

# Kit de sensibilisation à la cybersécurité

Comment utiliser les outils Nouvey ?



# Sensibiliser pour mieux se préparer

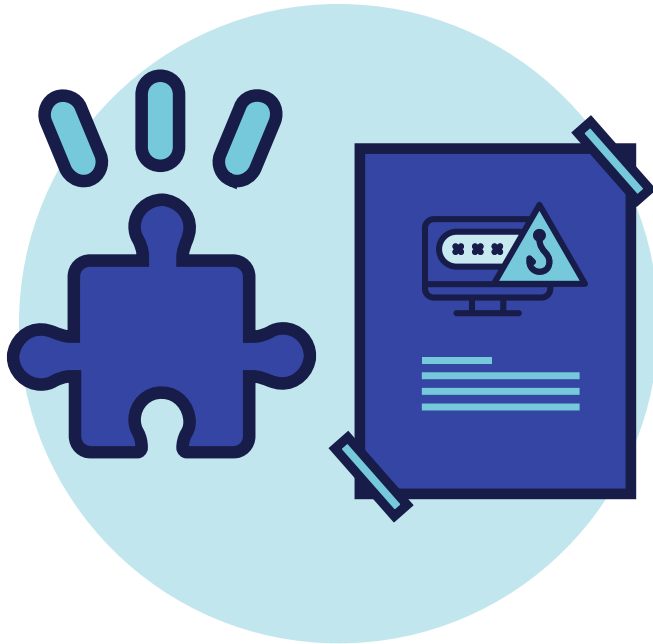


Pour mieux armer les professionnels face aux **cyberattaques** et préserver la continuité des soins apportés aux patients et leurs données de santé, **NOUVEY** propose des outils de sensibilisation pratiques à disposition de tous les acteurs de santé de La Réunion :

- ✓ Visuels (affiches, visuels pour les réseaux sociaux...)
- ✓ Jeux pédagogiques (escape game, question pour un cyberchampion...)
- ✓ Fiche réflexe en cas d'attaques

# Sommaire

Ce guide présente les outils de sensibilisation NOUVEY ainsi que nos préconisations pour une utilisation efficiente.



1. Utilisation des visuels NOUVEY
  - a. Affiches
  - b. Utilisation des affiches
  - c. Visuels réseaux sociaux
2. Fiche réflexe « Que faire en cas d'attaques ? »
3. Présentation des jeux sérieux
  - a. Mediscape
  - b. Question pour un cyberchampion
  - c. Code de la cybersécurité
  - d. Phish me if you can

# Les visuels NOUVEY

Des messages percutants, nouveaux  
et actualisés régulièrement.

# a. Les affiches NOUVEY

Ces affiches sont destinées à tous les acteurs du médico-social et du sanitaire. Nous avons choisi des analogies entre l'informatique et des symboles médicaux (seringue, bloc...) pour un message clair et percutant.

**Laisser entrer un intrus dans un bloc opératoire ?  
Quelle idée !  
Et sur votre ordinateur, on en parle ?**



**Quand je reçois un mail suspect :**  
Offre alléchante, apparence suspecte, pièce jointe inattendue, adresse d'expédition fantaisiste, demande de données confidentielles...


- Je ne clique pas sur les liens
- Je ne transmets pas mon mot de passe
- Je n'ouvre pas la pièce jointe

Scannez-moi pour en savoir plus



**NOUVEY**  
CYBERSÉCURITÉ  
SANTÉ RÉUNION


**Utiliser plusieurs fois la même seringue ? Quelle idée !  
Et votre mot de passe, on en parle ?**



**Au bureau comme à la maison :**

- Je ne partage jamais mon mot de passe
- J'utilise des mots de passe différents pour mes outils pros et persos
- Je crée des mots de passe complexes contenant chiffre, majuscule et caractère spécial

Scannez-moi pour en savoir plus



**NOUVEY**  
CYBERSÉCURITÉ  
SANTÉ RÉUNION

**Un pique-nique dans le bloc opératoire ? Quelle idée !  
Et le mélange vie pro/vie perso, on en parle ?**



**Quand je suis au bureau :**

- Je n'utilise pas mon adresse mail personnelle pour échanger au sujet des patients
- Je ne branche pas ma clé usb ou mon téléphone personnels aux ordinateurs
- Je ne stocke pas mes photos de vacances sur les postes de travail

Scannez-moi pour en savoir plus



**NOUVEY**  
CYBERSÉCURITÉ  
SANTÉ RÉUNION

## b. Utilisation des affiches

Diffusion de trois affiches par an dans les structures : chacune abordant une thématique de cybersécurité (phishing, mot de passe, confidentialité...)



### Nos préconisations :

- ✓ Choisir des lieux d'affichage stratégiques (cafétéria, salles de repos, ascenseurs...)
- ✓ Installer les affiches pour une durée de 3/4 mois (meilleure appropriation du message)
- ✓ Passer à la seconde affiche au bout de 4 mois (maintient la curiosité)
- ✓ Pour une impression interne, choisir un format couleur, en A3 de préférence (contacter TESIS si besoin)

## c. Visuels pour les réseaux sociaux

Parce qu'un professionnel averti en vaut deux, en relayant ces images, vous participez aussi à la démarche de sensibilisation, une des premières barrières de protection contre les attaques !



Facebook : photo de couverture 851x315  
 LinkedIn : 1128x191



Facebook, Twitter & LinkedIn : publication 1200x630



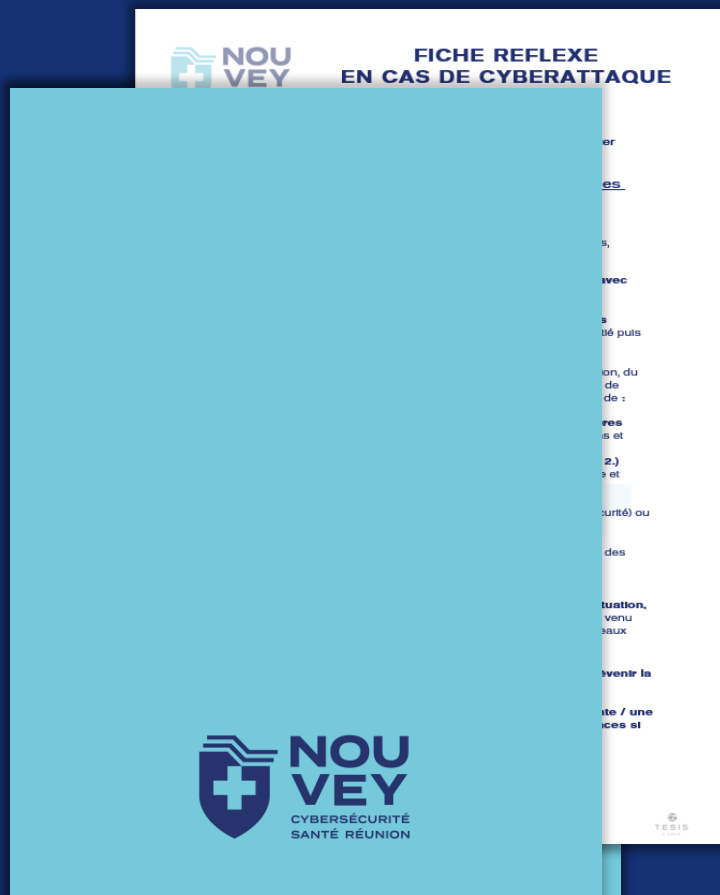
Pour accompagner ces visuels, des textes prêts à copier-coller sont disponibles dans le document word « Publications pour les réseaux sociaux » joint au kit.

# Fiche réflexe

Adopter les premiers réflexes  
en cas d'attaques.

## 2- Fiche réflexe

Cette fiche destinée aux directions d'établissements, recense les principales actions à mettre en place en cas de cyberattaques.



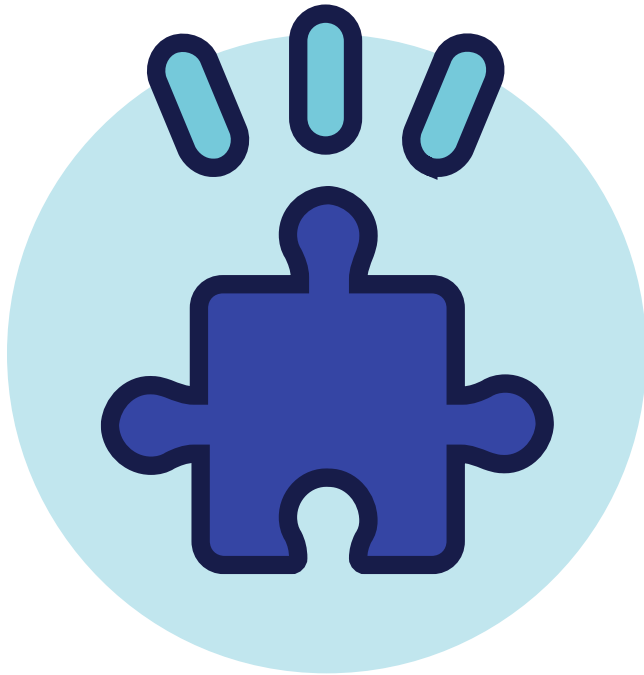
Cette fiche contient :

- ✓ une liste d'actions à mener pendant l'attaque
- ✓ une liste d'actions à suivre post-attaque
- ✓ les numéros à contacter

# Les jeux dits « sérieux »

Accroître la réceptivité des messages par le jeu.

# Les jeux sérieux



Pour sensibiliser une population, un seul vecteur de communication ne suffit pas. Pour qu'elle s'approprie une information, il faut varier le support, la tonalité et la forme du message !

C'est pourquoi, des sessions de **sensibilisations ludiques** par équipes, sont proposés aux acteurs de santé de La Réunion qui souhaitent améliorer leur niveau de connaissances en cybersécurité tout en s'amusant.



# a. Escape game

Médiscap est un jeu d'évasion. Transformés en journalistes infiltrés, vos collègues vont devoir, dans un temps imparti, trouver une information confidentielle en exploitant les mauvaises pratiques de sécurité.

The logo for Médiscap is displayed on a dark blue background. The word "MEDISCAP" is in white, with the "E" in "MED" highlighted in red. To the right of the text is a white padlock icon. The entire logo is framed by a thin red L-shaped bracket on the left side.

Organiser ce jeu dans votre structure :

- ✓ **Comment ?** Faire la demande aux équipes Sécurité du GCS TESIS
- ✓ **Où ?** Les sessions peuvent avoir lieu dans les locaux du GCS TESIS, ou dans la structure demandeuse
- ✓ **Combien de personnes ?** 6 participants max par session
- ✓ **Durée :** 45 minutes

## b. Questions pour un cyberchampion

Basé sur le principe du célèbre jeu télévisé, ce quizz aux multiples questions, vous permettra d'évaluer le niveau de connaissances de vos équipes tout en s'amusant.



Organiser ce jeu dans votre structure :

- ✓ **Comment ?** Faire la demande aux équipes Sécurité du GCS TESIS
- ✓ **Où ?** Les sessions peuvent avoir lieu dans les locaux du GCS TESIS, ou dans la structure demandeuse
- ✓ **Combien de personnes ?** 4 participants par session
- ✓ **Durée :** 8 à 15 minutes

## c. Code de la cybersécurité

Les participants répondent à des questions posées parmi plusieurs propositions à l'aide d'une manette. Le logiciel enregistre les scores et restitue les résultats ainsi que les bonnes réponses en fin de session.



Organiser ce jeu dans votre structure :

- ✓ **Comment ?** Faire la demande aux équipes Sécurité du GCS TESIS
- ✓ **Où ?** Les sessions peuvent avoir lieu dans les locaux du GCS TESIS, ou dans la structure demandeuse
- ✓ **Combien de personnes ?** De 4 à 12 participants par session
- ✓ **Durée :** 10 minutes

## d. Phish me if you can

Ce jeu demande à vos collaborateurs de reconnaître des messages malveillants (mail, SMS, mail sur mobile). En les analysant, à eux de décider s'ils doivent l'ouvrir ou non !



**PHISH ME**  
**IF YOU CAN**



Organiser ce jeu dans votre structure :

- ✓ **Comment ?** Faire la demande aux équipes Sécurité du GCS TESIS
- ✓ **Où ?** Les sessions peuvent avoir lieu dans les locaux du GCS TESIS, ou dans la structure demandeuse
- ✓ **Combien de personnes ?**  
Personnalisable
- ✓ **Durée :** 5 minutes par session

# Nous contacter

MATHIAS LAURENT  
Responsable de la Sécurité des Systèmes  
d'Information et DPD au sein de TESIS



[m.laurent@tesis.re](mailto:m.laurent@tesis.re)



0693 93 37 35



**NOU  
VEY**

**CYBERSÉCURITÉ  
SANTÉ RÉUNION**