Programme de sensibilisation à la cybersécurité 2026-2028

Table des matières

LA PROPOSITION

L'offre de cybersécurité proposée par le GRADeS s'inscrit dans les différents axes du programme CaRE (Cybersécurité Accélération et Résilience des Établissements).

Ce programme a pour but de rendre les établissements plus résilients et mieux préparés aux risques cyber. À ce titre, le GRADeS propose un service de sensibilisation à la cybersécurité sous la forme de déploiement de campagnes de sensibilisation à la sécurité informatique par modules vidéo. Le coût de ce service est pris en charge en intégralité par l'Agence Régionale de Santé.

La proposition du GRADeS inclut les éléments suivants :

🗓️ **Une campagne de sensibilisation pilotée par le GRADeS de deux ans** sous forme de modules envoyés par mail à l'utilisateur
🎬 **Un parcours thématique complet**, disponible tout au long de la campagne (pour permettre des sessions de sensibilisation en interne)
🎯 **2 exercices de phishing** par an, afin de tester la vigilance de l'utilisateur.

La campagne sera déployée sur une période de 24 mois à partir d'avril 2026. Merci de candidater avant le 1er mars 2026.

Etablissements sanitaires, sociaux et médico-sociaux, DAC des Hauts-de-France, cette offre est pour vous :

- Création **illimitée de comptes apprenants** pour vos équipes
- **Pilotage simplifié** par le GRADeS
- Suivi de **vos indicateurs par établissements** : rapports bimestriels envoyés automatiquement
- **Mise à jour annuelle possible des destinataires** en cas de renouvellement de vos équipes

POUR CANDIDATER :

GRADeS Inéa Sant& Numérique - Programme de sensibilisation à la cybersécurité – Remplir le formulaire

DETAILS DU PROGRAMME

▶ **1 à 2 modules tous les deux mois pendant deux ans**

📬 **Début de mois** : un mail invite chaque utilisateur à découvrir le / les modules du moment

🔔 **Relance automatique** à J+14 et J+28 pour les utilisateurs n'ayant pas encore participé

📂 **Accès en replay** : chaque vidéo reste disponible dans le **tableau de bord personnel** de l'utilisateur même après sa diffusion mensuelle !

🎯 **2 exercices de phishing** par an pour tester la vigilance des équipes

LES THEMATIQUES ET CONTEXTES DES MODULES

1.1.1 Avril-Mai 2026 - Envoi le 7 avril 2026

Sanitaire, Social et médico-social, DAC	**Cherche & Trouve de la Cyber - Au bureau**	Parcours sous forme d'un jeu télévisé inspiré des 7 erreurs. L'apprenant est invité à détecter les risques cyber potentiels dans un scénario interactif, et adopter les bonnes pratiques. Milieu : Le bureau - Nombre de risques à détecter : 5 - Durée : 5 minutes 🎯 Objectifs pédagogiques : • Identifier les comportements à risque dans un environnement de bureau • Adopter les bons réflexes pour protéger l'accès à son poste de travail et aux locaux (mot de passe, verrouillage de session, badge, documents sensibles, clef USB)

1.1.2 Juin-Juillet 2026 – Envoi le 2 juin 2026

Sanitaire, Social et médico-social, DAC	**Juin : Opération champion du monde**	🔎 Concept : Chaque mois, les hackers profitent des moments clés de l'année pour piéger leurs victimes. Soldes, vacances, événements sportifs, fêtes… Autant d'occasions où l'émotion prend le dessus et où notre vigilance baisse. Mais cette année, ils vont avoir du fil à retordre ! 📽️ Format : Une vidéo courte et percutante (2 min max) avec un storytelling immersif : suivez un groupe de hackers qui traquent la moindre faille, jouant sur l'excitation des soldes, l'euphorie des festivals ou encore la frénésie des fêtes. À vous de déjouer leurs pièges ! 🎯 Objectifs pédagogiques : • Reconnaître les techniques de cyberattaque (faux e-mails, fausses applications, QRcodes piégés) • Adopter les bons réflexes pour se protéger au quotidien.

		• Éviter les pièges en vérifiant les adresses mails, en téléchargeant les applications uniquement depuis les stores officiels, en prenant le temps de vérifier l'adresse de redirection avant de scanner un QR code. Renforcer sa vigilance numérique en situation de mobilité ou d'événement grand public
	ChatBot - Faits insolites	💡 Et si on apprenait la cybersécurité autrement ? À travers des faits insolites mais bien réels, ce chatbot ludique et interactif invite les collaborateurs à (re)découvrir les bonnes pratiques essentielles de cybersécurité. Un format conçu pour marquer les esprits et ancrer les bons réflexes au quotidien. 🎯 Objectifs pédagogiques : • Identifier les erreurs courantes en cybersécurité. • Reconnaître des risques cyber concrets à partir de situations réelles ou insolites, en lien avec les enjeux du secteur de la santé

1.1.3 Août-Septembre 2026 – Envoi le 18 août 2026

Sanitaire	**Consultation non autorisée de données sensibles**	Vidéo interactive d'1m30 de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre les risques juridiques et éthiques liés à la consultation non autorisée de données de santé • Adopter les bons réflexes pour respecter la confidentialité des informations et limiter les accès aux seules données nécessaires
	Soignant ou patient	Vidéo interactive de 2 min de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre pourquoi la consultation de son propre dossier médical via ses accès professionnels est interdite. • Identifier les risques liés à une utilisation inappropriée des accès professionnels. • Connaître la procédure légale et sécurisée pour accéder à ses données personnelles de santé.
Social et médico-social, DAC	**RGPD Introduction**	🎯 Objectifs pédagogiques : Expliquer l'importance du RGPD pour la protection des données personnelles / Identifier les principaux droits des personnes en matière de données personnelles.
	RGPD Notion de traitement	🎯 Objectifs pédagogiques : Comprendre comment les données personnelles sont collectées et utilisées en entreprise / Identifier les bonnes pratiques pour sécuriser les données personnelles dans le cadre professionnel.

1.1.4 Octobre-Novembre 2026 – Envoi le 6 octobre 2026

Sanitaire, Social et médico-social, DAC	**ChatBot - Phishing**	Un outil interactif spécialement conçu pour sensibiliser vos collaborateurs du secteur de la santé à la détection des mails de phishing. 🎯 Objectifs pédagogiques :

		• Identifier les signes d'un mail frauduleux, même lorsqu'il semble provenir d'un organisme de santé. • Adopter les bons réflexes pour protéger les données sensibles des patients et de l'établissement

1.1.5 Décembre-Janvier 2027 – Envoi le 2 décembre 2026

Sanitaire, Social et médico-social, DAC	**Calendrier de l'Avent de la Cyber**	Ce calendrier de l'avent de la cybersécurité propose, chaque jour, une courte vidéo thématique pour découvrir un risque, une bonne pratique ou un conseil utile. 🎯 Objectifs pédagogiques : • Identifier différents types de risques numériques courants au travail, • Reconnaître les signaux d'alerte liés à chaque thématique abordée, • Adopter les bonnes pratiques de cybersécurité dans son activité professionnelle quotidienne, • Développer de bons réflexes grâce à une exposition régulière et progressive aux messages de prévention.
	CYBER EVENTS - Janvier : Cyber Résolutions	🔎 Concept : Chaque mois, les hackers exploitent les failles du quotidien pour piéger leurs victimes. Grands événements, connexions publiques, promotions alléchantes… Autant d'opportunités où la précipitation l'emporte sur la prudence. Mais cette fois, la vigilance sera au rendez-vous ! 📽️ Format : Une vidéo immersive (4 min) avec une narration percutante : plongez dans l'univers de Hackers bien décidés à vous tromper en utilisant les bonnes résolutions et les offres promotionnelles alléchantes des soldes de janvier. À vous de garder vos données à l'abri et de déjouer leurs pièges ! 🎯 Objectif pédagogiques : • Vérifier l'authenticité d'un lien promotionnel à partir du site marchand en passant par un moteur de recherche. • Vérifier l'adresse de l'expéditeur d'un email promotionnel et signaler un email frauduleux. • Télécharger uniquement des outils/applications sécurisés depuis un site officiel. • Ne partager ni informations confidentielles ni personnelles sur les réseaux sociaux.

1.1.6 Février-Mars 2027 – Envoi le 2 février 2027

Sanitaire, Social et médico-social, DAC	**ChatBot - Mot de passe**	Un outil interactif spécialement conçu pour sensibiliser les professionnels de santé à la gestion des mots de passe. 🎯 Objectifs pédagogiques : • Identifier les bonnes pratiques adaptées au secteur de la santé pour créer des mots de passe forts. • Découvrir des techniques simples et sécurisées pour gérer et mémoriser efficacement ses mots de passe.

1.1.7 Mars 2027 – Envoi le 16 mars 2027

Sanitaire, Social et médico-social, DAC	**Evaluation à froid : Enquête d'impact et de satisfaction**	🎯 Objectifs : mesurer le degré de satisfaction des apprenants, recueillir des feedbacks pour améliorer les contenus, et mesurer l'impact comportemental en situation de travail.

1.1.8 Avril-Mai 2027 – Envoi le 6 avril 2027

Sanitaire	**RGPD Introduction**	🎯 Objectifs pédagogiques : Expliquer l'importance du RGPD pour la protection des données personnelles / Identifier les principaux droits des personnes en matière de données personnelles.
	RGPD Notion de traitement	🎯 Objectifs pédagogiques : Comprendre comment les données personnelles sont collectées et utilisées en entreprise / Identifier les bonnes pratiques pour sécuriser les données personnelles dans le cadre professionnel.
Social et médico-social, DAC	**Eradication des données sur le poste de travail**	Vidéo interactive de 3mn de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre l'importance de supprimer correctement les données sensibles sur son poste de travail pour éviter tout risque de fuite • Adopter les bons réflexes pour effacer de manière sécurisée les fichiers contenant des informations patients.
	PCA-PRA	Vidéo interactive de 3mn de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre l'importance du PCA/PRA pour garantir la continuité des soins en cas d'incident cyber. • Adopter les bons réflexes en situation de crise pour limiter les impacts sur l'activité de l'établissement.

1.1.9 Juin-Juillet 2027 – Envoi le 8 juin 2027

Sanitaire	**Eradication des données sur le poste de travail**	Vidéo interactive de 3mn de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre l'importance de supprimer correctement les données sensibles sur son poste de travail pour éviter tout risque de fuite • Adopter les bons réflexes pour effacer de manière sécurisée les fichiers contenant les informations patients.

	PCA-PRA	Vidéo interactive de 3mn de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. 🎯 Objectifs pédagogiques : • Comprendre l'importance du PCA/PRA pour garantir la continuité des soins en cas d'incident cyber. • Adopter les bons réflexes en situation de crise pour limiter les impacts sur l'activité de l'établissement.
Social et médico-social, DAC	**Objets connectés**	Vidéo interactive de sensibilisation sur la cybersécurité illustrant une situation à risque pour les établissements et services sociaux et médico-sociaux (2 min) 🎯 **Objectifs pédagogiques :** • Identifier les risques associés à l'utilisation d'objets connectés dans un environnement médico-social • Adopter les bonnes pratiques pour sécuriser les objets connectés et protéger les données sensibles qu'ils peuvent manipuler.
	Navigation sécurisée	Vidéo interactive de sensibilisation sur la cybersécurité illustrant une situation à risque pour les établissements et services sociaux et médico-sociaux (2 min) : 🎯 Objectifs pédagogiques : • Identifier les risques liés à une navigation non sécurisée sur Internet dans un environnement médico-social • Adopter les bonnes pratiques pour protéger les données sensibles lors de l'utilisation d'applications web et de sites en ligne.

1.1.10 Août-Septembre 2027 – Envoi le 20 août 2027

Sanitaire	**Usages pro/perso**	Une vidéo interactive de 2 min de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. Suivez Laurène, ophtalmologue en Centre Hospitalier. 🎯 Objectifs pédagogiques : • Comprendre les risques liés au mélange des usages professionnels et personnels sur un même appareil • Adopter les bons réflexes pour séparer ses usages et protéger les données sensibles de santé
	Utilisation d'applications non approuvées	Vidéo interactive d'1m30 de sensibilisation sur la cybersécurité illustrant une situation à risque dans le domaine de la santé. Suivez Hélène, psychologue en Centre Médico-Psychologique.
Social et médico-social, DAC	**Droit d'information**	Comprendre les droits d'information des personnes concernant leurs données personnelles / Identifier les situations où la fourniture d'informations est obligatoire dans le cadre du RGPD.
	Registre des activités	Comprendre l'importance du registre des activités de traitement / Identifier les informations clés à inclure dans ce registre.

1.1.11 Octobre-Novembre 2027 – Envoi le 5 octobre 2027

Sanitaire	**Octobre : Halloween**	🔎 Concept : Chaque mois, les hackers exploitent les failles du quotidien pour piéger leurs victimes. Voyages, connexions publiques, promotions alléchantes… Autant d'opportunités où la précipitation l'emporte sur la prudence. Mais cette fois, la vigilance sera au rendez-vous ! 📽️ Format : Une vidéo courte et immersive (2 min) avec une narration percutante : plongez dans l'univers des arnaques numériques qui fleurissent pendant les fêtes comme Halloween. Deep fake, faux SMS, escroqueries urgentes… À vous de repérer les pièges et de réagir comme un pro ! 🎯 Objectifs pédagogiques : • Identifier les techniques d'arnaque les plus fréquentes pendant les événements festifs (deep fake, smishing, escroquerie au président). • Repérer les signaux d'alerte dans un message ou un lien frauduleux, même bien déguisés. • Adopter les bons réflexes face à une tentative d'arnaque au président. • Rester vigilant, même quand le message semble venir d'une personne de confiance.
Social et médico-social, DAC	**Cherche et Trouve de la Cyber - Dans un e-mail**	Parcours sous forme d'un jeu télévisé inspiré des 7 erreurs. L'apprenant est invité à détecter les risques cyber potentiels dans un scénario interactif, et adopter les bonnes pratiques. Milieu : Dans un e-mail (phishing) - Nombre de risques à détecter : 5 - Durée : 5 minutes 🎯 Objectifs pédagogiques : • Détecter les éléments suspects dans un e-mail pouvant indiquer une tentative de phishing (expéditeur douteux, liens frauduleux, pièce jointe piégée…) • Adopter les bons réflexes pour vérifier la fiabilité d'un message avant de cliquer, télécharger ou répondre • Renforcer sa vigilance face aux techniques d'ingénierie sociale utilisées dans les courriels malveillants.

1.1.12 Décembre-Janvier 2028 – Envoi le 7 décembre 2027

Sanitaire, Social et médico-social, DAC	**Décembre : Noël sous Haute Surveillance**	🔎 Concept : Chaque mois, les hackers exploitent les failles du quotidien pour piéger leurs victimes. Voyages, connexions publiques, promotions alléchantes… Autant d'opportunités où la précipitation l'emporte sur la prudence. Mais cette fois, la vigilance sera au rendez-vous ! 📽️ Format : Une vidéo courte et immersive (4 min) avec une narration percutante : Plongez dans l'univers d'un hacker solitaire qui profite de la magie de Noël pour piéger ses victimes : notifications de livraison urgentes, réductions impossibles, poupées connectées détournées... Apprenez à reconnaître ses stratagèmes pour préserver la magie des fêtes en toute sécurité ! 🎯 Objectifs pédagogiques : • Identifier les tentatives de phishing liées aux achats et livraisons de Noël

		• Repérer les arnaques aux fausses promotions et sites frauduleux • Connaître les risques de sécurité des objets connectés • Adopter une méthodologie de vérification avant chaque action en ligne • Développer des réflexes de vigilance accrue pendant les périodes de fêtes

1.1.13 Février-Mars 2028 – Envoi le 8 février 2028

Sanitaire	**Chatbot - Ingénierie sociale**	Les cybercriminels jouent sur les biais cognitifs pour vous leurrer ! Le chatbot vient faire le point avec vous ! 🎯 Objectifs pédagogiques : • Identifier les attaques d'ingénierie sociale • Adopter les bons réflexes pour éviter de se faire piéger.
Social et médico-social, DAC	**Vidéo interactive – Mots de passe**	Parcours Microlearning composé d'une vidéo interactive comprenant des activités (5 min). De l'importance d'avoir un mot de passe fort et des règles à adopter. 🎯 Objectifs pédagogiques : Comprendre l'importance de créer des mots de passe robustes pour protéger ses comptes. Savoir comment gérer ses mots de passe de manière sécurisée

1.1.14 Mars 2028 – Envoi le 5 mars 2028

Sanitaire, Social et médico-social, DAC	**Evaluation à froid : Enquête d'impact et de satisfaction**	🎯 Objectifs : mesurer le degré de satisfaction des apprenants, recueillir des feedbacks pour améliorer les contenus, et mesurer l'impact comportemental en situation de travail

PREREQUIS

Il est impératif que les structures bénéficiaires soient situées dans les Hauts-de-France.

1.2 Formalités

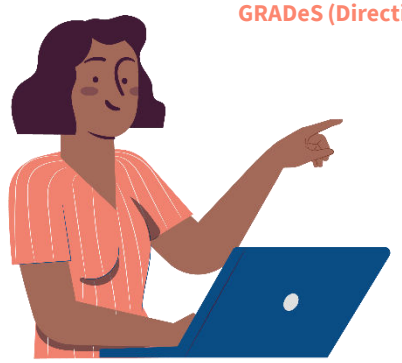
Devenir membre GRADeS Inéa (gratuit) si ce n'est pas le cas. Pour en faire la demande : **adhesion@esante-hdf.fr**

Signer le contrat d'adhésion au GRADeS (Direction)

Candidater via le formulaire d'inscription afin de transmettre les informations nécessaires à la rédaction et à l'envoi du contrat de service

Signer le contrat de service de sensibilisation à la cybersécurité

Transmettre de façon sécurisée via la page de dépôt Bluefiles de l'équipe Cyber Inéa, la liste des utilisateurs destinataires des campagnes de sensibilisation



Pour nous transmettre la liste des adresses mails des destinataires de la campagne, nous vous prions d'utiliser le fichier Excel « **2026-2028_Tempate_fichier_destinataires** » fourni dans le mail, et de le déposer complété sur la page de dépôt sécurisée du GRADeS Inéa : https://bluefiles.com/santnumeriquehdf/page-depot-equipecyber

⚠️ **Attention, il est impératif de remplir de manière exhaustive le document afin de bénéficier de statistiques complètes. Des indications de complétude sont fournies sous forme de notes dans le fichier Excel afin de vous aider. Les colonnes en vert sont des renseignements obligatoires à nous transmettre afin de permettre l'envoi de la campagne.**

1.3 Les paramétrages techniques

Pour permettre la bonne réception des courriels envoyés depuis la plateforme de sensibilisation Sensiwave, les IPs et noms de domaine des serveurs de messagerie sortants sont à inscrire en liste blanche (whitelister) :

- Principale : 35.181.11.152
- Backup : 195.154.231.91
- Hostname : postal.sensiwave.com; mail2.sensiwave.com; mail3.sensiwave.com

Vous pouvez également mettre en liste blanche les URLs suivantes (Mail + Web si vous utilisez un outil de filtrage ou un proxy) :

https://*.sensiwave.com
https://medias.sensiwave.com
https://fonts.googleapis.com
https://fonts.gstatic.com
https://use.fontawesome.com
https://cdn.ckeditor.com

Les URL de connexion des apprenants os utilisateurs seront renvoyés vers une url se présentant par défaut comme ceci : https://v3.sensiwave.com/votre_nom_entreprise/

Concernant l'exercice de phishing, il est nécessaire de whitelister les domaines et URL suivants :

- z3.tel, z4.tel, z5.tel, z6.tel, z7.tel

Quelques explications quant à ce whitelisting :

Sensiwave respecte des règles antispam et des standards de protection de la messagerie : DKIM, SPF, DMARC... L'éditeur a déclaré ses serveurs de mails auprès de nombreux hébergeurs pour éviter le blocage d'envoi de courriels. Toutefois, le circuit suivi par un mail de l'émetteur au destinataire passe par d'autres intermédiaires : les mails peuvent être hébergés chez des prestataires connus qui en général laissent passer les mails de Sensiwave, mais ils arrivent ensuite sur les systèmes de messagerie du destinataire pour lesquels les équipes IT peuvent appliquer leurs propres règles : limite du nombre de messages par heure sous peine de blocage temporaire ou définitif, filtrage de certaines plages d'adresses IP, blocage de certains mots-clés...

Une fois que Sensiwave a livré le message avec succès sur un serveur de mail, le traitement qui en est fait ne peut pas être connu (ex : mise en quarantaine). Il faut donc d'assurer que les adresses IP des serveurs de messagerie Sensiwave soient mis en liste blanche (whitelisting) sur les serveurs de messagerie en réception des mails de sensibilisation ou de faux phishing, et que les noms de domaines utilisés sur Sensiwave soient également mis en liste blanche des outils antispam.

Une campagne test sera envoyée à l'adresse électronique de/des personnes désignées destinataires des statistiques dans le fichier des destinataires de la campagne.

COMMUNICATION NECESSAIRE DE LA DIRECTION

1.4 Communication interne : un levier clé pour la réussite des campagnes de sensibilisation

Pour assurer un bon **taux de participation**, il est essentiel que les **équipes de Direction** (DSI, RSSI ou Direction Générale) s'impliquent activement en **communiquant dès le lancement** du programme. Des **rappels réguliers** sont également nécessaires pour maintenir l'engagement des professionnels tout au long des campagnes. En effet, **la qualité de la communication interne** joue un rôle déterminant dans **l'adhésion** des équipes aux actions de sensibilisation à la cybersécurité.

1.5 Soutien à la communication par le GRADeS

Le GRADeS met à disposition des **modèles de courriels** prêts à l'emploi pour accompagner les établissements :

1.5.1 Mail de lancement

Objet : Lancement du programme de sensibilisation à la cybersécurité

Bonjour à toutes et à tous,

Vous le savez, les établissements sanitaires, sociaux et médico-sociaux sont aujourd'hui des cibles privilégiées des cyberattaques.
L'actualité nous rappelle régulièrement que ces menaces sont bien réelles, et que leurs conséquences peuvent être lourdes, tant pour nos structures que pour les professionnels et les usagers.

Dans la majorité des cas, les failles de sécurité proviennent d'erreurs humaines : mot de passe faible, pièce jointe piégée, lien malveillant...
Face à ces risques, notre établissement, en partenariat avec le GRADeS Inéa Santé Numérique, déploie un **programme de sensibilisation à la cybersécurité**.

🎯 **Objectif :**

Vous transmettre, les bons réflexes à adopter pour réduire les risques et renforcer notre sécurité numérique collective.

Comment cela fonctionne ?

- Chaque deux mois, vous recevrez par courriel un ou deux module(s) **interactif(s)**
- Chaque vidéo abordera une **thématique clé** de cybersécurité avec des conseils simples et concrets sur votre espace personnel.

ℹ️ **Une question ?**

L'équipe **RSSI / DSI** reste disponible pour répondre à vos interrogations ou accompagner votre montée en compétences.
(À adapter selon votre structure)

Nous comptons sur votre participation active : la cybersécurité est l'affaire de tous.

1.5.2 Mail de rappel des vidéos de sensibilisation

Objet : Rappel des vidéos de sensibilisation

Bonjour à tous,

Les vidéos de sensibilisation à la cybersécurité de ce mois-ci arriveront très prochainement dans votre boîte mail.

Elles vous seront adressées par l'expéditeur grades-inea@sensibilisation.com, vous pouvez cliquer sur le lien sans crainte, en vérifiant bien l'adresse d'expédition et le lien de redirection. Pour information, il est indispensable de regarder la vidéo dans son intégralité, de répondre au quiz ET de dérouler le diaporama pour que votre participation soit prise en compte et la sensibilisation validée.

Remarque : les mails seront adressés par le GRADeS. Une redirection sera faite vers un site Web via le lien suivant : https://v3.sensiwave.com/

Nous vous remercions d'avance de votre sérieux dans le suivi de cette formation.

La cybersécurité est l'affaire de tous !

1.5.3 Support de communication

Nous proposons différents supports en complément de vos communications internes au travers du kit de sensibilisation « Les bons gestes cyber » en version dématérialisée ou en version papier animé au travers d'un stand de sensibilisation en établissement.

Pour bénéficier de ce kit, merci de prendre contact avec la chargée d'accompagnement de votre territoire.

Retrouvez leurs contacts sur notre site internet : https://esante-hdf.fr/contact/

VIE DE LA CAMPAGNE

1.5.4 Relances

Des relances automatiques sont programmées à J+14 et J+28 pour les utilisateurs n'ayant pas encore participé ou pas encore terminé la campagne.

1.5.5 Lecture des statistiques

Durant cette campagne, les personnes indiquées comme destinataires des statistiques dans le Fichier Excel fourni recevront par mail des statistiques de suivi, à l'issue de chaque campagne.

Les statuts de suivi de la campagne sont les suivants :

➢ Un utilisateur est « en cours » dès lors qu'il s'est connecté à la campagne

➢ Un utilisateur a « terminé » lorsqu'il a parcouru toutes les slides et effectué toutes les activités du ou des parcours, en fonction du score de progression indiqué lors du paramétrage de la campagne

➢ Le statut « réussi » dépend des valeurs définies au moment du paramétrage de la campagne (pourcentage de score + pourcentage de progression)

➢ Le pourcentage « Score moyen » est égal au score moyen des personnes qui ont terminé (on ne compte pas les en-cours)

Le total des utilisateurs abonnés à la campagne correspond à la somme des « pas connectés », des « en cours » et des « terminés ».

1.5.6 Statistiques d'une campagne de phishing

Le courriel de faux phishing est constitué d'un corps de mail contenant des liens cliquables piégés ; ce sont donc uniquement les clics sur les liens piégés contenus dans ce courriel qui sont comptabilisés. Un clic amène sur un contenu de sensibilisation :

1. Vous avez été piégé, mais ce n'était qu'un test.
2. Présentation des indices qui auraient permis de ne pas cliquer.
3. Rassurer sur le fait que rien n'a été envoyé/enregistré.

Les états indiqués dans le rapport peuvent donc être :

➢ Non cliqué « not connected » : l'utilisateur n'a pas cliqué sur le lien contenu dans le courriel.

➢ Cliqué et piégé « completed » : l'utilisateur a cliqué sur un des liens contenus dans le courriel.

1.5.7 Mise à jour du fichier « Utilisateurs »

Le fichier Excel peut être mis à jour une fois au cours de la campagne. Pour ce faire, il est nécessaire de nous transmettre le fichier initial en y ajoutant les nouveaux collaborateurs et en indiquant « non » dans la colonne « Actif » pour les personnes ayant quitté vos effectifs. Cette mise à jour est utile afin de garantir une bonne cohérence de vos statistiques.

1.5.8 Fin de la campagne

La campagne prendra fin en mars 2028. Vous pouvez également annuler la participation de votre structure à tout moment et vous retirer de la campagne.