Catalogue - Campagne de sensibilisation

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

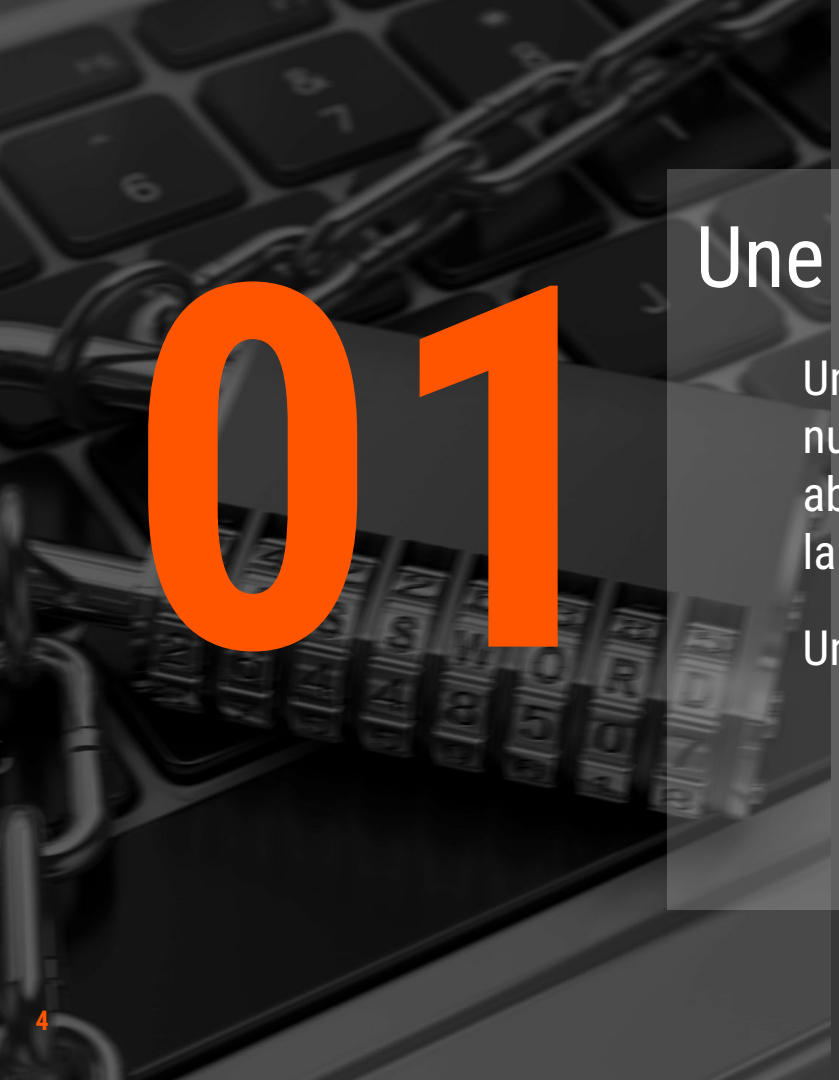
02 octobre 2023 - Hyères

CAPSI

Cellule d'Appui à la Protection des Systèmes d'Information

Sommaire

Sommaire



01

Une campagne de sensibilisation

Une campagne de sensibilisation à la sécurité numérique se traduit par la création d'un parcours abordant différentes thématiques liés au domaine de la cybersécurité.

Une telle campagne a plusieurs objectifs :

- Débuter une sensibilisation de votre personnel à l'hygiène et aux bonnes pratiques numériques ;
- Impulser une démarche de protection de votre établissement face aux cyber attaques.

Les préalables

Pour réaliser une campagne de sensibilisation vous allez devoir :

- Déterminer le choix de la forme de votre campagne : il vous faudra déterminer les modules que vous souhaitez obtenir pour la création de votre campagne
- Si votre établissement est référencé dans le ROR et vos utilisateurs décrits, une synchronisation est possible automatiquement pour enrôler vos collaborateurs sur la campagne choisie.
- Si ce n'est pas le cas, nous transmettre via notre outil de dépôt sécurisé BlueFiles, sous format CSV ou XLSX, la liste de vos utilisateurs (nom, prénom, adresse mail, nom de l'établissement)
- Nous transmettre les dates de début et de fin de campagne

Attention : nous vous rappelons qu'un parcours est personnel ce qui implique : une adresse e-mail = un compte

L'utilisateur a possibilité de débuter sa campagne et d'avancer à son propre rythme.

Nous vous conseillons de réaliser une campagne de faux phishing avant une première campagne de sensibilisation mais aussi à la fin de cette campagne.

Vous pouvez contacter l'équipe CAPSI pour obtenir le catalogue de nos faux phishing.

Côté utilisateurs :

Une fois la campagne de sensibilisation créée, vos utilisateurs recevront un mail d'invitation à participer à la campagne de sensibilisation.

Une fois leur parcours entièrement terminé, l'utilisateur reçoit un certificat (ce certificat n'a pas de valeur juridique).

Côté établissement :

Plusieurs possibilités s'offrent à vous :

- Nous pouvons automatiser les relances à la fréquence que vous souhaitez
- Nous pouvons les réaliser à votre demande qui se fera par mail

Il en est de même pour les rapports de statistiques :

- Nous pouvons automatiser l'envoi de ces rapports à la fréquence que vous souhaitez
- Ou simplement les envoyer à votre demande

Par ailleurs, nous vous proposons de vous créer un compte pour tester la solution avant de la déployer à vos utilisateur.

02

Les essentiels

Ces campagnes de sensibilisation se présentent soit :

- sous forme de saynètes et de quiz ;
- sous forme de vidéos interactives suivies de quiz.

3 possibilités sont proposées

Choix 1 : **Les essentiels de la sécurité** (saynètes)

Durée : 20 minutes

Cette campagne traite de notions essentielles :

- Mot de passe,
- Courriel,
- Protection de l'information,
- Ingénierie sociale,
- Mobilité,
- Accès physiques.

Chaque thématique est traitée par des mises en situation : des saynètes "cartoon" assorties de questions et d'explications.

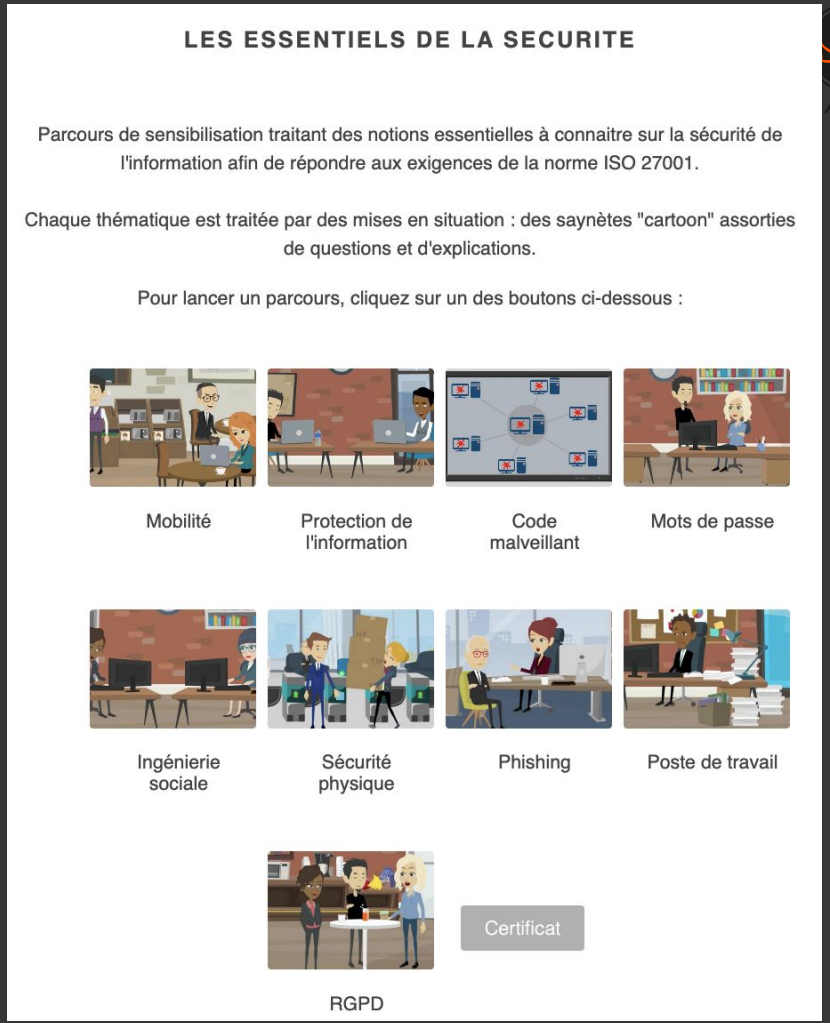
Choix 2 : **Les essentiels de la sécurité par thématiques**

(saynètes)

Durée : 20 minutes

Cette campagne traite de notions essentielles :

- Mobilité
- Protection de l'information
- Code malveillant
- Mot de passe
- Ingénierie sociale
- Phishing
- Sécurité physiques
- Poste de travail
- RGPD

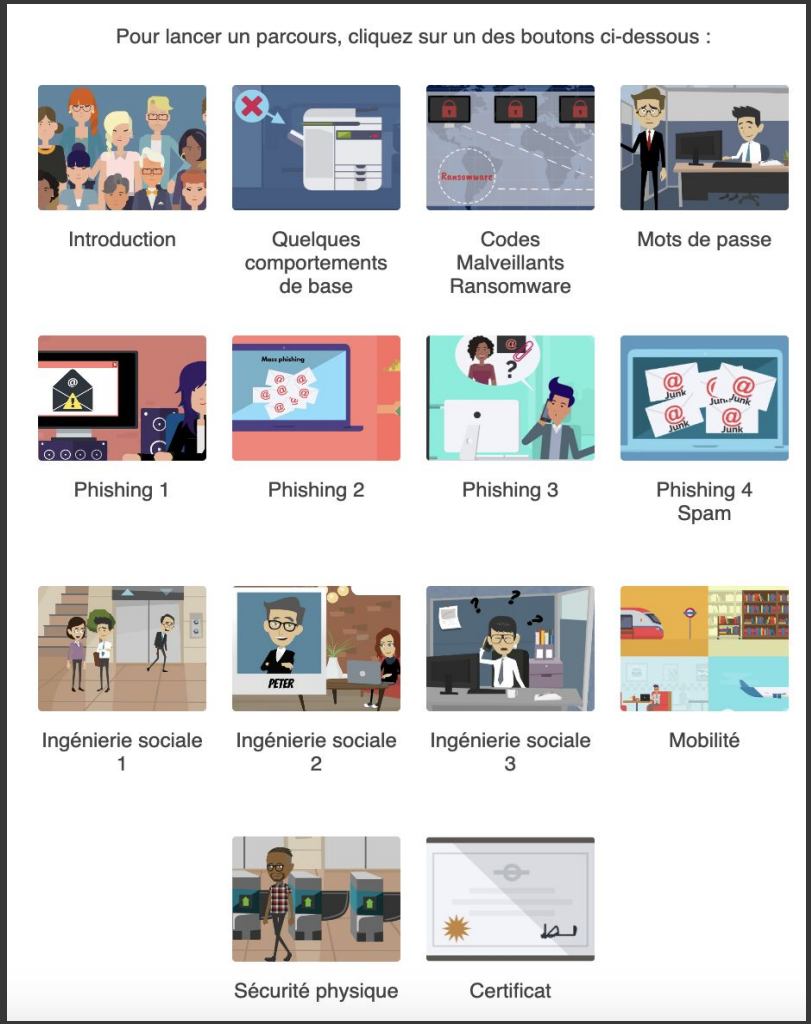


Choix 3 : **Les essentiels de la sécurité** (vidéos interactives)

Durée : 13 minutes

Cette campagne comprend 13 vidéos interactives traitant des principaux sujets en termes de sensibilisation à la sécurité de l'information :

- Les comportements de base
- Les ransomwares
- Mots de passe
- Phishing
- SPAM
- Ingénierie sociale
- Mobilité
- Sécurité physique



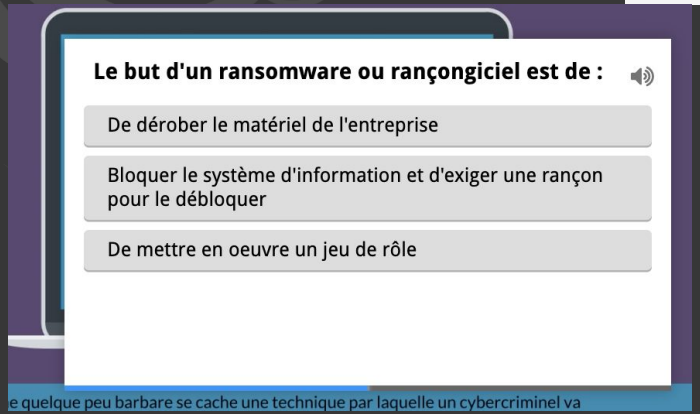
03

Les vidéos interactives

Une vidéo interactive est une capsule de microlearning constituée d'une courte vidéo qui contient 2 ou 3 quiz.

Vous pouvez donc lister les vidéos qui vous intéressent pour que nous puissions constituer votre campagne.

Ces vidéos interactives de 3 à 6 minutes maximum abordent différents thèmes (environ une cinquantaine).



Les thèmes :

- Cybercriminalité 1 : Quels acteurs et à quelles fins ?
- Cybercriminalité 2 : Moyens utilisés par les cybercriminels
- Cybercriminalité 3 : Les types d'attaques
- Cyberguerre
- Protection de l'information : Introduction
- Protection de l'information : Comportements de base
- Mot de passe
- L'authentification Double Facteur
- Ransomware
- Phishing : Introduction
- Phishing : les motivations des pirates
- Phishing : les bonnes pratiques
- Phishing : COVID-19
- Phishing : Cliquer sur un lien frauduleux
- Phishing : Cliquer une une pièce jointe frauduleuse
- Phishing : Saisir des données personnelles
- Smishing
- SPAM
- Ingénierie sociale : Introduction
- Ingénierie sociale : Anatomie d'une attaque
- Ingénierie sociale : Les bons comportements
- Deepfake Audio et Cyberattaques
- Escroquerie au président
- Mobilité
- Télétravail
- Sécurité Numérique à la maison

- Smartphone
- Objets connectés
- Réseaux sociaux
- Usurpation d’identité
- Le cloud
- Shadow IT
- Contenus illicites
- Sécurité physique
- Signalement des évènements de sécurité
- Attaque Man-in-the-middle
- Gestionnaire de mots de passe
- C'est quoi un virus informatique ?
- Navigation sûre
- Revue des habilitations
- Nouvel arrivant
- Fraude face aux fournisseurs
- Propriété intellectuelle
- Usage Pro/Perso
- Prenez le temps avant de cliquer
- Attaque aux formulaires de connexion
- Informations sensibles

04

Les livres interactifs

Le livre interactif est une forme de campagne de sensibilisation rapide qui se base sur des modules de cours (saynètes/vidéos interactives) suivis de quizz.

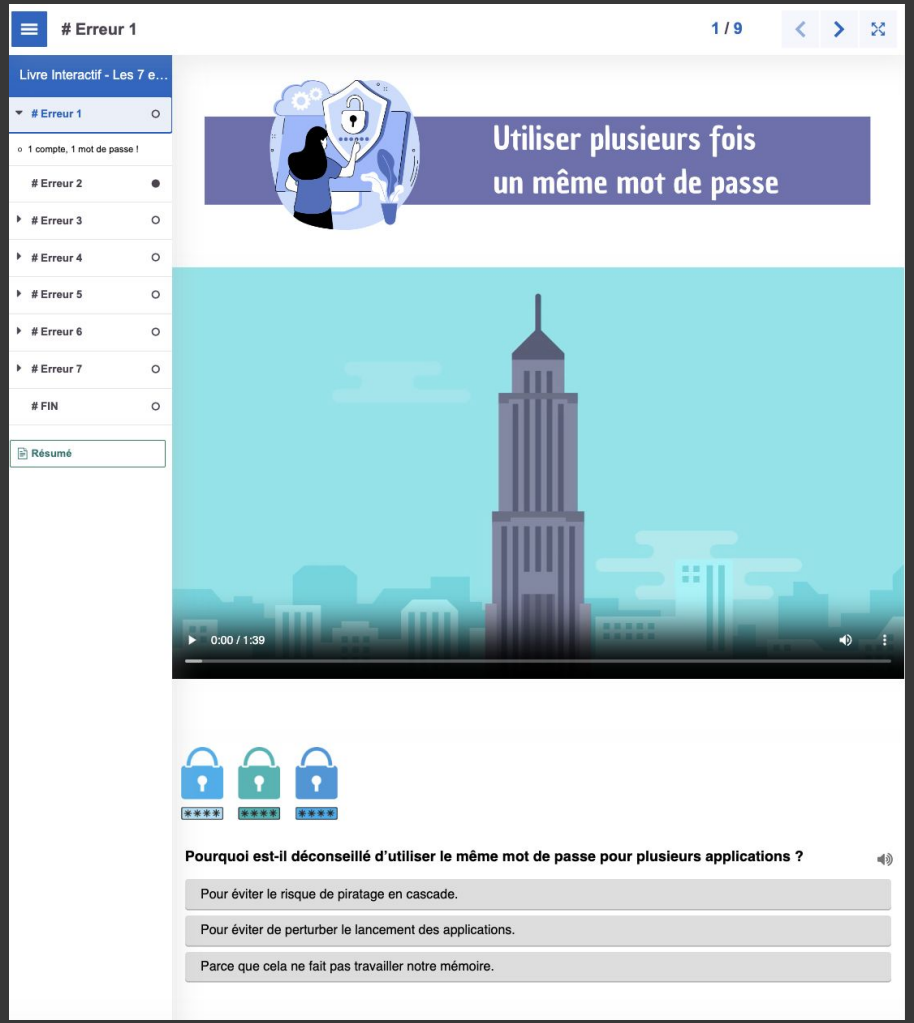
3 livres interactifs sont possibles.

Thème : **Les 7 erreurs les plus courantes en cybersécurité**

Durée : 15 minutes

Se compose de 7 modules de bases :

- Utilisation d'un même mot de passe
- Cliquer sur un lien dans un mail phishing
- Ne pas verrouiller son poste
- Utilisation d'outils non validés par la structure
- L'utilisation des réseaux sociaux
- La mise à jours des applications
- Protection des informations sensibles en déplacement

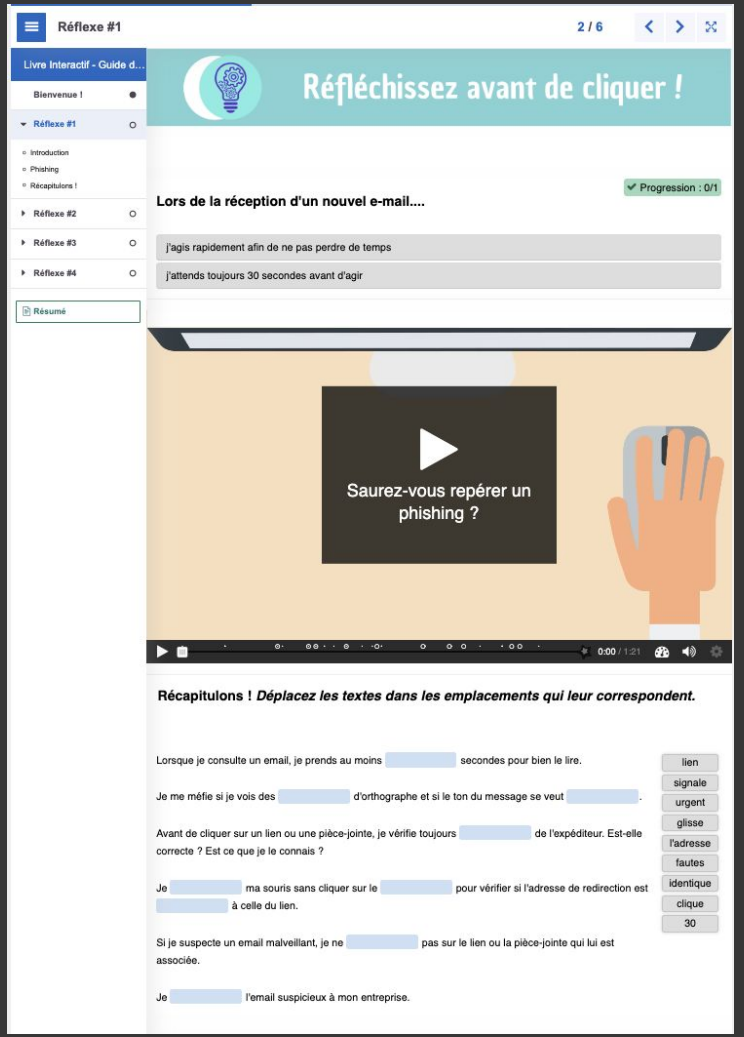


Thème : **Le guide du nouvel arrivant**

Durée : 20 minutes

Se compose de 4 modules :

- Vérification de l'origine des mails
- La sécurisation de l'accès aux comptes
- La protection du réseau et des informations de la structure
- Le télétravail

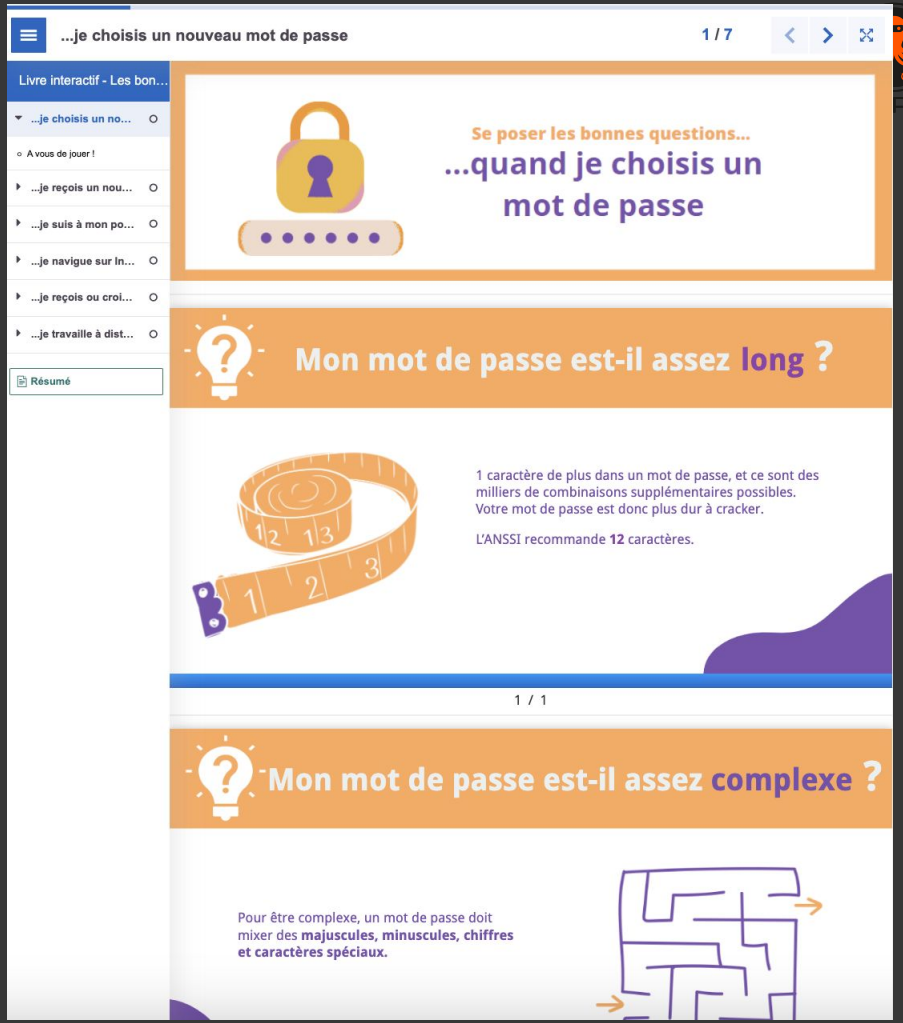


Thème : **Se poser les bonnes questions**

Durée : 15 minutes

Se compose de 6 modules :

- Mot de passe
- Mail
- Poste de travail
- Navigation sur internet
- Les visiteurs
- Le travail à distance



05

Cyber hero

Le parcours Cyber hero propose à votre utilisateur de devenir le héros de votre structure au travers d'un parcours de 9 vidéos interactives.

Thèmes abordés :

- Une introduction : 3 minutes
- Les codes malveillants : 10 minutes
- L'ingénierie sociale : 14 minutes
- Le phishing : 13 minutes
- Les postes de travail : 8 minutes
- Les mots de passe : 9 minutes
- La protection de l'information : 9 minutes
- La mobilité : 7 minutes
- La sécurité physique : 6 minutes

06

Funny but serious

“Funny but serious” sont des vidéos de sensibilisation d’une à deux minutes maximum sans quiz.

Thèmes abordés :

- 1 application, 1 mot de passe
- 1 faille pour bloquer votre entreprise
- Mot de passe secret, pas de regret
- Protégez vos mots de passe
- Double Authentification = Double Protection
- Codes malveillants à l'écoute
- Ne connectez pas d'appareils trouvés
- Clé USB: cadeau empoisonné
- Votre téléphone peut aussi être piraté
- Mieux vaut mettre à jour qu'appeler au secours
- Un clic, un risque !
- Attention aux pièces-jointes
- Une cyberattaque peut en cacher une autre
- Les technologies avancées pourraient aussi vous tromper...
- Soyez sûr de l'identité de vos interlocuteurs !
- Ordinateur verrouillé, ennui évité
- Phishing et Télétravail
- Bureau rangé, information protégée
- 1 doc 1 classification
- Documents sans surveillance, méfiance !
- A usage exclusivement professionnel
- Voyagez léger, restez discret
- Gardez un oeil sur votre mobile
- Je publie, je réfléchis
- Réfléchissez avant de partager
- N'importe qui peut se l'approprier
- Vérifiez votre auditoire !

- Coupez vos assistants vocaux pendant les réunions
- Pas de badge, pas d'accès
- L'IT est votre amie
- Utilisez uniquement les outils validés
- Votre service informatique, votre unique support technique !
- Téléchargement illégal
- Objet connecté mal configuré ? Porte ouverte aux pirates !
- Fraude au faux conseiller bancaire
- Smishing Netflix

07

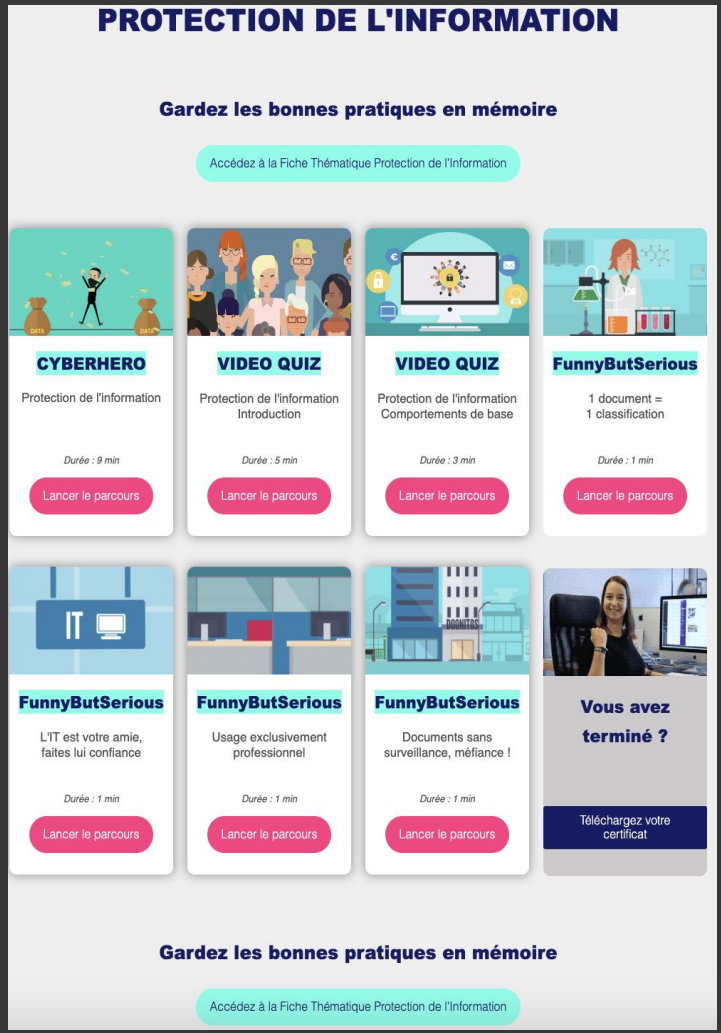
Par thématiques

Le choix d'une campagne par thématique implique le mélange de plusieurs types de vidéos :

- cyber heros
- vidéos interactives
- Funny but serious

On retrouve ainsi 8 grandes thématiques :

- La protection de l'information : 23 minutes
- Les codes Malveillant : 17 minutes
- Les mots de passe : 20 minutes
- Le phishing : 41 minutes
- L'ingénierie sociale : 42 minutes
- La mobilité : 14 minutes
- Les postes de travail : 17 minutes
- La sécurité physique : 9 minutes



MOT DE PASSE

Gardez les bonnes pratiques en mémoire

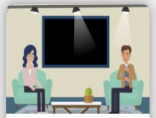
Accédez à la Fiche Thématique Mots de passe

CYBERHERO

Mot de passe

Durée : 9 min

Lancer le parcours



VIDEO QUIZ

Mot de passe

Durée : 4 min

Lancer le parcours

VIDEO QUIZ

Gestionnaire de mots de passe

Durée : 4 min

Lancer le parcours

FunnyButSerious

1 application =
1 mot de passe

Durée : 1 min

Lancer le parcours

FunnyButSerious

Mot de passe secret,
pas de regret

Durée : 1 min

Lancer le parcours

FunnyButSerious

Cryptez vos
mots de passe

Durée : 1 min

Lancer le parcours

Vous avez terminé ?

Téléchargez votre certificat

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Mots de passe

LE PHISHING

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Phishing

CYBERHERO

Le phishing

Durée : 13 min

Lancer le parcours

VIDEO QUIZ

Introduction

Durée : 4 min

Lancer le parcours

VIDEO QUIZ

Motivations des
pirates

Durée : 4 min

Lancer le parcours

VIDEO QUIZ

Les bonnes pratiques

Durée : 4 min

Lancer le parcours

VIDEO QUIZ

Spam

Durée : 3 min

Lancer le parcours

VIDEO QUIZ

Phishing
Covid-19

Durée : 5 min

Lancer le parcours

VIDEO QUIZ

Smishing

Durée : 5 min

Lancer le parcours

FunnyButSerious

Les codes malveillants
ont des oreilles

Durée : 1 min

Lancer le parcours

FunnyButSerious

Réfléchissez
avant de cliquer

Durée : 1 min

Lancer le parcours

FunnyButSerious

Attention aux
pièces-jointes

Durée : 1 min

Lancer le parcours

Vous avez terminé ?

Téléchargez votre certificat

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Phishing

INGENIERIE SOCIALE

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Ingénierie Sociale

CYBERHERO

Ingénierie sociale

Durée : 14 min

Lancer le parcours

VIDEO QUIZ

Ingénierie sociale :
Introduction

Durée : 3 min

Lancer le parcours

VIDEO QUIZ

Ingénierie sociale :
Anatomie d'une attaque

Durée : 6 min

Lancer le parcours

VIDEO QUIZ

Ingénierie sociale :
Les bons comportements

Durée : 7 min

Lancer le parcours

VIDEO QUIZ

Escroquerie
au président

Durée : 5 min

Lancer le parcours

VIDEO QUIZ

Deepfake Audio
et cyberattaques

Durée : 5 min

Lancer le parcours

FunnyButSerious

Je n'ai pas que
des amis

Durée : 1 min

Lancer le parcours

FunnyButSerious

Les technologies avancées
pourraient vous tromper

Durée : 1 min

Lancer le parcours

Vous avez terminé ?

Téléchargez votre certificat

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Ingénierie Sociale

CODES MALVEILLANTS

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Codes Malveillants

CYBERHERO

Codes malveillants

Durée : 10 min

Lancer le parcours

VIDEO QUIZ

Ransomware

Durée : 4 min

Lancer le parcours

FunnyButSerious

Les codes malveillants ont aussi des oreilles

Durée : 1 min

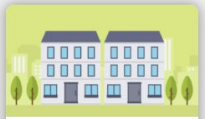
Lancer le parcours

FunnyButSerious

Ne connectez pas d'appareils trouvés

Durée : 1 min

Lancer le parcours



FunnyButSerious

Votre téléphone peut aussi être piraté

Durée : 1 min

Lancer le parcours

Vous avez terminé ?

Téléchargez votre certificat

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Codes Malveillants

MOBILITE

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Mobilité

CYBERHERO

Mobilité

Durée : 7 min

Lancer le parcours

VIDEO QUIZ

Mobilité

Durée : 3 min

Lancer le parcours

FunnyButSerious

Gardez un oeil sur votre portable

Durée : 1 min

Lancer le parcours

FunnyButSerious

Voyagez léger soyez discret

Durée : 1 min

Lancer le parcours

Vous avez terminé ?

Téléchargez votre certificat

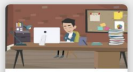
Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Mobilité

POSTE DE TRAVAIL

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Poste de travail

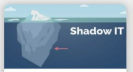


CYBERHERO

Poste de travail

Durée : 8 min

Lancer le parcours

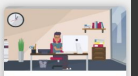


VIDEO QUIZ

Shadow IT

Durée : 5 min

Lancer le parcours



FunnyButSerious

Mieux vaut mettre à jour, qu'appeler au secours !

Durée : 1 min

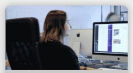
Lancer le parcours

FunnyButSerious

Usage exclusivement professionnel

Durée : 1 min

Lancer le parcours



Vous avez terminé ?

Téléchargez votre certificat

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Poste de travail

SECURITE PHYSIQUE

Gardez les bonnes pratiques en mémoire

Accédez à la Fiche Thématique Sécurité Physique

CYBERHERO

Sécurité physique

Durée : 6 min

Lancer le parcours

VIDEO QUIZ

Sécurité physique

Durée : 2 min

Lancer le parcours

FunnyButSerious

Pas de badge, pas d'accès

Durée : 1 min

Lancer le parcours

08

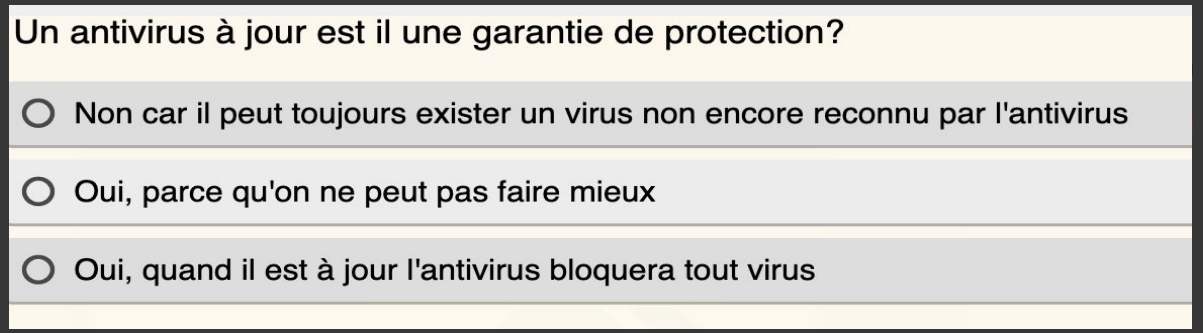
Quiz et évaluations

Sous un format plus ludique, vous pouvez réaliser des campagnes de quiz au sein de votre établissement.

Cependant, ce type de parcours ne contient pas de vidéos de sensibilisation.

Le baromètre de la sensibilisation à la sécurité de l'information 2023 : 10 minutes environ

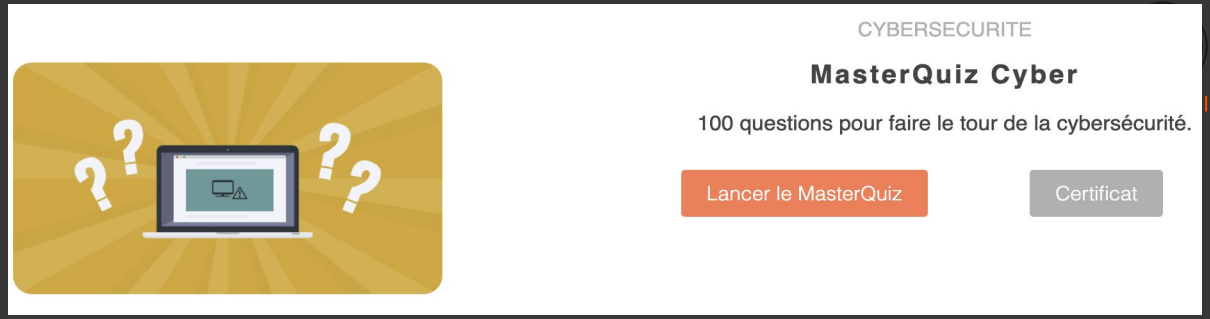
27 questions relatives aux bonnes pratiques pour sécuriser votre système d'information



Le **quiz thématique** : 100 minutes

10 quiz traitant des principaux sujets en termes de sensibilisation à la sécurité de l'information.
Allant de 6 à 14 questions par thèmes

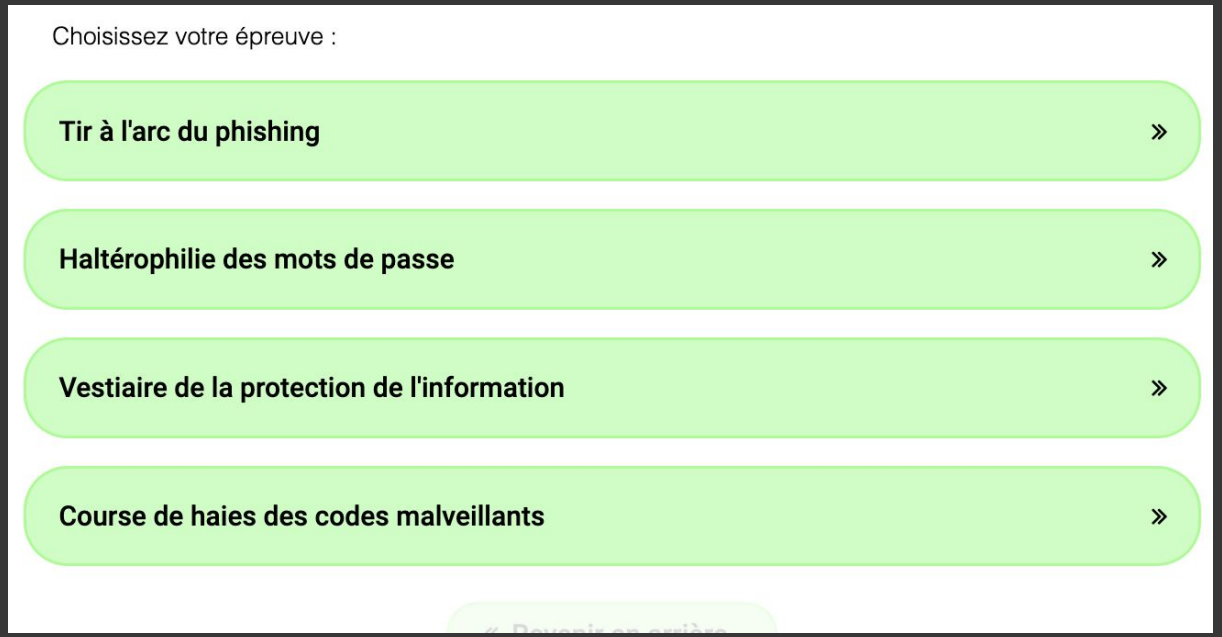
La **MasterQuizz Cyber** : 60 minutes environ
100 questions pour faire le tour de la cybersécurité



Les **Cyberympiques**

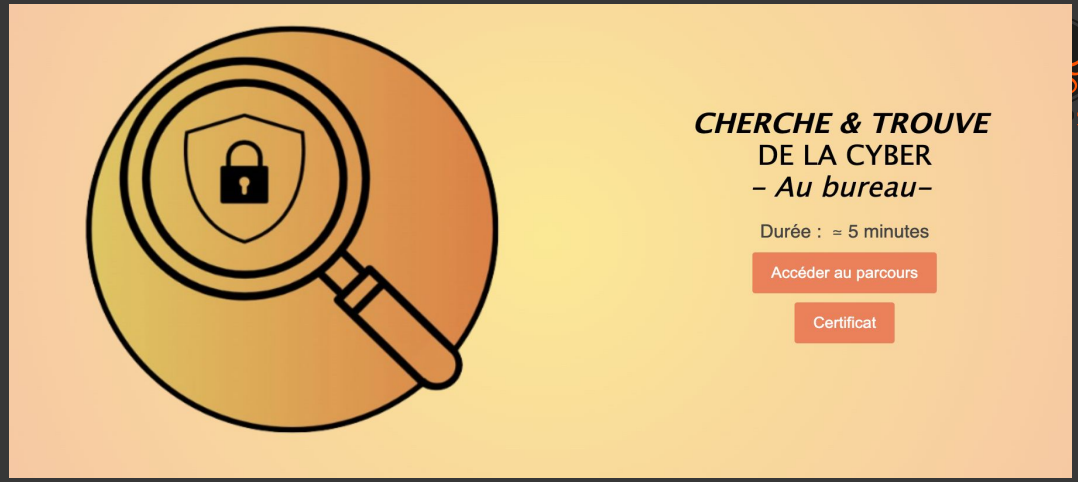
Durée : 20 minutes

Choisissez votre athlète, 4 épreuves vous attendent …



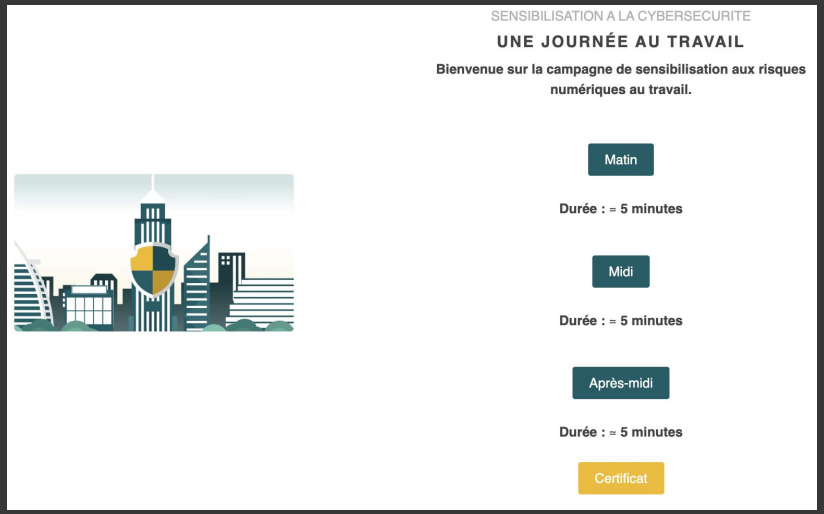
“**Cherche et trouve**” au bureau : à l’image d’une chambre des erreurs, l'apprenant est invité à détecter les risques cyber potentiels dans un scénario interactif, et adopter les bonnes pratiques.
5 risques à détecter

Durée : 5 minutes



“**Mini serious game**” une journée au travail : Parcours de sensibilisation pendant lequel l'apprenant accompagne Hermione dans une journée type au travail et l'aide à réagir aux situations à risques rencontrées.

Durée : 15 minutes



09

Établissement de santé

La plateforme Sensiwave s’est adaptée aux demandes des communautés de santé et a développé une partie spécifique “Cybersécurité Santé”.

Sur le même principe, on y retrouve des vidéos interactives

Les vidéos interactives

Thème : Protection de l'information

- Confidentialité des données bureaux : 20 minutes
- Confidentialité des données Hôpital : 20 minutes
- Partage des données personnelles : 1 minute

Thème : Mot de passe

- Partage de codes d'accès : 1 minute
- Stockage de mots de passe dans le navigateur : 1 minute

Thème : Mobilité

- Données sensibles en déplacement : 1 minute

Thème : Phishing

- Phishing ciblé : 1 minute
- Smishing : 1 minute
- Email Alarmant : 1 minute

Thème : Codes malveillant

- Ransomware : 1 minute
- Usages pro/perso : 1 minute
- En cas d'attaque : 1 minute

Thème : Internet

- Objets connectés : 1 minute
- Réseaux sociaux : 1 minute
- Utilisation du mail professionnel sur un site web : 1 minute
- Assistants vocaux : 1 minute
- Navigation sécurisée : 1 minute

Thème : Shadow IT

- Utilisation d'applications non approuvées : 1 minute
- Téléchargement d'une application : 1 minute

Thème : Poste de travail

- Session ouverte : 1 minute
- Clé USB - Centre d'Imagerie : 1 minute
- Clé USB : 1 minute

Thème : Données patients

- La confidentialité : 1 minute
- Consultation non autorisée de données sensibles : 1 minute
- Consultation d'un dossier patient d'un collègue : 1 minute
- Identitovigilance : 1 minute
- Doublon de dossier patient : 1 minute
- En dehors du temps d'activité : 1 minute

10

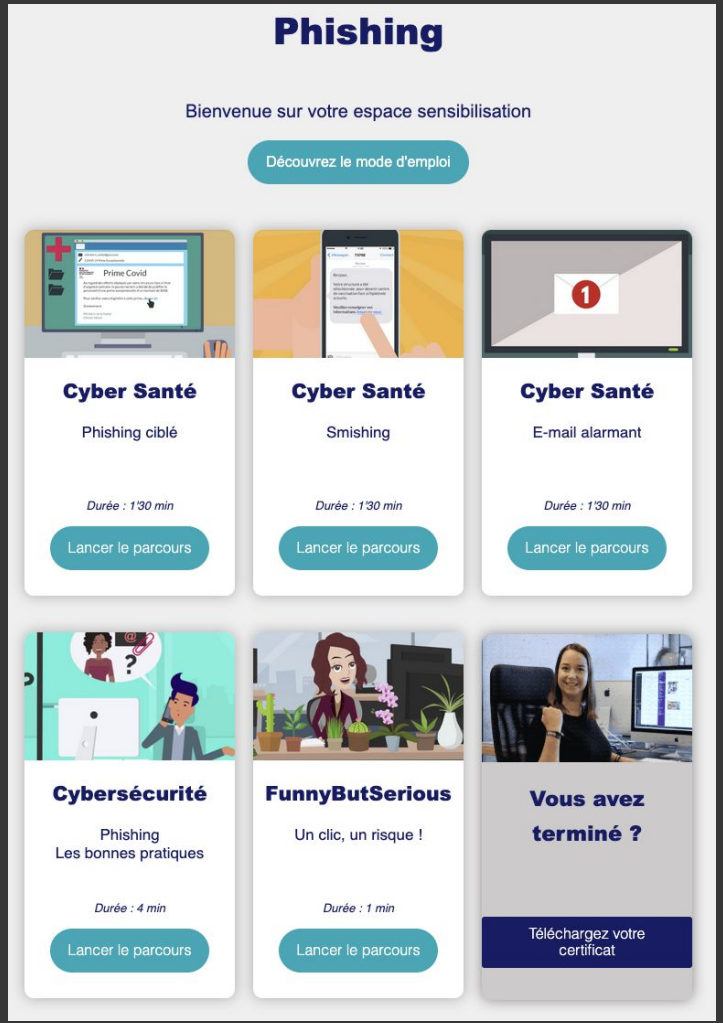
Par thématiques

Dans le même esprit que le module “Par thématiques” (cf 07), il vous est possible de démarrer des campagnes par grandes thématiques mélangeant ainsi plusieurs types de vidéos :

- vidéos interactives
- Funny but serious

On retrouve ainsi 12 grandes thématiques :

- Confidentialité et intégrité des données de santé : 9 minutes
- Protection de l'information : 10 minutes
- Phishing : 10 minutes
- Codes malveillants : 10 minutes
- Mot de passe : 8 minutes
- Usages pro/perso : 10 minutes
- Sécurité sur le web au travail - Partie 1 : 7 minutes
- Sécurité sur le web au travail - Partie 2 : 8 minutes
- Sécurité numérique au quotidien : 8 minutes
- Ingénierie sociale - Partie 1 : 7 minutes
- Ingénierie sociale - Partie 2 : 8 minutes
- Mobilité : 7 minutes



11

Etablissements/Services sociaux médico-sociaux

Le parcours ESMS regroupe des grandes thématiques sous format de vidéos suivies de quiz de 2 à 5 minutes.

Votre utilisateur va suivre Anna, psychiatre au C.S.A.P.A, Boris, moniteur d'atelier éducatif en ESAT ou encore Lou, assistante sociale face à des situations à risques lors de leurs déplacements.

Le parcours ESMS regroupe les thèmes suivants :

- Demandes d’accès données - applications mobiles : 2 minutes
- Une session, un utilisateur : 3 minutes
- Session ouverte : 2 minutes
- Phishing - Pièce Jointe : 2 minutes
- Phishing - Lien : 2 minutes
- Usage pro/perso : 2 minutes
- Mises à jour : 2 minutes
- Utilisation Wifi Public : 2 minutes
- Réagir en cas d'attaque : 2 minutes
- Données sensibles en déplacement : 2 minutes
- Utilisation d’applications non approuvées : 2 minutes
- Mot de passe : 2 minutes
- Clé USB - Imagerie médicale : 2 minutes
- Stockage mot de passe navigateur : 3 minutes
- Demande de mot de passe par téléphone : 2 minutes
- Smishing : 2 minutes
- Ransomware : 5 minutes

12

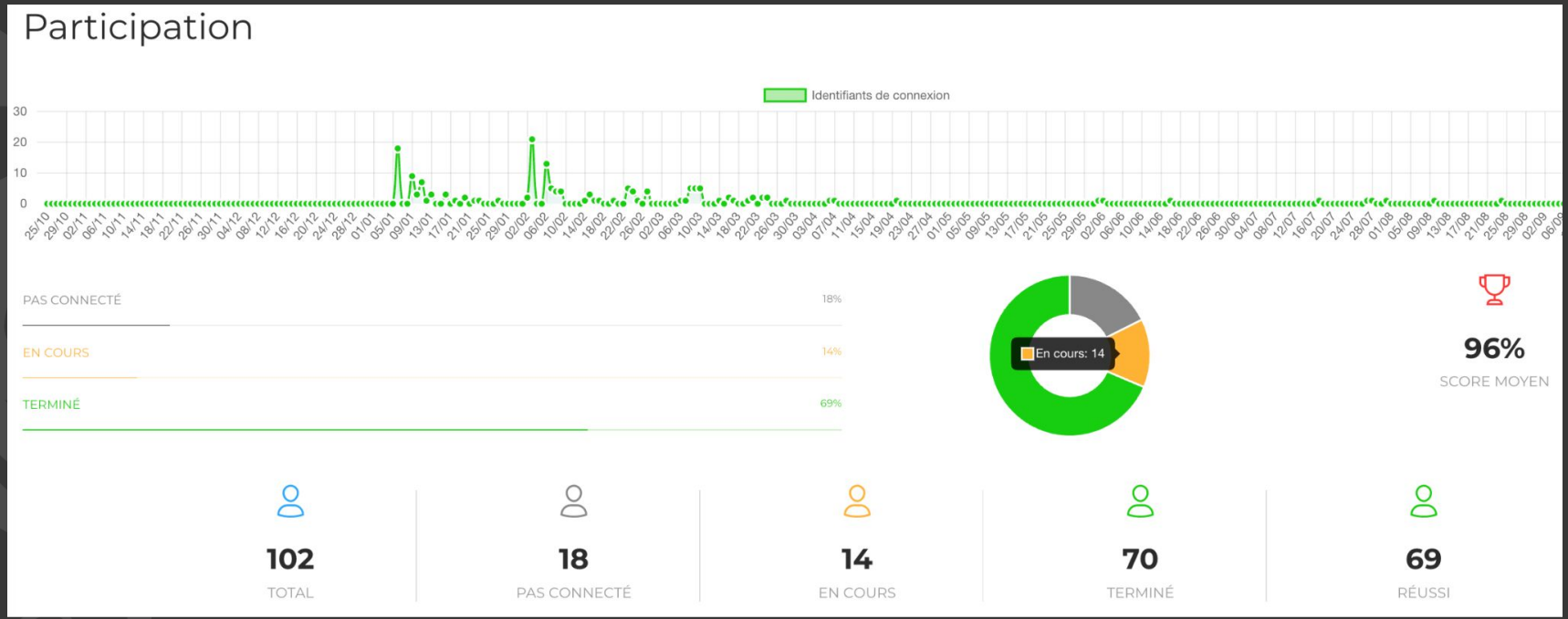
Rapports de statistiques

Des rapports de statistiques de taux de participation à votre campagne de sensibilisation vous sont envoyés.

Comme énoncé en préambule :

- Nous pouvons automatiser l'envoi de ces rapports à la fréquence que vous souhaitez
- Ou simplement les envoyer à votre demande

Exemple de rapport



Sur le total de vos utilisateurs, vous pourrez connaître le taux de participation ainsi que de réussite de votre campagne de sensibilisation.

Vous souhaitez organiser une campagne de sensibilisation ?

Contacter l'équipe CAPSI qui vous aidera à organiser cette campagne de sensibilisation et pourra également vous aider à mettre en oeuvre au profit de vos utilisateurs une campagne de formation à l'hygiène numérique destinée à acquérir les gestes barrières pour éviter un incident numérique au sein de vos établissements.

Nous vous invitons à remplir ce formulaire pour connaître votre choix : Formulaire de création de la campagne de sensibilisation

Ces campagnes de formation mais également ces opérations de faux phishing sont réalisées à l'aide de la plateforme régionale CAPSI de formation et de sensibilisation à la sécurité numérique administrée par l'équipe CAPSI.

Ces ressources mutualisées sont accessibles gratuitement à tous les établissements sanitaires et médico-sociaux de la région PACA grâce au financement conjoint de l'ARS PACA et du GRADeS PACA innovation e-Santé Sud dont le centre de ressources régional CAPSI fait partie.

Merci