



Financé par
l'Union européenne
NextGenerationEU

Renforcement de la cybersécurité dans les établissements sanitaires

LA SENSIBILISATION

Réunion ARS Ile-de-France / DCGDR / SESAN

Jeudi 21 avril 2022



**l'Assurance
Maladie**

Agir ensemble, protéger chacun



Ordre du jour



Informations pratiques sur le webinaire

3

Constat et contexte de la Cybersécurité en santé

4

La sensibilisation

12

Pour aller plus loin

22

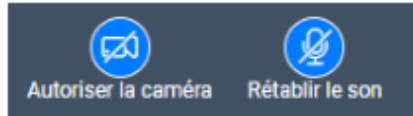


Informations pratiques

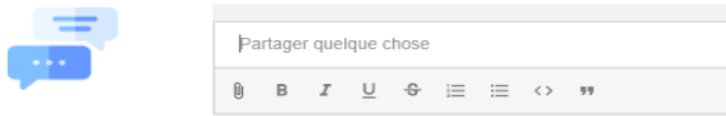
Bonnes pratiques de participation au webinaire



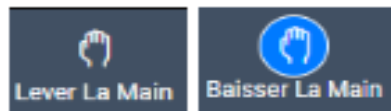
- Je (re)nomme mon nom d'utilisateur : « Etablissement – Nom Prénom »
- Je coupe mon micro et ma caméra quand je ne parle pas



- Les questions doivent être posées par écrit, j'utilise le chat en bas de l'écran pour rebondir, poser mes questions ou commenter. Une réponse concise/synthétique sera effectuée à l'oral. Si besoin un retour dédié sera fait par email ou par une prise de contact.



- Si vous souhaitez compléter oralement, levez la main et la parole vous sera donnée.



Mise en ligne de l'enregistrement vidéo de la session : suivez le lien fourni ultérieurement



Bienvenue !

Constat et contexte de la cybersécurité en santé



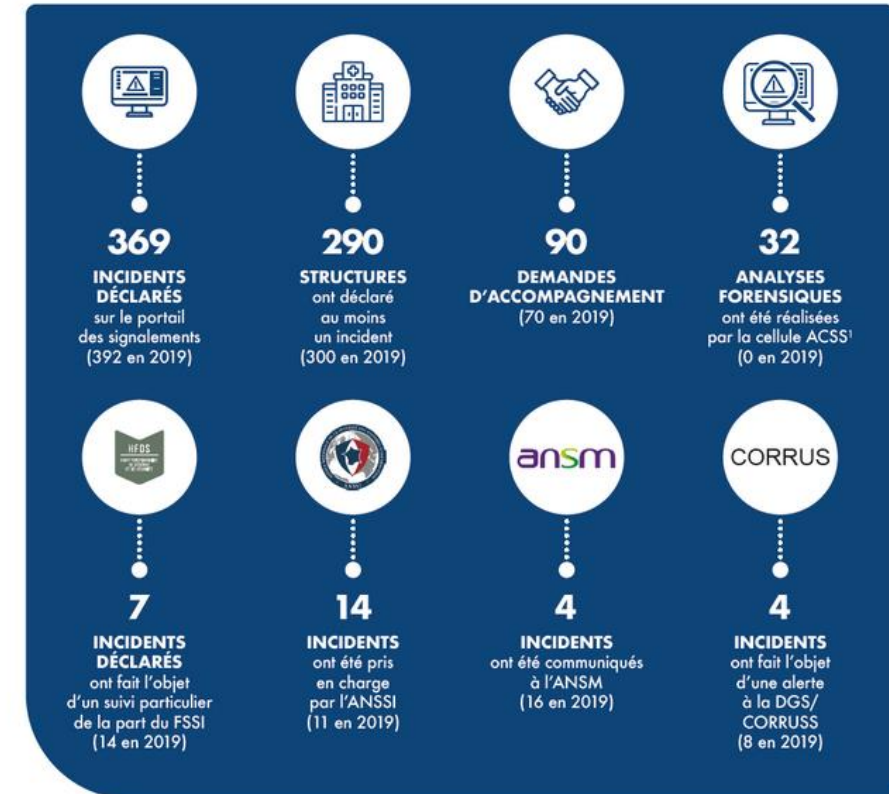


Constat et contexte de la cybersécurité en santé

Quelques chiffres – incidents 2021



- **Les déclarations d'incidents de sécurité informatique en hausse de 80%** sur la période de janvier à septembre 2021 pour les ES.
- **Le secteur médico-social a connu une hausse de 20%** sur la même période.
- **468 incidents déclarés** (contre 369 en 2020)



Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé - Rapport public 2020



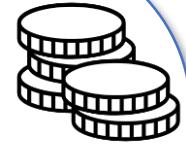
Constat et contexte de la cybersécurité en santé

Les menaces



- **La valeur des données de santé en constante augmentation**

- Les données agrégées servent dans de domaine la recherche médicale et de l'IA.
- Les données médicales individuelles peuvent faire l'objet de revente sur le darkweb.
- La sensibilité des données de santé (2020, chantage de patients finlandais avec leurs dossiers de psychothérapie).



- **Les établissements de santé ont un besoin important en disponibilité**

- Un fonctionnement permanent des conséquences potentielles sur le pronostic vital des personnes.
- Une opportunité intéressante pour les rançongiciels.



- **Le manque de ressources dans le domaine de la SSI**

- Peu de ressources allouées à la SSI dans les projets.
- Manque de profils qualifiés sur le marché de l'emploi.





Constat et contexte de la cybersécurité en santé

Contexte réglementaire



- **Programmes nationaux de HN à SUN-ES (Segur) – 2011 à 2022**
 - Prérequis de sécurité
- **Instruction 309, plan d'action SSI d'application immédiate – 2016**
- **Signalement obligatoire des incidents de sécurité – 2017**
 - Etablissements de santé
 - Hôpitaux des armées
 - Centre de radiothérapie
 - Etablissements sociaux et médico-sociaux – 2020
- **Nomination des Etablissements supports de GHT comme OSE – 2021**



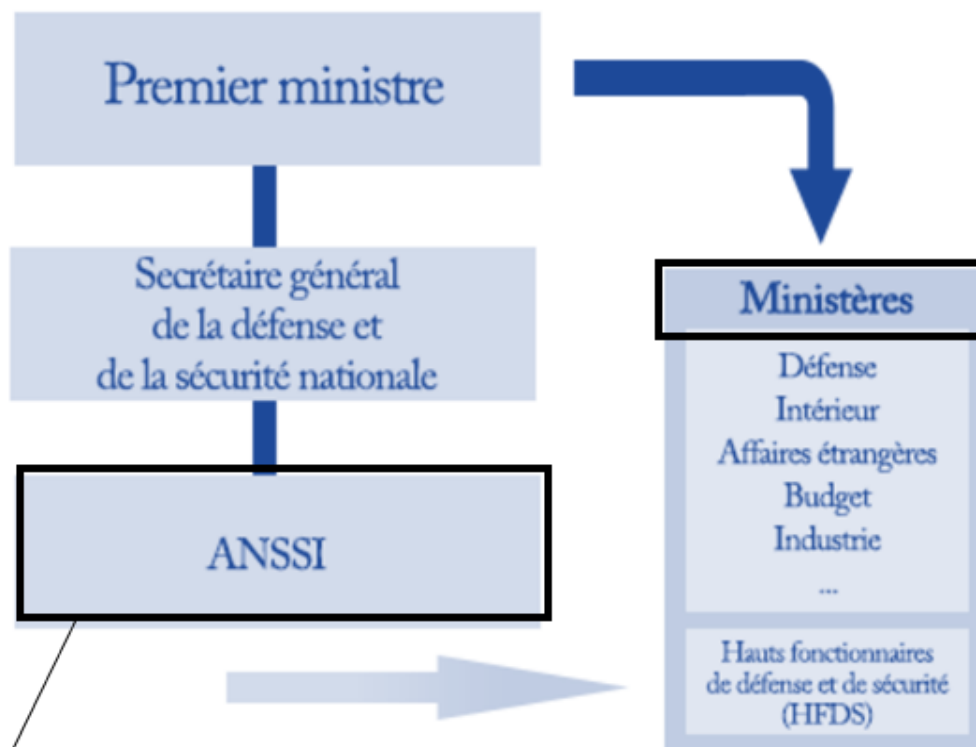
Constat et contexte de la cybersécurité en santé

Acteurs nationaux et régionaux



L'**ANSSI** s'est substituée à la direction centrale de la sécurité des systèmes d'information (DCSSI):

- contribue à l'orientation de la recherche nationale en matière de SSI
- Prévoit un accompagnement renforcé des OSE et des OIV



**MINISTÈRE
DES SOLIDARITÉS
ET DE LA SANTÉ**
*Liberté
Égalité
Fraternité*

Chaque ministre est responsable de la SSI
dans son domaine de compétence
→ Est assisté par un HFSD
→ Lui-même assisté par un FSSI

Le ministère de la santé compte une **délégation ministérielle** dans le numérique:
DNS assure:
- Le pilotage de la transformation du numérique en santé.
- Le pilotage resserré de l'**Agence du Numérique en Santé**.





Constat et contexte de la cybersécurité en santé

CERT Santé



- Pour accompagner, appuyer les structures de santé et du médico-social dans la gestion des actes de cybermalveillance

<https://esante.gouv.fr/produits-services/cert-sante>

POUR ACCOMPAGNER LE SECTEUR SANTÉ :

LE CERT SANTE

Le signalement des incidents de sécurité des systèmes d'information des structures de santé est obligatoire depuis le 1^{er} octobre 2017.



PORTAIL DE VEILLE, D'ALERTE ET D'ÉCHANGE :
www.cyberveille-sante.gouv.fr

CONTACTER LE CERT SANTÉ :
cyberveille@esante.gouv.fr
+33 (0)9 72 43 91 25

Permanence les jours ouvrés de l'ANS, 9h-18h

CONTACTER HFDS/FSSI :
ssi@sg.social.gouv.fr

CONTACTER L'ANSSI :
cert-fr.cossi@ssi.gouv.fr

Opération



Attention : Déclarer vos incidents sur <https://signalement.social.gouv.fr>
Allez dans la rubrique "Vous êtes un professionnel de santé"

CYBERSÉCURITÉ :
QUELQUES RÈGLES CLÉS À RESPECTER

ORGANISATION

- GOVERNANCE PAR LE MANAGEMENT DES RISQUES
- CARTOGRAPHIE DES RISQUES QUI PREND EN COMPTE LE RISQUE CYBER
- UN (E) RESPONSABLE EN CHARGE DE LA SÉCURITÉ DU NUMÉRIQUE (RSSI)
- UN (E) DÉLÉGUÉ (E) À LA PROTECTION DES DONNÉES PERSONNELLES
- PRISE EN COMPTE DE LA SSI DANS LES BUDGETS SI (≈10%)

SÉCURISATION

- PLAN D'ACTION CYBER MIS À JOUR EN CONTINU
- RÉALISER RÉGULIÈREMENT DES AUDITS DE SÉCURITÉ
- NÉCESSITÉ DE MAINTENIR DES SAUVEGARDES HORS RÉSEAU (CE QUI DIMINUE LARGEMENT LES IMPACTS D'UNE ATTAQUE PAR RANÇONGIERIE)

SENSIBILISATION

- FORMER AUX ENJEUX DE LA CYBERSÉCURITÉ ET AUX PRINCIPES D'HYGIÈNE NUMÉRIQUE
- RAPPELER LES RÈGLES D'USAGE EN MATIÈRE D'UTILISATION DE LA MESSAGERIE

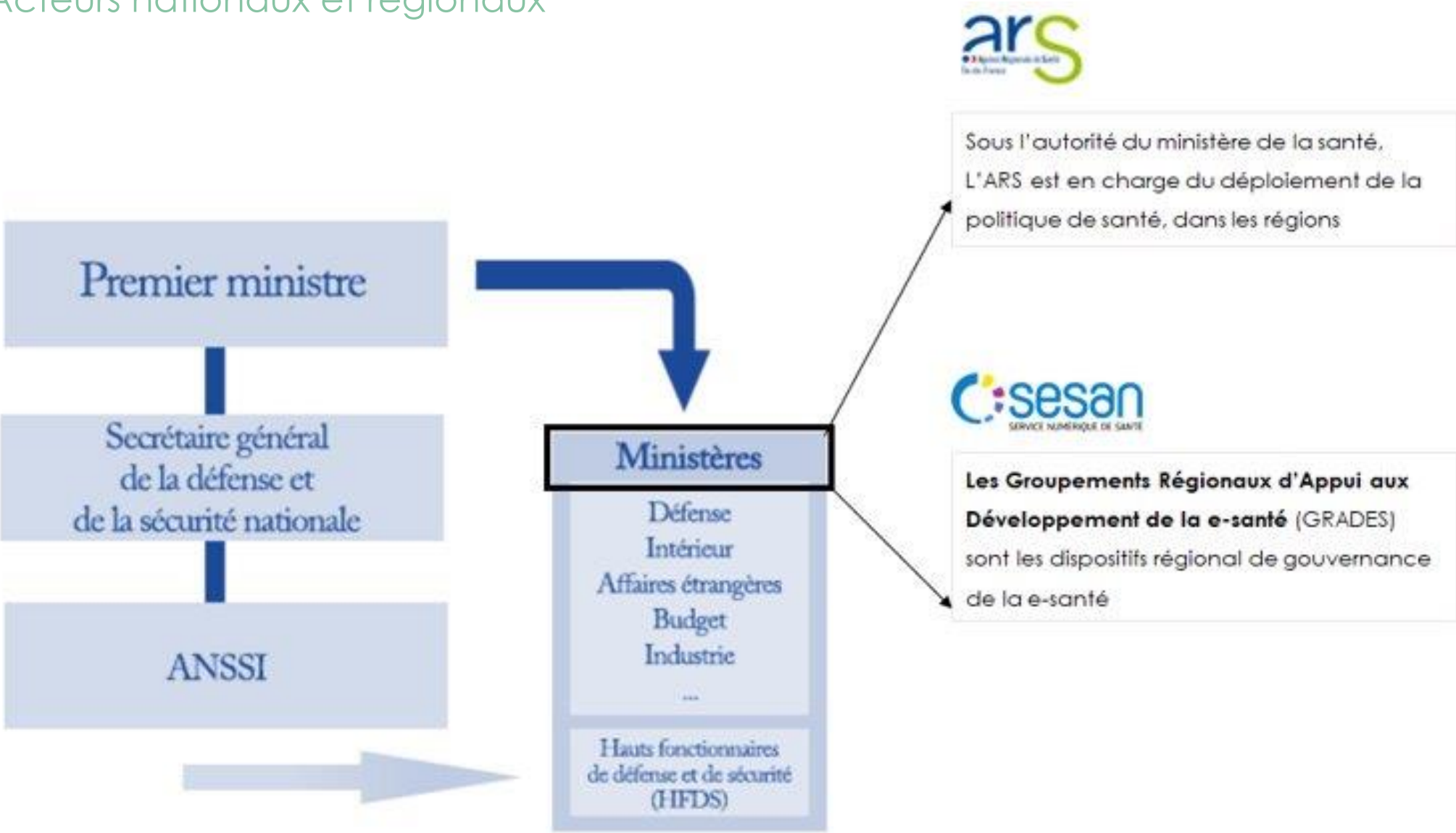
GESTION DES INCIDENTS

- DÉFINIR ET FAIRE CONNAÎTRE LA PROCÉDURE D'ALERTE ET DE RÉACTION EN CAS D'INCIDENT
- RÉALISER DES EXERCICES DE CONTINUITÉ D'ACTIVITÉ EN MODE "NUMÉRIQUE DÉGRADÉ"
- DÉCLARER TOUT INCIDENT SI SUR LE PORTAIL DE SIGNALEMENT DES ÉVÉNEMENTS SANITAIRES



Constat et contexte de la cybersécurité en santé

Acteurs nationaux et régionaux





Constat et contexte de la cybersécurité en santé

Acteurs de la SSI en établissement



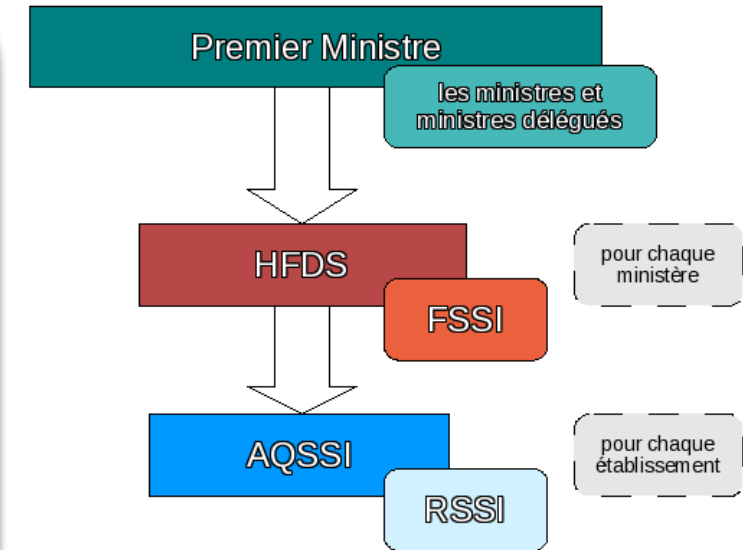
- **AQSSI - Autorité qualifiée pour la SSI**

- Assurer la responsabilité globale du niveau de sécurité requis
- Veiller à la mise en œuvre des dispositions réglementaires
- Procéder aux arbitrages

Attention : "Leur responsabilité ne peut pas se déléguer"

- **RSSI**

- Définit la politique du SI et veille à son application
- Chargé de la gestion et du suivi des moyens de sécurité des SI
- Procéder aux contrôles



La sensibilisation





La sensibilisation

Tous Cybervigilants



• Kit de communication tous Cybervigilants pour les établissements de santé

<https://esante.gouv.fr/sites/default/files/2022-01/kit-com-cybersecurite-etablissements-sante.zip>

- Affiche A4
- Bannière-Visuel Réseaux Sociaux
- Dossier d'information (Stratégie Nationale, Panorama des incidents, rôle du CERT Santé, Campagne d'information)
- Triptyque : La sécurité numérique, socle de la "Transformation du numérique en santé" (règles clés à respecter, ...)





La sensibilisation

CyberMalveillance



- Kit de sensibilisation
 - Fiches pratiques et réflexes,
 - mémos,
 - affiche A2,
 - BD,
 - vidéos, ...

10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1 Utilisez un mot de passe différent pour chaque service.

2 Utilisez un mot de passe suffisamment long et complexe.

3 Utilisez un mot de passe impossible à deviner.

4 Utilisez un gestionnaire de mots de passe.

5 Changez votre mot de passe au moindre soupçon.

6 Ne communiquez jamais votre mot de passe à un tiers.

7 N'utilisez pas vos mots de passe sur un ordinateur partagé.

8 Activez la double authentification lorsque c'est possible.

9 Changez les mots de passe par défaut des différents services auxquels vous accédez.

10 Choisissez un mot de passe particulièrement robuste pour votre messagerie.

ADOPTER LES BONNES PRATIQUES

LES RÉSEAUX SOCIAUX EN BD

FAITES ATTENTION À QUI VOUS PARLEZ

1. Connaissez-vous l'identité réelle de vos interlocuteurs ?

2. À leur lieu, même vos contacts peuvent vous partager des contenus malveillants.

3. Méfiez-vous de certaines offres alléchantes, qui peuvent cacher des arnaques.

PROTÉGEZ L'ACCÈS À VOS COMPTES

1. Pas besoin d'être dans l'océan pour protéger l'accès à vos comptes...

2. Un conseil : utilisez des mots de passe uniques, différents et robustes.

3. Lorsque votre service le permet, activez également la double authentification.

KIT DE SENSIBILISATION AUX RISQUES NUMÉRIQUES



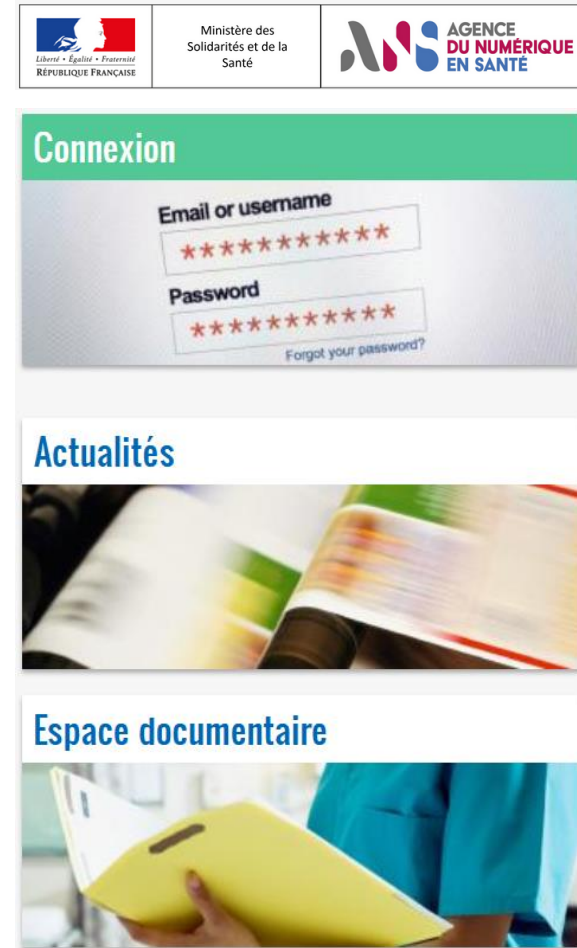
DISPOSITIF NATIONAL D'ASSISTANCE
AUX VICTIMES D'ACTES DE CYBERMALVEILLANCE

www.cybermalveillance.gouv.fr



Site relais de la communication du Cert-santé

- **Veille et alerte** sur les vulnérabilités et menaces critique ou relatif à la SSI santé
- Evènements et webinaire de l'ANS
- Espace documentaire
 - Guides de bonnes pratiques
 - Instructions ministérielles et PGSSIS





La sensibilisation

Newsletter



Utilisez la newsletter mensuelle de SESAN pour vos sensibilisations

<https://segurnumerique.sante-idf.fr/animation-regionale/cybersecurite/>



Veille réalisée auprès de sites institutionnels (ANS, CNIL, ANSSI...) et de sites spécialisés.



La sensibilisation

8 Affiches

CYBERSÉCURITÉ

Adoptez les bons réflexes

MOT DE PASSE

Plus votre mot de passe est compliqué,
plus il faudra du temps aux hackers pour le pirater.

4 chiffres	8 lettres majuscules & minuscules	10 lettres majuscules & minuscules + chiffres	14 lettres majuscules & minuscules + chiffres + caractères spéciaux
Piratage 1 seconde	Piratage 22 minutes	Piratage 7 mois	Piratage 200 000 000 années

Quelques recommandations

- Votre mot de passe doit être différent pour chaque compte
- Il doit être suffisamment long et complexe
- Ne le communiquez jamais à un tiers



CYBERSÉCURITÉ

Adoptez les bons réflexes

LE PHISHING/HAMEÇONNAGE

Venez récupérer votre cadeau, cette voiture de sport
est à vous ! Vous trouvez ça louche ? Vous avez raison !

Offert ! Gratuit !
0€

Quelques recommandations

En cas de doute :

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Contactez directement l'organisme concerné pour confirmer

Si vous avez été victime :

- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués / compromis
- Signalez-le sur les sites spécialisés (signal-spam.fr, cybermalveillance.gouv.fr)

TOUS CYBER VIGILANTS

sesan ars
SERVICE NUMÉRIQUE DE SANTÉ

CYBERSÉCURITÉ

Adoptez les bons réflexes

L'ARNAQUE AU PRÉSIDENT

Votre directeur vous fait une demande saugrenue?
N'agissez pas précipitamment.

Faites moi
IMMÉDIATEMENT
un virement de
100.000€ !!

Quelques recommandations

- Redoublez de vigilance pendant les périodes de congés
- vérifiez l'identité de l'interlocuteur via une source fiable
- recontactez votre directeur sur son numéro habituel

Si vous avez été victime de l'arnaque :

- Conservez toutes les preuves
- Signalez la fraude à votre structure

TOUS CYBER VIGILANTS

sesan ars
SERVICE NUMÉRIQUE DE SANTÉ



La sensibilisation

Organiser un exercice de Cybercrise



Exercice de Cybercrise – Sensibilisez les directeurs au risque Cyber

- Une démarche d'anticipation des risques Cyber et de prévention
- Un kit "Débutant" mis à disposition par  **AGENCE
DU NUMÉRIQUE
EN SANTÉ**
 - Kit actuellement testé par quelques établissements Pilote
 - Mise à disposition dans les prochains jours
- Objectif :
 - Prendre conscience de sa dépendance aux SI
 - Définir un plan d'action pour prendre en compte le risque Cyber dans son PCA



La sensibilisation

Organiser un exercice de Cybercrise

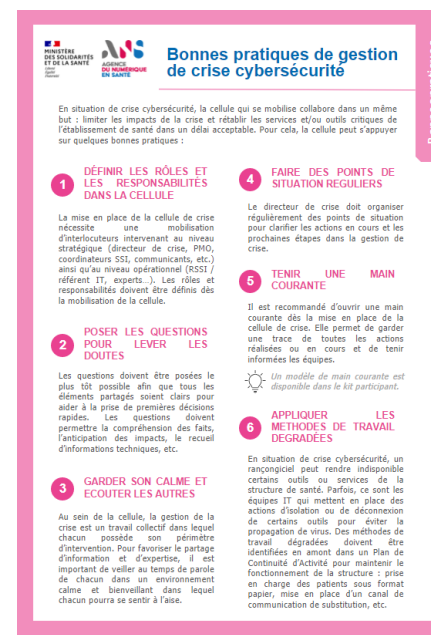
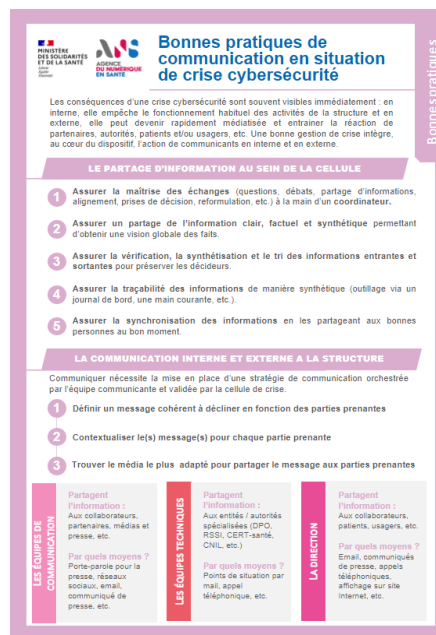


Contenu du Kit :

- **Livret Animateur** (bonnes pratiques d'animation, scénario, organisation de l'exercice, animation du briefing, animation de l'exercice, animation du débriefing, le rôle de l'observateur...)
- **Livret Participant** (règles du jeu, bonnes pratiques de communication en situation de crise, bonnes pratiques de gestion de crise Cyber, ...)



En toute autonomie





1/ Sensibilisez tout au long de l'année

2/ Alternez les modes de sensibilisation

- Affiche,
- Signature de mail,
- Flyer,
- Visuel réseaux sociaux,
- Présentation physique,
- Évènement majeur...



La sensibilisation

Conclusion



Synthèse des ressources disponibles

- Kit de sensibilisation "Tous Cybervigilants" : <https://esante.gouv.fr/sites/default/files/2022-01/kit-com-cybersecurite-etablissements-sante.zip>
- Kit de sensibilisation CyberMalveillance : <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation>
<https://www.cybermalveillance.gouv.fr/bonnes-pratiques>
- CyberveilleSanté : <https://cyberveille-sante.gouv.fr/>
- Newsletter SESAN : <https://securnumerique.sante-idf.fr/animation-regionale/cybersecurite/>
- Affiches SESAN : <https://securnumerique.sante-idf.fr/docutheque/>
- Autres liens utiles :
<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales>
<https://www.ssi.gouv.fr/particulier/precautions-elementaires/dix-regles-de-base/>
<https://www.ssi.gouv.fr/particulier/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel/>

Pour aller plus loin avec le
GRADEs SESAN





Pour aller plus loin - SESAN

Campagne de sensibilisation



- **Catalogue de vidéos SSI santé**
 - Accès aux données de santé
 - Echange et partage entre professionnels
- **Parcours de sensibilisation interactifs**
 - Quizz, vidéos,
 - Durée d'1m30 en moyenne
 - Sensibilisation personnalisée et contextualisé (contact ES, charte graphique,...)



Exemples de campagnes CYBERSECURITE SANTE

Des vidéos interactives d'1m30 illustrant des situations à risques que l'on peut rencontrer dans le secteur de la santé.



Session ouverte



Phishing ciblé



Consultation non
autorisée de
données sensibles



Partage de codes
d'accès



Pour aller plus loin - SESAN

Escape Game



- **X'cape Santé**

X'cape Santé est la déclinaison francilienne de l'escape game mis au point par le GCS Pays de la Loire. Il a été mis au point par SESAN sous l'impulsion de l'ARS Ile de France, en collaboration avec Orange Cyberdéfense. X'cape Santé reprend le principe de l'escape game d'origine. Le jeu est proposé aux adhérents SSI de SESAN sous forme de kit. L'équipe du département sécurité de SESAN fournit un ensemble de supports pour l'organisation du jeu et accompagne l'adhérent lors de la première séance du jeu. L'adhérent est ensuite autonome pour réitérer le jeu autant de fois qu'il le souhaite.



Bonjour amis journalistes,

Comme vous le savez Paris People vit des moments difficiles et le nombre de lecteurs ne cesse de diminuer. Afin d'éviter de déposer le bilan, nous devons redynamiser nos ventes et pour cela nous avons besoin d'un scoop.

Johnny Jackson, super star internationale, grand chanteur et inventeur du Lune Walk a disparu depuis peu des écrans. On présage des problèmes de santé, mais personne pour le moment n'a été en capacité de le prouver.

Une information obtenue auprès de certains proches indique que Johnny Jackson fréquente l'Institut médical des étoiles depuis peu.



PRÊTS À RELEVER LE DÉFI ?

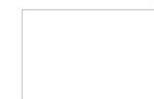


LE

À

Inscription :

Les informations de Johnny Jackson
resteront-elles secrètes ?





Pour aller plus loin - SESAN

Test de Phishing



- Nombre d'adresses mail illimité
- Possibilité d'ajouter un portail de saisie d'informations personnelles
- Portail de sensibilisation pour les personnes "piégées"
- Statistiques de la campagne

Bonjour,

L'espace disque de votre boîte mail est utilisé à 96%.
Pour éviter qu'il soit saturé, veuillez demander à votre DSI de l'espace supplémentaire

Pour faire une demande de hausse de quota, veuillez faire une demande GLPI

OUVERTURE DE TICKET

Message généré automatiquement, ne pas répondre

Cordialement,
La DSI

OUVERTURE D'UN TICKET

Veuillez saisir vos identifiants

Identifiant

Mot de Passe

Envoyer

Bonjour,

L'espace disque de votre boîte mail est utilisé à 96%

Pour éviter qu'il soit saturé, veuillez demander à
votre DSI de l'espace supplémentaire

Pour faire une demande
veuillez faire une demande
<http://www.smkc.com/4617ph0t0f0y0d0b02p0q0t0h0z0f0w0?signature=12f0b03d0cf06090ee0c030de0807ac2fd70e2b481f0fe00e0deb35e0b0900b00>
Cliquez ou appuyez pour suivre le lien.

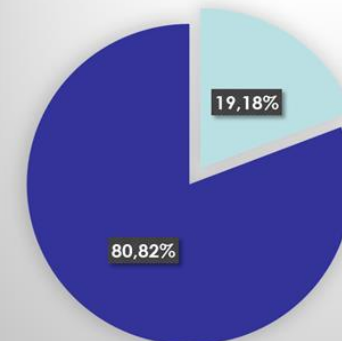
OUVERTURE DE TICKET

Message généré automatiquement, ne pas répondre

Cordialement,
La DSI

Si vous survolez ce lien (ou le bouton) avec
votre curseur, l'URL apparaîtra : **Pensez-
vous qu'elle est fiable ?**

Population globale



■ Destinataires victimes
du hameçonnage

■ Destinataires n'ayant
pas cliqué sur le faux
lien



Pour aller plus loin - SESAN

Autres supports de sensibilisation



- Affiches complémentaires
- Images de sensibilisation au format 16:9 pour les écrans de veille
- Calendrier
- Affichettes...

**Ceci est l'antivirus
le plus efficace au monde**



Réfléchissez avant de cliquer

Lorsque je reçois un mail:

- Je vérifie l'adresse de l'expéditeur
- Je vérifie que les liens affichés correspondent aux liens réels en passant ma souris dessus
- En cas de doute, je préviens le service informatique

ars
SESAN accompagne vos collaborateurs et les aide à améliorer la sécurité de leur système d'information.

sesan
SERVICE NUMÉRIQUE DE SANTÉ

06 Juin 2022

LU MA ME JE VE SA DI

30 31 1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 1 2 3

Régulièrement, tes mots de passe tu changeras

« JE SUIS UN GARS SÉRIeux - JE CHANGERAIS MON MOT DE PASSE TOUTES LES SEMAINES ! »
« LES ROMAINS, QU'EST-CE QUE C'EST ? »
« LES ROMAINS INTERNET, C'EST SÈRE ! »

#TousCyberVigilants

Selon leur niveau de complexité, les mots de passe peuvent être piratés dans le temps. Les changer régulièrement permet de réduire ce risque.

Calendar Model par SESAN - Design : Fix - Tous droits réservés.

sesan
SERVICE NUMÉRIQUE DE SANTÉ

CYBERSÉCURITÉ
Adaptez les bons réflexes

MISES À JOUR
Faire des mises à jour régulières équivaut à vacciner vos appareils contre les virus informatiques

Quelques recommandations

- Ne retardez pas la mise à jour de vos appareils
- Téléchargez les mises à jour uniquement depuis les sites officiels
- Activez l'option de téléchargement et d'installation automatique des mises à jour



sesan
SERVICE NUMÉRIQUE DE SANTÉ

Protection des données

Je nettoie
mon espace de travail pour protéger les données.

Je chiffre
les données sensibles avant de les partager.

Je ne transmets pas
mes identifiants.

Je vérifie
l'exactitude des mails que je reçois.

Je m'assure
de ne pas conserver les données plus que nécessaire.

Je me protège
J'utilise un mot de passe par site et j'utilise un coffre-fort de mots de passe.

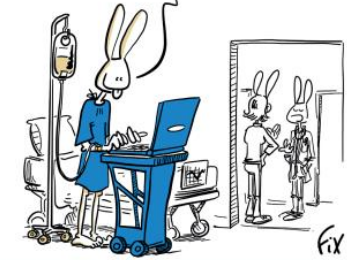
1/1



sesan
SERVICE NUMÉRIQUE DE SANTÉ

**En cas d'absence,
ton poste tu verrouilleras**

ET HOP ! JE ME PRESCRIS DES MASSAGES, UN GOÛTER, ET UN FLAX DE MORPHINE !



Verrouiller son poste, même en cas de courte absence permet d'éviter toute indiscretion sur les informations contenues et permet également d'éviter les actions malveillantes telles que le vol de données.

Tous droits réservés à SESAN - Design : Fix 2022

ars
sesan
SERVICE NUMÉRIQUE DE SANTÉ



Pour aller plus loin - SESAN

Organiser des exercices de Cybercrise



- 10 exercices réalisés à ce jour
- Nouvel Appel d'Offre en cours
 - Exercice de Cybercrise
 - Personnalisation du scénario en fonction de votre SI
 - Cellule Stratégique et/ou opérationnelle
 - Animation de l'exercice
 - Simulation de la pression médiatique via les réseaux sociaux
 - Debriefing "à chaud" et "à froid"
 - Plan d'action d'amélioration
 - Accompagnement à l'amélioration de la gestion d'une crise Cyber

Démonstration





SESAN

Contact



Des questions ?

Contactez : ssi@sesan.fr

