Sécurité numérique en santé

Financé par l'Union européenne NextGenerationEU

Sécurité numérique en Santé

SÉCURITÉ DES DONNÉES : TOUS CONCERNÉS, TOUS MOBILISÉS

Actualités cyber et accompagnement régional

RÉPUBLIQUE FRANÇAISE

Agence Régionale de Santé Pays de la Loire

GRADeS Pays de la Loire

Pays de la Loire

Actualités cyber-tourmentées

Yvelines : le Centre hospitalier de Versailles en difficulté après une cyberattaque

Publié le 06/12/2022 10:34

https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/yvelines-le-centre-hospitalier-de-versailles-en-difficulte-apres-une-cyberattaque_5526741.html

Cible d'une cyberattaque depuis le 3 décembre, le Centre hospitalier de Versailles (Yvelines) tourne au ralenti et doit s'adapter à des conditions difficiles.

Bien que des rendez-vous soient maintenus, l'activité de l'hôpital Mignot est toujours en difficulté, deux jours après la cyberattaque survenue samedi 3 décembre. Ainsi, l'établissement a choisi de privilégier les urgences aux consultations programmées. *"Le docteur m'a reçue, mais le seul problème, c'est que je n'ai pas les résultats écrits parce que la secrétaire n'a plus rien pour les faire"*, témoigne une patiente.

Du personnel appelé en renfort

Pour continuer son activité, l'hôpital a dû revoir son organisation. Ainsi, du personnel a été appelé en renfort, mais travailler sans informatique n'est pas facile pour les employés. *"C'est un manque pour des éléments de communication. C'est un manque pour des éléments de traçabilité sur les dossiers"*, constate le docteur Pierre Raynal. Les services les plus impactés sont la maternité et les urgences. Les perturbations devraient durer encore plusieurs semaines.

Actualités cyber-tourmentées

Essonne. Centre hospitalier visé par une cyberattaque: une rançon de 10 millions de dollars demandée

L'hôpital de Corbeil-Essonnes a été attaqué par un rançongiciel, dans la nuit de samedi 20 à dimanche 21 août 2022. Un plan blanc a été déclaré pour éviter que les patients n'en pâtissent.

Ouest-France
avec AFP
Modifié le 22/08/2022 à 17h24
Publié le 22/08/2022 à 11h14

Abonnez-vous

ÉCOUTER
LIRE PLUS TARD
PARTAGER
NEWSLETTER CORONAVIRUS

Le Centre Hospitalier Sud Francilien (CHSF), hôpital situé à Corbeil-Essonnes, en septembre 2011. | JOEL SAGET / AFP

Le Centre hospitalier Sud Francilien (CHSF) à Corbeil-Essonnes, au sud-est de Paris, est victime d'une attaque informatique depuis la nuit de samedi 20 à dimanche 21 août 2022 vers 1 h, perturbant fortement ses services et la prise en charge des urgences, possiblement pour des semaines, selon sa direction.

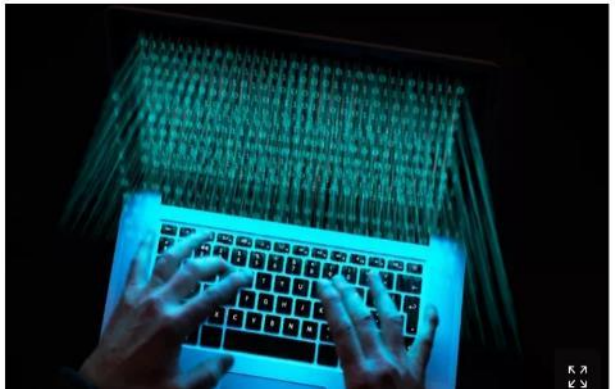
Cyber-attaque au Centre Hospitalier Sud Francilien (CHSF) : l'ARS Île-de-France coordonne la continuité des prises en charge des patients et active une cellule de crise

26 août 2022

L'ARS Île-de-France a été alertée par le Centre Hospitalier Sud Francilien (CHSF) d'une cyberattaque sur leur réseau informatique qui s'est produite dans la nuit de samedi à dimanche. L'Agence est mobilisée pour venir en appui sur les mesures de gestion et

Un Ehpad victime d'une cyberattaque dans l'Eure

Par Le Figaro avec AFP
Publié le 24/08/2022 à 16:50, mis à jour le 24/08/2022 à 16:57



La prise en charge des patients n'est pas impactée mais des procédures dégradées ont été mises en place.

L'Ehpad de Beuzeville (Eure) a été victime d'une cyberattaque mercredi, a-t-on appris auprès du groupe hospitalier du Havre, hôpital support de l'établissement pour personnes âgées, qui assure que la prise en charge des patients n'était «*pas impactée*».

Le plan blanc déclenché

Le réseau informatique des autres établissements du groupe hospitalier a été isolé et le processus de retour à la normale est en cours, selon l'hôpital. La direction, qui n'avait pas reçu de «*demande de rançon formelle*», a annoncé qu'elle déposera plainte.

Actualités cyber-tourmentées

Angers. La Clinique de l'Anjou victime à son tour d'une cyberattaque

Après la ville d'Angers, l'établissement de santé est lui aussi l'objet d'une attaque qui paralyse ses serveurs informatiques. La direction assure que cela n'a aucune conséquence pour les patients.

L'attaque s'est produite à 4 heures du matin ce samedi, affectant progre… ordinateurs de l'établissement jusqu'à ce que les serveurs soient coupés. | LAURENT COMBET

- Retour à un fonctionnement papier
- Résumés de passage aux urgences non transmis pendant plusieurs mois
- Disponibilité des lits de soins critiques non remontée
- Gestions des stocks de médicaments « à l'aveugle »
- …

NEUCHÂTEL

Un des cabinets médicaux piratés s'explique

Publié 5 avril 2022, 19:28

Selon un communiqué diffusé mardi, les données de plus de 20'000 patients auraient été soustraites. Impossible, donc, de tout analyser et de pouvoir contacter individuellement chaque personne potentiellement concernée.

Oui, ils ont été victimes d'une cyberattaque. Non, ils n'ont pas fait preuve d'imprudence, ayant encore récemment renforcé les protocoles de sécurité informatique. Et non, ils ne payeront pas de rançon, se conformant ainsi aux recommandations des autorités et des spécialistes de cybersécurité. C'est ainsi qu'on peut résumer le communiqué publié mardi par les médecins réunis au sein d'un cabinet de La Chaux-de-Fonds visé au mois dernier par des pirates informatiques. Ceux-ci ont tenu à expliquer le déroulé des faits et à alerter le plus largement possible leurs patients, ainsi que ceux des médecins ayant travaillé auparavant dans ce cabinet. Ils ont aussi tenu à présenter leurs excuses aux patients.

Les hackers ont **déjà publié les données volées** à ce cabinet et à un autre du canton sur le darknet, avant de les retirer en donnant un nouvel ultimatum à leurs victimes pour payer la rançon. Une manoeuvre déjà répétée deux fois depuis fin mars, la prochaine échéance étant fixée à ce jeudi. Les médecins chaux-de-fonniers semblent toutefois déterminés à ne rien verser aux pirates: «Suivant le conseil des autorités, nous avons choisi de ne pas payer de rançon. Premièrement, il n'y a aucune garantie que cela aurait influencé le comportement des pirates informatiques et que les données ne seraient pas publiées, à un moment ou à un autre. Deuxièmement, le cabinet ne souhaitait pas financer le crime organisé et encourager ces actes de chantage», écrivent-ils dans leur communiqué.

Parfois les prestataires en cause…

Au tribunal de Montpellier : le technicien licencié se venge sur des IRM

Trois machines touchées par ce mauvais geste. / ILLUSTRATION MIKAEL ANISSET

En 2013, le quinquagénaire, technicien en maintenance, avait modifié des données informatiques. Sans réelles conséquences.

C'est parce qu'il ne s'est pas senti soutenu par son supérieur au moment de son licenciement que cet ex-salarié de Philips France a décidé de se venger. En janvier 2013, il s'introduit dans le système informatique de la société et modifie ainsi certaines des données informatiques de trois appareils d'imagerie par résonance magnétique (IRM), qui étaient alors en fonction au sein d'établissements hospitaliers.

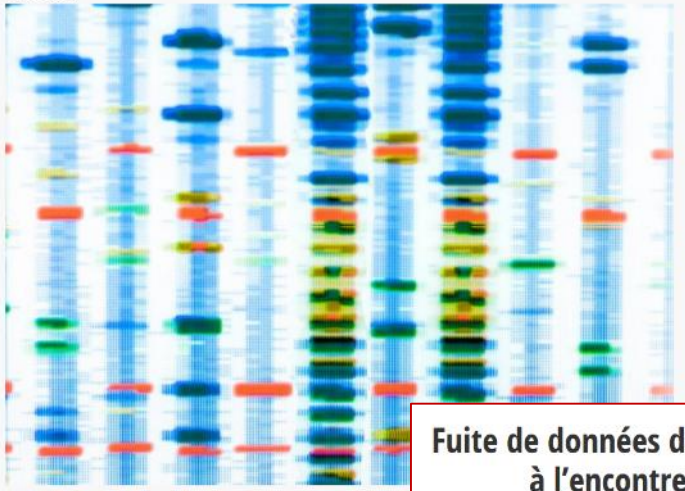
De quoi justifier ces six mois d'embastillement, assortis d'un sursis simple et de 2 500 € d'amende à l'encontre d'un homme sans passif judiciaire. Et qui, actuellement, travaillerait dans le même domaine à Dzaoudzi (Mayotte). Un délibéré plus tard, les magistrats l'ont condamné à la peine d'emprisonnement réclamée. Mais aussi à 3 000 € de dommages et intérêts.

Les informations confidentielles de 500 000 patients français dérobées à des laboratoires et diffusées en ligne

Article réservé aux abonnés

Selon les spécialistes, la fuite est d'une ampleur inédite en France pour des données ayant trait à la santé. Le fichier en question, que «CheckNews» a pu consulter, contient l'identité complète de près d'un demi-million de Français, souvent accompagnée de données critiques, comme des informations sur leur état de santé ou même leur mot de passe. Initialement partagée sur des forums de pirates informatiques, cette base de données est de plus en plus largement diffusée.

Développer



(Tek Images/Getty Images/Science Photo Library RF)

par Fabien Leboucq, Florian Gouthière, Vincent Coquaz et Alexandre Horn
publié le 23 février 2021 à 16h15

Le fichier comporte 491 840 lignes. Pour presque autant de patien
informations différentes sur une même personne : numéro de Séc
sanguin, adresse, numéro de téléphone portable, médecin prescri
parfois l'état de santé. «*Grossesse*» revient souvent. Dans certains
des pathologies sont précisés : «*Levothyrox*», «*tumeur au cerveau*

Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE

21 avril 2022

Le 15 avril 2022, la formation restreinte de la CNIL a sanctionné la société DEDALUS BIOLOGIE d'une amende de 1,5 million d'euros, notamment pour des défauts de sécurité ayant conduit à la fuite de données médicales de près de 500 000 personnes.

Parfois les professionnels…

Un médecin pirate les ordinateurs de ses confrères : 4 mois de prison avec sursis

Par F. Na le 11-04-2018

Un médecin du CHU de Nice a été condamné par la Cour de cassation à quatre mois de prison avec sursis pour avoir installé un logiciel espion sur les ordinateurs de deux autres praticiens hospitaliers. Les faits remontent à l'automne 2013. Le service informatique du CHU de Nice découvre qu'un logiciel espion a été installé sur les ordinateurs de deux praticiens hospitaliers titulaires . Le programme permet d'espionner la frappe du clavier et de capter des données. Rapidement l'enquête s'oriente vers un médecin contractuel, en conflit avec sa hiérarchie, et...

Violations de données de santé : la CNIL sanctionne deux médecins

17 décembre 2020

Le 7 décembre 2020, la formation restreinte de la CNIL a prononcé deux amendes de 3 000 € et 6 000 € à l'encontre de deux médecins libéraux pour avoir insuffisamment protégé les données personnelles de leurs patients et ne pas avoir notifié une violation de données à la CNIL.

Une pédiatre de l'AP-HM condamnée pour traitement illicite de données de santé

#DMP #Données #Sécurité #DossierPatient

18/09/2017 1045

MARSEILLE, 18 septembre 2017 (TICsanté) - Une pédiatre de l'Assistance publique-hôpitaux de Marseille (AP-HM) a été condamnée en juin dernier à 5.000 euros d'amende par le tribunal de grande instance (TGI) pour avoir mis en oeuvre un traitement de données à caractère personnel sans autorisation de la Commission nationale informatique et libertés (Cnil), a relayé le 12 septembre le site d'information Legalis.

Le jugement a fait suite au dépôt d'une plainte pour violation du secret professionnel à l'encontre de l'hôpital Nord de Marseille en 2013, par une femme ayant accouché 5 ans auparavant dans l'établissement.

En tapant son nom sur le moteur de recherche Google, la patiente avait eu accès au dossier de naissance de son fils comprenant des informations sur l'état de santé du bébé, des observations médicales, ainsi que son numéro de sécurité sociale et d'autres dossiers médicaux.

Sécurité des systèmes d'information

Qualité et continuité des soins

Disponibilité

L'information doit être disponible à tout moment aux personnes qui ont accès à cette information.

Intégrité

L'information doit être précise, complète et ne doit ni être altérée, ni altérable. Les informations ne doivent pouvoir être modifiées que par les personnes autorisées.

Secret professionnel

Confidentialité

S'assurer que l'information est seulement accessible à ceux qui en ont l'autorisation.

Responsabilité

Preuve et le Contrôle

Assurer la non-répudiation c'est-à-dire l'impossibilité de nier avoir reçu ou émis un message (preuve) et le contrôle du bon déroulement d'une fonction c'est-à-dire l'auditabilité.

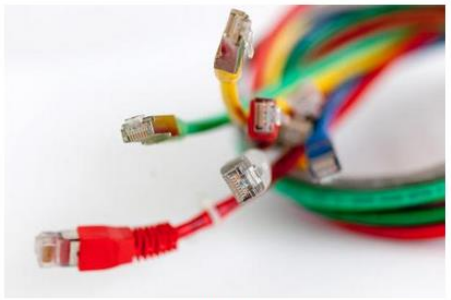
Adopter une bonne hygiène numérique

- **Assurer la sécurité physique de vos équipements :**
  - Alimentation électrique
  - Accès à vos équipements informatiques / numériques : ordinateurs, smartphones, supports de stockage...
  - N'acceptez pas de supports amovibles non maîtrisés (patients, prestataires…)

« On est comme sourd et aveugle », un médecin privé d'Internet raconte ses mésaventures

PAR STÉPHANE LONG - PUBLIÉ LE 01/07/2017

32 RÉACTIONS COMMENTER



internet
Crédit photo : PHANIE

Depuis le 10 juin, le Dr Bertrand Rose et ses deux confrères généralistes sont revenus quelques années en arrière, bien malgré eux. Installés à Blendecques (Pas-de-Calais), ils sont privés d'accès à Internet en raison d'une panne sur le réseau d'Orange, désorganisant totalement leur cabinet : plus de messagerie sécurisée, aucune télétransmission, pas d'accès aux informations médicales en ligne… Il a fallu revenir aux bonnes vieilles méthodes.

Impossible depuis près de trois semaines de se faire dépanner, malgré des démarches insistantes auprès de leur opérateur. Exaspérés, les médecins multiplient les appels à l'aide, auprès du Conseil de l'Ordre, de la mairie, de leurs relations professionnelles… Sans succès. Jusqu'à ce jeudi 29 juin. Il aura fallu une intervention du vice-président de la communauté d'agglomération auprès de la direction régionale d'Orange pour débloquer la situation.

- **Vérifier les contrats avec les fournisseurs d'accès internet : temps de rétablissement, prêt de matériel…**
- **Intégrer la sécurité dans les contrats avec les tiers (prestataires, fournisseurs…)**

Adopter une bonne hygiène numérique

- **Protéger l'accès à votre poste de travail et vos applications**
  - Gardez votre code PIN de CPS / e-CPS secret
  - Verrouillez votre poste lorsque vous vous absentez, même quelques minutes
  - Utilisez des mots de passe robustes et différents pour chaque service
  - Ne les enregistrez pas dans votre navigateur

Adopter une bonne hygiène numérique

- **Maîtriser les accès aux données :**
  - Disposer d'une charte informatique s'il y a plusieurs utilisateurs du système d'information
  - Utilisez une messagerie sécurisée de santé pour l'échange de données sensibles

Des médecins britanniques s'envoient les données de leurs patients sur Snapchat

Un étude sur le service de santé britannique, le NHS (National Health Service), dévoile que certains praticiens n'ont d'autres choix que de communiquer par Snapchat tellement les moyens de leurs services sont obsolètes. Mais l'utilisation de l'application qui permet d'envoyer des images, immédiatement effacées, soulève la question de la sécurité des données.

Par Arthur Laffargue
Rédigé le 06/07/2017

Saint-Brieuc. Le secret médical mis à mal à l'hôpital Yves-Le Foll

Un patient a été victime d'une violation délibérée du secret médical par une infirmière de l'hôpital de Saint-Brieuc. L'homme, âgé de 63 ans, demeurant à Lamballe, dénonce les failles du système d'information de l'établissement. Par l'intermédiaire de son avocat, il réclame une indemnisation.

Adopter une bonne hygiène numérique

- **Sauvegarder régulièrement les données :**
  - Chez un prestataire spécialisé et certifié pour l'hébergement de données de santé
  - Sur des supports amovibles chiffrés, isolés du réseau, stockés dans un rangement sécurisé, protégé des vols et sinistres

- **Disposer d'un antivirus à jour**

- **Être vigilant lors de l'ouverture d'un mail :**
  - Provenant d'un destinataire inconnu
  - Vous demandant des identifiants d'accès à des services sensibles

- **Appliquer les mises à jour dès qu'elles sont proposées**

Plan de renforcement cyber 2021

MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ
Liberté
Égalité
Fraternité

Le Directeur de cabinet

Paris, 30 JUIL. 2021

SHFDS-2021-40

NOTE

aux directeurs généraux des agences régionales de santé

Objet : Plan de renforcement 2021 de la cybersécurité des établissements de santé.

Réf. : Note ministre du 22 juillet 2019 relative au plan de renforcement de la cybersécurité des établissements de santé.
Instruction 2016-340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé.
Instruction 309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action sur la sécurité des systèmes d'information dans les structures de santé.

PJ. : Feuille de route cyber 2021 – 2022 des agences régionales de santé

Dans les derniers mois, le secteur de la santé a déploré une multiplicité de cyberattaques par rançongiciel, et d'incidents numériques provoquant la fuite de données personnelles de santé. Cette situation entraîne dans certains territoires une perturbation du fonctionnement des services médicaux, aggravé par le contexte de la crise sanitaire.

Comme l'a souligné le Président de la République dans la présentation de la stratégie nationale pour la cybersécurité le 18 février 2021, le niveau de menace cyber auquel notre pays est actuellement confronté nous impose une réaction supplémentaire à la hauteur des enjeux, sous peine d'assister à une désorganisation de notre système de santé.

J'ai évoqué avec vous le 2 juillet dernier les nouvelles mesures de renforcement de la stratégie ministérielle de cybersécurité en santé prises en 2021, avec le rôle clé confié aux ARS dans leur déclinaison territoriale. Il s'agit notamment de s'assurer que l'ensemble des responsables des structures de santé soit bien mobilisé pour faire face aux risques cyber, qui vont continuer à s'accroître.

En cohérence avec le Ségur de la santé et la feuille de route stratégique du numérique en santé de « Ma santé 2022 », le plan de renforcement 2021 de la cybersécurité est prioritairement orienté vers les établissements de santé, en étroite coordination avec l'ANSSI.

Pour autant, les actions de sensibilisation et d'accompagnement sur la cybersécurité s'adressent à l'ensemble des acteurs de santé et du médico-social, comme le montre la campagne nationale de communication sur la cybersécurité en santé « Tous cyber vigilants », lancée par le ministre des solidarités et de la santé le 9 juin dernier. Cette campagne de communication, qui va se dérouler sur toute l'année 2021, doit permettre de sensibiliser l'ensemble du secteur aux enjeux de sécurité numérique.

Dans le cadre de la gouvernance en matière de cybersécurité installée en mars 2021, la mise en œuvre effective des actions du plan de renforcement est suivie par le cabinet du ministre chargé de la santé, au travers du comité de pilotage cyber santé mensuel, dans lequel les ARS sont représentées.

.../...

14 AVENUE DUQUESNE – 75350 PARIS 07 SP
TÉLÉPHONE : 01 40 56 60 00

- **Suite aux annonces présidentielles du 18/02/21**

- **Sur la base de plusieurs constats :**
  - **Poursuites des cyberattaques** par rançongiciels avec des impacts potentiels graves sur la prise en charge des usagers
  - Nécessité de **renforcer la prise de conscience** de la menace qui pèse sur le secteur santé social (dont le risque systémique).
  - **Faible niveau de maturité** cyber de nombreux ES
  - **Sensibilisation des personnels** à renforcer
  - **Réponse à incident cyber à renforcer**

- **Des actions territoriales à conduire autour de 4 thématiques :**
  - Sensibilisation aux risques cyber
  - Animation territoriale
  - Appui des structures de santé
  - Contrôle

Sécurité numérique en santé

La Sécurité numérique en Pays de la Loire

Formations

- Référents sécurité des SI
- Animation d'un COPIL sécurité des SI
- Séminaire secteur médico-social
- Analyse de risques et homologation

Journées régionales

- A destination de tous les acteurs sanitaires, médico-sociaux et libéraux

Appui à la gestion des incidents

- Diffusion alertes
- Soutien en cas d'incident
- GT Entraide SSI

Veille technologique et réglementaire

- https://www.scoop.it/t/ssi-sante

Webinaires

- Exploiter la SSI au quotidien
- Sécuriser les sites et serveurs web

Base documentaire régionale

- Modèles de documents / mémos thématiques
- Fiches d'aide à la mise en œuvre (inst. 309 Plan d'action SSI)
- Formation/action à l'appropriation des docs

Préparation à la crise cyber

- Soutien à la réalisation d'exercices de crise cyber
- Soutien des ESMS à l'identification de mesures prioritaires
- Centre de ressources SSI accessibles aux structures médico-sociales les moins dotées

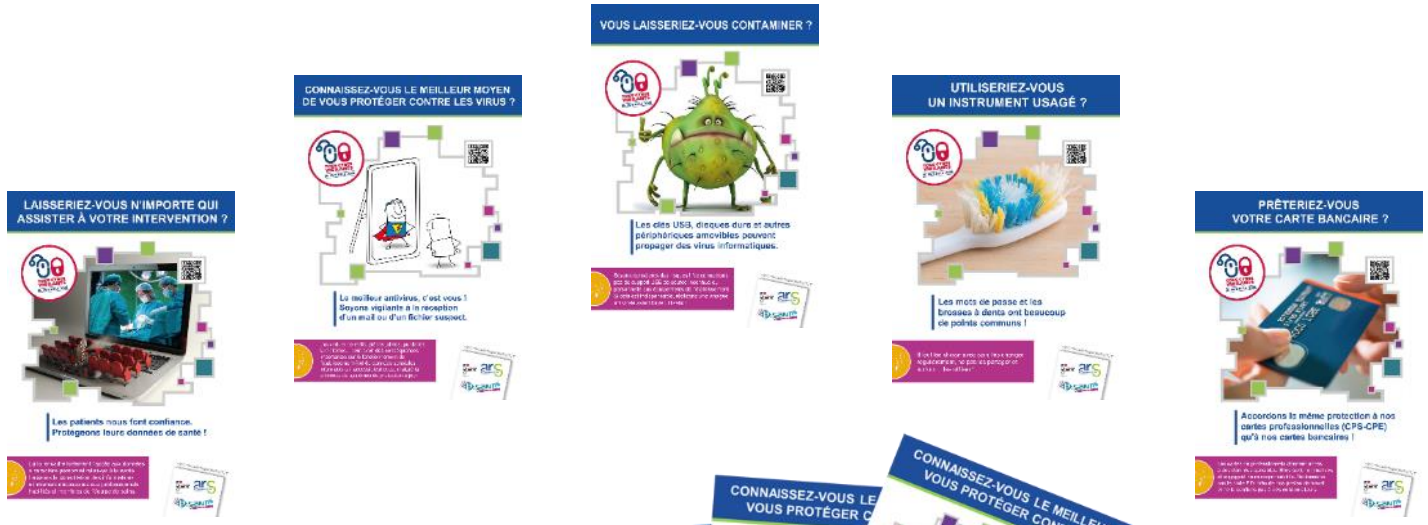
Outils de sensibilisation

- Affiches / fonds d'écran
- Escape game
- Badges / stickers
- e-learning
- Vidéos de sensibilisation
- Flyer de sensibilisation des entrepreneurs
- Cache webcam
- Datablockers
- Faux phishing

RÉPUBLIQUE FRANÇAISE
ARS Agence Régionale de Santé Pays de la Loire
e-SANTÉ GRADeS Pays de la Loire
Financé par l'Union européenne NextGenerationEU
SÉGUR NUMÉRIQUE
FRANCE RELANCE

Affiches de sensibilisation

- **16 affiches déclinées en cartes postales.**



- **Et en fonds d'écran**

https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-111.html

Vidéos de sensibilisation

- **Suite à une initiative de l'AP-HP, le GCS e-santé Pays de la Loire a acquis les droits d'usage sur des vidéos courtes (1min 30) pour ses adhérents pour une durée de 5 ans (juillet 2024).**

- **Ces outils viennent en support des sessions de sensibilisation organisées lors de sessions présentielles. Cinq thématiques sont abordées :**
  - Confidentialité du mot de passe
  - Usurpation d'identité
  - Secret professionnel
  - Divulgation d'informations
  - Fuites d'informations

- **Ces vidéos s'adressent directement aux utilisateurs du système d'information en détaillant les risques et en expliquant les sanctions possibles.**

Sécurité numérique en santé

Sant'escape – Sécurité numérique

LES TALENTS DE LA E-SANTÉ 2020

PRIX DE LA SÉCURITÉ

Le concept de l'escape game permet de reproduire des **situations réelles et crédibles** dans lesquelles les participants se reconnaitront. Les mises en situation procurées permettent une véritable **prise de conscience** et garantissent ainsi une très bonne **appropriation** des messages

Une méthode de sensibilisation innovante, ludique qui implique les apprenants

Un scénario contextualisé au secteur de la santé pour une expérience immersive

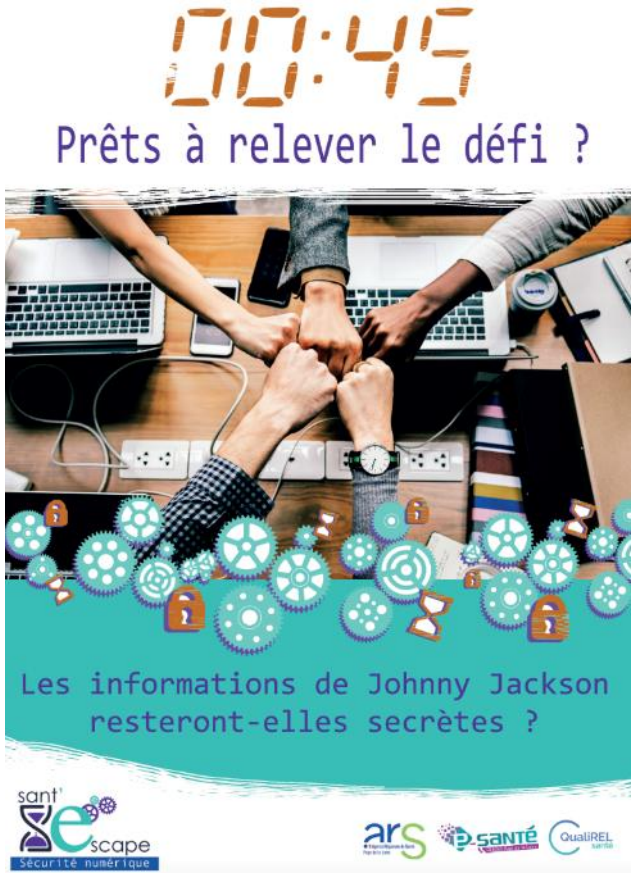
« Les participants à l'escape doivent se mettre dans la peau de personnages imaginaires : 5 journalistes peu scrupuleux d'un magazine People qui doivent décrocher un scoop sur l'état de santé d'une célébrité pour sauver leur journal de la faillite.

Le directeur de la rédaction a relevé dans la presse locale la mention de plusieurs incidents dans cette structure qui laissent à penser que les bonnes pratiques de base de sécurité numérique ne sont pas correctement appliquées. Ils demandent à ses journalistes de profiter de l'absence momentanée de trois professionnels d'exploiter leur non-respect de ces règles d'hygiène numérique pour récupérer les informations souhaitées.

Défi à relever en 45 minutes, pas une de plus ! »

Une durée de jeu de 45 min pour ne pas mobiliser les professionnels plus d'1h (briefing / débriefing inclus)

Sant'escape – Sécurité numérique



- **Une méthode de sensibilisation innovante, ludique qui implique les apprenants ;**
- **Ne nécessite aucune connaissance technique particulière, s'adresse à tous publics ;**
- **Des participants qui doivent se mettre dans la peau "des méchants" et exploiter les mauvaises pratiques ;**
- **Un scénario contextualisé au secteur santé ;**
- **Une durée de jeu de 45 min pour ne pas mobiliser les professionnels plus d'1h (briefing / débriefing inclus) ;**
- **Une formation et un kit de ressources permettant aux structures ligériennes d'être autonomes dans la mise en œuvre.**

Depuis sa création :

974 participants sensibilisés

(personnels SI, directeurs, infirmières coordinatrices d'EHPAD, qualiticiens / gestionnaires de risques, personnels administratifs et financiers…)

MERCI POUR VOTRE ATTENTION