"> - Définir et mettre en œuvre des politiques de mots de passe. - Définir des règles de mots de passe en matière de complexité et de durée de validité. - Définir des règles de mots de passe en matière de confidentialité.
<p>7. Comment sécurisez-vous votre messagerie ?</p> <ul style="list-style-type: none"> - Identifier les professionnels. - Protéger la confidentialité des messages professionnels via des logiciels sécurisés. - Protéger d'un système d'analyse contenu. - Activer la fonction de la recherche de contenu (Transport Layer Security - TLS). 	<p>8. Comment sécurisez-vous vos usages informatiques ?</p> <ul style="list-style-type: none"> - Créer des comptes utilisateurs dédiés. - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges. - Au départ d'un collaborateur, faire l'installation de ses outils et son logiciel. 	<p>9. Comment sécurisez-vous le risque matériel lié au matériel des professionnels ?</p> <ul style="list-style-type: none"> - Sécuriser rigoureusement vos données. - Couvrir vos matériels informatiques. - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges.
<p>10. Comment vous informez-vous ?</p> <ul style="list-style-type: none"> - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges. 	<p>11. Servez-vous comment réagit en cas de cyberattaque ?</p> <ul style="list-style-type: none"> - Organiser des exercices de crise cybernétique. - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges. - Définir des règles de mots de passe et de privilèges. 	<p>12. Avez-vous fait évoluer la couverture de votre police d'assurance cyber ?</p> <ul style="list-style-type: none"> - Couvrir vos données et vos clients. - Couvrir vos données et vos clients. - Couvrir vos données et vos clients.
<p>13. Multipliez-vous les réponses matérielles liées à vos relations avec des tiers ?</p> <ul style="list-style-type: none"> - Identifier et évaluer dans les contrats les clauses relatives à la confidentialité. - Identifier et évaluer dans les contrats les clauses relatives à la confidentialité. - Identifier et évaluer dans les contrats les clauses relatives à la confidentialité. 		

https://esante.gouv.fr/sites/default/files/media_entity/documents/ANS_GUIDECYBER_PHASE%201-EXE%20-V2.pdf

WEBINAIRES !

Présentation du Centre de ressources SSI mutualisées à destination des ESMS*

Mardi 14/05/24, 9h15 à 10h.

Mardi 28/05/24, 14h15 à 15h.

* Lien vers le webinaire accessible en cliquant sur la date correspondante.

Sensibilisation à la cybersécurité

Pour aller plus loin

- Plateforme (e-learning, faux-phishing) proposée aux adhérents du GCS e-santé afin de sensibiliser les collaborateurs aux bonnes pratiques d'hygiène numérique.
- Contenu contextualisé à la santé :
 - E-learning : courte vidéo de sensibilisation (quiz, saynètes, ...) portant sur différentes thématiques cyber, possibilité de suivre des parcours, ...
 - Modèles de mails de faux-phishing pré-paramétrés.

E-learning



- 2 modes d'accès :
 - Acquisition licence(s) par la structure,
 - Intégration du programme annuel prédéfini, piloté par le GCS e-santé (mode opéré).
- Signature convention de services.

Faux-phishing



Cher(e) Client(e),
Votre service client **GlobalExpress** vous informe que vous recevez ce message en dernier avis concernant votre dossier n° 4868.
En effet, plusieurs tentatives infructueuses de vous joindre sur votre téléphone personnel nous autorise à vous l'adresser.
Nous avons enregistré un double débit sur votre compte client, servant pour la même mensualité comptant pour la somme de 105,90€ (soit 52,95€ x 2).
Pour résoudre le problème maintenant et obtenir des informations supplémentaires, UnionExpress reste à votre disposition en cliquant ci-dessous :

Cliquez ici !

Nous vous remercions de votre confiance,
Cordialement,
Votre service client **GlobalExpress**

DANGER PHISHING



CECI EST UNE TENTATIVE DE PHISHING

Heureusement, ce n'était qu'un test à vocation purement pédagogique.
Voici les 4 indices qui auraient pu vous alerter :

1

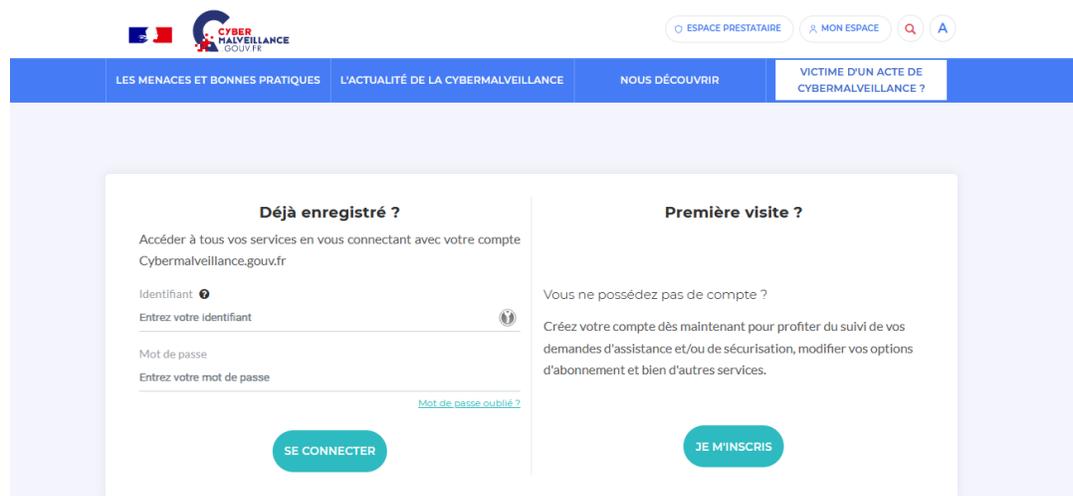
L'adresse mail de l'expéditeur est-elle légitime ?

GlobalExpress <global.express@coom.site>
À moi

Sensibilisation à la cybersécurité

Pour aller plus loin

- **SensCyber** : Module de e-sensibilisation mis à disposition par le site Cybermalveillance.gouv.fr adapté au grand public et petites organisations (<https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre>).
 - Gratuit, accès via la création d'un compte sur la plateforme, nombre d'essais illimité.
 - Programme en 3 modules (Comprendre / Agir / Transmettre), avec une durée de 30 à 45 minutes / module.
 - Objectif : se familiariser en peu de temps aux enjeux de la cybersécurité à travers une activité ludique et donner du sens aux bonnes pratiques.
 - Attestation de suivi téléchargeable en fin de programme (si score minimal de 60%).



Module 1 : Comprendre (43min)

- Quelles menaces aujourd'hui ?
- Quels risques pour moi et mon organisation ?
- Que faire si je suis victime d'une attaque ?

Module 2 : Agir (33min)

- Quelles bonnes pratiques au quotidien ?
- Quels bons réflexes dans mes usages ?

Module 3 : Transmettre (33min)

- Sensibiliser, pourquoi et comment ?
- Pour aller plus loin: Acteurs nationaux et textes de référence.

MERCI

Pour toutes questions :
cyber@esante-paysdelaloire.fr

