



Sensibilisation cybersécurité - Guichet CPTS

08/01/2026

13/01/2026

Sommaire

01

L'écosystème de la cyber

Quelques chiffres

Les acteurs et ressources

02

Les risques et impacts

03

Les bonnes pratiques

Reconnaître un phishing

Sauvegarder ses données

Naviguer sur internet

Echange de données de santé

04

Gestion des incidents

Comment réagir

Qui contacter



01

L'écosystème de la cyber

Quelques chiffres

Etat de la situation en quelques faits

Des pirates siphonnent 6000 données de rendez-vous chez Doctolib

Ce vol ne concerne pas les dossiers médicaux mais met en relief la difficulté à protéger de précieuses données de santé.

Par Damien Licata Caruso
Le 23 juillet 2020 à 20h02

Une cyberattaque contre Weda, logiciel utilisé par des milliers de médecins, provoque paralysie du système et fuite de données

Dans toute la France, des cabinets de santé ont fonctionné au ralenti pendant plusieurs jours, sans avoir accès aux dossiers de leurs patients. Ces derniers figurent parmi les victimes potentielles de cette attaque informatique.



Données de médecins français vendues pour 1 000\$

Posted On 22 Fév 2021 By : Damien Bancal Comments: 16 Tag: blackmarket, centre hospitalier, piratage

Je vous racontais, il y a peu, comment j'avais pu mettre la main sur des données piratées liées à la santé de plus de 490 000 Français. Quelques jours plus tard, le CERT France, via le Ministère de la Santé, alertait sur une vente de 50 000 informations concernant des médecins Français. Je suis rentré en contact avec le pirate. Un sale type parmi des milliers d'autres.

Assurance Maladie : vol de données de 510 000 assurés (MAJ)

Jacques Cheminat, publié le 18 Mars 2022

Des pirates se sont connectés sur des comptes de soignants et ont dérobé des données de plus de 500 000 assurés. Il ne s'agit que de données administratives, tente de rassurer l'Assurance Maladie qui a communiqué sur cet incident.

Des accès non autorisés au portail Amelipro a permis aux pirates de dérober des données de 510 000 assurés. (Crédit Photo : Assurance Maladie)

[Aller à la page régionale](#)

Cybercriminalité : des cabinets médicaux de Gironde contraints de payer une rançon à des hackers

Publié le 19/04/2022 à 15h16 • Mis à jour le 19/04/2022 à 19h00
Écrit par [Cendrine Albo](#)

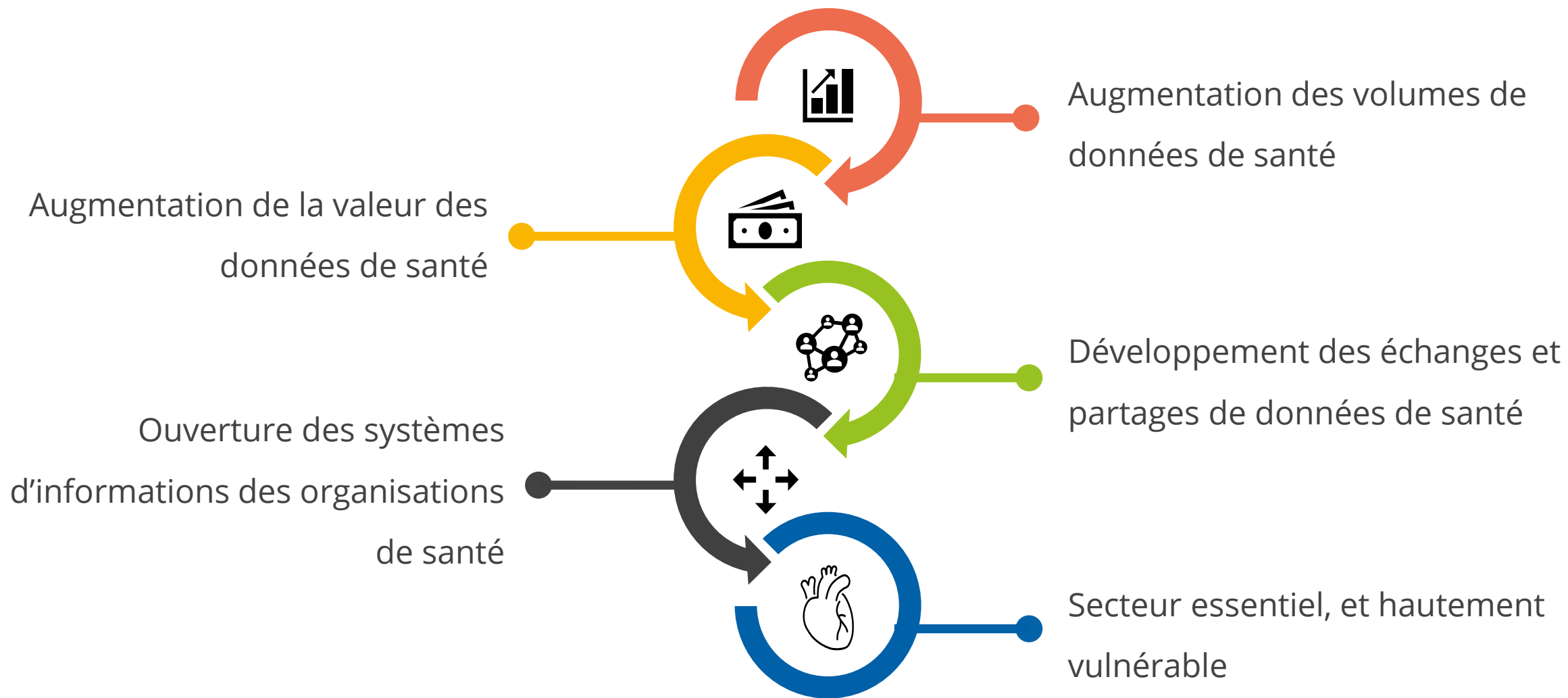
Deux pirates informatiques condamnés pour avoir attaqué l'ARS d'Ile-de-France

Le tribunal correctionnel de Paris a condamné vendredi 25 novembre 2022 deux hommes jugés pour avoir piraté le système informatique de l'Agence régionale de santé d'Ile-de-France en 2016.

L'auteur du piratage a été identifié comme Ali T., gérant de la société Ceps informatique ingenierie, ancien prestataire de l'ARS, chargée de la mise en place de solutions de sauvegarde au sein de l'agence. À la suite d'une décision de non-renouvellement du contrat entre l'agence et le prestataire, l'auteur du piratage a eu l'idée de "faire la panne" au sein de l'agence, a-t-il avoué lors de l'audience.



Pourquoi le monde de la santé est-il particulièrement ciblé ?



Menaces et attaques informatiques

Acteurs de la cybercriminalité

Nous classons les acteurs de la cybercriminalité selon leurs moyens et leurs motivations.

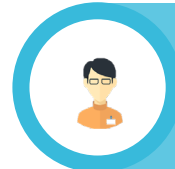
Parmi les types de cybercriminels:



Néophytes / Script kiddies



Hacktiviste



Interne



Etatique

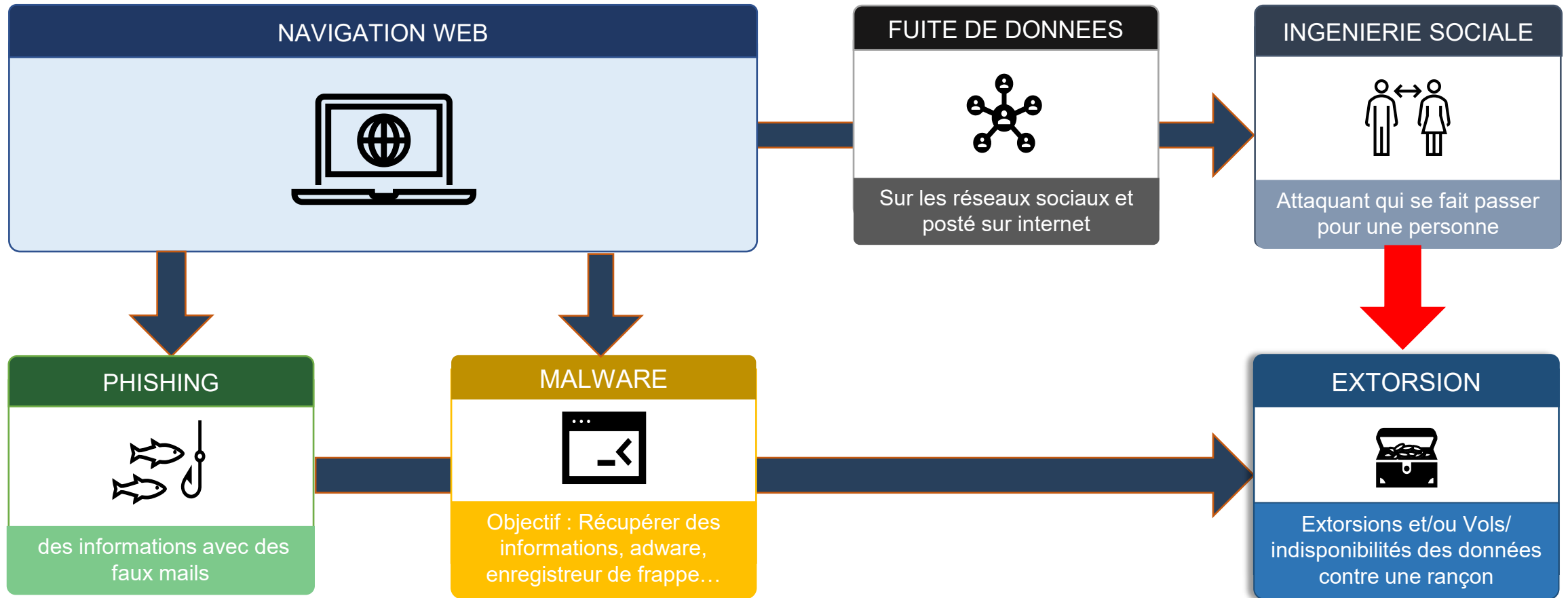


Crime Organisé

02

Les risques et impacts

Risques liés à nos usages



NOS USAGES PEUVENT AVOIR DE LOURDES CONSÉQUENCES

Combien de temps faut-il à un pirate pour trouver votre mot de passe 2025

12 x RTX 5090 | bcrypt (10)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					



Hive Systems

› hivesystems.com/password

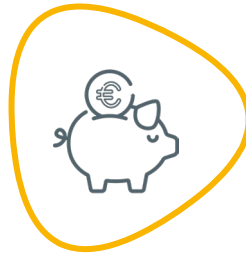
Cyberattaques : quelles raisons ?



Déstabiliser

JO de Paris 2024

*68 cyberattaques
déjouées*



Demander une rançon

Septembre 2022

*Le groupe Lockbit attaque
l'hôpital de Corbeil-Essonnes*



Revendre les données

Février 2024

*Les données de santé de 33
millions de français piratés*

Méthode la plus simple : **vous pousser à la faute !**

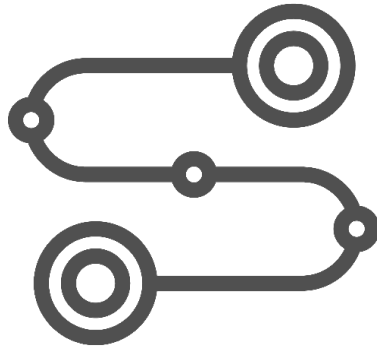
90% des cyberattaques commencent par du phishing

Cybersécurité : mythes et réalités

Ce que l'on imagine !



Ce que c'est aussi !



→ Nous sommes tous un **maillon** de la chaîne de sécurité numérique

Les impacts d'une cyberattaque

Image

- Patients / cabinet
- Partenaires et Professionnels de santé

Financier

- Risque financier
- Coût lié à la reprise d'activité

Visible dès le début de la crise

Invisible au début de la crise

Juridique

- Enquêtes et audits
- Amendes liées au RGPD / CNIL

Désorganisation

- Désorganisation de l'activité avec une indisponibilité des rendez vous, une absence d'accès aux bases de données,
- Perte d'informations médicales sur un patient avec impact possible sur la prise en charge,
- Possible modification d'informations médicales de patients,

Social

- Travail en mode dégradé
- Réorganisation du travail
- Surcharge



03

Les bonnes pratiques


Reconnaître un phishing


Sauvegarder ses données

Echange de données de santé







Question 1

Vrai ou Faux ? Ce mail est un phishing



Copieur Xerox RDC-02 <scan@support-si.net>
À  Nicolas PUYET

Scan_lono_Durand.pdf
841 KB

 Répondre Répondre à tous Transférer

lun. 09/09/2024 10:32

Vous ne recevez pas souvent de courriers de la part de scan@support-si.net. [Découvrez pourquoi cela est important](#)

URL d'origine :
<https://support-si.net/gwzlibtoel0x5vc97cnjqgkpgub6oup?signature=74243816ca3412b71ea009298cdfedf7217e8fb06017fa5c9c8e332800e362ad>
Cliquez ou appuyez pour suivre le lien.

Bonjour,

Le document numérisé depuis une imprimante réseau est disponible.
[Cliquez ici](#) pour voir le document.

Cordialement,
Le service informatique

** Printer scan data **
Printer: Xerox-Workcentre-RDC-02
Pages: 1
File format: pdf
Scan date: september 17, 2024
Recipient's email:


Ceci est un mail automatique. Merci de ne pas y répondre.

Vrai !


Question 2

Vrai !


Vrai ou Faux ? Ce mail est un phishing


 **Luke Johnson** <luke.json8000@gmail.com>
à moi ▼ 11:06


Luke Johnson a partagé un document


 Luke Johnson (luke.json8000@gmail.com) vous a invité à **modifier** le document suivant :

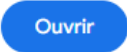
Bonjour, Voici le document demandé. N'hésitez pas à me contacter si vous avez besoin d'autre chose.

 Budget 2025 du service ☆



 Luke Johnson est le propriétaire

 Dernière modification de Luke Johnson il y a 1 heure

 <http://drive--google.com/d/6374pcjdsob833987cidkqwlsl9134>

Si vous ne souhaitez pas recevoir de fichiers de cet expéditeur, [bloquez-le](#) dans Drive

En passant la souris sur ce lien ou en appuyant de manière prolongée dessus, vous verrez qu'il ouvre le domaine non sécurisé "drive--google.com", qui n'appartient pas à Google.

Question 3

Vrai ou Faux ? Ce mail est un phishing



Dropbox <no-reply@dropboxmail.com>
à moi ▼

Une recherche rapide d'informations sur le site "dropboxmail.com" révèle qu'il s'agit d'une adresse légitime.

11:11



Faux !

Bonjour,

Votre Dropbox est pleine, et les fichiers n'y sont plus synchronisés. Les nouveaux fichiers ajoutés à votre dossier Dropbox ne seront pas accessibles sur vos autres appareils ni sauvegardés en ligne.

Mettez à niveau votre Dropbox aujourd'hui pour obtenir un espace de stockage de 1 To (1 000 Go) et bénéficier de puissantes fonctionnalités de partage.

Mettre à niveau votre Dropbox

<https://www.dropbox.com/buy>

Pour découvrir d'autres moyens

L'URL est un lien légitime et sécurisé vers "dropbox.com".

comment obtenir plus d'espace.

Profitez pleinement de votre Dropbox :

- L'équipe Dropbox

P.S. Si vous avez besoin d'encore plus d'espace, envisagez de souscrire un forfait [Dropbox for Business](#).

Question 4

Vrai ou Faux ? Ce mail est un phishing



Google <no-reply@google.support>
à moi ▼

L'adresse d'expédition "google.support"
n'est pas utilisée.

11:14

Vrai !

Une personne connaît votre mot de passe

Bonjour,

Une personne vient d'utiliser votre mot de passe pour tenter de se connecter à votre compte Google.

Information :

jeudi 25 septembre 2025 à 11:14:30 GMT+02:00
Slatina, Roumanie
Navigateur Firefox

Google a bloqué cette tentative de connexion. Vous devriez changer immédiatement de mot de passe

MODIFIER LE MOT DE PASSE

<http://myaccount.google.com-securitysettingpage.ml-security.org/signonoptions/>

Cordialement,

L'équipe de messagerie

Ce lien redirige vers un sous-domaine de
"ml-security.org", et non vers Google.

Recommandations

Toujours vérifier :

- L'adresse mail de l'expéditeur : interne ? Externe ? Connue ?
- Le lien de redirection : https ? Connu ?
- Le caractère du message : urgent ? Incitatif ? Alléchant ?

→ Je prends le temps d'analyser le mail et de faire des recherches

→ En cas de doute, je supprime le mail (contacter votre prestataire informatique en cas de doute)

→ Si je me suis fait piéger, je suis la procédure et je préviens mon prestataire informatique !

Vous souhaitez vous entraîner ?

Quizz sur le phishing



Sauvegardez vos données

La règle du 3-2-1

Opération qui consiste à dupliquer et mettre en sécurité les données contenues dans un système informatique. Cela permet de pouvoir augmenter les chances de reprise d'activité après incident.

La méthode



Identifier les données critiques à sauvegarder
Appliquer la règle du « 3-2-1 »
Chiffrer les données sensibles

L'outils



Hébergements Cloud, les outils cloud peuvent être pertinents, cependant il faut s'assurer que l'hébergeur soit certifié HDS

3 - EXEMPLAIRES DES DONNÉES SAUVEGARDÉES

Dans l'idéal, créer trois exemplaires de sauvegardes de vos données



2 - SUPPORTS DE SAUVEGARDE DIFFÉRENTS

Utiliser deux supports différents, ne pas tout stocker au même endroit.



1 - SUPPORT DÉCONNECTÉ DU RÉSEAU INTERNET

Stocker les données essentielles hors réseau, en cas d'incident elles ne seront pas affectées.



Limiter les accès aux données : *le bon accès pour la bonne personne*



Des accès personnalisés et sécurisés

Chaque utilisateur doit avoir **un identifiant unique** et des **droits adaptés**.

Authentification : MDP

Bloquez l'accès aux données avec des **MDP robustes** et **individuels**

Le principe du "besoin de savoir"

Seules les personnes qui ont **vraiment besoin** d'accéder aux données doivent y avoir accès.

Révoquer les accès inutiles

Dès qu'un collaborateur quitte l'équipe ou change de rôle, ses accès doivent être supprimés ou modifiés.



Stocker facilement mes MDP

Keepass est une solution souveraine gratuite, hébergée en France et répondant aux exigences de sécurité.

On ne vous demandera jamais vos identifiants

VOUS NE DONNERIEZ PAS VOS IDENTIFIANTS DE CARTE BLEUE ?



NE COMMUNIQUEZ PAS NON PLUS VOS IDENTIFIANTS E-CPS

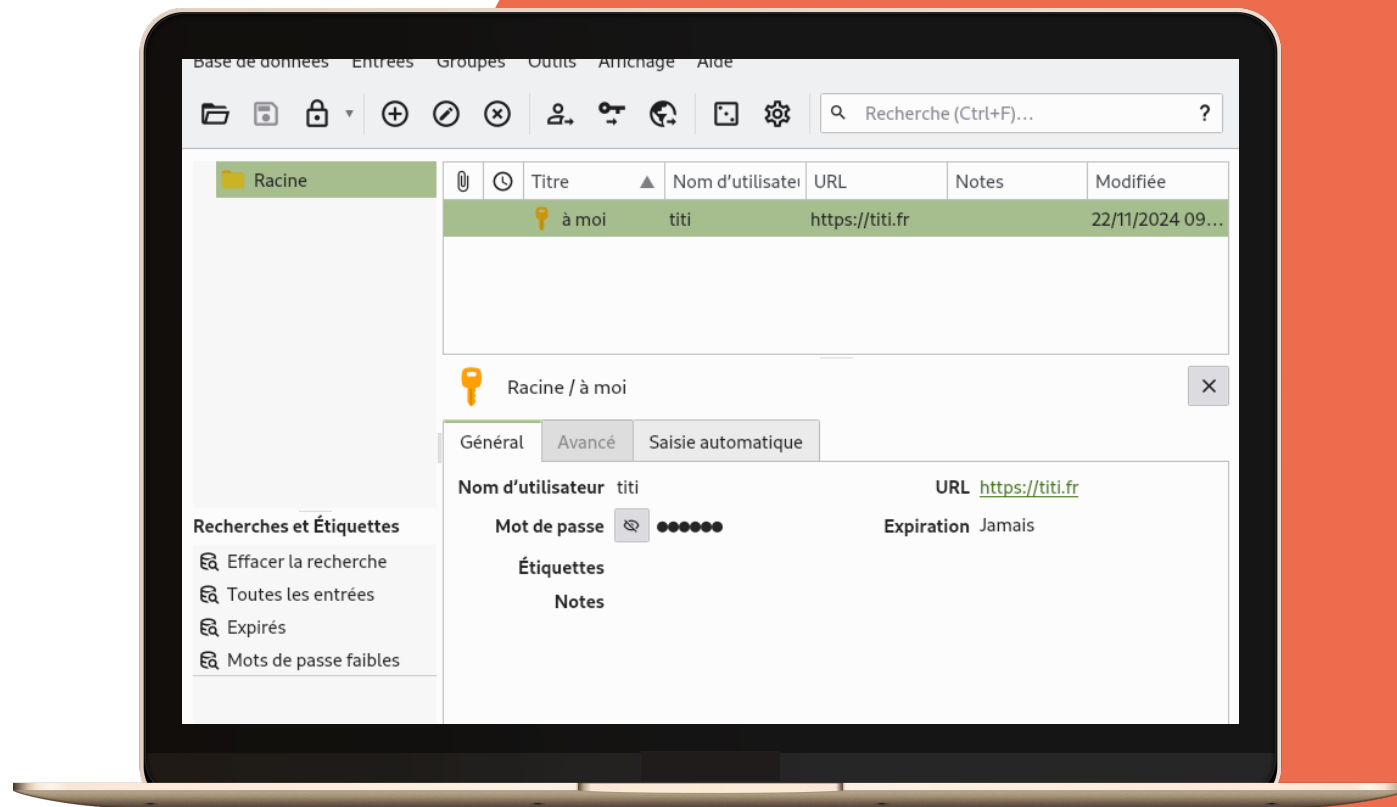


Ne transmettez pas de codes SMS

Ne partagez pas l'écran de votre ordinateur / smartphone



Démonstration Keepas



Echange de données de santé entre professionnels

Données de santé = données sensibles

La CNIL peut imposer des sanctions administratives ou pénales pour les échanges de données de santé non conformes.

UTILISATION D'APPLICATION SÉCURISÉES

De nombreuses applications existent pour échanger des données de manière sécurisées.

LE BON OUTIL POUR LA BONNE UTILISATION

- Le choix de la bonne application pour le bon usage, exemple :
 - je souhaite demander un avis à un confrère : outil de téléexpertise ?
 - Organiser la prise en charge autour d'un patient ? SPICO
 - Mise à disposition de documents médicaux : espace de partage sécurisé
 - Echanger avec un autre professionnel : MIS ?

CONFORMITÉ RÉGLEMENTAIRE

Une application utilisée pour l'échange de données de santé doit garantir

- un hébergement HDS
- Des règles conformes au RGPD
- Les données recueillies doivent être collectées pour des finalités déterminées, explicites et légitimes.

Ex : Le stockage des messages et des éléments échangés sur WhatsApp se fait sur des serveurs non médicaux et non agréés par l'Etat français



medimail 

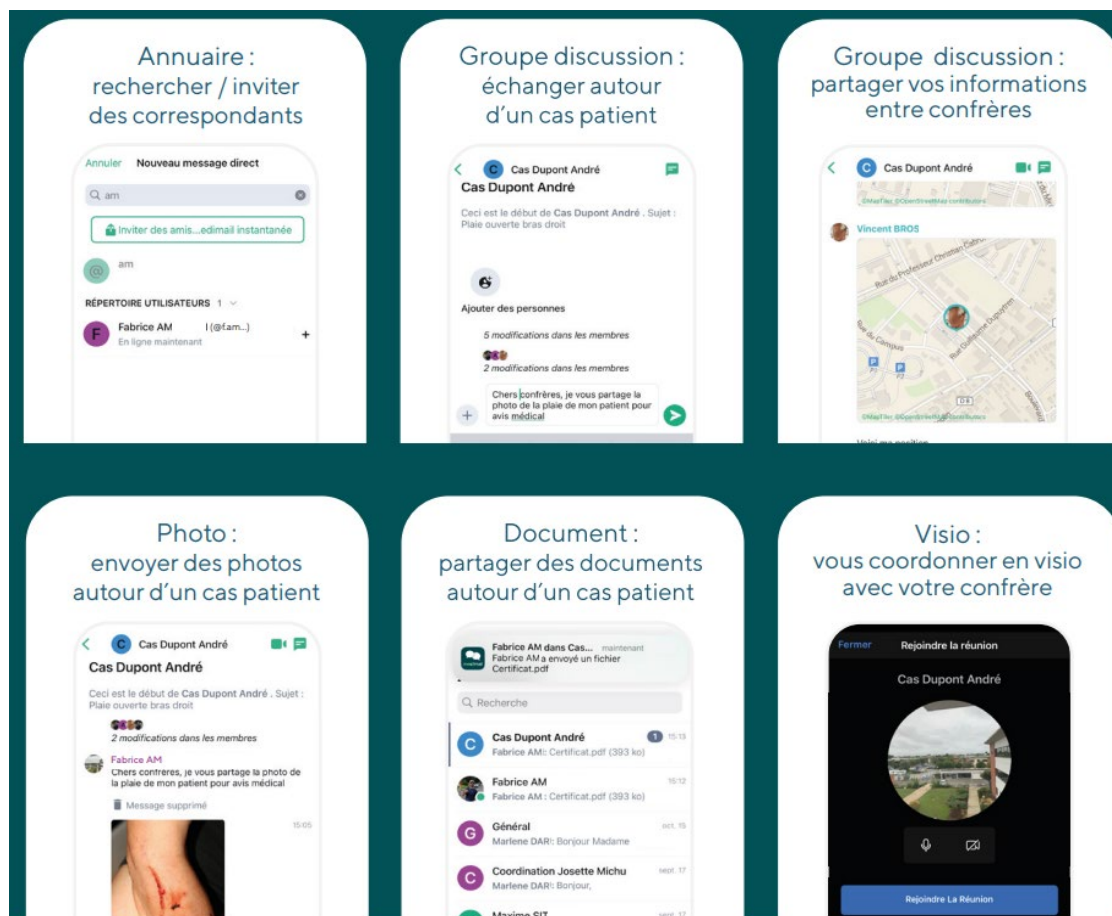
mon
ESPACE
SANTÉ



SPICO
Système de Partage d'Informations
et de Coordination en Occitanie



Les grandes fonctionnalités de Medimail Instantanée



04

Comment réagir en cas d'incident ?

Comment réagir en cas d'attaque ?



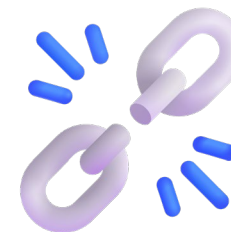
Je me suis fait piéger par un phishing

- J'ai cliqué sur un lien/ouvert un fichier frauduleux
- J'ai entré mes identifiants et mot de passe sur un site douteux



Mon ordinateur à un comportement étrange

Comportement inhabituel ou fortement ralenti
Extensions de fichiers changées, ou des fichiers ont disparu
Un message de rançon s'affiche



Je n'arrive plus à accéder à mes logiciels/Je suis constamment déconnecté

Tout le monde peut se faire piéger ! Il faut agir au plus vite !

Qu'est ce qu'il ne faut PAS faire en cas de cyber-attaque ?



Ne jamais communiquer avec les hackers (ni par mail, ni par téléphone).



Ne jamais leur verser d'argent en cas de rançongiciel

En effet, rien ne garantit que vous pourrez accéder de nouveau à vos données sensibles.

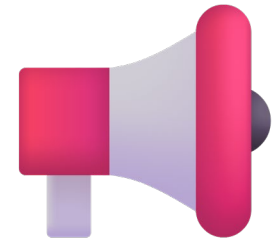
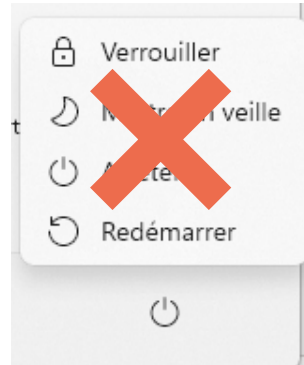
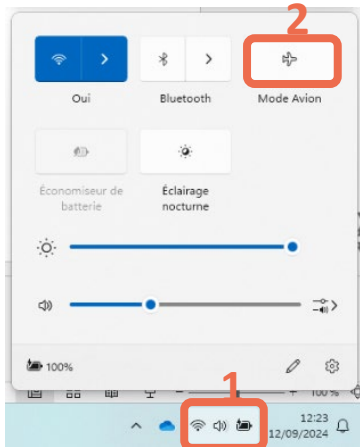
Que faire immédiatement en cas d'incident ?

1. Je déconnecte la machine du réseau

2. Je n'éteins pas l'appareil

3. J'alerte mon assistance informatique

4. Je n'utilise plus l'appareil et préviens mes collègues



Vers qui puis-je me tourner ?

L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

Chargée de proposer des règles en matière de protection des systèmes d'information de l'Etat. Elle assure également **un service de veille et de détection des attaques informatiques** et **conseille** les entreprises privées pour la sécurisation de leurs systèmes d'information

<https://www.ssi.gouv.fr/>



LA PLATEFORME NATIONALE D'ASSISTANCE AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

- Des **conseils** / vidéos en savoir plus sur **les bonnes pratiques et les risques**
- Des **services de proximité** en cas de dommages causés par une attaque informatique : <https://www.cybermalveillance.gouv.fr/>



Assistance et prévention en sécurité numérique

DÉPOSER PLAINTE

En cas de cyberattaque, il est **nécessaire de déposer plainte**, soit auprès des autorités compétentes (Gendarmerie Nationale, Police Nationale), soit en écrivant directement au Procureur de la République et **de tenir à disposition** des enquêteurs **tous les éléments de preuves techniques en votre possession**.



*En cas de cyberattaque avec violation de données à caractère personnel, **vous avez 72h pour faire une déclaration à la CNIL***

