Groupement e-santé Pays de la Loire

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

Sensibilisation à la sécurité numérique

WEBINAIRE URML PDL – 03/07/25

Avec le soutien de :

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Pays de la Loire

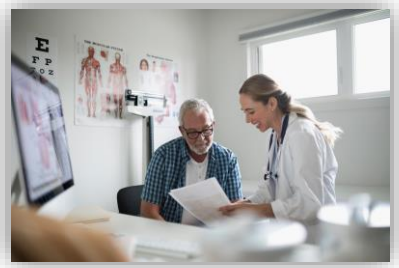
Cofinancé par l'Union européenne

RÉGION PAYS DE LA LOIRE

Quelques idées reçues sur la cybersécurité en santé

La cybersécurité, c'est trop compliqué. Je ne suis pas un(e) expert(e) en informatique.

La sécurité du SI, c'est l'affaire de mon prestataire informatique. Je ne suis pas concerné(e).



Les données de mon « petit SI » n'intéressent pas les cyberattaquants. Il n'y a que les grosses structures (type CHU ou CH) qui sont « visées » par les cyberattaques.

Les menaces pesant sur le secteur de la santé / social

Attaques à finalités lucratives

- Chiffrement des données via rançongiciels à des fins d'extorsion
- Exfiltration de données à des fins d'extorsion et / ou de revente

Compromissions à des fins de fraudes

- Vol d'accès de professionnels de santé pour établir de faux documents (exemples : passes sanitaires, ordonnances…)

Espionnage

- Données médicales d'individus ou données de recherche

Déstabilisation

- Déni de service distribué
- Défiguration de sites web
- Exfiltration de données pour divulgation publique

Ces faux arrêts maladie très crédibles vendus sur Snapchat.
Des faussaires usurpent l'identité de vrais médecins pour vendre des arrêts de travail à des coûts très compétitifs, un préjudice lourd pour la Sécu.

lepoint.fr
Ces faux arrêts maladie très crédibles vendus sur Snapchat
Des faussaires usurpent l'identité de vrais médecins pour vendre des arrêts de travail à des coûts très compétitifs, un préjudice lourd pour la Sécu.

https://www.lepoint.fr/societe/ces-faux-arrets-maladie-tres-credibles-vendus-sur-snapchat-12-03-2023-2511747_23.php#11

> En 2023, des médecins généralistes libéraux ont été ciblés par un phishing usurpant Doctolib, entraînant le vol d'identifiants, le blocage de l'agenda en ligne et un accès non autorisé à des données patients.

Cybercriminalité : une dizaine de cabinets dentaires attaqués, contraints de payer une rançon

Un jour tout bascule…

L'histoire n'est pas nouvelle ni unique d'ailleurs mais elle concerne cette fois-ci une dizaine de cabinets simultanément, tous localisés en Gironde. Attaqués via un ransomware, toutes leurs données ont été cryptées. Impuissants et dans l'impossibilité de continuer à travailler, ils ont payé les sommes réclamées par les cyberpirates.

Source de l'article

Les enjeux de la cybersécurité dans le secteur de la santé

Qualité et continuité de la prise en charge des patients

Disponibilité - *L'information doit être **disponible à tout moment** aux personnes qui y ont accès.*

Intégrité - *L'information doit être **précise, complète, ni altérée, ni altérable**. Les informations ne doivent pouvoir être modifiées que par les personnes qui y sont habilitées.*

Secret professionnel

Confidentialité - *Veiller à ce que l'information soit **seulement accessible** à celles et ceux qui en ont **l'autorisation**.*

Données des SI de santé

Preuve et contrôle

Responsabilité – *Assurer la **non-répudiation** (impossibilité de nier avoir reçu ou émis un message (preuve)) et le **contrôle** du bon déroulement d'une fonction (audibilité).*

A vous de jouer !

Kahoot!

Cyberquiz

A vos smartphones

ETAPE 1 : CONNEXION

Accéder à l'adresse https://kahoot.it/ et rentrer le code PIN

ETAPE 2 : INSCRIPTION

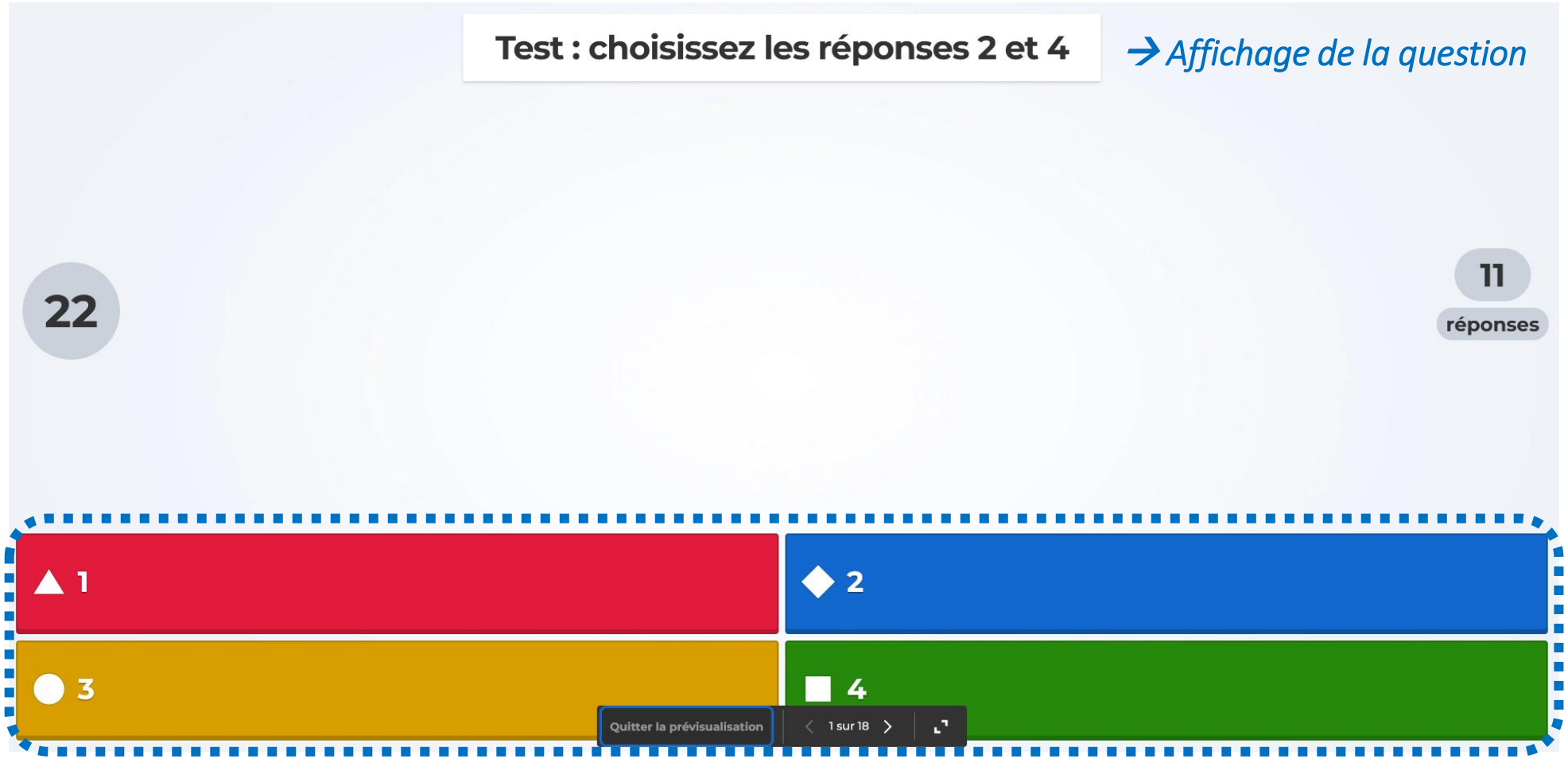
Choisissez un pseudonyme (jusqu'à 3 propositions)

ETAPE 3 : FONCTIONNEMENT

- Affichage à l'écran du type de réponse attendu (vrai/faux, réponses multiples) avant de voir la question.
- Projection de la question sur l'écran principal pendant quelques secondes avant de s'afficher sur vos téléphones avec les propositions de réponses.
- Sélection de la ou des réponses voulues (Chrono pris en compte dans le podium).

Cyberquiz

Présentation du type de question



→ *Affichage de la question*

Chrono en secondes

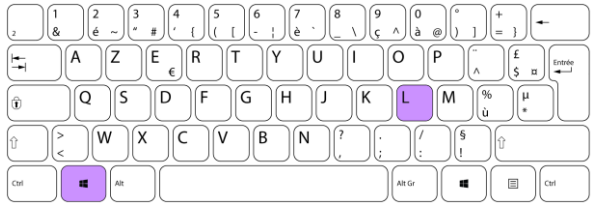
Nombre de personnes ayant répondu à la question (en temps réel)

Affichage des propositions de réponses

Mots de passe

Rappel des bonnes pratiques

- 1 mot de passe = 1 seul usage.
- Utiliser un **mot de passe robuste** pour l'accès à la session utilisateur et **verrouiller** cette dernière lorsque le terminal n'est plus sous surveillance.
  - Windows : **Windows + L**
  - Mac : **Contrôle + Commande + Q**
- Définir un **mot de passe fort / robuste :**
  - *au moins 12 caractères OU phrase d'au moins 7 mots,*
  - *majuscules + minuscules + caractères spéciaux + chiffres.*
- **Eviter les incrémentations** lors d'un renouvellement de mot de passe (au début ou à la fin) :
  - Motdepasse*12*
  - Motdepasse*13*
  - *14*Motdepasse
  - …



Exemple

ACCUEIL › SOCIÉTÉ

Assurance maladie : Le site Ameli piraté, les données de plus de 500.000 Français dérobées

HACKERS La Cnam assure qu'aucune coordonnée de contact ou bancaire n'a été dérobée

20 Minutes avec agences | Publié le 18/03/22 à 11h20

Mots de passe

Rappels des bonnes pratiques

- Ne pas enregistrer les mots de passe dans les navigateurs web.
    - Privilégier **l'utilisation d'un gestionnaire ou coffre-fort numérique de mots de passe** (exemples : KeePassXC, KeePass, Bitwarden, …).

Exemple *: fin juillet 2024, disparition des mots de passe enregistrés dans le navigateur Google Chrome pour 15 millions d'utilisateurs, pendant presque 18h.*

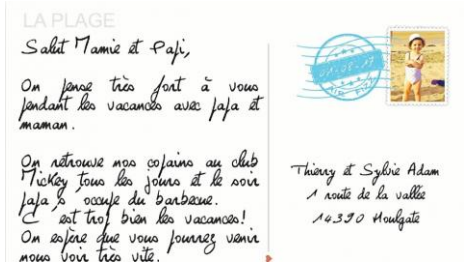
- **Modifier les codes PIN par défaut de vos outils numériques** (téléphones professionnels, tablette, …) et **garder les secrets.**

- Utiliser **l'authentification à plusieurs facteurs** dès qu'elle est disponible (PRO-SANTE CONNECT / eCPS, CPS, U2F, TOTP…).

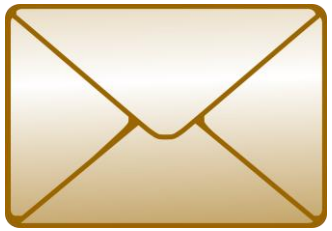
Messagerie

Messagerie « classique » versus MSSanté

- 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 (via « Mon Espace Santé »).



Messagerie Classique (Gmail, Outlook, …)



MSSanté (messagerie sécurisée)

- **Eviter le renvoi ou transfert de mails** depuis votre **boîte professionnelle** vers votre messagerie **personnelle** et vice et versa.

Messagerie

Rappel des bonnes pratiques

- **Rester vigilant** lors de la réception de mail incluant des **pièces jointes** et/ou un **lien à cliquer** (tentative de phishing ou hameçonnage).

Se méfier des contenus à caractère urgent / alléchant ou demandant des informations sensibles.

Vérifier les points de contrôle pouvant vous alerter.

Signaler le message (spam) et bloquer l'expéditeur.

Astuce : « ***have I been pwned*** », site qui permet de savoir si son adresse de messagerie est présente dans une ou plusieurs fuites de données et si oui, lesquelles.

Messagerie

Attention au Phishing (ou Hameçonnage)

*Un objet de mail et/ou contenu trop **alarmiste** ou **alléchant.***

*Un **nom d'expéditeur inhabituel** et/ou une **adresse d'expédition fantaisiste** mais pas que …*

- De plus en plus d'usurpation de noms de contacts ou services connus et d'attaque par ingénierie sociale sont constatées.
- 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.

Remboursement impôts

C Cybercriminel <JaiDeMauvaisesIntentions@office36o.com>
À IsidoreTRUC

Madame, Monsieur,

Suite aux derniers calculs de l'exercice fiscal de l'année précédente, nous vous informons que vous êtes admissible à recevoir un remboursement d'une somme de **120,70€**.

Pour percevoir votre remboursement d'impôt dans les plus brefs délais, vous devez nous transmettre impérativement la demande de remboursement dans un délai de **48h maximum**.

Pour accéder au formulaire de remboursement d'impôt, cliquez ci-dessous :

Go

Un remboursement peut être retardé pour diverses raisons. Par exemple, la soumission du dossier non-valide ou une inscription trop tardive au formulaire de remboursement.

Direction Générale des Impôts

*Une **demande inhabituelle**, potentiellement associée à une demande **d'infos confidentielles**, avec un **caractère d'urgence**.*

Ne négligez pas les alertes de votre antivirus et/ou de votre antispam

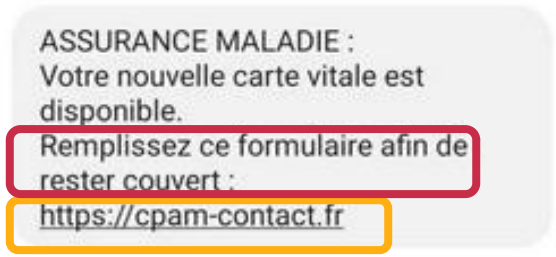
*Une incitation à **cliquer sur un lien** (positionner le curseur de sa souris sur le lien, sans cliquer pour vérifier l'URL) ou à télécharger une **pièce jointe**.*

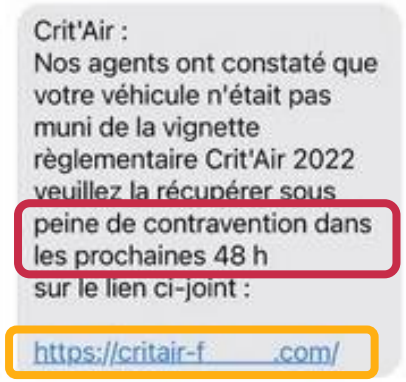
Groupement e-santé Pays de la Loire | RÉPUBLIQUE FRANÇAISE | ars Agence Régionale de Santé Pays de la Loire

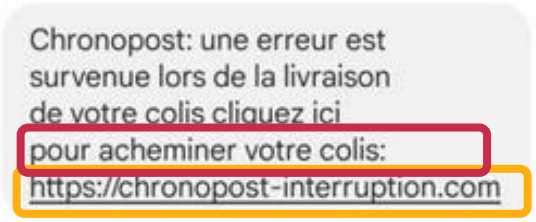
TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

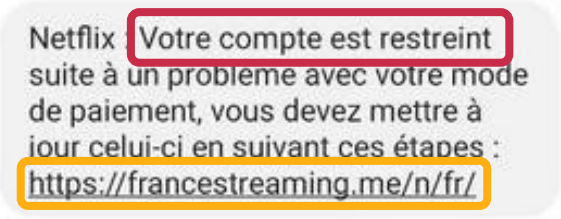
Smishing ou hameçonnage par téléphone

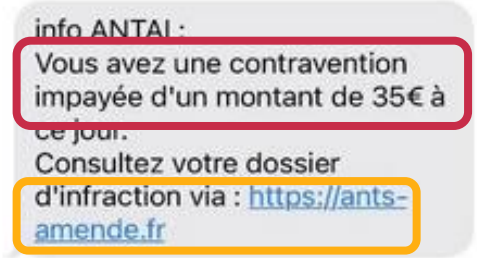
Un sms envoyé sur votre téléphone, souvent **alarmant**, vous **incitant à réaliser rapidement une action** telle qu'une connexion sur un lien, une confirmation, une mise à jour, un paiement, une mise à jour, …











Smishing ou hameçonnage par téléphone

Rappel des bonnes pratiques :

- Ne **jamais communiquer d'informations sensibles** à la suite d'un SMS ou message Whatsapp.
- **Vérifier l'information** du message **par vous-même** (contacter directement l'organisme, se rendre sur son espace personnel via le site Internet ou l'application mobile officielle).
- **Ne pas cliquer sur le lien**. En cas de doute, aller directement sur le site Internet de l'organisme par vos moyens habituels.

Signalement **: 33 700 ou https://www.33700.fr**

Logiciels et applications

Rappel des bonnes pratiques

- **Ne pas partager** d'informations à caractère personnel (nom, prénom, photo, …) via des **applications non maitrisées** (Ex : WhatsApp, IA générative, …).
- Ne pas télécharger ou installer de **logiciels, applications ou produits non maîtrisés** sur votre matériel professionnel (ordinateur, smartphone, …).
- Privilégier l'installation d'applications officielles via les **plateformes de téléchargement reconnues** (Play Store, Apple Store, …).
- Veiller **au respect de la sphère privée des patients** (photos, vidéos, infos, …).
- **Installer un antivirus** et s'assurer de sa bonne mise à jour.

Renforcer la sécurité de mon Système d'Information

Bonnes pratiques

- Utiliser des **terminaux / systèmes / logiciels** dont le **maintien en conditions de sécurité est garanti** et **appliquer les mises à jour de sécurité dès qu'elles vous sont proposées.**

- **Refuser** l'usage de **dispositifs amovibles** (clé USB, disque dur externe, carte SD, smartphone, gadget USB et même un simple câble…) non maitrisés.
  - *A minima, lancer systématiquement une analyse anti-virus avant toute utilisation.*

- Activer le **chiffrement** du / des **périphérique(s)** de stockage (aussi bien internes que externes).

- Assurer la **sécurité physique** de vos équipements :
  - *prise parafoudre pour l'alimentation électrique,*
  - *accès restreints et contrôlés aux ordinateurs / smartphones / supports de stockage, …*

Exemple

Usages et nomadisme

Rappel des bonnes pratiques

- **Eviter les usages pros / persos** : ne pas utiliser son matériel professionnel à des fins personnelles, et réciproquement.
- En déplacement, privilégier :
  - Le **partage de connexion 4G ou 5G** depuis son smartphone et éviter de se connecter sur des Wifi publics, non maitrisés.
  - L'utilisation d'un **filtre de confidentialité** (écran ordinateur, smartphone).
  - **Le chargement via prise électrique** pour vos smartphones, tablettes, …
    - *Eviter le rechargement de vos appareils mobiles sur des ports USB publics ou inconnus (hôtel, aéroport, transport en commun, train, …).*
    - *Utiliser un datablocker pour bloquer le passage des données (vers et depuis votre appareil) si rechargement via un port USB.*

Sauvegardes

Bonnes pratiques

- **Sauvegarder** régulièrement les données :
  - Chez éditeur ou prestataire spécialisé, certifié Hébergeur de Données de Santé (HDS).
  - 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*).

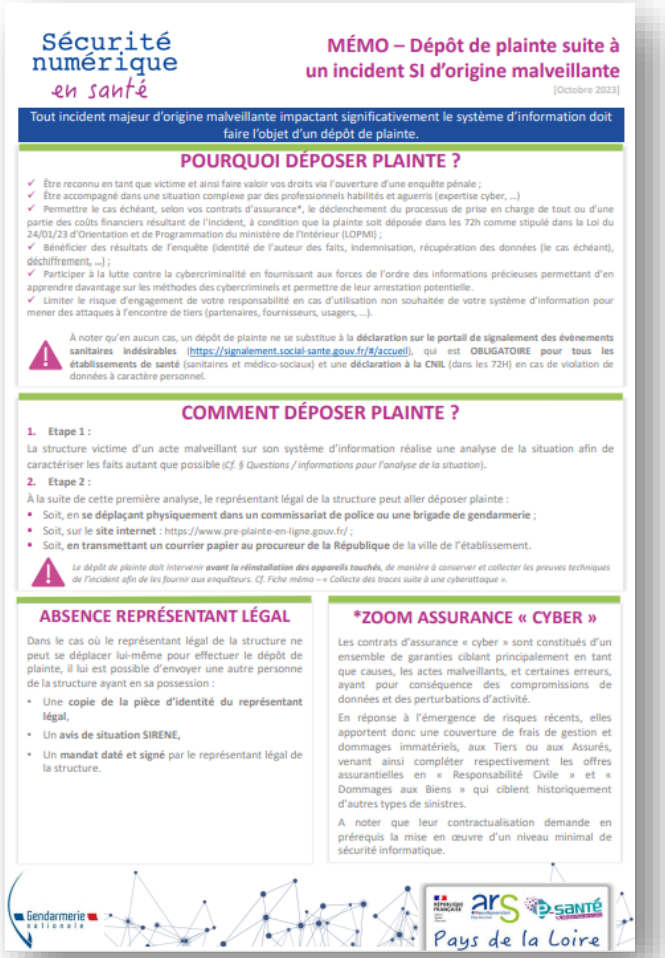
Exemples

Panique chez Google Drive : des fichiers supprimés soudainement, sans action de la part des utilisateurs !

Réagir en cas d'incident

Bonnes pratiques

- **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 fournisseur de service ou support informatique** pour obtenir une assistance.
- **Signaler** l'incident de sécurité :
    - **Contacter** le centre de réponse à incident cyber territorial : **Pays de la Loire Cyber Assistance,** Tel **: 0 800 100 200**, Service disponible **24h/24 et 7j/7**. (https://www.paysdelaloire.fr/economie-et-innovation/entreprise/mon-organisation-subit-une-cyberattaque).
    - **Décrire l'incident** de sécurité sur le site www.cybermalveillance.gouv.fr et suivre les conseils donnés.
- **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 — e-santé

Protection des données et RGPD

Bonnes pratiques

- Prendre en compte **les exigences du RGPD** et la **réglementation en vigueur** en termes d'information aux patients, tenue des registres, conservation des données, etc.
- Ne laisser accéder aux données / documents / informations que les **personnes habilitées** à en prendre connaissance.
- **Vérifier les contrats avec les prestataires** concernant le respect de la protection des données.
- **Informer les patients** de l'obligation du respect de la protection de vos données personnelles (voix, visage, …) lors des consultations.

Quelques exemples de sanctions de la CNIL en 2024

06/24	MEDECIN GENERALISTE (procédure simplifiée)	Non-respect du droit d'accès (dossier médical) Défaut de coopération avec la CNIL	Amende administrative de 4 000 euros
10/24	ORTHOPHONISTE (procédure simplifiée)	Absence de réponse à l'injonction et non conformité (procédure d'injonction)	Liquidation d'astreinte de 4 000 euros
10/24	CHIRURGIEN DENTISTE (procédure simplifiée)	Non respect du droit d'accès (dossier médical) Défaut de coopération avec la CNIL	Amende administrative 3 000 euros et injonction
12/24	STOMATOLOGUE (procédure simplifiée)	Non respect du droit d'accès (dossier médical) Défaut de coopération avec la CNIL	Amende administrative de 5 000 euros
12/24	MEDECIN GENERALISTE (procédure simplifiée)	Absence de réponse à l'injonction (procédure d'injonction)	Liquidation d'astreinte de 2 000 euros

Un non-respect du droit d'accès au dossier médical

Un professionnel de santé n'avait pas fait droit aux demandes de communication des données de santé qu'il avait reçues.

Les professionnels de santé doivent pourtant faire droit à ces demandes, en vertu de l'article 64 de la loi Informatique et Libertés. En effet, la non-communication du dossier médical **porte atteinte aux droits des personnes** et aux principes fondamentaux de la protection des données personnelles. Ce manquement est d'autant plus grave **qu'il concerne le suivi médical d'un enfant et peut nuire à sa prise en charge médicale**.

En conséquence, la CNIL a sanctionné d'une amende ce professionnel de santé.

COMPRENDRE LA CHAÎNE RÉPRESSIVE CNIL.

https://www.cnil.fr/sites/cnil/files/atoms/files/infographie_chaine-repressive_fr.pdf

Conseil National de l'Ordre des Médecins – Gestion du dossier patient : https://www.conseil-national.medecin.fr/medecin/exercice/dossier-patient

Pour aller plus loin

Sensibilisation à la sécurité numérique

Pour aller plus loin

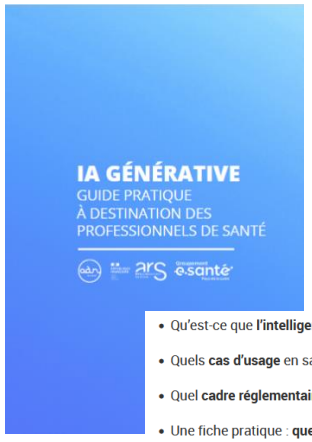
- Livret sur la cybersécurité « Tous cyber vigilants ! » de l'Inter URPS des Pays de la Loire :

https://www.urps-mk-paysdelaloire.fr/wp-content/uploads/2024/10/Brochure-CyberSecurite.pdf

- « Les bonnes pratiques de cybersécurité pour les médecins libéraux » par l'ANS et l'Ordre National des médecins :

https://www.urps-med-idf.org/wp-content/uploads/2024/07/Fiche-pratique-Cybersecurite-Medecins-VF-1.pdf

- Guide sur l'Intelligence Artificielle générative, issu d'une concertation entre l'ARS, ADN Ouest et le Groupement e-santé Pays de la Loire :



https://www.esante-paysdelaloire.fr/media-files/5217/ia-generative_guide-pratique_vf.pdf

- Qu'est-ce que **l'intelligence artificielle générative ?**
- Quels **cas d'usage** en santé ?
- Quel **cadre réglementaire** ?
- Une fiche pratique : **quelles questions se poser** avant d'utiliser un système d'IA générative ?
- Des **recommandations concrètes** : quelle IA pour quel usage ?
- Comment **se faire accompagner** ?
- Et pour aller plus loin : une **sélection de ressources utiles.**

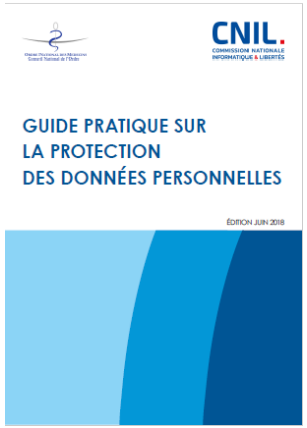
Sensibilisation à la sécurité numérique

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 **sécurité numérique 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

MERCI !!

Groupement e-santé Pays de la Loire

5 boulevard Vincent Gâche, 44200 Nantes

Avec le soutien de :