Webinaire Cyber ESMS

29 août 2023

Ordre du jour

- Présentation Appel à candidature Renforcement de la cybersécurité
- Présentation des nouveaux parcours de la plateforme e-learning Cyber ESMS

Appel à candidature

Déploiement & Accompagnement des Conseils départementaux

Contexte

Contexte national :

- Au premier semestre 2023, le **chantier national cybersécurité social et médico-social** a permis de mener :
  - Une concertation auprès de 60 organismes gestionnaires
  - 8 ateliers de co-construction avec les acteurs du secteur
  - Un plan d'action 2023/2027 ambitieux, adapté, et cohérent avec la feuille de route sanitaire.

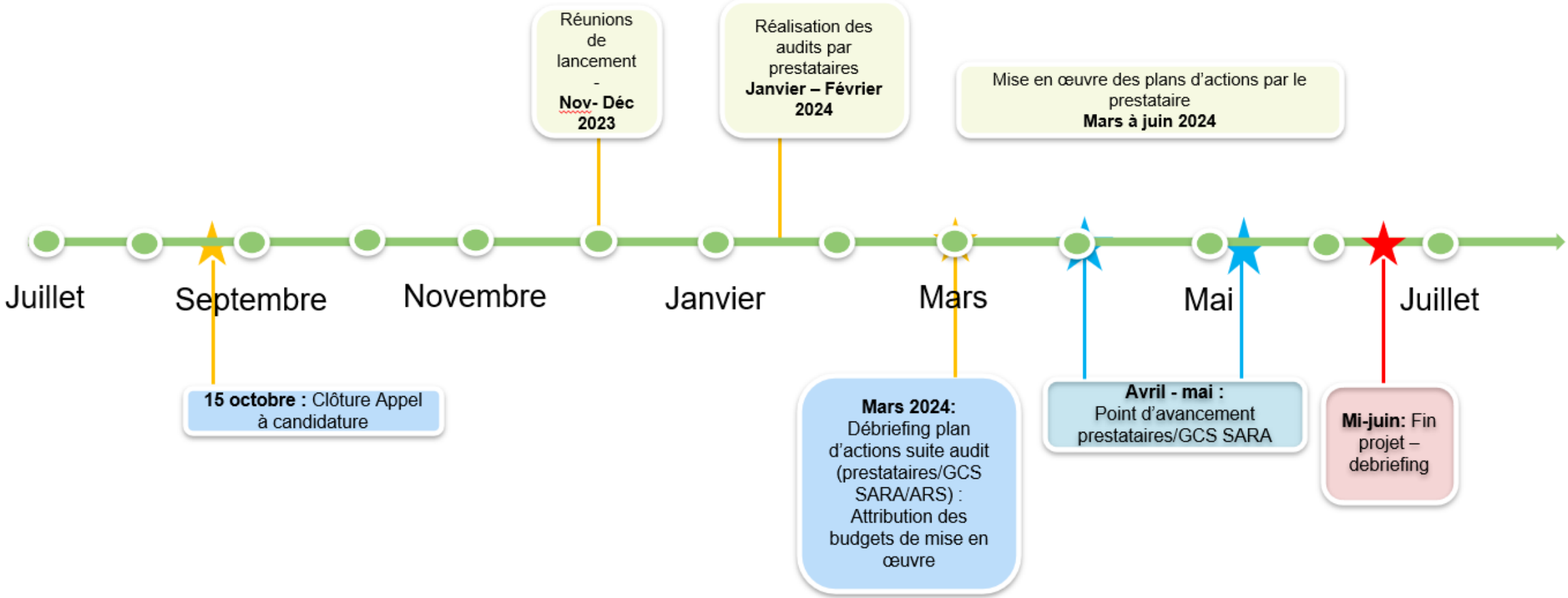
- **Le plan CARE** : plan de financement uniquement sanitaire dans un premier temps mais qui est en train d'être élargi au secteur médico-social, prévoit un plan ambitieux de mesures et actions pour améliorer la sécurité des SI. Néanmoins, pour le moment, aucun budget précis n'a été fléché pour le médico-social.

- **La grille Maturin MS** : une grille produite par l'observatoire des SI, pour évaluer le niveau de maturité des SI et qui a vocation à devenir obligatoire (devra être remplie par l'ensemble des ESMS)

Ambition régionale :

- Déterminer la capacité des établissements à pouvoir renseigner eux-mêmes des grilles d'évaluation
- Evaluer d'un point de vue méthodologique l'accompagnement à réaliser auprès des établissements dans leur diagnostic et mise en œuvre de plan d'action pour améliorer leur maturité en matière de cybersécurité.

Calendrier


Réunions de lancement - Nov- Déc 2023
Réalisation des audits par prestataires Janvier – Février 2024
Mise en œuvre des plans d'actions par le prestataire Mars à juin 2024
Juillet
Septembre
Novembre
Janvier
Mars
Mai
Juillet
15 octobre : Clôture Appel à candidature
Mars 2024: Débriefing plan d'actions suite audit (prestataires/GCS SARA/ARS) : Attribution des budgets de mise en œuvre
Avril - mai : Point d'avancement prestataires/GCS SARA
Mi-juin: Fin projet – debriefing

Modalités de candidature

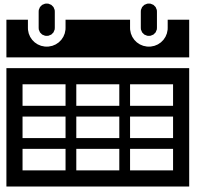
- Répondre au questionnaire suivant avant le 15 octobre à minuit
- Pièces à fournir dans l'appel à candidature
  - Une note de présentation expliquant la motivation de l'OG
  - Une lettre d'engagement signée, précisant que l'organisme gestionnaire s'engage à se rendre disponible (ainsi que les professionnels identifiés) pour la bonne réalisation des audits et de la mise en place des actions, sous respect d'un délai de prévenance de 15 jours à minima par le prestataire
- Priorisation en fonction des niveaux de risques (secteur/taille de l'OG/niveau de maturité existant)
- Nécessité d'avoir un interlocuteur identifié pour les échanges avec le prestataire en charge de l'audit

Nouveaux parcours e-learning

Mise en oeuvre

1. Tous les établissements en région ARA sont éligibles
2. Accès gratuit
3. Support et administration des comptes réalisés par le GCS SARA :
   - Un compte référent (ou plus) pour chaque établissement
   - Nombre de comptes utilisateurs illimités et organisés en population structurée (ex : équipe médicale, médecins, infirmières, etc.)
4. Plan de sensibilisation proposé à l'échelle régionale :
   - 2 programmes de sensibilisation fixés à diffusion mensuelle avec une vidéo quiz courte (<3 minutes)
   - 7 programmes de sensibilisation annuels sans contrainte de diffusion (composé de plusieurs vidéos ; <25 minutes)
   - Un programme de campagne de mails factices d'hameçonnage (Phishing) proposé chaque trimestre

Programme mensuel : principes



- Un parcours thématique différent chaque mois composé d'une seule vidéo (<3min) avec 2 ou 3 questions
- Démarrage du premier parcours le 2/10/2023 ; fin du dernier parcours le 31/09/2024
- En début de mois, les utilisateurs inscrits reçoivent un mail redirigeant vers une vidéo courte, d'une durée d'environ 2 minutes, qui reprend une grande thématique cyber
- Un mail de relance est envoyé en milieu de mois pour les participants qui n'ont pas commencé ou terminé le parcours
- Il n'est pas possible de revoir une vidéo thématique mensuelle après son slot de diffusion (autrement dit et en exemple, si l'inscription est faite en novembre 2023, il ne sera pas possible pour les participants de revoir la vidéo d'octobre 2023)

Parcours thématiques pour ESMS

Capsule micro-Learning

Parcours thématiques pour ESMS

Mois	Année	Campagne	Module	Thématique	Début	Fin	Validité	Durée
10	2023	2023-MF10-ESMS-Sensibilisation Phishing	[ESMS] Phishing - Lien	PHISHING	01-oct	01-nov	31,00	01:37
11	2023	2023-MF11-ESMS-Sensibilisation Ransomware	[ESMS] Utilisation d'applications non approuvées	CODE MALVEILLANT	01-nov	01-déc	30,00	01:37
12	2023	2023-MF12-ESMS-Sensibilisation Bonnes pratiques IT	[ESMS] Réagir en cas d'attaque	BONNES PRATIQUES IT	01-déc	01-janv	31,00	01:15
1	2024	2024-MF01-ESMS-Sensibilisation Sécurité de l'authentification	[ESMS] Une session, un utilisateur	SÉCURITÉ DE L'AUTHENTIFICATION	01-janv	01-févr	31,00	03:00
2	2024	2024-MF02-ESMS-Sensibilisation Usage Pro Perso	[ESMS] Usage pro/perso	USAGE PRO PERSO	01-févr	01-mars	29,00	01:58
3	2024	2024-MF03-ESMS-Sensibilisation Mobilité	[ESMS] Données sensibles en déplacement	MOBILITÉ	01-mars	01-avr	31,00	01:20
4	2024	2024-MF04-ESMS-Sensibilisation Applications mobiles	[ESMS] Demandes d'accès données - applications mobiles	APPLICATION MOBILES	01-avr	01-mai	30,00	01:56
5	2024	2024-MF05-ESMS-Sensibilisation Protection de l'information	[ESMS] Mises à jour	PROTECTION DE L'INFORMATION	01-mai	01-juin	31,00	01:39
6	2024	2024-MF06-ESMS-Sensibilisation Bonnes Pratiques IT	[ESMS] Session ouverte	BONNES PRATIQUES IT	01-juin	01-juil	30,00	02:13
7	2024	2024-MF07-ESMS-Sensibilisation Phishing	[ESMS] Phishing - Piece Jointe	PHISHING	01-juil	01-août	31,00	01:40
8	2024	2024-MF08-ESMS-Sensibilisation Ingénierie sociale	[ESMS] Utilisation Wifi Public	INGÉNIERIE SOCIALE	01-août	01-sept	31,00	01:52
9	2024	2024-MF09-ESMS-Sensibilisation Mot de passe	[ESMS] Mot de passe	MOT DE PASSE	01-sept	01-oct	30,00	02:20

Programme annuel

➢ Principe : 7 parcours thématiques différents et à la carte - Durée de validité : un an

Livre Interactif - Les 7 erreurs les plus courantes en cybersécurité	• Disponibilité : du 1/10/23 au 1/10/2024 • Inscription à tout moment • Durée : 15mn
Livre interactif - Guide du nouvel arrivant	• Disponibilité : du 1/10/23 au 1/10/2024 • Inscription à tout moment • Durée : 20mn
Livre interactif - Protection des données de santé	•Disponibilité : du 1/10/23 au 1/10/2024 •Inscription à tout moment •Durée : 20mn
Livre interactif - Se poser les bonnes questions	• Disponibilité : du 1/10/23 au 1/10/2024 • Inscription à tout moment • Durée : 15mn
Parcours de sensibilisation ES	•Disponibilité : du 1/10/23 au 1/10/2024 •Inscription à tout moment •Durée : 20mn
Parcours de sensibilisation ESMS	• Disponibilité : du 1/10/23 au 1/10/2024 • Inscription à tout moment • Durée : 20mn
Parcours de sensibilisation des cadres	• Disponibilité : du 1/10/23 au 1/10/2024 • Inscription à tout moment • Durée : 15mn

Remarque : attention sur le vocabulaire utilisé (exemple : « entreprise » au lieu d'établissement »)

Livre Interactif - Les 7 erreurs les plus courantes en cybersécurité

Le saviez-vous ?

85% des failles informatiques utilisées par les pirates
sont le fait d'erreurs commises par les utilisateurs.

Comment éviter qu'elles ne profitent aux attaques pirates ?

Découvrez les 7 erreurs les plus fréquemment commises en cybersécurité.

Adoptez les bons comportements pour les éviter !

Utiliser plusieurs fois
un même mot de passe

Cliquer sur un lien
dans un email de phishing

Ne pas verrouiller
son poste de travail

Utilisez des outils
non validés par l'entreprise

Ne pas protéger ses informations
sensibles en déplacement

Etre trop bavard
sur les réseaux sociaux

Ne pas mettre à jour
ses applications

Livre Interactif - Guide du Nouvel Arrivant

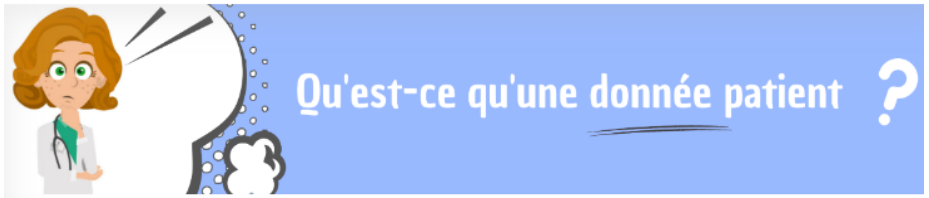
Ayez les cyber réflexes !

La cybersécurité est primordiale au maintien et au développement de notre activité

En adoptant quelques cyber-réflexes, chacun de nous participe à renforcer considérablement nos défenses face aux cybermenaces.

Votre collaboration sur ces sujets est donc essentielle !

Livre interactif - Protection des données de santé



Livre interactif - Se poser les bonnes questions

Se poser les bonnes questions...

...quand je choisis un mot de passe

Se poser les bonnes questions...

...quand je navigue sur Internet

Se poser les bonnes questions...

...quand je reçois un e-mail

Se poser les bonnes questions...

...quand je reçois ou croise un visiteur

Se poser les bonnes questions...

...quand je travaille à distance

Se poser les bonnes questions...

...quand je suis à mon poste de travail

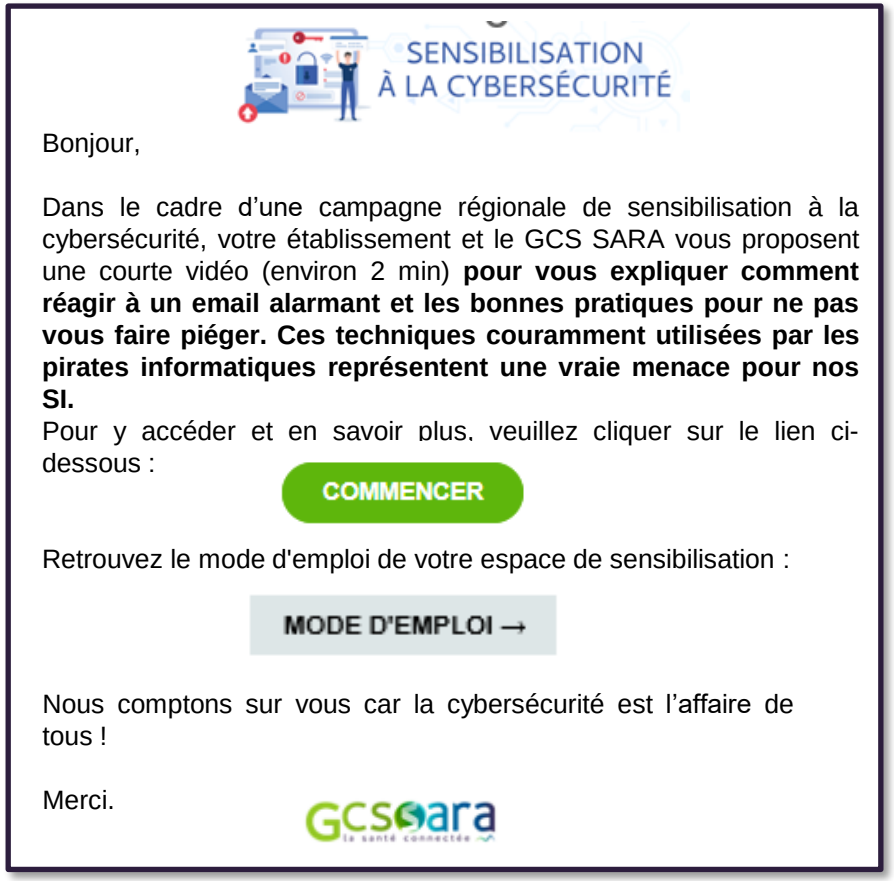
Parcours sensibilisation ESMS

Parcours de sensibilisation « Cadres »

- La menace : les types d’attaques
- Retex CHU Dax et CHSF
- Offre de service du CERT Santé

3 vignettes

Programme mensuel



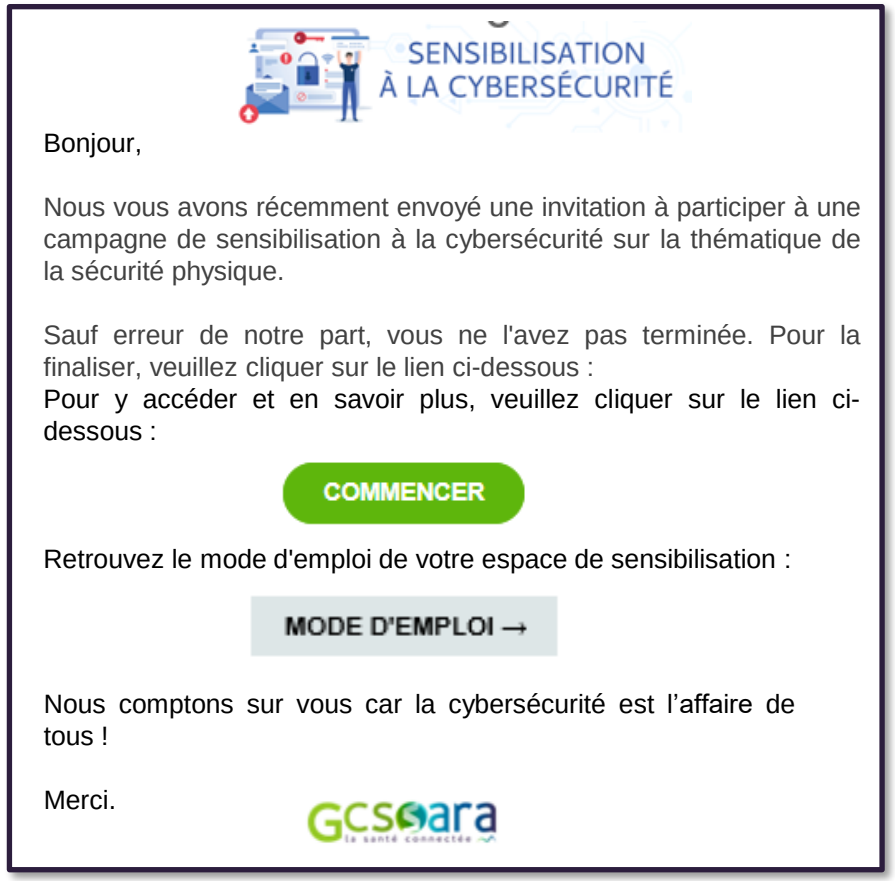
Description du mail reçu par chaque participant :

- Adresse d'émission : ***gcs-sara@sensibilisation.com***
- L'émetteur du mail sera identifié comme **« GCS Sara »**
- Logo « **Sensibilisation à la Cybersécurité** » en entête dans le corps du mail
- Logo GCS SARA en pied de page dans le corps du mail
- L'utilisateur devra suivre le lien indiqué dans le mail afin de visualiser le contenu de sensibilisation du mois (bouton COMMENCER).
- Le mail sera adapté en fonction du contenu.
- Un lien permettra également d'accéder à un mode d'emploi (bouton MODE D'EMPLOI)

Important : Il est nécessaire qu'en parallèle le RSSI, la Direction et/ou la DSI informe au préalable de l'envoi de cette campagne.

Programme mensuel

- Un **mail de relance** sera envoyé en milieu de mois pour les utilisateurs n'ayant pas commencé ou terminé un parcours thématique. Exemple :

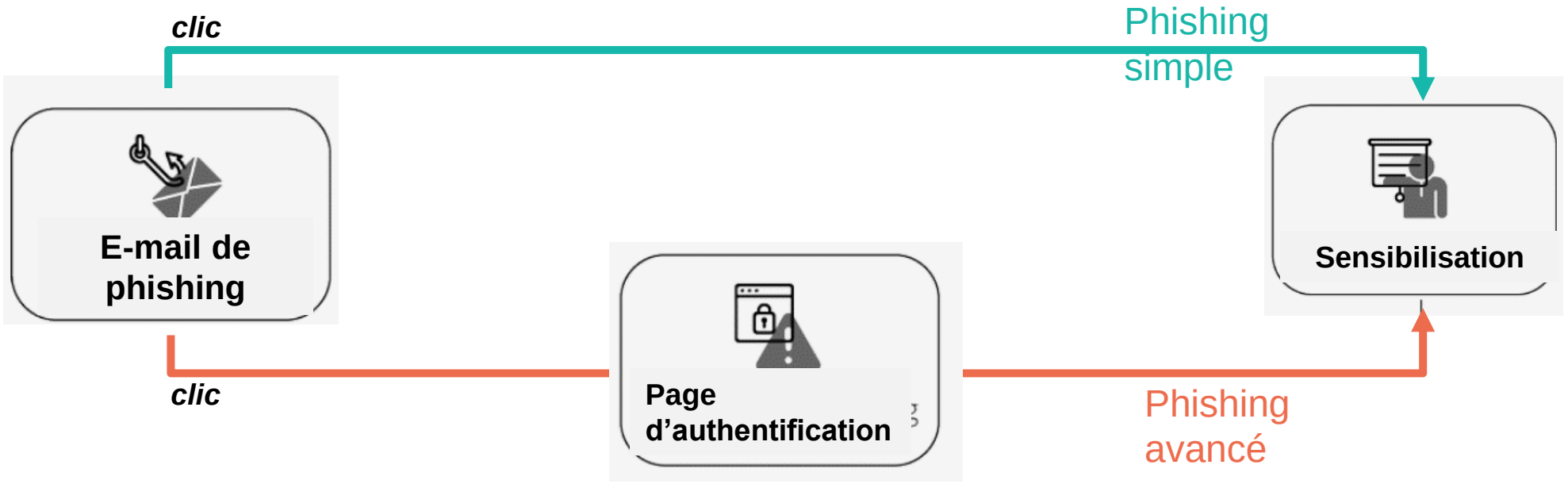


Mail factice d’hameçonnage (Phishing)

Campagnes d'hameçonnage : 2 options

Réalisation de campagnes d'hameçonnage (ou phishing) avec deux modes possibles :

- **Simple :** clic sur lien dans email frauduleux redirection vers contenu de sensibilisation
- **Avancé :** clic sur lien dans email frauduleux redirection vers une page d'authentification validation et redirection vers contenu de sensibilisation



NB : Informations non sauvegardées

Exemple d’hameçonnage simple

Piégé

Mail de phishing

Module d’explication

Exemple d’hameçonnage avancé

Piégé

Objet : Bioaxiome : consultation de vos résultats en ligne

Bonjour,

Votre dernier compte-rendu d'analyses de biologie est disponible, veuillez cliquer sur le lien suivant afin d'y accéder : **serveur de résultats**

Numéro de dossier : PO2202245087
Date du dossier : 06/06/2022
Date d'envoi des résultats : 06/06/2022 23:23

Si le message d'erreur "Le certificat de sécurité de ce site Web présente un problème." est affiché, merci de bien vouloir cliquer sur "Poursuivre avec ce site Web."
*Si vous n'arrivez pas à ouvrir le fichier PDF du compte-rendu sur le site, vous devrez télécharger et installer un logiciel gratuit de lecture PDF, par exemple : **Adobe Reader***

Cordialement,

3L LABORATOIRE DE BIOLOGIE

Mail de phishing

VOSANALYSES

Le portail internet de mon laboratoire d'analyses médicales

Saisissez vos identifiants

Nom

Prénom

Fonction

Les données transmises sont chiffrées (redirection vers un site https)

Récupérer mon compte rendu

Nous vous rappelons que vos résultats sont disponibles à la date prévue lors de votre prélèvement et pour une durée de 7 jours. Si vous en avez fait le choix auprès de votre laboratoire, la date de mise à disposition de vos résultats peut vous être notifiée par SMS.

Pour accéder à vos résultats au format PDF, entrez votre nom, prénom ou fonction dans le cadre en haut à gauche de ce site.

Page d’authentification

Ceci était une tentative de phishing

Heureusement, ce n'était qu'un test à vocation pédagogique :

- vous avez reçu un email et cliqué sur le lien alors que vous n'auriez pas dû,
- puis vous avez saisi des informations sur un faux site Microsoft.

Découvrez les indices qui auraient pu vous alerter...

SUIVANT

1 / 6

Module d’explication

Sensibilisation ciblée pour les personnes piégées

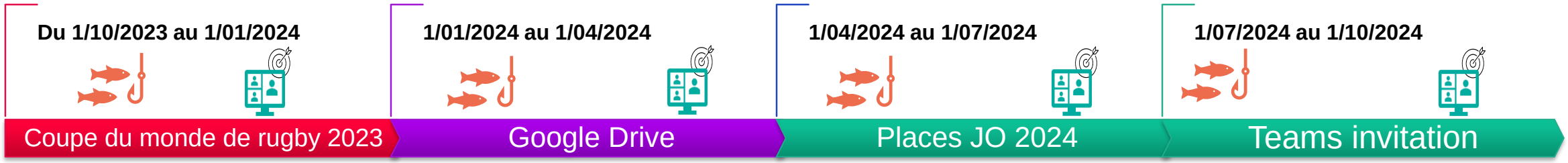
Phishing : les bonnes pratiques

Ransomware

Le phishing ciblé

Campagnes d’hameçonnage (faux Phishing)

Programme de mails factices (combinaison de faux phishing simple et avancé)



Tests phishing

Sensibilisation ciblée pour les personnes piégées

Calculer son "Score Phishing"

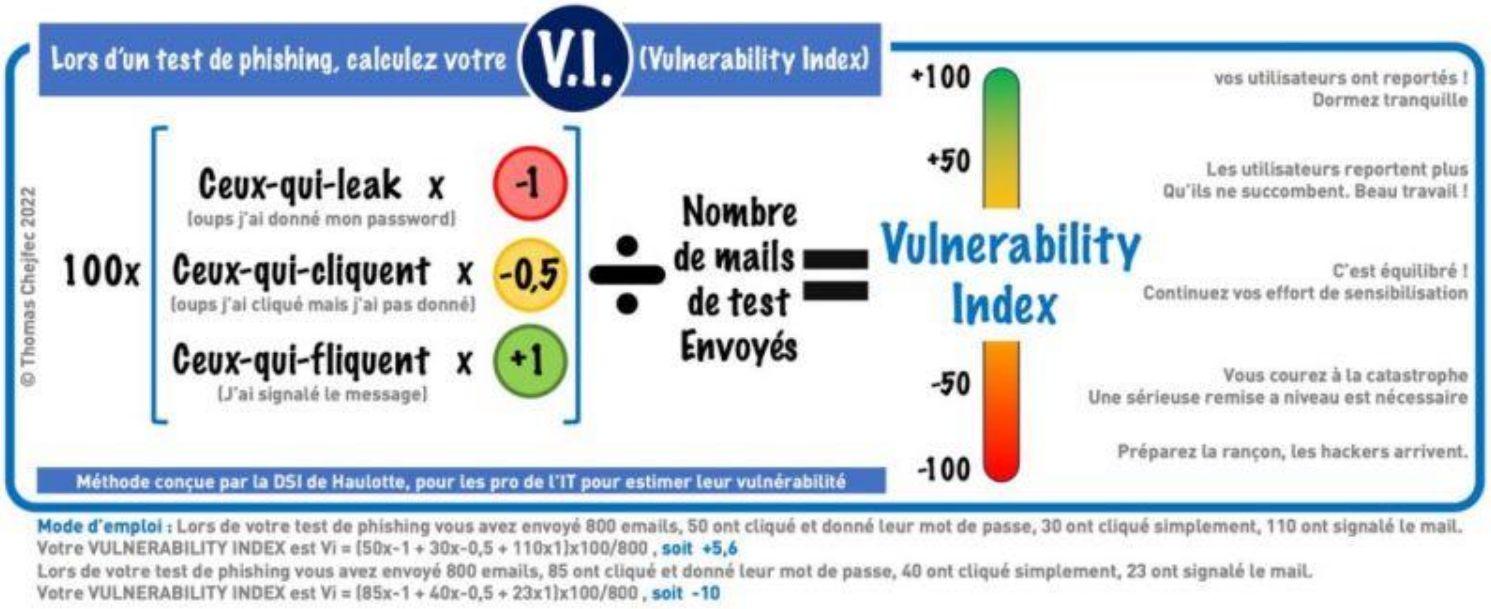
Méthode qui consiste à calculer son score phishing (index de vulnérabilité) sur une campagne phishing en utilisant la formule ci-dessous :

- Index de vulnérabilité = pourcentage de la somme des "scores phishing", divisé par le nombre de mails envoyés

Base de calcul du "score phishing" :

- Un utilisateur qui donne ses informations : -1
- Un utilisateur qui ne clique pas et ne signale pas le mail à la DSI, RSSI, etc. : 0
- Un utilisateur qui clique sur le lien : -0.5
- Un utilisateur qui signale le mail : +1

Si votre score égale à 100, vous pouvez dormir tranquille.



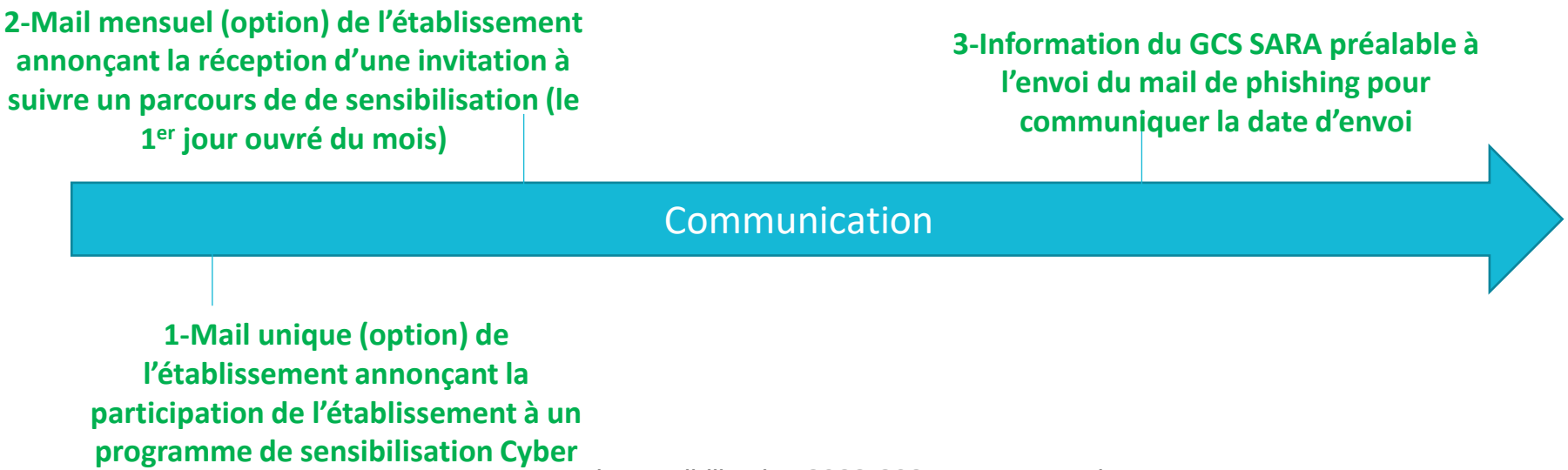
Préparation préalable

Mailing : rôle de « sponsor » indispensable de la direction, RSSI, DSI

- Pour permettre aux campagnes de sensibilisation d'être regardées par le maximum des utilisateurs, il est indispensable qu'au niveau RSSI/Direction et/ou DSI, **une communication et des rappels réguliers soient adressés pour permettre une adhésion maximale au programme.** Cette communication permettra aussi d'apporter de la légitimité aux emails adressés par le GCS SARA.

  Remarque : Une différence notable **dans les taux de participation** est observée en fonction de la communication interne ou non par l'établissement.

- Le GCS SARA mettra à disposition des mailings à adresser à différents moments du programme. **Nous vous encourageons vivement à diffuser au maximum ces mails.**



Exemple de mailing* interne : lancement du programme

Bonjour à tous,

Vous n'êtes pas sans savoir que les cyberattaques sont à l'origine de nombreuses difficultés pour les établissements de santé. L'actualité nous montre que la menace est constante et les conséquences graves pour les structures, les agents/salariés et parfois même les patients.*
Les risques de sécurité sont majoritairement introduits par le facteur humain : mot de passe pas assez robuste, introduction involontaire de logiciels malveillants via la messagerie…
Ces risques sont nombreux et difficilement appréhendables dans votre activité quotidienne, c'est pourquoi notre établissement, en partenariat avec le GCS SARA, lance un programme de sensibilisation sur 12 mois. Objectif : adopter les bonnes pratiques pour éviter au maximum les risques liées aux attaques.
*Chaque mois, une vidéo interactive d'une durée d'environ 2 minutes vous sera adressée à partir de l'adresse suivante : **gcs-sara@sensibilisation.com** afin d'aborder une thématique de cybersécurité et vous donner les clés pour éviter certaines attaques. Les vidéos déjà diffusées seront accessibles à tout moment sur le portail dédié et l'équipe RSSI/DSI* est à votre disposition pour répondre à vos interrogations complémentaires.*
Remarque : les mails seront adressés par le GCS Sara ; 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 du programme.
La cybersécurité est l'affaire de tous !

** A adapter au contexte de l'établissement*

Exemple de mailing* : rappel mensuel avant chaque campagne de sensibilisation

Bonjour à tous,

La vidéo de sensibilisation en cybersécurité de ce mois-ci arrivera très prochainement sur votre boîte mail, elle vous sera adressée par l'adresse ***gcs-sara@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 Quizz ET de dérouler le diaporama pour que votre participation soit prise en compte et la sensibilisation validée.

Remarque : les mails seront adressés par le GCS Sara ; 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 !

** A adapter au contexte de l'établissement*

Finalisation d'un parcours

- La participation est comptabilisée si le score du Quizz est à minima **de 60% (bonne réponse) ET** que la progression de la vidéo est **de 100%**
- Pour que la progression soit validée, il faut dérouler l'ensemble des diapositives comme il suit **ET** finir la vidéo :

Remarque : en cas de mauvaise réponse, il est possible de **Recommencer** la vidéo afin de valider son parcours et obtenir ainsi son certificat

Finalisation d’un parcours

- Certificat disponible si la condition évoquée précédemment est remplie :

GCSoara la santé connectée

Sensibilisation Phishing

Validé

A participé avec succès à la campagne de sensibilisation: **Sensibilisation Phishing**

22 Sep 2022

CERTIFIED

Certiticat Nº: 3DopbvjgjkFPioCAE6Cl9OXfiYkihNmJ

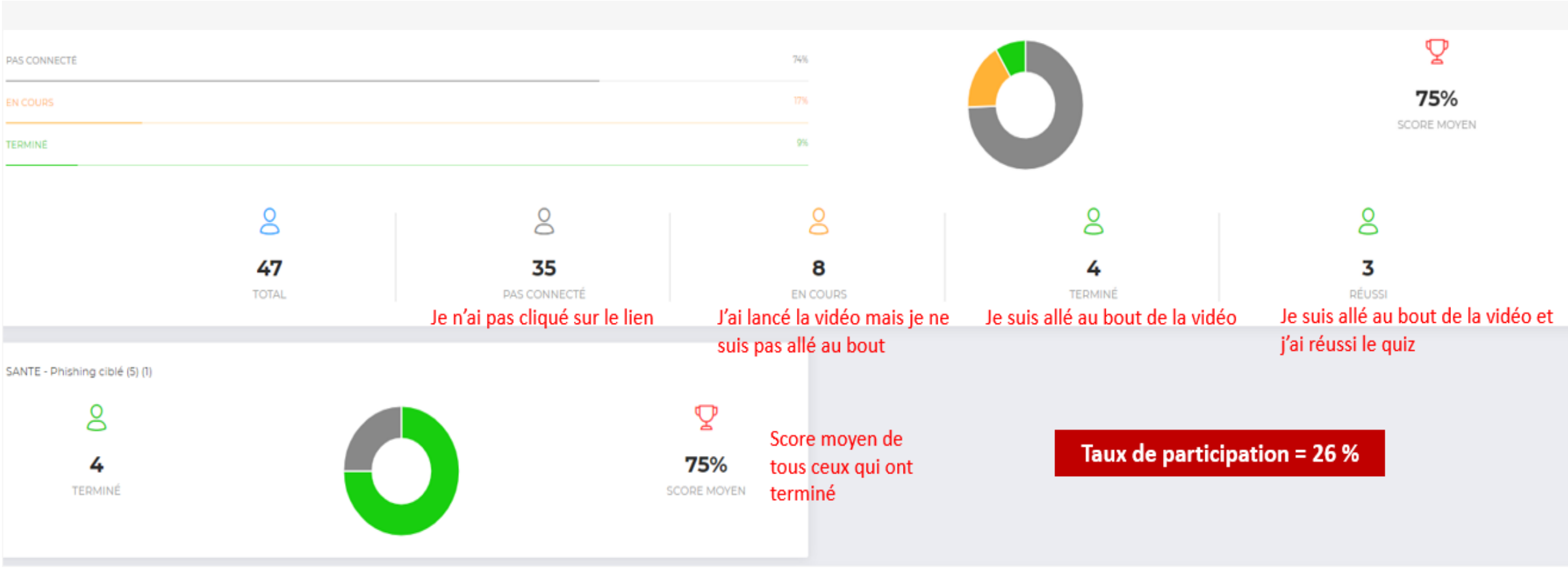
Rapports & Statistiques

Rapport de statistiques : format

- Réception de 2 mails distincts le dernier jour du mois :
  - L'un contenant un **fichier Excel** en pièce jointe
  - L'autre contenant des graphes dans le corps de mail et un **fichier PDF** en pièce jointe

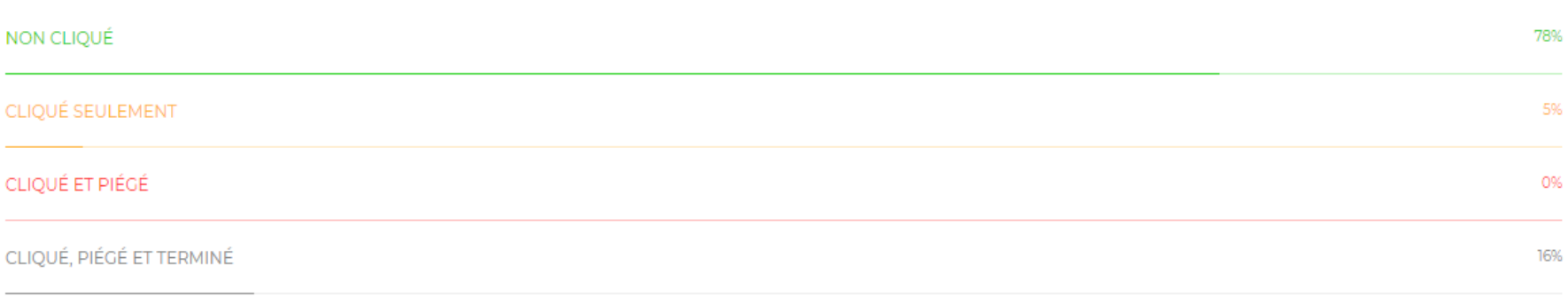
Rapport : statistiques sensibilisation

- Envoi en fin de mois



Rapport : parcours de mail factice (Phishing)

- Envoi en fin de mois

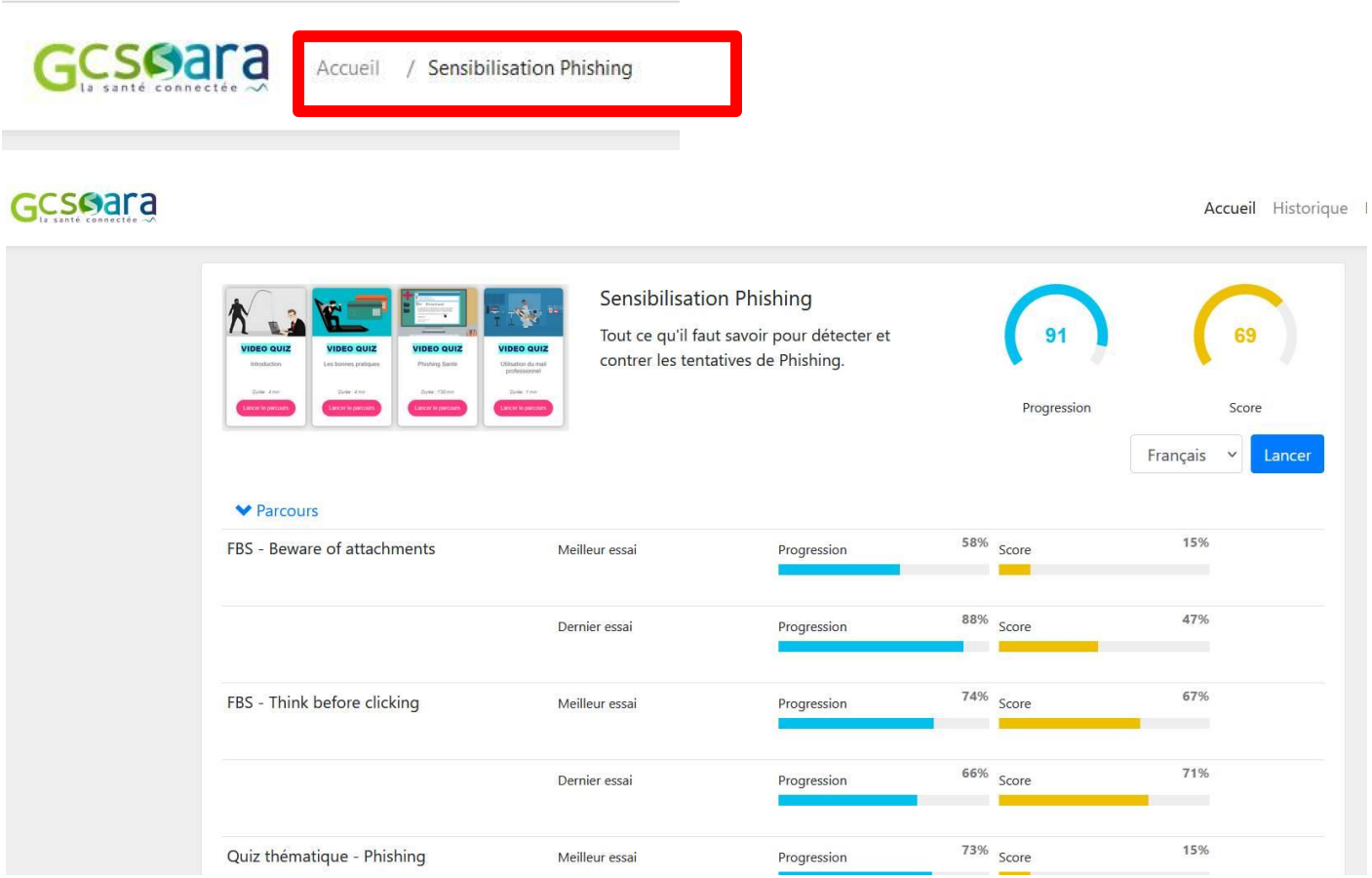


97	76	5	0	16
TOTAL	NON CLIQUÉ	CLIQUÉ SEULEMENT	CLIQUÉ ET PIÉGÉ	CLIQUÉ, PIÉGÉ ET TERMINÉ
Nombre de personnes ayant reçu la campagne	Nombre de personnes n'ayant pas cliqué sur le mail	Personne ayant cliqué sur le lien du mail uniquement	Personne ayant cliqué sur le lien, a validé le formulaire (phishing avancé) mais n'a pas suivi le module d'explication	Personne ayant cliqué sur le lien, a validé le formulaire (phishing avancé) et a suivi le module d'explication

Votre Taux de clics = 21,6 %

Tableau de bord : progression

- Un utilisateur peut retrouver sa progression en cliquant sur « Accueil » en haut à gauche dans le menu du Portail



Adhésion et kit documentaire

Adhésion : mode opératoire

➢ Avant le **1/10/2023**, merci d'effectuer les actions suivantes :

1. Renseigner le formulaire d'inscription https://forms.office.com/e/zcv3zn32R1
2. Envoyer de manière sécurisée la liste de vos utilisateurs organisée en fonction de vos services (fichier Excel à retrouver dans le kit documentaire https://shorturl.at/mqux5)
   - ➢ Le fichier doit être soit protégé par un mot de passe soit chiffré avec la solution ZED) ; le mot de passe doit être envoyé par SMS au 06601026 soixante-dix-huit en indiquant également le nom de l'établissement
3. Valider les paramétrages techniques / prérequis: autoriser la réception de mails provenant de l'adresse **gcs-sara@sensibilisation.com** et les mails de faux phishing (voir doc de paramétrages dans kit)
4. Communiquer au sein de votre établissement

Kit documentaire : contenu

- Fichier Excel des apprenants à compléter
- Mode d’emploi à destination des apprenants
- Fiches thématiques Cyber
- Guide de paramétrages techniques
- Modèles de mails de communication

Campagnes d’affichages

Affiches/posters de sensibilisation Cyber

- Afin de permettre de renforcer l'adhésion au programme de sensibilisation, le GCS SARA distribuera aux établissements participants, des affiches à disposer dans la structure
- Ces affiches reprendront des thématiques abordées durant le programme de sensibilisation
- Les thématiques sont les suivants :
  - Protections données sante
  - Mot de passe
  - Phishing
  - Ransomware
  - Ingénierie sociale
  - Poste de travail

Divers

Les navigateurs compatibles

- Microsoft Edge
- Firefox 57 et supérieur
- Google Chrome 72 et supérieur
- Safari 7 et supérieur

Proxy qui bloque la vidéo => lorsque cela arrive, il faut mettre en liste blanche les URLs suivantes :

https://*.sensiwave.com

https://sensiwave3-prod.s3.eu-west-3.amazonaws.com

En fonction de vos contenus il faut parfois y ajouter pour améliorer la présentation :

https://fonts.googleapis.com

https://fonts.gstatic.com

https://use.fontawesome.com

et

https://cdn.ckeditor.com

Glossaire

- ANSSI : https://www.ssi.gouv.fr/entreprise/glossaire/a/
  - Phishing
  - Ransomware
  - Virus
- Cyber-lexique : http://cyber-serenite.fr/cyber-lexique

Nous vous remercions de votre attention

Pour nous contacter : ssi@sante-ara.fr