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

Financé par l'Union européenne NextGenerationEU

Cyber quiz – A vos smartphones

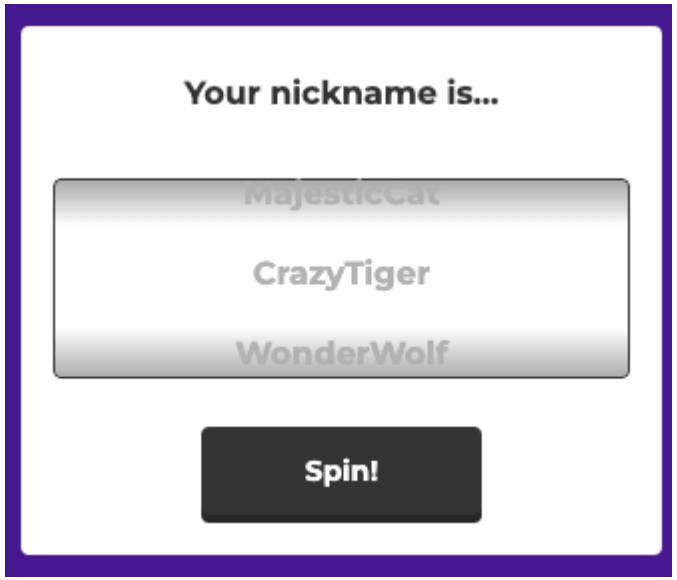
ETAPE 1 : CONNEXION

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

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

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

ETAPE 2 : INSCRIPTION



Financé par l'Union européenne NextGenerationEU

Cyber quiz – Présentation des questions

Affichage des propositions de réponses (2 ou 4)

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

Financé par l'Union européenne NextGenerationEU

A vous de jouer !

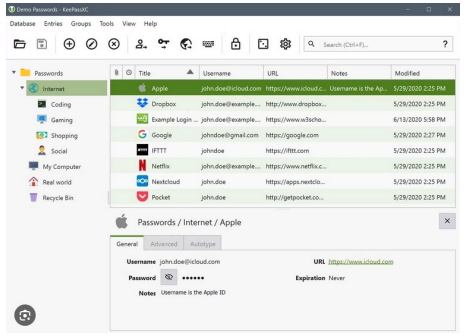
Financé par l'Union européenne NextGenerationEU

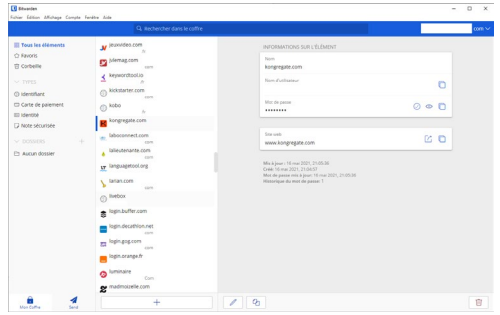
Mot de passe

- **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** »*

Keepass XC





Bitwarden

Financé par l'Union européenne NextGenerationEU

A vous de jouer !

Financé par l'Union européenne NextGenerationEU

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 maitrisés**.
- **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.

Exemple >

Financé par l'Union européenne NextGenerationEU

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 !

Financé par l'Union européenne NextGenerationEU

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*).

Exemples

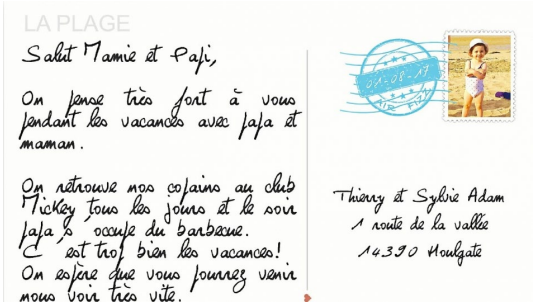
Financé par l'Union européenne NextGenerationEU

A vous de jouer !

Financé par l'Union européenne NextGenerationEU

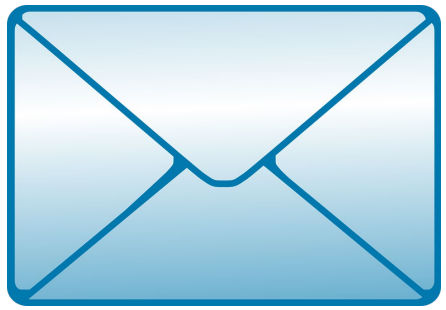
Messagerie

- 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.



Messagerie Classique (Gmail, Outlook, …)

MSSanté (messagerie sécurisée)



Financé par l'Union européenne NextGenerationEU

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

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

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

Financé par l'Union européenne NextGenerationEU

A vous de jouer !

Financé par l'Union européenne NextGenerationEU

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

Exemple

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.

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

Financé par l'Union européenne NextGenerationEU

A vous de jouer !

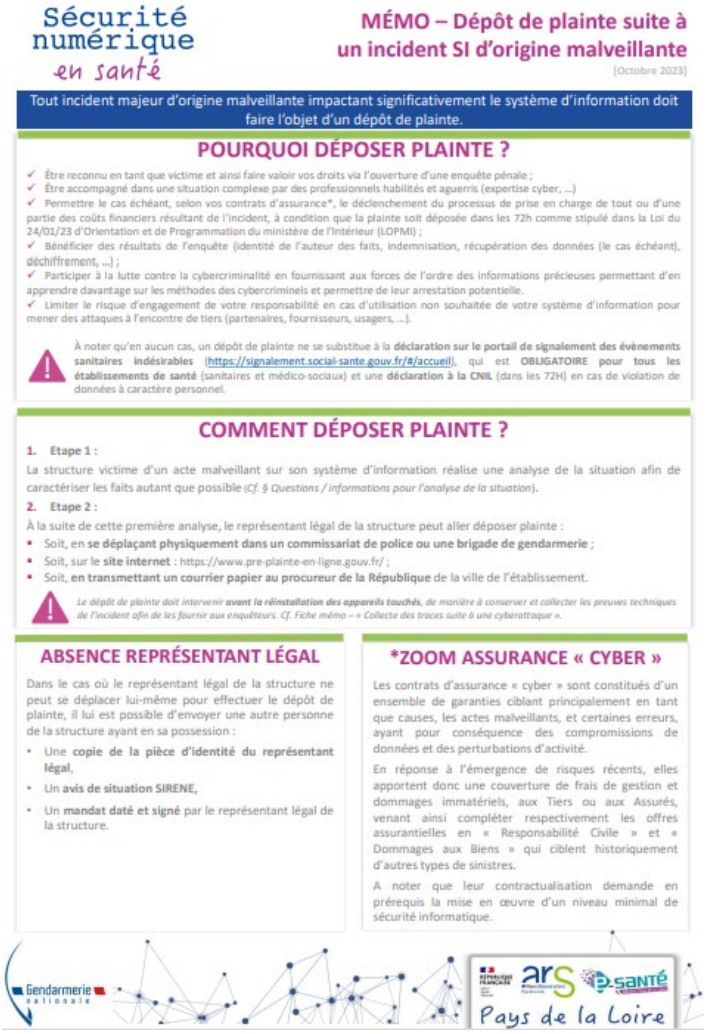
Financé par l'Union européenne NextGenerationEU

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
Déclarer l'incident (obligation réglementaire) : https://signalement.social-sante.gouv.fr/ 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.** 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**).	**Décrire** l'incident de sécurité sur le site www.cybermalveillance.gouv.fr et suivre les conseils donnés. Service gratuit. La description de l'incident permet d'obtenir un **premier diagnostic** avec des **conseils adaptés** à la situation rencontrée. Si besoin, les victimes sont mises en relation avec des **prestataires de proximité spécialisés**, référencés, susceptibles d'aider dans la résolution du problème. Vous pouvez également contacter le **Centre régional de réponses aux incidents de sécurité informatique et cyberattaques** (Pays de la Loire Cyber Assistance - CSIRT régional).

- **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 évènements 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 ?

1. **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*).

2. **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.

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

Gendarmerie nationale

ars Pays de la Loire

Financé par l'Union européenne NextGenerationEU

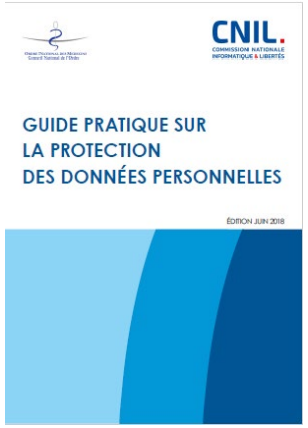
Sensibilisation à la cybersécurité

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/referentiel_-_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_cnom_cnil_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

Financé par l'Union européenne NextGenerationEU

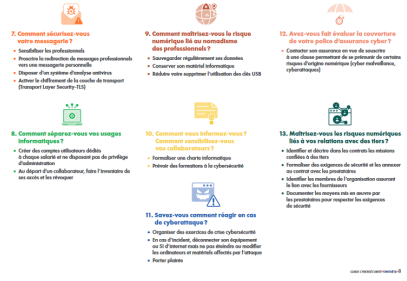
Sensibilisation à la cybersécurité

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* ».



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.*

Financé par l'Union européenne NextGenerationEU

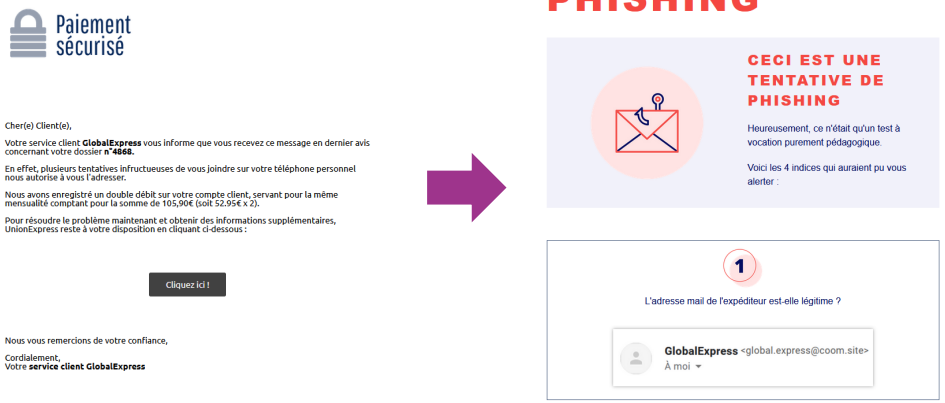
Sensibilisation à la cybersécurité

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

Faux-phishing



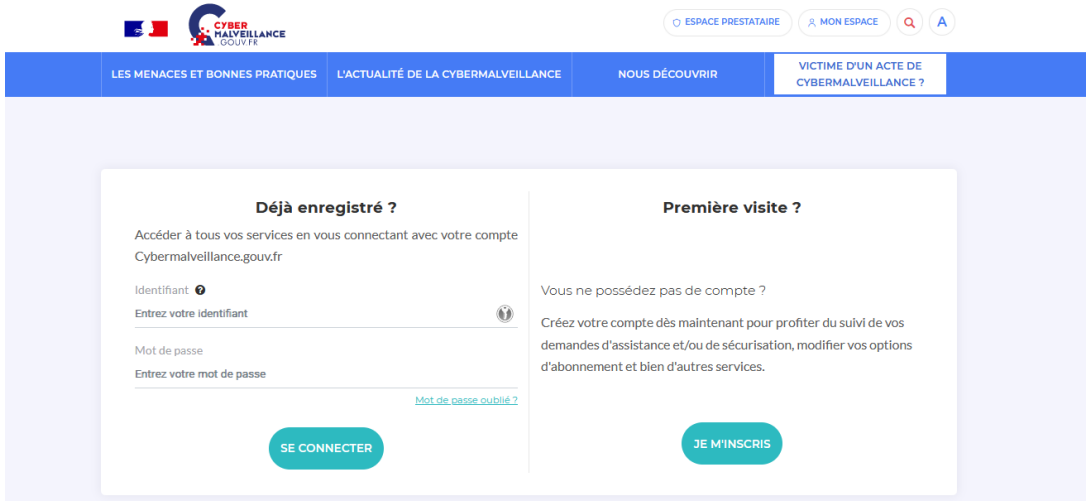
- 2 modes d'accès :
  - Acquisition licence(s) par la structure,
  - Intégration du programme annuel prédéfini, piloté par le GCS e-santé (mode opéré).
- Signature convention de services.

Financé par l'Union européenne NextGenerationEU

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%).



Financé par l'Union européenne NextGenerationEU

MERCI

Pour toutes questions :

cyber@esante-paysdelaloire.fr

Financé par l'Union européenne NextGenerationEU