LIVRE BLANC

Maximiser la participation et l'engagement aux sensibilisations cyber dans les collectivités territoriales

conscio
Technologies

SOMMAIRE

INTRODUCTION

Dans un contexte où les **cyberattaques se multiplient** et **ciblent de plus en plus les collectivités territoriales**, la sensibilisation à la cybersécurité devient un **enjeu majeur**. Les collectivités gèrent une quantité considérable de données sensibles et sont confrontées à des défis uniques en matière de cybersécurité : budgets restreints, infrastructures informatiques hétérogènes et utilisateurs aux profils variés. Pourtant, malgré la montée des risques, la participation aux actions de sensibilisation reste **souvent insuffisante**.

Chez **Conscio Technologies**, nous avons développé une **démarche spécifique pour les collectivités territoriales** afin de vous aider, RSSI et DSI, à structurer et optimiser vos initiatives de sensibilisation. Nos **analyses** et **retours d'expérience** montrent que la mise en place d'un **programme dédié** aux agents territoriaux permet d'améliorer considérablement **l'adoption des bonnes pratiques** en cybersécurité. Une récente **infographie issue de nos campagnes de sensibilisation** met en évidence des données dans ce secteur : participation moyenne sur l'ensemble des campagnes de sensibilisation, meilleure identification des risques et un excellent taux de bonnes réponses sur l'ensemble de leur(s) campagne(s).

Notre approche repose sur la **méthodologie OKISPRI**, un cadre structurant conçu pour **renforcer l'engagement** des collaborateurs et **ancrer durablement les bons comportements**. En intégrant des contenus contextualisés, des formats courts et interactifs ainsi qu'une approche progressive, nous vous permettons d'adapter la sensibilisation aux **réalités opérationnelles de vos agents**.

Afin de vous accompagner dans l'optimisation de votre stratégie de sensibilisation, nous avons organisé un **webinaire** dédié à l'engagement et la participation des agents. Ce livre blanc en synthétise les principaux enseignements et propose un retour d'expérience détaillé d'un RSSI d'une grande métropole, dont l'identité reste volontairement anonymisée.

Ce **cas concret** illustre l'impact d'une telle démarche. Conscient des défis spécifiques aux collectivités territoriales, ce RSSI a mis en place plusieurs actions pour **adapter la sensibilisation aux contraintes et aux besoins de ses équipes**. Grâce à ces ajustements, il a pu constater une évolution et une amélioration notable des comportements face aux cybermenaces. Ce retour d'expérience, détaillé dans ce **livre blanc**, met en lumière les **leviers actionnables** pour relever le niveau de de la sensibilité à la sécurité informatique au sein des collectivités et instaurer une **culture cyber durable**.

L'objectif de cette publication est **d'offrir une méthodologie éprouvée** et des **recommandations pragmatiques** pour **maximiser la participation** aux sensibilisations et ancrer une véritable **culture cyber** au sein de votre collectivité.

ACCOMPAGNER LES COLLECTIVITÉS : UNE DÉMARCHE SUR-MESURE POUR RENFORCER LA CULTURE CYBER

1.1 UN CONTEXTE DE MENACE CROISSANTE

Les collectivités territoriales sont confrontées à des risques cyber de plus en plus récurrents et sophistiqués. En 2022, une **recrudescence des attaques** a été constatée, touchant aussi bien les grandes métropoles que les petites communes. Les **rançongiciels**, le **phishing** et **l'ingénierie sociale** comptent parmi les menaces majeures auxquelles elles doivent faire face. Or, ces cyberattaques ont des conséquences lourdes : interruption des services administratifs, coûts financiers élevés, vol et copie de données sensibles, ainsi qu'une atteinte à la réputation de la collectivité.

Le facteur humain joue un rôle clé dans la cybersécurité et peut être à l'origine de certaines vulnérabilités. En effet, **30% des collectivités ont déjà été victime d'un rançongiciel** (ransomware). Sensibiliser vos agents devient donc une **priorité absolue** pour renforcer la résistance de votre collectivité face aux cybermenaces.

1.2 UNE APPROCHE ADAPTÉE AUX SPÉCIFICITÉS DES COLLECTIVITÉS

Conscio Technologies accompagne, **depuis plus de 10 ans**, les collectivités territoriales dans la **mise en place de stratégie de sensibilisation à la cybersécurité**. L'objectif est d'offrir une **solution clé en main** adaptée à la diversité des populations identifiées et à leurs besoins spécifiques. En effet, les collectivités regroupent des profils variés : élus, agents administratifs, techniciens, encadrants, personnels en télétravail, utilisateurs de données sensibles, etc... Chacun de ces profils est exposé à des **risques différents** et nécessite un **accompagnement ciblé**.

L'offre de Conscio Technologies repose sur plusieurs piliers :

- **Une plateforme dédiée « Sensiwave »** : une solution alliant sensibilisation et tests de phishing, spécifiquement conçue pour répondre aux besoins des collectivités.
- **Des contenus variés et engageants conçus pour les collectivités** : scénarios immersifs, vidéos interactives, livres interactifs, quiz, podcasts, chatbot, etc...

- **Un programme annuel (ou pluriannuel) structuré** : des campagnes de sensibilisation bimensuelles, articulées autour des grandes thématiques cyber (poste de travail, rançongiciels, phishing, protection de l'information, mots de passe, ingénierie sociale, etc...).
- **Un accompagnement personnalisé** : une équipe Customer Success dédiée, qui vous suit constamment et ajuste les campagnes en fonction des retours et des besoins identifiés.

1.3 UNE SENSIBILISATION EFFICACE ET MESURABLE

L'efficacité d'une sensibilisation repose sur **l'implication des agents** et sur la **capacité à mesurer les progrès réalisés**. La solution de Conscio Technologies permet **d'évaluer le niveau de sensibilisation** des agents et **d'ajuster les actions** en conséquence. Plusieurs indicateurs sont suivis, notamment :

- Le **taux de participation** aux campagnes de sensibilisation,
- Le **taux de réussite** aux évaluations et aux quiz,
- Le **niveau d'intérêt et de satisfaction** des agents,
- Les **résultats des tests de phishing**.

Les retours d'expérience des collectivités accompagnées montrent un fort engagement des agents. Le **score moyen de satisfaction des formations est de 4,5/5**, et plus de deux tiers des agents **recommandent les modules de sensibilisation à leurs collègues**. Ces résultats témoignent de **l'efficacité des programmes** et de leur **pertinence** pour répondre aux enjeux des collectivités territoriales.

1.4 DES RÉSULTATS CONCRETS POUR UNE MEILLEURE RÉSILIENCE

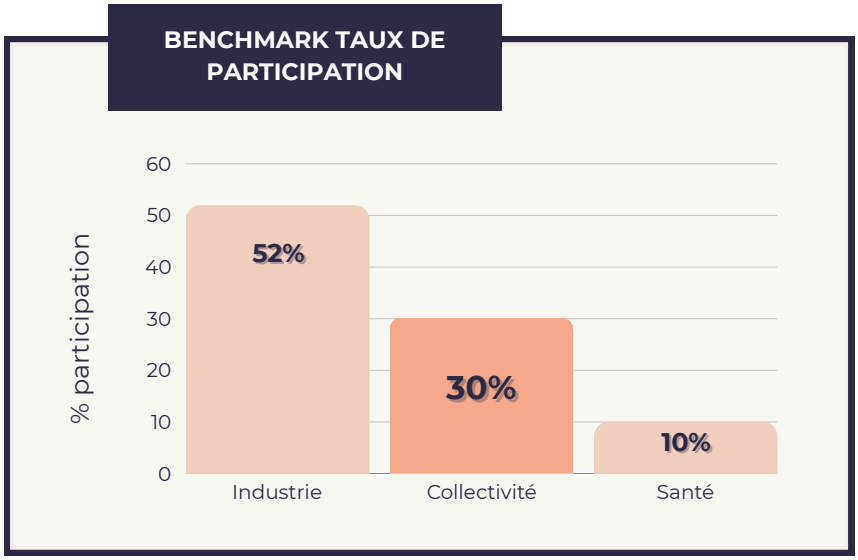
Grâce à cette approche, les collectivités peuvent **renforcer significativement leur posture en cybersécurité**. Les agents deviendront plus vigilants face aux tentatives de phishing et aux autres menaces numériques. Les élus et les responsables IT (RSSI, DSI, DPO) disposent d'un outil performant pour **structurer la sensibilisation** et **pérenniser les bonnes pratiques**.

INFOGRAPHIE 2024 : ÉTAT DES LIEUX ET PERSPECTIVES DES SENSIBILISATIONS CYBER DANS LES COLLECTIVITÉS

2.1 UN TAUX DE PARTICIPATION PERFECTIBLE

Les campagnes de sensibilisation à la cybersécurité dans les collectivités territoriales, **menées sur notre base d'abonnés**, ont mobilisé en 2024 **plus de 62 000 agents**, soit une **augmentation de 37 %** par rapport à 2023.

Toutefois, le taux de participation **reste limité à 30 %**, avec une **légère hausse observée** au sein des conseils départementaux (**+3 points** par rapport aux autres types de collectivités).



Ce chiffre, bien que révélateur d'un **engagement modéré**, souligne la nécessité d'**optimiser les stratégies d'adhésion** des agents aux campagnes de sensibilisation. Des **pistes d'actions sont d'ailleurs détaillées** plus loin dans ce livre blanc.

2.2 LES THÉMATIQUES ET FORMATS PRIVILÉGIÉS

Les sujets **les plus abordés** dans les campagnes de sensibilisation sont le **phishing**, suivi des **codes malveillants**, des **mots de passe**, de la protection des informations et des rançongiciels. Le format « ***vidéo interactive*** », d'une durée moyenne de **3 minutes**, est **plébiscité par les collectivités**. Ce choix s'explique par la capacité de ces contenus courts à **capter l'attention** des agents et à **s'intégrer facilement dans leur quotidien professionnel**.

2.3 RÉSULTATS DES CAMPAGNES DE PHISHING

Les tests de phishing révèlent **qu'un collaborateur sur dix a cliqué sur un lien frauduleux** et que **6% des collaborateurs** ont saisi leurs identifiants ou téléchargé des pièces jointes frauduleuses. Malgré une **meilleure compréhension des menaces**, ces comportements à risque rappellent la nécessité de **renforcer la vigilance des agents** et **d'intégrer des rappels réguliers** sur les bonnes pratiques de cybersécurité. En poursuivant les efforts de formation et d'accompagnement, vous pouvez **améliorer durablement la résilience** de vos agents face aux cybermenaces.

2.4 STRATÉGIES D'ENVOI ET DE RELANCE

En 2024, les collectivités ont **déployé en moyenne 6 campagnes de sensibilisation**, illustrant un **engagement constant** en matière de cybersécurité. La **fréquence bimestrielle** des envois permet de **rythmer l'apprentissage**, tandis que la mise en place de **relances stratégiques à J+15** permettent aux agents n'ayant pas encore entamé leur sensibilisation d'être relancés et d'avoir une nouvelle opportunité de participer aux campagnes. Cette approche progressive **favorise une montée en compétence** des agents, en assurant une **répétition des concepts essentiels** et en **renforçant les réflexes** de cybersécurité au sein des collectivités.

2.5 PERFORMANCES ET AXES D'AMÉLIORATION

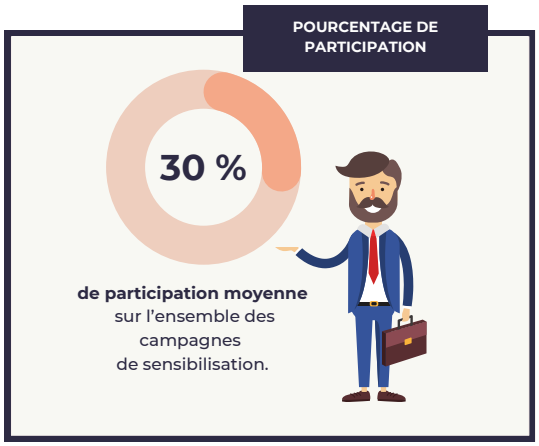
Les collectivités affichent un **taux moyen de bonnes réponses de 88 %** sur l'ensemble des campagnes. Cela témoigne d'une **assimilation notable des messages de sensibilisation**. Toutefois, plusieurs **axes d'amélioration** ont été identifiés :

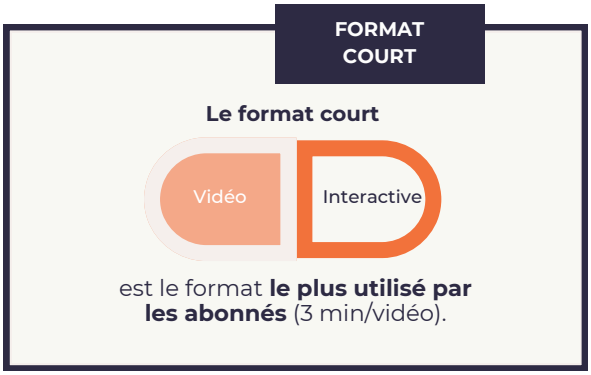
- **Optimiser la participation** : avec un taux moyen de 30%, la marge de progression est significative. Des stratégies incitatives et une meilleure intégration des formations dans le quotidien des agents pourraient favoriser l'engagement. C'est dans cette optique que Conscio Technologies a conçu son nouveau support le « Game Map » par son côté ludique et localisé qui favorise l'engagement des utilisateurs.

- **Affiner le ciblage des campagnes** : actuellement, les collectivités ciblent en majorité l'ensemble de leurs agents lors de l'envoi de campagnes de sensibilisation. Bien que cette pratique soit nécessaire pour exposer un maximum d'utilisateurs aux connaissances de base de la sécurité informatique, il est nécessaire d'affiner dans le temps le ciblage des campagnes pour maintenir l'intérêt des agents. En effet, l'exposition à des cas concrets de problématiques de sécurité en lien avec les différents métiers permet de mieux capter l'attention des apprenants et rendre le processus de sensibilisation plus pertinent aux yeux des agents.

- **Renforcer la sensibilisation au phishing** : bien que des progrès soient notés chez la majorité de nos abonnés, il est essentiel de continuer à sensibiliser les agents aux techniques d'hameçonnage et aux bonnes pratiques à adopter en cas de tentative d'attaque, les menaces continuant d'évoluer quotidiennement.

L'analyse des campagnes de sensibilisation menées en 2024 met en évidence des **avancées notables**, mais aussi des **défis persistants**. **L'augmentation du nombre d'agents sensibilisés** et les **bons taux de réussite** témoignent d'un **engagement croissant**, mais le **taux de participation limité** souligne la **nécessité d'une mobilisation plus large**. Les collectivités ont su **structurer un programme efficace**, et les **stratégies de relance permettent de maximiser l'exposition aux contenus pédagogiques**. Toutefois, un **ciblage plus précis** et une **diversification des formats** pourraient renforcer l'adhésion des agents. La cybersécurité étant un enjeu prioritaire, la montée en maturité des collectivités sur ces questions demeure essentielle pour **assurer la protection des données et des infrastructures publiques**.





RETOUR D'EXPÉRIENCE : COMMENT UN RSSI DE MÉTROPOLE A RENFORCÉ LA PARTICIPATION AUX SENSIBILISATIONS

3.1 CONTEXTE ET ENJEUX

Lors du webinaire organisé dans le cadre des « ***RDV cyberCoTer*** » de Conscio Technologies, un **RSSI exerçant dans une grande métropole** a partagé son retour d'expérience sur la **mise en place d'une stratégie efficace visant à maximiser l'engagement des agents**. Pour rappel, pour des raisons de confidentialité, ce retour d'expérience restera anonyme. Son approche repose sur plusieurs **actions concrètes**, **articulées autour de la communication**, de la **structuration** et du **développement d'une véritable culture cyber**.

3.2 DÉVELOPPER LES CANAUX DE COMMUNICATION

L'un des premiers leviers activés a été la **diversification des supports de communication** pour **toucher un maximum d'agents** et **s'adapter aux différentes habitudes de travail**. Plusieurs canaux ont été exploités :

- **Emails** : des campagnes de sensibilisation envoyées régulièrement avec des messages courts et impactants.
- **Intranet** : une section dédiée à la cybersécurité, mise à jour avec des ressources pratiques.
- **Affiches et écrans de veille** : présence de messages de sensibilisation dans les lieux de passage des agents.
- **Phishing simulé** : envoi de campagnes de phishing factices pour tester et améliorer la vigilance des collaborateurs.
- **Présentiel et e-learning** : sessions de formation en ligne et interventions ponctuelles pour renforcer l'engagement.

L'objectif était d'**adapter les contenus en fonction du support**, en **vulgarisant les messages** et en les **rendant aussi concrets et personnalisés que possible**.

3.3 METTRE EN PLACE UN ESPACE CYBER ACCESSIBLE

Pour ancrer la cybersécurité dans le quotidien des agents, un **espace cyber** a été créé. Celui-ci centralise plusieurs éléments :

- Les **politiques** et **chartes de sécurité** de la collectivité,
- Des **guides** et **bonnes pratiques** à destination des agents,
- La **stratégie cybersécurité en place** et les **prochaines actions**,
- Une **veille cyber** pour sensibiliser aux menaces émergentes.

Cet espace a permis de **structurer l'information** et **d'offrir aux agents un point d'entrée unique** pour **s'informer** et **approfondir leurs connaissances** en fonction de leurs besoins.

3.4 S'INSCRIRE DANS UNE STRATÉGIE À LONG TERME

Un autre facteur clé de succès a été **l'intégration des actions de sensibilisation dans une stratégie globale et pérenne**. Cette approche repose sur plusieurs axes :

- **Définition des budgets** et **objectifs** pour garantir la continuité des actions.
- **Planification annuelle des événements** et **campagnes de communication**.
- **Mise en place d'indicateurs de suivi** pour mesurer la progression et ajuster la stratégie.
- **Partage des rapports** et **bilans** avec la direction et les parties prenantes.

L'anticipation et la **planification** ont **permis d'éviter une approche ponctuelle** et **d'assurer un impact durable**.

3.5 DÉVELOPPER UNE CULTURE CYBER AU TRAVERS DE PROJETS CONCRETS

Suite à une attaque d'un établissement proche de leur périmètre, la direction s'est **emparée du sujet cybersécurité**. La DSI a été sollicitée pour **travailler en collaboration** avec les différentes directions adjointes afin de **structurer** et **co-construire un PCA**, au cas où une attaque cyber interviendrait sur leur périmètre. Ce projet concret a permis de **casser le sentiment d'invulnérabilité** au sein de la gouvernance et d'inscrire la démarche cyber comme **essentielle dans la continuité des services**.

3.6 TROIS PHASES POUR MAXIMISER L'ENGAGEMENT

Pour synthétiser les enseignements du webinaire et le retour d'expérience du RSSI, nous vous proposons **trois phases clés pour maximiser l'engagement des agents** :

1. **Susciter l'intérêt** : lancer la campagne sur un temps fort, personnaliser les messages et démontrer l'intérêt individuel de la cybersécurité.
2. **Maintenir l'intérêt** : relancer régulièrement, varier les supports et impliquer d'autres services comme la communication ou les RH.
3. **Augmenter l'intérêt** : encourager la participation avec des challenges et renforcer l'aspect communautaire en s'appuyant sur l'actualité cyber. De nombreuses autres pistes sont évoquées dans notre livre blanc sur la « sensibilisation impliquante ».

3.7 RÉSULTATS ET ENSEIGNEMENTS

Grâce à cette approche, la **participation aux sensibilisations cyber a connu une nette progression**. Les agents ont progressivement **pris conscience des enjeux** et ont **développé des réflexes plus solides** face aux cybermenaces. Les indicateurs de suivi ont montré une **augmentation significative du taux de participation aux formations** et une **meilleure identification des tentatives de phishing**.

Le retour d'expérience de ce RSSI démontre qu'une **sensibilisation efficace** repose sur une **stratégie structurée**, combinant **diversité des supports**, **engagement des agents** et **ancrage dans le temps**. Ce modèle peut être appliqué par d'autres collectivités souhaitant **renforcer leur culture cyber** et **assurer la protection de leurs systèmes d'information**.

OKISPRI : UNE MÉTHODOLOGIE STRUCTURÉE POUR UNE SENSIBILISATION EFFICACE ET ENGAGEANTE

4.1 LA MÉTHODE OKISPRI : UNE APPROCHE COMPLÈTE ET STRUCTURÉE

Développée par Conscio Technologies, la méthodologie **OKISPRI** repose sur sept piliers permettant **d'organiser** et **d'optimiser la sensibilisation en cybersécurité** :

- **O pour Objectifs** : définir clairement les finalités de la sensibilisation, qu'il s'agisse de réduire les incidents de sécurité, d'améliorer la culture cyber ou encore de renforcer la conformité réglementaire.
- **K pour KPIs** : mettre en place des indicateurs clés de performance permettant de mesurer l'efficacité des actions menées, comme le taux de participation, le taux de succès aux quiz ou encore la réactivité face aux campagnes de phishing.
- **I pour Sensibilisation IMPLIQUANTE** : utiliser des techniques de psychologie de la persuasion et de l'engagement pour transformer la sensibilisation en un levier de changement comportemental durable.
- **S pour Stratégie** : structurer les campagnes en définissant les populations ciblées, les messages adaptés et les formats les plus pertinents.
- **P pour Pilote** : tester les campagnes sur un groupe restreint afin d'affiner les contenus et les supports avant un déploiement à grande échelle.
- **R pour Run** : déployer les campagnes à l'ensemble de l'organisation tout en suivant les statistiques de participation et d'engagement.
- **I pour Impact** : évaluer l'évolution des comportements grâce à des enquêtes et des mesures post-campagnes.

4.2 LES LEVIERS CLÉS POUR MAXIMISER LA PARTICIPATION DES AGENTS

Les campagnes de sensibilisation menées en 2024 auprès des collectivités territoriales ont permis **d'identifier plusieurs leviers d'optimisation** pour **améliorer la participation** des agents. Parmi eux, la **structuration de la stratégie** grâce à OKISPRI joue un rôle central :

- **Un ciblage plus précis des agents** : aujourd'hui, les campagnes sont majoritairement adressées à l'ensemble des agents sans distinction. En appliquant la segmentation définie dans OKISPRI, il est possible d'adapter les messages aux profils des utilisateurs (élus, agents administratifs, techniciens, etc...).
- **Des formats engageants et interactifs** : l'intégration de vidéos interactives et de formats courts permet de capter l'attention des agents et de s'adapter à leur disponibilité.
- **Une fréquence optimisée** : les relances à J+15 et l'adoption d'un rythme bimestriel permettent de maximiser l'exposition aux messages de sensibilisation.

4.3 TÉMOIGNAGE DU RSSI D'UNE GRANDE MÉTROPOLE ET MISE EN PERSPECTIVE AVEC OKISPRI

Lors d'un webinaire dédié à comment maximiser la participation des agents, le RSSI a partagé son retour d'expérience sur la sensibilisation de ses agents. Il a notamment **mis en avant plusieurs défis et bonnes pratiques**, qui **font écho à la méthodologie OKISPRI** :

- **Problématique de l'engagement des agents** : un des freins majeurs reste l'adhésion des agents aux formations cybersécurité. La méthode OKISPRI, en mettant l'accent sur la sensibilisation impliquante et la segmentation des cibles, répond précisément à cette difficulté en adaptant le message et les supports aux différents profils d'utilisateurs.
- **Besoin d'une stratégie continue et évolutive** : il a insisté sur l'importance d'une approche progressive et régulière, ce qui rejoint la structure d'OKISPRI avec un déploiement en plusieurs phases (Pilote, Run, Impact) et l'adaptation des messages en fonction des résultats obtenus.
- **Importance des KPIs pour évaluer les progrès** : il a également souligné l'intérêt de mesurer précisément l'impact des campagnes afin de justifier leur nécessité auprès des décideurs. L'approche OKISPRI repose justement sur la définition de KPIs clairs et actionnables, permettant de suivre et d'ajuster les campagnes en fonction des retours.

Ce retour d'expérience illustre la **pertinence d'une approche structurée** comme celle d'OKISPRI pour **optimiser la sensibilisation dans les collectivités territoriales**. Il démontre que, loin d'être une simple formalité, la **sensibilisation bien pensée** et **pilotée** peut devenir un **levier majeur** pour **renforcer la posture cyber des collectivités**.

BONNES PRATIQUES ET RECOMMANDATIONS

Maximiser la participation aux sensibilisations cyber dans vos collectivités requiert une **approche structurée**, **adaptée à vos contraintes** et à la **diversité de vos agents**. À travers le retour d'expérience et les méthodologies partagées dans ce livre blanc, plusieurs bonnes pratiques se dégagent, vous permettant **d'optimiser l'adhésion** et **l'efficacité de vos campagnes de sensibilisation**.

Diversifier les canaux et **les formats** est essentiel pour **toucher l'ensemble de vos agents**. L'e-learning seul ne suffit pas : les emails, les affiches, l'intranet, les simulations de phishing et les sessions en présentiel **doivent être intégrés à une stratégie globale**. L'information doit être **claire**, **accessible** et **adaptée** aux besoins spécifiques de vos collectivités.

Les actions ponctuelles ont un effet limité. Inscrire la sensibilisation dans une **démarche continue**, avec une **planification annuelle**, un **budget dédié** et des **indicateurs de suivi**, garantit une **montée en maturité progressive**. **L'engagement** passe également par une **approche dynamique**, qui suscite **l'intérêt dès le départ**, le **maintien par des relances régulières** et le **renforce grâce à des initiatives engageantes** comme des **retours d'incidents concrets** ou **des challenges internes**.

L'implication de votre direction et de **vos relais internes**, tels que les RH et les managers, **crédibilise les campagnes** et leur donne une **portée plus large**. Enfin, **l'évaluation** et **l'adaptation** de vos actions en fonction des retours et des indicateurs permettent **d'affiner votre stratégie** et de **l'aligner avec les réalités du terrain**.

En appliquant ces bonnes pratiques, vous pouvez non seulement **renforcer la culture cyber de votre collectivité**, mais aussi **mieux vous prémunir contre les menaces numériques**, en faisant de vos agents des **acteurs engagés et conscients des enjeux de cybersécurité** !

TÉLÉPHONE : 01 84 80 82 00

MAIL : contact@conscio-technologies.com

SITE : www.conscio-technologies.com

ADRESSE : 3 rue Camille Claudel, 56890 PLESCOP

conscio
Technologies