

# Exercice de gestion de crise numérique

## CAPSI

---

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



CAPSI

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

# Les enjeux et objectifs

## Les enjeux

- Comprendre les spécificités de la crise cyber
- S'inscrire dans l'actualité du domaine de la santé et du médico-social
- Inscrire l'exercice dans une réflexion globale de renforcement de la résilience

## Les objectifs pédagogiques de l'exercice

- Partager les bonnes pratiques en cas de crise cyber
- Réfléchir aux méthodes de travail « en dégradé »
- Offrir l'opportunité aux métiers d'éprouver leurs dispositifs de continuité d'activité.

# Planning **organisationnel**

Un exercice de gestion de crise numérique se déroule en présentiel sur une **demi-journée**. Nous vous invitons à déterminer le plus tôt possible la demi-journée lors de laquelle vous souhaitez réaliser l'exercice.

Une fois la date choisie, nous vous encourageons à désigner une **personne complice** qui nous assistera dans la **création du scénario** et dans l'identification des problématiques spécifiques à votre structure. Ces ateliers de personnalisation sont essentiels pour élaborer le scénario de l'exercice.

Le complice, qui ne participera pas directement le jour de l'exercice, **observera** la cellule de crise. Il recevra une formation préalable sur l'observation avant le jour de l'exercice.

Par la suite, un nouvel atelier sera mis en place pour partager les observations faites pendant l'exercice, dans le but de formuler une **proposition de plan d'action**.

# Planning - Vue d'ensemble

Etapes	Réunion(s) de préparation	Envoi du kit participant aux participants	Exercice	Débriefing	Envoi du bilan
Durée	2 à 3h selon le contexte	-	2h	1/2 heure	Possibilité de réaliser le retex en visio
Echéances	T0 - 3 à 4 semaines	T0 - 1 semaine	T0	T0 + 2h	T0 + 3 semaines
Dates planifiées	../../2024	../../2024	../../2024	../../2024	../../2024

# Déroulé de l'exercice

Etablissement/OG  
Cellule de crise

Prestataire  
Equipe d'animation

Possibilité de réponse à ces stimuli

**Participants** : Jouer leur propre rôle pour gérer la crise en suivant les règles de l'exercice.

**Animateur secondaire** : Animer l'exercice en envoyant les éléments immersifs

Envoi de stimuli

Questions et communication des actions et décisions

**Animateur principal** : Animer et gérer l'exercice le déroulement de l'exercice : briefing/debriefing et répondre aux questions des participants

Communique sur l'évolution avec l'animateur

**Observateur** : Observer et évaluer la réaction de la cellule de crise pour le RETEX

# Profils recommandés des participants

**Nous préconisons entre 10 et 15 participants à l'exercice de crise**

Ces différents profils sont des **recommandations**, nous vous invitons à faire participer les personnes qui selon vous, peuvent être **nécessaires** lors d'une crise :

- Directeur ou Directeur général : (responsable de la direction générale de l'organisme)
  - Responsable de la Cellule de Crise
- Un(e) **secrétaire de crise** (assistant(e) de direction, intendance...)
  - Gestion de la Main Courante
- Un(e) **Responsable de la DSI / DSN, RSSI / OSSI** ou équivalent
- Un **référént juridique / DPO**
- Des **représentant des différents métiers** de l'organisme (responsable communication, RH, qualité, chefs de service, médecin coordinateur...)
- Des **représentants de la gouvernance des établissements** rattachés

# Actions à mettre en oeuvre

1. Déterminer le **niveau de l'exercice** que vous souhaitez réaliser
2. Identifier les **participants** nécessaires à l'exercice et bloquer leurs agendas
3. Réserver une **salle de réunion** pour l'animation de l'exercice
4. Participation de la personne en charge de la planification de cet exercice à la **réunion de préparation** pour la personnalisation de l'exercice
5. Diffuser le **kit participant** à vos participants une semaine avant l'exercice (vous pouvez imprimer le kit et le mettre à disposition lors de l'exercice)
6. Vous avez la possibilité de mettre à disposition de vos participants, toute **documentation** (processus, procédures...) le jour de l'exercice

# Autres ressources et outils à votre disposition :

### PARTICIPATION

Pour vivre l'aventure : il vous suffit de prendre contact avec l'équipe CAPSI qui vous proposera des dates de participation.

Si vous souhaitez aller plus loin, sachez que vous pouvez devenir ambassadeur CAPSI (sur la base du volontariat) et déployer vous-même cet escape game dans votre établissement ! Nous pouvons pour cela vous former et, au choix, vous prêter un kit de jeu pour 1 mois ou vous accompagner dans la création de votre propre kit de jeu (et c'est très simple, il suffit de 4 vieux PC portables, d'une webcam et de quelques accessoires pour vous lancer).

### COÛT

L'acquisition de cet escape game, créé par la GRADES Pays de la Loire en collaboration avec Orange Cyberdefense, a été financée par l'ARS PACA sous l'impulsion de l'équipe CAPSI.

En tant que professionnels du secteur de la santé de la région PACA, vous pouvez donc en bénéficier gratuitement !

**CONTACT**  
capsiles-sud.fr

**CAPSI**  
Centre National de Protection des Systèmes d'Information  
https://capsitech



## Tentez l'expérience !

Découvrez les grands principes de la sécurité en passant du côté obscur.

Prêt à relever le défi ?



# CRACK'N HACK

Escape Game

**CONTACT** : capsiles-sud.fr  
HTTPS://CAPSIT.ECH




**Cybersécurité**

**Gestes barrières aux risques numériques**

**Sécuriser les usages numériques**

**Faux phishing**

**Être un acteur responsable et informé de la sécurité numérique de son établissement ou de sa structure**

**Jouer son rôle au sein de la chaîne de sécurité numérique**

**Hygiène numérique**

**Acquérir les réflexes d'un usage numérique responsable**

**CAPSI**

**CONTACT** : capsiles-sud.fr  
HTTPS://CAPSIT.ECH



## Plateforme régionale CAPSI FORMATION ET SENSIBILISATION à la sécurité numérique



**CAPSI**  
Centre National de Protection des Systèmes d'Information

Disposez gratuitement d'une plateforme régionale de formation et de sensibilisation personnalisable et adaptable à vos besoins en matière de sécurité numérique à destination de vos équipes, utilisateurs du SI et collaborateurs.

### PRINCIPES

Pendant une aventure collective de 45 minutes, immergez vos collaborateurs dans l'univers CRACK'N HACK dans le but de résoudre collectivement l'énigme qui vous est proposée en vous mettant dans la peau d'un pirate numérique. Nil besoin d'être un spécialiste de l'informatique, il s'agira plutôt de faire confiance à son instinct et à son bon sens pour mener à bien la mission proposée au groupe.

### OBJECTIFS

- Un format ludique de sensibilisation à la sécurité numérique qui donne l'occasion à chaque collaborateur d'expérimenter et de mettre en pratique les règles d'hygiène numériques ;
- Un moment collaboratif et de cohésion de groupe où chaque joueur apporte sa contribution pour permettre au groupe de résoudre collectivement l'énigme qui lui est proposée ;
- Une expérience de formation originale à la cybersécurité et aux gestes barrières pour limiter au quotidien la prise de risques à l'occasion des usages numériques tant personnels que professionnels ;
- Un temps d'échange autour des bonnes pratiques pour permettre à chaque collaborateur d'être informé et acteur de la chaîne de sécurité numérique de son organisation.

### THÉMATIQUES

- Cybersécurité numérique
- Gestes barrières aux risques numériques
- Sécuriser les usages numériques
- Acquérir les réflexes d'un usage numérique responsable
- Prendre conscience de son rôle au sein de la chaîne de sécurité numérique
- Devenir acteur de la sécurité numérique de son établissement ou de sa structure.
- Hygiène numérique
- Sécuriser les usages numériques
- Faux phishing

### DURÉE

- 45 minutes de jeu pour un groupe de 4 à 6 personnes.
- 15 minutes d'échanges et de debriefing en fin de séance avec les participants.

## INFORMEZ-VOUS et faites adopter les bons réflexes par votre équipe

**Comment ?** En contactant CAPSI pour vous permettre d'emmener vos utilisateurs sur notre plateforme numérique régionale de formation disponible pour tous les établissements référencés sur le Portail de santé PACA.

**Quand ?** A tout moment, c'est vous qui choisissez vos parcours et les thèmes sur lesquels vous souhaitez former vos équipes.

**Où ?** De partout car notre plateforme est accessible en ligne !

**Pour quoi faire ?** Contribuez à renforcer la chaîne de sécurité de votre établissement et rendez vos équipes et collaborateurs acteurs responsables et impliqués de la sécurité numérique de votre structure.

**J'ai d'autres choses à faire !**  
Nous sommes conscients que votre temps est précieux, mais chacun a un rôle à jouer dans la sécurité numérique des activités professionnelles. Aussi, soyez rassurés, chaque module de formation ne dure pas plus de quelques minutes.

**Quelle plus-value apportée par l'outil ?**  
Outre les parcours de formation, notre solution vous permet d'obtenir efficacement et de manière personnalisée et adaptée à vos besoins, la montée en compétences de vos équipes à l'aide de jeux de rôle et de faux phishing intégrés dans la solution.

### Principes pour disposer de notre solution dans votre établissement

- Faites-vous accompagner par l'équipe CAPSI pour choisir le parcours adapté à vos besoins.
- Pour l'immersion de vos utilisateurs, nos équipes sont à votre disposition pour vous aider.
- Invitez vos utilisateurs enrôlés à accéder à leurs parcours individuels de formation.
- Relancez automatiquement vos utilisateurs si cela s'avère nécessaire.
- Obtenez des rapports réguliers sur la progression de vos campagnes de formation et de sensibilisation.
- Consultez les statistiques de réussite des équipes enrôlées.

### Objectifs

Former et tenir à jour vos équipes des bonnes pratiques, des postures et des gestes réflexes à adopter en matière de cybersécurité et de conformité numérique. Évaluer la maturité et la pertinence de vos campagnes de formation à l'aide des outils de faux phishing.

### Intérêts

- Des parcours et des campagnes de formation au choix en fonction de vos priorités de sensibilisation à la sécurité numérique.
- Un parcours et un suivi individuel pour vos utilisateurs incluant des relances régulières.
- Une progression au rythme de chacun et en temps choisi.
- Une accès depuis le lieu de travail ou au domicile dans le cadre du télétravail.
- Des contenus ludiques et accessibles.
- Un effort de formation reconnu et validé par une attestation de progression.



# Autres ressources et outils à votre disposition :



*Sensibilisation ludique à l'aide de jeux de plateau dédiés à la sécurité numérique*

 <p><b>PRÊTEZ-VOUS VOTRE CARTE BANCAIRE ?</b></p> <p>Attention, votre carte bancaire est un objet personnel et sensible. Ne la prêtez jamais à un tiers, même si vous connaissez bien la personne. Une carte bancaire est un moyen de paiement sécurisé, mais elle peut être utilisée pour effectuer des achats en ligne ou dans des magasins. Si elle tombe entre de mauvaises mains, vous pouvez vous retrouver avec des frais et des problèmes de sécurité.</p>	 <p><b>UN PETIT OBJET QUI PEUT VOUS FAIRE TRÈS MAL</b></p> <p>Une clé USB, un disque dur externe, un téléphone portable, une tablette... Ces objets sont très utiles, mais ils peuvent aussi contenir des données sensibles. Si vous les perdez, vous risquez de divulguer des informations importantes. Protégez-les avec un mot de passe et ne les prêtez jamais à un tiers.</p>	 <p><b>QUI A MODIFIÉ LE DOSSIER DU PATIENT ?</b></p> <p>Modifier un dossier médical est un acte grave qui peut avoir des conséquences graves pour la santé d'une personne. Assurez-vous que seuls les professionnels de santé autorisés ont accès à ces données et vérifiez régulièrement que les informations sont correctes et à jour.</p>	 <p><b>LE MYSTÈRE DES DONNÉES À CARACTÈRE PERSONNEL</b></p> <p>Les données à caractère personnel sont des informations qui vous identifient ou vous permettent d'être identifié. Elles sont collectées par de nombreuses entreprises et organismes. Assurez-vous que ces données sont traitées de manière sécurisée et que vous avez le contrôle sur leur utilisation.</p>	 <p><b>PLACE NETTE AVANT DE LEVER L'ANCRE</b></p> <p>Avant de commencer une activité en ligne, vérifiez que vous êtes sur un site sécurisé (https://). Ne fournissez jamais vos coordonnées personnelles à un site que vous ne connaissez pas. Utilisez un navigateur sécurisé et vérifiez l'adresse du site.</p>	 <p><b>UNE SEULE CLÉ À NE PAS OUBLIER</b></p> <p>Une seule clé à ne pas oublier : votre mot de passe. Choisissez un mot de passe complexe et unique pour chaque compte. Ne le partagez jamais et ne l'écrivez nulle part. Utilisez un gestionnaire de mots de passe pour vous aider à les mémoriser.</p>	 <p><b>ÀIE SENSIBLE S'ABSTENIR. VOICI UNE VICTOIRE DE L'HACKER</b></p> <p>Ne cliquez jamais sur des liens suspects ou des pièces jointes inattendues. Ne téléchargez jamais de logiciels ou de fichiers provenant de sources inconnues. Vérifiez l'authenticité des sites et des applications que vous utilisez.</p>
 <p><b>ÉVITEZ TOUT PASSER À BORD</b></p> <p>Ne divulguez jamais vos coordonnées personnelles ou vos données sensibles sur des réseaux sociaux ou sur des sites non sécurisés. Utilisez des mots de passe forts et différents pour chaque compte.</p>	 <p><b>NE DIVULGUEZ PAS TOUTS VOS SECRETS À VOTRE ÉQUIPAGE</b></p> <p>Partagez vos données personnelles avec les personnes que vous connaissez bien et faites confiance à leur capacité à protéger vos informations. Ne partagez pas vos données sensibles avec des personnes que vous ne connaissez pas.</p>	 <p><b>EST-CE QUE VOUS AVEZ UN PRÉSERVATIF USAGE ?</b></p> <p>Assurez-vous que vos données personnelles sont protégées par des mesures de sécurité appropriées. Utilisez des logiciels antivirus et des pare-feu pour protéger votre ordinateur et votre téléphone.</p>	 <p><b>LE TRAITEMENT DES DONNÉES PERSONNELLES</b></p> <p>Les données à caractère personnel sont des informations qui vous identifient ou vous permettent d'être identifié. Elles sont collectées par de nombreuses entreprises et organismes. Assurez-vous que ces données sont traitées de manière sécurisée et que vous avez le contrôle sur leur utilisation.</p>	 <p><b>VÉRIFIEZ VOS SOURCES AVANT DE PARTIR À LA CHASSE AU TRÉSOR</b></p> <p>Ne cliquez jamais sur des liens suspects ou des pièces jointes inattendues. Ne téléchargez jamais de logiciels ou de fichiers provenant de sources inconnues. Vérifiez l'authenticité des sites et des applications que vous utilisez.</p>	 <p><b>ASSUREZ-VOUS DE L'IDENTITÉ DE VOTRE INTERLOCUTEUR.</b></p> <p>Ne fournissez jamais vos coordonnées personnelles à un site que vous ne connaissez pas. Utilisez un navigateur sécurisé et vérifiez l'adresse du site.</p>	 <p><b>Laissez-vous votre COFFRE À TRÉSORS OUVERT ET SANS SURVEILLANCE ?</b></p> <p>Ne cliquez jamais sur des liens suspects ou des pièces jointes inattendues. Ne téléchargez jamais de logiciels ou de fichiers provenant de sources inconnues. Vérifiez l'authenticité des sites et des applications que vous utilisez.</p>

*Kits d'affiches CAPSI disponibles sur notre site internet*

# Merci

---



Nous contacter : Innovation e-Santé Sud

[capsi@ies-sud.fr](mailto:capsi@ies-sud.fr)

<https://capsi.tech>

Page LinkedIn : <https://www.linkedin.com/showcase/capsi-paca>