|  |
| --- |
| CHU Ynov |
| Plan de sensibilisation à la cybersécurité |
| [Sous-titre du document] |

|  |
| --- |
| Xavier Martin  [Date] |

Table des matières

[1 / Pourquoi sensibiliser tous les agents et personnels médical du CHU ? : 2](#_Toc199195431)

[2 : Les objectifs du plan de sensibilisation : 3](#_Toc199195432)

[3 : La sensibilisation des différentes catégories d’agents du CHU : 6](#_Toc199195433)

# 1 / Pourquoi sensibiliser tous les agents et personnels médical du CHU ? :

Une menace en forte augmentation :

La sensibilisation de tous les effectifs du CHU est quelque chose de très important car, les établissements de santé sont pour les cybercriminels une cible de choix et aussi le secteur le plus visé par les cyberattaques dans le pays. Selon les chiffres de l’Agence National de la Sécurité des Systèmes d’Information, en 2023 le secteur de la santé à subi 10% des attaques par rançongiciel (en hausse de plus de 10% comparer à 2022).

Voici une autre donnée qui conforte dans l’idée que la sensibilisation aux cyberattaques est primordiale : Le nombre d’incidents de cybersécurité déclarer au CERT Santé en France entre 2022 et 2023 est de 1173 ce qui est élever, et cela témoigne de la persistance et de la gravité de la menace pour les acteurs du monde de la santé et plus particulièrement les Hôpitaux.

D’après le CERT-FR, depuis 2020, la part des signalements traités par l’ANSSI qui concernerait la santé est passé d’un taux de 2.9% à un taux de 11.44% du total de tous les incidents que l’agence traite. Cela souligne le fait qu’il y a une augmentation significative des tentatives de compromissions des systèmes d’informations dans le milieu hospitalier.

Autre donnée qui ne rassure pas forcément, c’était que plus de la moitié des incidents recensés auprès de l’anssi en 2023 était d’origine malveillante.

Ce qui illustre une fois de plus le caractère délibéré et ciblé de toutes ces attaques, et que malheureusement la santé et une cible de choix pour les cyberattaquants.

Les attaques contre les acteurs du secteur de la santé peuvent avoir de lourdes conséquences sur eux. Cela peut entrainer une paralysie du SIH, et si celui-ci est bloquer cela peut restreindre l’accès aux dossiers des patients. Une cyberattaque sur un acteur du milieu de la santé peut entrainer des fuites de dossiers patients et ou des données personnelles médicales ou administratives qui sont considérer comme des données sensibles. Cela peut aussi être impactant sur la réalisation des soins.

Afin de faire face à cette nouvelle menace contre les établissements de santé qui est de plus en plus croissante, l’agence du numérique en santé à lancé le programme CaRE (Cybersécurité Accélération et Résilience des établissements). Ce programme lancer fin 2023 à pour but de renforcer la résistance et la résilience des hôpitaux en termes de cybersécurité. Et qu’ils soient bien plus équiper et prêt en cas de cyberattaque. Dans le programme il y a aussi un point d’honneur qui est mis sur la formation et la sensibilisation de tous les personnels des établissements.

# 2 : Les objectifs du plan de sensibilisation :

**Objectif Général :**

L’objectif général de ce plan de sensibilisation pour le CHU, serait de voir apparaitre une culture cyber au sein du CHU.

Cela se fera avec le temps et en responsabilisant l’ensemble des agents de l’hôpital qu’ils ont tous un rôle déterminant dans la sécurisation de celui-ci.

La finalité étant que chaque agent soit un acteur de près ou de loin à la cybersécurité de l’établissement, car chaque maillon de la chaine est très important.

**Les objectifs spécifiques :**

**Objectif spécifique numéro 1 :**

Comme première objectif spécifique celui-ci sera la réduction du facteur de risque de compromission humain dans les cyberattaques.

Pour réaliser cet objectif les mesures suivantes vont être mise en place :

* Identification des principaux vecteurs d’attaque par ingénierie sociale dans le cadre du CHU.
* Diminution du taux de clic réaliser par les agents sur les liens malveillants qui sont dissimuler dans les mails de fausse campagne de phishing à moins de 3% d’ici 12 mois
* Avoir le taux le plus élevé possible de signalement proactif des différentes anomalies et des éventuelles comportements suspects (mails, activités sur le SIH, connexions anormales).

Pour pouvoir réaliser cet objectif nous pouvons nous appuyer sur le guide d’hygiène numérique de l’ANSSI, ainsi que le PGSSI-S.

**Objectif spécifique numéro 2 :**

Le second objectif spécifique est de pouvoir intégrer la cybersécurité dans tous les processus métiers et les habitudes de tout le personnel du CHU.

Pour réaliser cet objectif les mesures suivantes vont être mise en place :

* Faire de la sensibilisation avec des messages qui soit adapté au milieu de la santé, ainsi qu’aux réalités de tous les métiers qui sont réaliser dans le CHU.
* Arrivé à former tous le CHU aux différents gestes barrières numériques dans les douze moins par l’intermédiaire d’ateliers ainsi que de formation en e-learning).
* Intégrer des rappels de cybersécurité dans tous les processus RH.
* Intégrer la cybersécurité dans tous les contrats qui sont passer avec des partenaires extérieures au CHU, afin d’être contractuellement couvert en cas de besoin.

**Objectif spécifique numéro 3 :**

Le troisième objectif spécifique est d’élever le niveau de maturité en termes de cyber dans tous le CHU (en respectant et en utilisant le cadre CaRE et de l’ANS).

Pour réaliser cet objectif les mesures suivantes vont être mise en place :

* Se conformer à au plan qui est prévus en termes de cybersécurité dans le CaRE sur la partie formation et sensibilisation des utilisateurs.
* Faire une cartographie complète de tous les différents profils au sein du CHU, afin de pouvoir identifier les profils à risque pour leur proposer des sessions spécifiques de sensibilisations. Dans le but de les faire progresser et tenant compte de leur niveau.
* Faire des analyses de risque pour mesurer le niveau de maturité du CHU et pour suivre les progrès de celui-ci. Cela se fera avec des outils comme la méthode ebios rm de l’ANSSI, le cyberscore de l’ANS et le référentiel d’analyse CaRE.

Le but à moyen terme serait d’obtenir un score de maturité supérieur à 3/5 sur le référenciel de la « culture de la cybersécurité » dans les évaluations faire par CaRE.

Un autre but serait de réaliser des simulations d’attaques qui sont ciblées sur des services en particulier, en commencent par les services les plus critiques (la réanimation, les urgences, le bloc opératoire er l’imagerie).

**Objectif spécifique numéro 4 :**

Le quatrième objectif spécifique est de renforcer la capacité de détection et de réaction des agents dont l’informatique n’est pas leur métier pour qu’ils soient prêt comment réagir en cas d’incident.

Pour réaliser cet objectif les mesures suivantes vont être mise en place :

* Former les utilisateurs à reconnaître une potentiel compromission le plutôt possible (ralentissement anormal du SIH, des écrans bloqués à répétitions, des messages suspects dans les interfaces des logiciels ou n’importe quel compostant du SIH)
* Former et normaliser l’utilisation des différents canaux de signalement d’incident (téléphone RSSI, formulaire interne, ticketing)
* Organiser au moins deux fois par ans des exercices de simulation de gestion de crise SSI impliquant des personnels non-DSI, afin d’être sûr que tous les effectifs soit prêt en cas de réel compromission du CHU (cellule de crise, mode dégradé, journal papier, etc.).

Cet objectif à deux buts bien précis, dans un premier temps de réduire le temps moyen de signalement d’un incident de cybersécurité (<30 minutes après détection).

Le second but serait de réduire le taux de propagation d’incidents grâce à une réaction immédiate des premiers témoins.

**Objectif spécifique numéro 5 :**

Le cinquième objectif spécifique est de renforcer la conformité règlementaire du CHU, vis-à-vis des différentes lois qui sont imposer par le régulateur.

Que celui-ci soit conforme aux réglementaires nationaux suivant :

* PGSSI-S
* HDS
* MSSanté

Que celui-ci soit aussi conforme aux réglementaires suivant :

* RGPD
* NIS 2

Le fait de ce conformé à ces différentes va permettre de dans un premier temps d’être en règle aux yeux du régulateur national ainsi que de l’entité de contrôle national pour le régulateur européen.

D’être en conformité avec ces différentes directives et règlements permet de démontrer la maturité du CHU en termes de cybersécurité. Et garantir que 100% des agents ayant accès à des informations à caractère personnel ou de santé sont formés sur les obligations légales qu’ils sont obligés respecter dans le cadre de leurs fonctions.

Être conforme avec ces différentes directives et règlements va permettre de diffuser en continue les politiques internes de SSI, ainsi que les bonnes pratiques qui sont dans la charte informatique du CHU que tous les agents doivent respecter.

Le respect de ces différentes directives et règlements sera aussi de bon sujet à intégrer dans les différentes formations à la cybersécurité réaliser par tous les agents du CHU.

Sensibilisation des agents a la cybersécurité :

**Objectif spécifique numéro 6 :**

Le sixième objectif spécifique est d’instaurer une culture continue de la cybersécurité au sein de tous le CHU.

Cela va permettre de maintenir une certaine vigilance de toutes les équipes du CHU, afin d’être le plus réactif et prêt possible. Avec des rappels assez réguliers, ainsi que au moins une fausse campagne de phishing par moins (pour que les agents soit toujours vigilent avec les mails qu’ils peuvent recevoir).

Un réseau de référents cybersécurité va être mis en place. La finalité est qu’il y ait un référent cybersécurité par grands pôles du CHU.

S’il vient à avoir des incidents de cybersécurité dans l’établissement, les retours d’expériences post-incidents seront pris en compte pour améliorer les process. Ainsi que dans les outils et les campagnes de sensibilisation.

# 3 : La sensibilisation des différentes catégories d’agents du CHU :

La stratégie de sensibilisation ne peut-être uniforme. Le CHU Ynov regroupe une grade variété de profils d’utilisateurs, chacun ayant un niveau d’interaction différent avec le SI, des habitudes professionnelles distinctes, et une maturité inégale face aux enjeux numériques.

La segmentation des différentes catégories d’agents permet de pouvoir adapter les contenus pédagogiques. Afin que les formats de communication et les exigences de sécurité pour que la sensibilisation soit le plus efficace, engageant et contextualisée.

**3.1 : Personnel médical (praticiens hospitaliers, chefs de service, internes, médecins en mobilité)**

Risques spécifiques :

* Accès étendu à des données sensibles (DPI, imagerie, prescriptions).
* Utilisation fréquente de la messagerie MSSanté ou d’appareils personnels (BYOD).
* Téléconsultation, mobilité, postes partagés dans les services.

Vulnérabilités observées :

* Faible attention aux alertes SI.
* Usage de supports non sécurisés (clés USB non chiffrées, partages non conformes).
* Réutilisation de mots de passe ou contournement de procédures.

Objectifs de sensibilisation :

* Sécuriser l’usage du DPI et des plateformes métier.
* Utiliser correctement MSSanté et les systèmes de téléconsultation.
* Appliquer les principes de confidentialité, y compris dans les discussions informelles.

Format adapté :

* Capsules vidéo spécifiques (5 minutes max).
* Micro-formations pendant les temps de service ou en staff.
* Cas pratiques sur incidents médicaux fictifs.

**3.2 : Personnel paramédical (IDE, AS, kinés, manipulateurs radio, sages-femmes)**

**Risques spécifiques :**

* Usage régulier de postes partagés et de lecteurs de carte CPS.
* Accès partiel ou en lecture seule au DPI, mais exposition directe aux dispositifs biomédicaux.
* Manipulation quotidienne d’informations sensibles (identité, données de soins).

**Vulnérabilités observées :**

* Sessions laissées ouvertes dans les salles de soins.
* Connexions de collègues sous un même compte.
* Dépendance aux systèmes pour la continuité des soins.

**Objectifs de sensibilisation :**

* Appliquer rigoureusement la politique de verrouillage automatique.
* Comprendre les conséquences d’une faille de sécurité dans un service de soins.
* Réagir efficacement face à une alerte système ou une suspicion de compromission.

**Format adapté :**

* Affichage visuel (pictogrammes, affiches dans les services).
* Scénarios illustrés / BD sur écran tactile ou fiche plastifiée.
* Intégration aux réunions de pôle ou relèves d’équipe.

**3.3 Personnel administratif (accueil, facturation, RH, direction, juridique)**

**Risques spécifiques :**

* Manipulation de données personnelles, sociales, voire bancaires.
* Utilisation intensive de la messagerie électronique (cible privilégiée de phishing).
* Interfaces avec des prestataires ou organismes externes (assurance maladie, employeurs, etc.).

**Vulnérabilités observées :**

* Faible détection des tentatives d’hameçonnage ou d’usurpation.
* Ouverture de fichiers infectés (Excel, PDF).
* Négligence dans la gestion des droits d’accès (documents partagés sur le réseau).

**Objectifs de sensibilisation :**

* Reconnaître les signaux faibles d’un e-mail malveillant.
* Sécuriser la manipulation et la transmission des documents administratifs.
* Être vigilant lors d’échanges avec des organismes externes.

**Format adapté :**

* Ateliers interactifs (quizz, étude de cas concrets).
* Simulations de phishing ciblées.
* Newsletter cybersécurité mensuelle avec conseils pratiques.

**3.4 Personnel technique et biomédical**

**Risques spécifiques :**

* Accès aux systèmes du CHUs, dispositifs médicaux connectés (IoMT), réseaux OT.
* Interfaces avec des prestataires pour la maintenance ou l’installation.
* Failles physiques (ports USB, salles techniques non sécurisées, configurations par défaut).

**Vulnérabilités observées :**

* Manque de cloisonnement des réseaux entre systèmes critiques.
* Pratiques informelles (mots de passe partagés, configurations non documentées).
* Absence de suivi post-intervention des prestataires.

**Objectifs de sensibilisation :**

* Appliquer les protocoles de cybersécurité industrielle (SSI OT).
* Sécuriser les accès aux dispositifs biomédicaux.
* Intégrer des exigences SSI dans la gestion de sous-traitance.

**Format adapté :**

* Formation technique courte sur les erreurs courantes (type CERT Santé).
* Guide de cybersécurité pour la maintenance (check-list).
* Affichage en atelier et salles machines.

**3.5 Nouveaux arrivants, étudiants, stagiaires, internes en rotation**

**Risques spécifiques :**

* Moindre acculturation aux SI hospitaliers et à leurs contraintes.
* Emploi de dispositifs personnels (ordinateurs, clés USB, smartphones).
* Sens de responsabilité encore peu ancré face aux données de santé.

**Vulnérabilités observées :**

* Utilisation d’identifiants d’un tiers.
* Accès depuis des réseaux non sécurisés.
* Manque de connaissance des procédures d’alerte.
* Manque de connaissance des procédures interne au CHU.

**Objectifs de sensibilisation :**

* Appliquer les gestes numériques de base dès l’arrivée.
* Respecter les politiques de sécurité du SI et les usages autorisés.
* Savoir signaler une anomalie ou un incident.

**Format adapté :**

* Module d’accueil cybersécurité (15 min).
* Document synthétique type « Passeport numérique CHU ».
* Inclusion dans les sessions d’intégration RH ou des universités partenaires.

**3.6 : Prestataires, sous-traitants, intervenants externes (SSI, entretien, intérim, sociétés de service)**

**Risques spécifiques :**

* Accès temporaire mais potentiellement critique à des segments du SIH.
* Entrées/sorties fréquentes sans dispositif de suivi formel.
* Utilisation de matériel et logiciels personnels ou non homologués.

**Vulnérabilités observées :**

* Absence de charte SSI signée ou de clause contractuelle cybersécurité.
* Non-respect des politiques internes (installation de logiciels, ports réseau).
* Risque d’introduction de malwares (clé USB infectée, PC non patché).

**Objectifs de sensibilisation :**

* Formaliser les obligations de sécurité dans les contrats de prestation.
* Éduquer les prestataires à l’environnement numérique hospitalier.
* Mettre en place un processus de vérification post-intervention.

**Format adapté :**

* Signature obligatoire d’un engagement SSI.
* Accès restreint à des modules de sensibilisation en ligne pour prestataires.
* Vérification de conformité avant tout accès au réseau.

# **4 : Axes pédagogiques et thématiques**

L'efficacité d'une campagne de sensibilisation repose sur sa capacité à adapter ses contenus aux risques réels, aux comportements à corriger, ainsi qu’aux environnements professionnels des agents.

Les axes pédagogiques du plan sont organisés autour de six grandes thématiques transversales, permettant de toucher l’ensemble des agents du CHU, quel que soit leur niveau d’implication dans le SI.

**4.1 : L’ingénierie sociale et le phishing :**

Objectif : Identifier et désamorcer les attaques qui ciblent l’humain comme point d’entrée du système d’information.

Contenus pédagogiques :

* Reconnaître les formes courantes d’hameçonnage (emails, SMS, appels frauduleux).
* Apprendre à lire les signaux faibles d’un message suspect (adresses, fautes, urgences fictives).
* Réagir correctement : ne pas cliquer, alerter le DSI ou RSSI, transférer pour analyse.

Moyens pédagogiques :

* Campagnes de phishing simulé régulières.
* Capsules vidéos illustrant des scénarios d’arnaque dans un contexte hospitalier.
* Guide pratique « 10 réflexes contre le phishing ».

Référentiels associés :

* ANSSI – Guide « Se protéger contre l’ingénierie sociale »
* CaRE – Mécanisme de détection utilisateur

4.2 : Hygiène numérique et bonnes pratiques de sécurité

Objectif : Instaurer une culture de base de la cybersécurité dans les usages numériques quotidiens.

Contenus pédagogiques :

* Sécuriser les mots de passe (unicité, robustesse, MFA).
* Utiliser correctement les postes de travail : verrouillage, session nominative, pas de post-it.
* Identifier les comportements à risque : navigation non professionnelle, téléchargement non contrôlé, usage de supports amovibles.

Moyens pédagogiques :

* Affiches de rappel dans les locaux (salles de soin, secrétariats, salles techniques).
* Checklist de cybersécurité quotidienne ou hebdomadaire (imprimable ou numérique).
* Tutoriels de paramétrage : MFA, verrouillage automatique, mise à jour.

Référentiels associés :

* PGSSI-S – Politique de sécurité des SI de santé
* ANSSI – Guide D’Hygiène informatique

4.3 : Protection des données personnelles et des données de santé (RGPD & secret médical)

Objectif : Garantir le respect des obligations légales et éthiques liées au traitement de données sensibles.

Contenus pédagogiques :

* Ce qu’est une donnée de santé et une donnée personnelle.
* Principes RGPD appliqués à l’hôpital (minimisation, durée de conservation, droits des patients).
* Confidentialité dans les conversations, les écrans visibles, les impressions.

Moyens pédagogiques :

* Mini-jeux interactifs : quiz RGPD contextualisé aux services hospitaliers.
* Fiches illustrées « Ce que je peux / ne peux pas faire avec les données patients ».
* Témoignages d'agents ou exemples concrets de sanctions/erreurs.

Référentiels associés :

* RGPD (Art. 5 à 32)
* PGSSI-S – Bloc confidentialité et gestion des identités
* CNIL – Guide « Données de santé en établissement »

**4.4 : Réaction face à un incident de sécurité ou une cyberattaque :**

Objectif : Préparer chaque agent à réagir rapidement et de façon adéquatement en cas de compromission, pour limiter l'impact sur le CHU et protéger la continuité des soins.

Contenus pédagogiques :

* Signaux d’alerte d’un incident (poste lent, fichiers chiffrés, message de rançongiciel).
* Premiers réflexes à adopter (ne pas redémarrer, déconnecter le réseau, alerter la DSI).
* Chaîne d’alerte interne (référents cybersécurité, procédure de remontée).

Moyens pédagogiques :

* Simulations d’incidents avec scénario fictif (serious game ou table ronde).
* Procédure imprimable en format A5 ou intégrée à l’intranet.
* Numéro d’alerte affiché sur chaque poste critique.

Référentiels associés :

* Plan de réponse à incident du CHU
* CERT Santé – Recommandations post-attaque
* CaRE – Volet gestion de crise SSI

4.5 : Sécurisation des usages numériques en mobilité et à distance

Objectif : Encadrer l’usage des outils numériques en situation de télétravail, de mobilité interne, d’intervention ou de consultation à distance.

Contenus pédagogiques :

* Risques liés aux connexions Wi-Fi publiques ou non sécurisées.
* Bonnes pratiques sur smartphone et tablette : verrouillage, chiffrement, suppression à distance.
* Utilisation sécurisée de la messagerie MSSanté et des VPN hospitaliers.

Moyens pédagogiques :

* Vidéo explicative : "Travailler en mobilité en toute sécurité"
* Fiches réflexes pour les soignants en déplacement ou les astreintes.
* Charte mobilité numérique signée par les professionnels concernés.

Référentiels associés :

* PGSSI-S – Messagerie sécurisée de santé
* ANSSI – Guide sur les terminaux mobiles

**4.6 : Sécurité des dispositifs médicaux connectés et des accès techniques**

Objectif : Impliquer les personnels techniques et biomédicaux dans la sécurisation des équipements connectés (IoMT, SCADA, domotique hospitalière).

Contenus pédagogiques :

* Identification des failles potentielles dans les dispositifs (mots de passe usine, OS obsolètes).
* Cloisonnement réseau et gestion des ports physiques.
* Intégration de la cybersécurité dès l’achat ou la maintenance d’un équipement.

Moyens pédagogiques :

* Fiches techniques sécurité à intégrer dans les procédures biomédicales.
* Formations ciblées pour les ingénieurs, techniciens et prestataires.
* Scénarios d’audit ou de test de pénétration encadrés.

Référentiels associés :

* ANSM – Cybersécurité des dispositifs médicaux
* HDS – Hébergement sécurisé des données
* PGSSI-S – Sécurité des équipements biomédicaux

**5 : Méthodes pédagogiques**

Le choix des méthodes pédagogiques constitue un levier stratégique majeur pour garantir l’efficacité, la rétention et l’appropriation des messages de cybersécurité. Compte tenu de la pluralité des métiers, de la charge de travail élevée et du contexte hospitalier, le programme de sensibilisation repose sur une approche multimodale, combinant des outils numériques, des actions présentielles et des mécanismes ludiques ou immersifs.

5.1 Pédagogie par contextualisation métier :

Principe : Adapter les contenus à la réalité quotidienne de chaque groupe professionnel (médecins, soignants, techniciens, administratifs) afin de maximiser la pertinence perçue.

Exemples :

* Cas concrets de compromission de DPI pour les praticiens.
* Scénarios de vol de badge ou session ouverte pour les paramédicaux.
* Incidents de type phishing RH ou fraude au RIB pour les administratifs.
* Accès non autorisé à un automate biomédical pour les techniciens.

Bénéfices : Meilleure mémorisation, réduction de la résistance au changement, impact comportemental accru.

**5.2 Micro-learning et séquences courtes :**

Principe : Proposer des modules de formation courts (3 à 8 minutes) pour tenir compte des contraintes de temps du personnel hospitalier.

Supports possibles :

* Capsules vidéo animées.
* Micro-modules e-learning thématiques (mots de passe, e-mail, RGPD, etc.).
* Podcasts audios internes diffusés dans les salles de repos.

Bénéfices : Engagement plus fort, accessibilité sur poste ou mobile, meilleure disponibilité.

5.3 Ateliers et sessions présentielles ciblées :

Principe : Organiser des sessions de sensibilisation en petits groupes ou lors de moments-clés (intégration, staff, journée de formation continue).

Formats envisagés :

* Ateliers pratiques (analyse de mail suspect, configuration de sécurité).
* Débriefs d'incidents réels ou simulés.
* Table ronde interdisciplinaire avec RSSI, DPO et cadres de santé.

Publics ciblés en priorité :

* Personnels exposés (accueil, imagerie, DSI).
* Nouveaux arrivants et internes.
* Encadrement de proximité.

Bénéfices : Interaction directe, réponses aux questions, renforcement de la culture cyber au sein des équipes.

5.4 Apprentissage par le jeu (serious game, quiz, simulation) :

Principe : Favoriser l’appropriation des messages par des dispositifs ludiques, compétitifs ou immersifs.

Outils possibles :

* Quiz interactifs mensuels sur l’intranet.
* Jeux de rôles : "vous êtes le RSSI d’un hôpital attaqué".
* Simulations d’attaques par rançongiciel : gestion d’un service perturbé.

Bénéfices : Engagement émotionnel, impact pédagogique durable, détection des lacunes de compréhension.

5.5 Campagnes récurrentes et progressives :

Principe : Ne pas limiter la sensibilisation à une action ponctuelle, mais l'inscrire dans la durée selon un calendrier pédagogique structuré.

Organisation :

* Un thème par mois ou par trimestre (ex. : avril = phishing, juin = RGPD, octobre = cybersécurité OT).
* Relances régulières (newsletter cybersécurité, affiches tournantes, rappels automatiques).

Intégration dans les temps forts : Octobre (mois européen de la cybersécurité), JIQHS, Journée du numérique en santé.

Bénéfices : Maintien de la vigilance dans le temps, ancrage comportemental progressif.

5.6 : Simulations d’attaque (phishing, rançongiciel, fuite de données)

Principe : Tester en situation réelle la réaction des agents face à une tentative de compromission contrôlée.

Types d’exercices :

* Envoi d’e-mails factices pour détecter les clics sur des liens suspects.
* Simulation d’un blocage informatique avec demande de rançon (affichage simulé).
* Tests de récupération d’un badge égaré ou d’un mot de passe partagé.

Suivi :

* Analyse anonyme des comportements.
* Rapport statistique par service (sans sanction).
* Formation corrective ou renforcement ciblé.

Bénéfices : Évaluation du niveau réel de vigilance, amélioration de la résilience collective.

5.7 : Formalisation et traçabilité des actions de sensibilisation

Principe : Garantir que les actions menées sont suivies, mesurées et valorisées.

Outils associés :

* Attestations de sensibilisation obligatoires pour les internes, prestataires, et nouveaux agents.
* Traçabilité des formations dans le système RH (via un LMS ou tableau Excel de suivi).
* Indicateurs de pilotage (taux de participation, taux de clics sur phishing simulé, taux de conformité).

Bénéfices : Conformité réglementaire (audits, CNIL, ARS), retour sur investissement des actions, pilotage stratégique.

**6 : Gouvernance du programme**

6.1 : Pilotage stratégique

Objectif :

Assurer l’alignement du programme avec la stratégie globale de cybersécurité de l’APHM et l’intégrer dans les politiques de gestion des risques, de qualité et de conformité.

Acteurs clés :

* Directeur général : portage institutionnel du programme, inscription dans la feuille de route numérique du CHU.
* Responsable de la sécurité des systèmes d’information (RSSI) : garant de la stratégie cyber, des contenus pédagogiques, et de la cohérence globale du dispositif.
* Délégué à la protection des données (DPO) : veille au respect des obligations RGPD et au bon traitement des données personnelles lors des actions pédagogiques.
* Direction des ressources humaines (DRH) : intégration dans les parcours professionnels (formations, onboarding, sanctions).
* Direction des systèmes d'information (DSI) : appui technique, infrastructure LMS, outils de communication.

Instances de pilotage :

* Comité de gouvernance SSI / numérique / cybersécurité : suivi trimestriel des indicateurs, validation des grandes orientations.
* Réunions RSSI / DPO / DRH mensuelles : coordination opérationnelle.

6.2 Coordination opérationnelle

Objectif :

Mettre en œuvre, suivre et ajuster le plan de sensibilisation au jour le jour, en lien étroit avec les services métiers et les référents locaux.

Cellule de coordination :

* Pilotée par le RSSI (ou un chef de projet cybersécurité), elle regroupe :
* Chargé de projet sensibilisation / formateur cyber.
* Référents cybersécurité métiers ou DSI (par pôle ou service).

Représentants du personnel (cadres de santé, agents relais numériques).

Responsable de la communication interne.

Rôles principaux :

* Planification des campagnes et supports pédagogiques.
* Répartition des modules selon les cibles et les temporalités.
* Suivi des retours utilisateurs, des taux de complétion et d’engagement.
* Proposition d’ajustements annuels du programme.

6.3 : Réseau de relais internes (référents cybersécurité)

Objectif :

Appuyer le déploiement local du programme grâce à des acteurs de proximité au sein des services.

Profil :

* Agents volontaires ou désignés.
* Personnels soignants, administratifs ou techniques disposant d’une sensibilité numérique.
* Formés par le RSSI ou le formateur interne.

Missions :

* Relayer les messages et affiches.
* Aider à l’animation des quiz ou ateliers locaux.
* Faire remonter les difficultés ou besoins spécifiques.
* Participer aux audits de sensibilisation ou à l’amélioration continue.

6.4 : Partenariats et appuis externes

Objectif :

Bénéficier de ressources, d’outils et de conseils issus de l’écosystème national de la cybersécurité en santé.

Partenaires envisageables :

* CERT Santé (ANS) : guides, kits de sensibilisation, appui en cas d’incident.
* Agence du Numérique en Santé (ANS) : référentiels PGSSI-S, CaRE, cyberscore HOP’EN.
* ANSSI / Cybermalveillance.gouv.fr : kits « Les essentiels de la cybersécurité ».
* CNIL : fiches pédagogiques RGPD, supports pour les établissements de santé.
* Cabinets ou prestataires spécialisés (audit de maturité, phishing simulé, formations sur mesure).

6.5 : Suivi, indicateurs et amélioration continue

Objectif :

Évaluer objectivement la portée et l’efficacité du programme afin d’en ajuster les modalités.

Indicateurs clés (KPI) :

|  |  |  |
| --- | --- | --- |
| Indicateur | Source | Fréquence |
| Taux de complétion des modules de formation | LMS ou plateforme interne | Trimestrielle |
| Taux de clic lors des campagnes de phishing simulé | Outil de simulation | Bimestrielle |
| Nombre de signalements de mails suspects | Boîte d’alerte dédiée ou outil de remontée | |  | | --- | |  |  |  | | --- | | Mensuelle | |
| Niveau de maturité SSI des services | Grille CaRE ou autoévaluation ANSSI | Annuelle |
| Feedback qualitatif des agents (satisfaction, clarté) | Sondage post-formation | Après chaque action |

Revue annuelle :

* Bilan annuel présenté en COPIL numérique ou comité qualité/sécurité.
* Ajustement des thématiques, outils et modalités pédagogiques.
* Réactualisation du plan selon l’évolution des risques (rétro-ingénierie d’incidents, retour d’expérience).

6.6 : Intégration dans les politiques de sécurité et qualité

Objectif :

Assurer la pérennité du programme en l’intégrant dans les processus existants de l’établissement.

Intégrations prévues :

* Charte informatique et charte cyber intégrée aux règlements intérieurs.
* Sensibilisation obligatoire intégrée dans le parcours d’intégration des nouveaux arrivants.
* Liaison directe avec le plan de continuité d’activité (PCA) et le plan de réponse à incident (PRI).
* Inclusion dans les audits internes et revues qualité (HAS, DREES, ARS).

**7 : Évaluation de l’impact et amélioration continue**

L’évaluation du programme de sensibilisation est essentielle pour mesurer son efficacité, ajuster les dispositifs pédagogiques et garantir l’amélioration continue du niveau de maturité cybersécurité au sein de l’établissement. Elle repose sur des indicateurs qualitatifs, quantitatifs et comportementaux, ainsi que sur une démarche itérative de pilotage.

7.1 Objectifs de l’évaluation

Mesurer l’efficacité réelle des actions de sensibilisation (changement de comportement, adoption de bonnes pratiques).

Détecter les points de fragilité résiduels par population ou service.

Valoriser les progrès réalisés dans une logique de pilotage stratégique.

Ajuster les formats, les contenus ou les cibles en fonction des retours et des incidents observés.

Renforcer l’engagement managérial et l’adhésion des équipes à la culture cyber.

7.2 Indicateurs de performance clés (KPI)

Les indicateurs sont suivis par le RSSI et la cellule de coordination, puis analysés en comité de gouvernance cybersécurité.

a. Indicateurs de participation et d’engagement