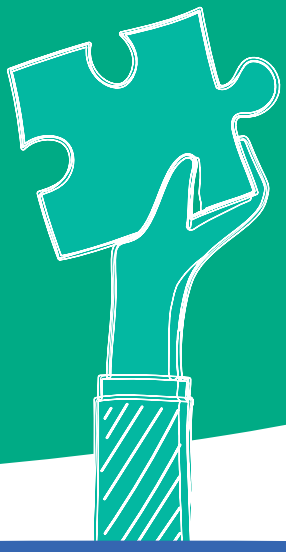
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

CYBERSÉCURITÉ

Méthode clé en main pour sensibiliser les agents des collectivités



WWW.CYBERMALVEILLANCE.GOUV.FR
en partenariat avec l'AMF

AMF
ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ

ÉDITOS

Ces dernières années, les collectivités ont été les cibles de très nombreuses cyberattaques. Si une prise conscience collective commence à s'opérer, il reste encore beaucoup à faire pour atteindre un bon niveau de sécurité et démystifier ce sujet.

Obscure pour certains, anxiogène pour d'autres, la cybersécurité est encore trop souvent perçue comme une contrainte et comme un sujet uniquement technique. Mais si l'aspect technologique est essentiel pour assurer la cybersécurité des collectivités, la partie humaine ne doit pas être minimisée pour autant.

Nous le voyons chaque jour à travers les centaines de demandes d'assistance sur la plateforme Cybermalveillance.gouv.fr, la plupart des attaques ciblent l'humain. Et nombre d'entre elles auraient pu être évitées avec une sensibilisation efficace aux risques numériques et un apprentissage des bonnes pratiques au quotidien.

C'est pourquoi Cybermalveillance.gouv.fr et l'Association des maires de France et des présidents d'intercommunalité (AMF) ont souhaité proposer aux collectivités une méthodologie « clé en main » et les outils associés pour faire face à la menace. Une démarche qui s'inscrit parfaitement dans le cadre de la mission d'intérêt général de Cybermalveillance.gouv.fr et qui vise à accompagner les collectivités souhaitant initier une démarche de cybersécurité auprès de leurs agents en leur apportant à la fois des notions théoriques et les outils pratiques pour la mener à bien.

L'objectif ? Permettre aux collectivités de disposer des clés nécessaires pour appréhender le sujet, préparer, former et responsabiliser les agents face aux enjeux de la cyber et en faire de véritables partenaires de la sécurité de leur collectivité.

J'espère que cette méthodologie vous sera utile et vous aidera à renforcer jour après jour la cybersécurité de votre collectivité.

Bonne lecture et bonne mise en œuvre !

© Guillaume Lechat

JÉRÔME **NOTIN**

*Directeur général du GIP ACYMA**

Dispositif Cybermalveillance.gouv.fr

* GIP ACYMA : Groupement d'Intérêt Public (GIP) Actions contre la cybermalveillance (ACYMA)

La cybersécurité est une exigence durable et complexe pour toute organisation, y compris publique. La numérisation croissante des usages et des pratiques fait augmenter significativement le risque de cyberattaques sur les collectivités. L'espace numérique, à l'instar du monde physique, est devenu un milieu à risque dans lequel il faut savoir évoluer.

Les communes et intercommunalités sont des cibles à part entière. Elles doivent donc se prémunir et s'organiser en conséquence.

Pour aider les mairies, l'AMF s'est associée à Cybermalveillance.gouv.fr pour éditer ce guide méthodologique afin de sensibiliser les agents des collectivités à la cybersécurité. Ces derniers constituent le premier maillon de la chaîne sécurité dans nos communes face au risque cyber. Des conseils simples et de bon sens sont présentés dans cet ouvrage pour organiser et faire passer les messages de prévention.

Faire face aux crises, c'est s'y préparer. Toutes les actions présentées dans ce guide sont autant de clés permettant d'augmenter l'immunité de nos communes et collectivités face au risque de cyberattaques. La cybersécurité est l'affaire de tous.

© Arnaud Février pour l'AMF

DAVID **LISNARD**

Président de l'Association des maires de France et des présidents d'intercommunalité

SOMMAIRE

PRÉAMBULE

La méthode clé en main qui vous est présentée s'adresse à l'ensemble des collectivités qui initient une démarche de sensibilisation. Présentée dans son intégralité, elle est une illustration idéale d'un programme de sensibilisation global. **Sa mise en œuvre dépendra de la priorité donnée au risque cyber, de la disponibilité et des ressources à y dédier.**

Cette méthodologie est conçue comme une **« boîte à outils cyber » modulable et personnalisable.** *Elle permet ainsi d'élaborer un plan d'action adapté en se concentrant par exemple sur 2 clés et 1 ou 2 thématiques sur une période plus courte, ce qui constituera un premier pas dans la sensibilisation des agents de la collectivité à la cybersécurité.*

POURQUOI SENSIBILISER LES AGENTS DES COMMUNES ET DES EPCI*?

Dans le cadre de sa mission de prévention, Cybermalveillance.gouv.fr s'adresse à différents publics, dont les collectivités territoriales, particulièrement exposées au risque.
Comment faire pour inverser cette tendance ? Quels bénéfices en retirer ?
À travers sa démarche de prévention, Cybermalveillance.gouv.fr répond à toutes ces questions.

Des collectivités très exposées et peu conscientes du risque
Alors que les cyberattaques sont légion – Cybermalveillance.gouv.fr enregistrait une augmentation de près de 70 % de demandes d'assistance en ligne en 2021 - le risque cyber est omniprésent et touche aujourd'hui tout type de structure.
Les collectivités territoriales ne font pas exception : intercommunalités, communes… Désormais, plus aucune entité publique n'échappe à la menace. Or, si les grandes entreprises sont plus « armées » pour faire face aux défis de la cybersécurité, les collectivités territoriales, et notamment les plus petites, en sont encore loin.

L'étude** menée par Cybermalveillance.gouv.fr auprès des collectivités de moins de 3 500 habitants met ainsi en exergue **leur faible préparation vis-à-vis de l'enjeu cyber.**
Au-delà d'un manque de connaissance et d'information sur le sujet pour plus des deux tiers des publics concernés, maires, adjoints, DGS et agents, l'enquête de Cybermalveillance.gouv.fr révèle le défaut de formation à la cybersécurité des responsables ou des prestataires informatiques des collectivités.
Plus encore, la plupart des personnes interrogées ne sont pas du tout au fait des obligations relatives aux compétences et responsabilités qui incombent aux collectivités et aux élus en matière de sécurité numérique.
Des résultats qui témoignent du fait que les collectivités territoriales constituent une cible particulièrement vulnérable.

Il est urgent de sensibiliser et de responsabiliser TOUS LES AGENTS

On le sait aujourd'hui, le facteur humain est à l'origine de nombreuses attaques. Un utilisateur averti permet de réduire considérablement les risques et contribue même à élever le niveau de sécurité collectif, d'où la nécessité d'impliquer toute la collectivité dans cette démarche, du stagiaire à l'élu en passant par les agents.

Fort de ces constats, Cybermalveillance.gouv.fr a souhaité, en partenariat avec l'AMF, proposer à chaque collectivité une **méthodologie « clé en main »**, pour sensibiliser l'ensemble des agents, composée à la fois :
- d'une approche théorique avec « 5 clés pour une sensibilisation réussie » ;
- une proposition de plan d'action concrète et facilement réalisable ;
- ainsi qu'un ensemble d'outils et de contenus pédagogiques dédiés.

L'objectif de cette prévention ?
Responsabiliser, préparer et former les agents pour être plus fort face au risque cyber.

* Établissement public de coopération intercommunale
** Étude menée auprès de 524 collectivités de moins 3 500 habitants publiée en mai 2022.

5 CLÉS POUR UNE SENSIBILISATION RÉUSSIE

Cybermalveillance.gouv.fr et l'AMF
proposent de s'appuyer sur **5 CLÉS**
pour définir un **PROGRAMME DE SENSIBILISATION**
à destination des agents de la collectivité.
SUIVEZ LE GUIDE !

1 Prendre conscience du risque cyber

RÉALISER LES CONSÉQUENCES D'UNE CYBERATTAQUE

Le préalable de cette campagne de sensibilisation est d'aborder les enjeux auxquels sont exposés les agents au quotidien. L'objectif étant de leur faire prendre conscience des risques, des impacts potentiels immédiats et à plus ou moins long terme pour la collectivité en cas de manquement aux bonnes pratiques.

COMPRENDRE LES IMPACTS D'UNE CYBERATTAQUE

Il suffit d'une seule intrusion dans un système pour entraîner :

- **la perturbation des services**, voire l'arrêt de l'activité de la collectivité ;
- **l'inaccessibilité, la destruction**, le vol, ou la diffusion des données de la collectivité et des administrés, des difficultés à revenir à l'état précédant l'attaque ;
- **des dommages collatéraux** avec un effet « domino » pour l'écosystème de la collectivité (administrés, prestataires externes et autres structures publiques…) ;
- **des pertes financières** directes ou indirectes ;
- **des atteintes à l'image**, à la réputation de la collectivité, voire une rupture de la confiance numérique entre la collectivité et ses parties prenantes (administrés, prestataires…) ;
- **des risques sociaux** et psycho-sociaux pour les agents ;
- **des risques juridiques** : la responsabilité* (civile, pénale et administrative) de la collectivité peut en effet être engagée.

RECONNAÎTRE LES USAGES À RISQUE

En effet : un seul clic sur un lien malveillant, le téléchargement d'une pièce jointe infectée ou encore, la réutilisation d'un mot de passe tombé entre de mauvaises mains, peuvent ainsi avoir de graves conséquences.

TOP 3 DES ATTAQUES

Rançongiciel, hameçonnage et piratage de compte constituent le top 3 des attaques auprès des collectivités. Des techniques qu'il convient de comprendre et de faire connaître à tous les agents pour mieux les appréhender et les former sur les gestes essentiels de sécurité.

* Guide sur les obligations et les responsabilités des collectivités locales en matière de cybersécurité en collaboration avec la CNIL

5 CLÉS POUR UNE SENSIBILISATION RÉUSSIE

2 Impliquer les agents des collectivités

LA CYBERSÉCURITÉ EST L'AFFAIRE DE TOUS

Une cyberattaque est souvent le fait d'une négligence humaine. Il suffit parfois d'une simple erreur pour rendre toute une collectivité vulnérable.
Si chaque agent en est conscient, alors, chacun à son niveau peut être acteur d'une politique cyber et contribuer à protéger sa collectivité, notamment en adaptant son comportement.

ADOPTER LES BONS RÉFLEXES

Une fois que les agents ont pris conscience des risques cyber et des impacts encourus par la collectivité, il devient plus légitime d'introduire les règles à suivre ou les bons réflexes à adopter. Ainsi, en cas de doute face à une situation à risque ou inhabituelle, Cybermalveillance.gouv.fr recommande :

- d'être vigilant et ne pas prendre en main seul le problème éventuel ;
- et le cas échéant, de contacter immédiatement son responsable informatique, son référent cyber si la collectivité en a un, ou son prestataire.

ATTEINDRE SES PUBLICS

Afin d'optimiser la démarche de prévention de la collectivité, tous les agents (quelle que soit la taille de la commune) doivent être régulièrement sensibilisés à travers :

- **différents messagers ou relais de communication** (contact cyber privilégié, élus ou agents en charge du sujet etc.) ;
- **l'expérience, les témoignages et les initiatives d'autres collectivités** (attaques, bonnes pratiques, usages etc.) pour rendre le sujet plus concret afin que les agents puissent s'identifier et s'en emparer plus facilement ;
- **des supports ou visuels de communication originaux** et disruptifs pour les interpeller, à l'instar des campagnes ci-contre :

IDENTIFIER UN CONTACT PRIVILÉGIÉ ET S'APPUYER SUR LA COMMUNICATION

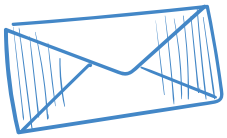
Le plus

Toutes les collectivités ne bénéficient pas nécessairement d'experts ou de spécialistes de la cyber, voire d'un directeur de la communication pour les aider à conduire des campagnes. L'idéal ? Identifier un contact au sein de la collectivité sur ce sujet de la cyber pour répondre aux questions des agents et les rassurer. De la même façon, pour les communes ne disposant que d'un ou quelques agents, bénéficier du soutien d'un élu engagé pour valoriser le sujet et recueillir l'adhésion de tous les agents, tous services et fonctions confondus est clé.

3 S'appuyer sur les bonnes ressources pédagogiques

RENFORCER SES MESSAGES AVEC LES BONS CONTENUS

Conscients des enjeux et impliqués dans la démarche de sensibilisation, les agents vont avoir besoin d'être régulièrement nourris de contenus illustrant les exemples à retenir ou à proscrire en matière de cybersécurité. Et pour s'assurer de capter leur attention dans le temps, le choix des messages et des contenus et leur contextualisation en fonction de la ou des collectivités concernées sera déterminant.



PERSONNALISER LA COMMUNICATION

Pour maintenir l'engagement des publics, il importe de commencer par :

1. ***Identifier les différentes cibles*** (agents, élus et autres parties prenantes) et de définir des profils (2 ou 3 maximum) selon leur niveau de maturité.

2. ***Définir son discours.*** Une fois cette première étape franchie, il suffira de « calibrer » les messages (le fond, *i. e.* thématiques et leur forme, *i. e.* ton à adopter) en fonction :
   - des différents profils à sensibiliser en procédant par priorité avec les profils les plus à risque,
   - des objectifs quantitatifs et qualitatifs à atteindre.

3. ***Choisir les bons contenus pour les bons profils.*** En fonction des profils et de leur maturité, il restera à sélectionner les contenus correspondant à ces publics en privilégiant les solutions à retenir plutôt que les messages anxiogènes.

4. ***Sélectionner les bons canaux de diffusion.*** Enfin, après avoir défini les différents publics et les contenus dont ils ont besoin, la dernière étape consiste à mettre en face de chaque cible les canaux les plus adaptés (réunion de visu ou en visioconférence, affichage, intranet, campagne e-mail, SMS…).

Le plus

TESTER LE PROGRAMME DE SENSIBILISATION…

…pour vérifier la bonne adéquation messages/cibles/canaux, identifier un contact représentatif de la cible pour tester le dispositif et recueillir de premiers commentaires afin d'ajuster le discours ou les vecteurs retenus.

4 Décliner et répéter les messages

RÉPÉTER POUR GARANTIR LA MÉMORISATION DU MESSAGE

Pour optimiser l'efficacité et le succès des campagnes de sensibilisation, la mémorisation passe par la répétition. Le défi est de réussir à répéter sans lasser ses cibles afin d'entretenir l'intérêt pour le sujet, tout en développant leur culture cyber.

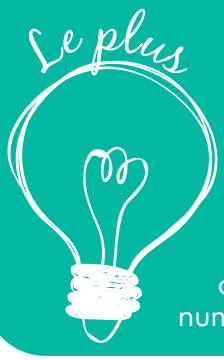
ÉLABORER UN PLAN D'ACTION ET UN CALENDRIER

Pour assurer la pérennité des messages et leur ancrage auprès des cibles, définir des actions ou des temps forts en échelonnant les communications dans le temps est particulièrement efficace.

De cette façon, mettre en place un programme de sensibilisation et un plan de communication permettra :

- *aux messages de s'inscrire dans la durée*
  par vagues successives en ayant recours à différents supports (affichage, mails, vidéos…) ;
- *de faire monter en puissance les messages*
  selon les thématiques sécurité ;
- *de favoriser l'apprentissage progressif des cibles*
  qui gagneront peu à peu en maturité cyber.

Le plus



DONNER VIE À LA SENSIBILISATION

Utiliser des illustrations, qu'il s'agisse de photos ou vidéos pour mettre en avant des exemples, des initiatives ou des témoignages est particulièrement pertinent en termes de messages, à l'instar des méthodes utilisées sur les réseaux sociaux.

Par ailleurs, il s'avère particulièrement judicieux pour marquer les publics d'utiliser des métaphores comme le domaine médical pour expliquer l'hygiène numérique et les bons réflexes à adopter en matière de cybersécurité.

MISE EN PRATIQUE
EXEMPLE D'UN PROGRAMME DE SENSIBILISATION DES AGENTS

5 Vérifier l'assimilation des messages

POUR S'ASSURER DE L'EFFICACITÉ DU PROGRAMME DE SENSIBILISATION

Il est utile de vérifier régulièrement la bonne compréhension des messages et leur mise en pratique.

CONFRONTER LES RETOURS D'EXPÉRIENCE

Pour mesurer la compréhension des messages, des moments d'échanges pourront être organisés sur les thématiques abordées dans la sensibilisation. L'opportunité de revenir sur des notions ou réflexes à suivre qui auraient pu être mal compris et si besoin, d'adapter des comportements pour suivre les bonnes pratiques. Autant de retours et commentaires utiles et précieux pour nourrir et parfaire la sensibilisation des différents publics.

TESTER LA THÉORIE…

Des tests d'évaluation ou des quiz ludiques sont particulièrement pertinents pour aller plus loin dans l'appréciation des contenus partagés sur le plan théorique.

… ET LA PRATIQUE

Pour apprécier la mise en application de toutes ces notions, rien ne vaut mieux que des tests en conditions réelles. À titre d'exemple, une campagne de faux hameçonnage conduite avec bienveillance est une méthode efficace pour revenir vers l'utilisateur qui a commis une erreur et lui permettre de la comprendre et adopter un comportement cyber responsable.
Par ailleurs, les résultats chiffrés des campagnes constituent un outil de mesure et de vrais arguments auprès de la direction pour prolonger la sensibilisation dans le temps.

Le plus

MESURER LE TAUX D'ENGAGEMENT À LA CAMPAGNE DE SENSIBILISATION

Pour mesurer l'adhésion au projet, une enquête pourra être soumise aux agents pour mesurer leur perception et faire émerger d'éventuels axes d'amélioration pour une future campagne.

MISE EN PRATIQUE
EXEMPLE D'UN PROGRAMME DE SENSIBILISATION DES AGENTS

Après la théorie, place à la pratique !

Comment mettre sur pied un programme de sensibilisation pour les agents ? Rien de plus simple, suivez le guide !

Cybermalveillance.gouv.fr et l'AMF proposent de mettre en application les 5 clés présentées dans le chapitre précédent en créant dès aujourd'hui un programme de sensibilisation à destination des agents de votre collectivité.

Pour ce faire, nous mettons à disposition un exemple concret de plan d'action ainsi que tous les contenus nécessaires pour le mener à bien.

Ce plan s'appuie sur **4 fondamentaux**

1 **Les thématiques** telles que :
- L'hameçonnage,
- La gestion des mots de passe,
- Le comportement à adopter sur les réseaux sociaux,
- Le piratage de compte.

2 **Les contenus clé en main à décliner sous différentes formes**
Comme évoqué dans la première partie, diversifier les formats pour répéter les messages et instaurer un réflexe auprès des agents est indispensable. C'est pourquoi Cybermalveillance.gouv.fr met à disposition des collectivités 4 supports différents :
- Des vidéos courtes et faciles d'accès pour aborder le sujet cyber,
- Des fiches pratiques pour approfondir, comprendre et développer ses connaissances,
- Des mémos pour retenir l'essentiel,
- Des quiz pour tester son apprentissage de façon ludique.

3 **Les canaux de diffusion**
À choisir en fonction des publics parmi les canaux existants dans la collectivité : intranet, panneaux d'affichage, mails, visioconférence ou salles de réunion…

4 **Le pilote du programme**
Enfin, pour garantir la cohérence des contenus et légitimer la démarche de sensibilisation auprès des agents, Cybermalveillance.gouv.fr suggère d'incarner ces messages au sein de la collectivité, en désignant un pilote du programme de sensibilisation, identifié comme contact privilégié sur ce sujet. Véritable chef de projet, son rôle consistera à planifier et organiser les différentes étapes de la sensibilisation à travers un plan d'action. C'est lui qui saura mobiliser le ou les élus sur ce sujet pour leur proposer d'initier la démarche en marquant son lancement auprès de toute la collectivité.

Le programme de sensibilisation en 3 actes

Acte 1: la réunion de lancement

Il s'agit d'un rendez-vous important pour mobiliser les parties prenantes et les « sensibiliser » aux enjeux de la cyber. C'est un moment clé car c'est elle qui doit susciter d'emblée l'adhésion des agents au projet.

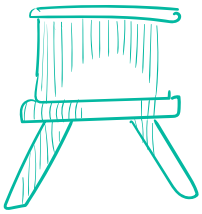
Et compte tenu de l'importance du sujet, le présentiel est à privilégier. Idéalement, une invitation préviendra en amont les agents de la réunion, avec un objet clair, les informant du projet.

Concrètement, la réunion reviendra sur :

- le contexte et les objectifs de la démarche cyber pour la collectivité,
- l'annonce du lancement d'un programme de sensibilisation,
- ses temps forts,
- les réponses aux questions pour rassurer les agents,
- les prochains rendez-vous du programme.

Acte 2: le cœur de la sensibilisation

Les thématiques de la sensibilisation seront définies en fonction des priorités. Chacune d'entre elles reprendra des messages de prévention via différents supports. Ceux-ci seront diffusés de manière échelonnée dans le temps en suivant un planning de communication précédemment défini.



Acte 3: la réunion de fin de programme

Tout aussi cruciale que la réunion de lancement, cette étape a pour but de réunir les agents (idéalement en présentiel) afin de :

- revenir sur les objectifs initiaux du projet cyber ;
- partager avec eux le bilan du programme ;
- comprendre comment ils l'ont vécu ;
- identifier leurs besoins et attentes ;
- les remercier et les féliciter de leur implication ;
- imaginer avec eux la suite du projet : nouvelles campagnes d'information, tests réguliers, rencontres avec des collectivités ayant mis en place des initiatives, etc.

Cybermalveillance.gouv.fr suggère de clore ce premier programme avec un questionnaire de satisfaction destiné aux agents pour évaluer leur engagement.

Enfin,
poursuivre la démarche dans le temps est nécessaire afin que les agents conservent les connaissances acquises lors de la sensibilisation. De plus, les menaces évoluent sans cesse et il est important que les agents y soient préparés. Et pour les nouveaux arrivants, il sera utile de prévoir une session de formation afin que tous les agents bénéficient du même niveau de connaissance sur les cybermenaces et les bonnes pratiques à adopter au quotidien.

MISE EN PRATIQUE
EXEMPLE D'UN PROGRAMME DE SENSIBILISATION DES AGENTS

Calendrier du plan d'action

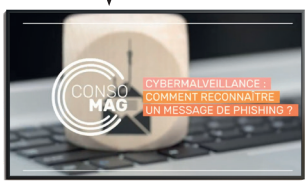
Voici un exemple de plan d'action décliné en 4 périodes avec une thématique différente à chaque fois. Il appartient à chaque collectivité de se l'approprier selon ses besoins, sa taille et ses moyens.

LANCEMENT
PRÉSENTATION DE LA DÉMARCHE

POUR SUSCITER L'INTÉRÊT

PÉRIODE 1
HAMEÇONNAGE

Vidéo
Fiche
Quiz
Mémo



POUR INITIER AU SUJET

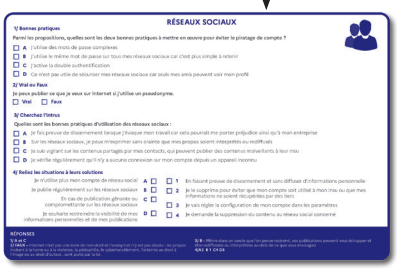
PÉRIODE 2
MOTS DE PASSE

Vidéo
Fiche
Quiz
Mémo

POUR DÉVELOPPER SES CONNAISSANCES

PÉRIODE 3
RÉSEAUX SOCIAUX

Vidéo
Fiche
Quiz
Mémo



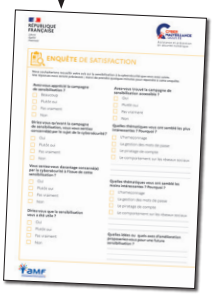
POUR TESTER SES CONNAISSANCES

PÉRIODE 4
PIRATAGE DE COMPTE

Vidéo
Fiche
Quiz
Mémo

POUR RETENIR L'ESSENTIEL

CONCLUSION
RÉUNION DE CLÔTURE



POUR MESURER L'ADHÉSION

Ces contenus sont téléchargeables via le QR code ci-dessous:

Pour aller **plus loin**

FACE À L'ENJEU QUE REPRÉSENTE LA MENACE auprès de cibles aussi exposées que les collectivités, Cybermalveillance.gouv.fr et l'AMF ont souhaité mettre à disposition cette méthode « clé en main ». Le plan d'action, les thématiques et les contenus sont autant de propositions susceptibles d'aider les entités publiques dans leur démarche de sensibilisation.

Néanmoins, ces contenus peuvent être largement enrichis et personnalisés afin de répondre au mieux aux besoins et spécificités de chaque collectivité.

Pour ce faire, voici une liste de ressources supplémentaires :

RESSOURCES UTILES POUR LES COLLECTIVITÉS
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales

LISTE DE L'ENSEMBLE DES RESSOURCES DE SENSIBILISATION DE CYBERMALVEILLANCE.GOUV.FR
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

GUIDE SUR LES OBLIGATIONS ET LES RESPONSABILITÉS DES COLLECTIVITÉS LOCALES EN MATIÈRE DE CYBERSÉCURITÉ
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillance-gouv-fr-et-la-cnil-publient-un-guide-sur-les-obligations-et-les-responsabilites-des-collectivites-locales-en-matiere-de-cybersecurite

GUIDE AMF-ANSSI « CYBERSÉCURITÉ : TOUTES LES COMMUNES ET INTERCOMMUNALITÉS SONT CONCERNÉES »
www.amf.asso.fr/documents-cybersecurite-toutes-les-communes-intercommunalites-sont-concernees/40406

GUIDE DE LA BANQUE DES TERRITOIRES
www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programme-sensibilisation-risques-numeriques-collectivites-territoriales#h-guides-pratiques-en-cybers-curit

LE MOOC DE L'ANSSI
https://secnumacademie.gouv.fr

CONTACTS SUSCEPTIBLES DE VOUS AIDER À SENSIBILISER

- La gendarmerie : www.magendarmerie.fr
- La police nationale : www.moncommissariat.fr
- Le prestataire informatique de votre collectivité
- Un organisme de mutualisation
- Intervention des conférenciers de Cybermalveillance.gouv.fr
- Les délégués régionaux de l'ANSSI : www.ssi.gouv.fr/agence/cybersecurite/action-territoriale
- Une société spécialisée en sensibilisation proposant des outils adaptés et personnalisables

ENFIN, LA PLATEFORME ET LES ÉQUIPES DE CYBERMALVEILLANCE.GOUV.FR RESTENT ACCESSIBLES POUR COMPLÉTER CES ÉLÉMENTS.

RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR

Assistance et prévention en sécurité numérique

PREMIÈRE MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE LA JUSTICE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'ÉDUCATION NATIONALE ET DE LA JEUNESSE

REMERCIEMENTS

Ce guide a été réalisé en collaboration avec les membres de Cybermalveillance.gouv.fr, notamment ceux du Groupe de Travail « Collectivités » auxquels nous adressons nos sincères remerciements : Association des maires de France et des présidents d'intercommunalité, Agence nationale de la cohésion des territoires, Agence nationale de la sécurité des systèmes d'information, AVICCA, Banque des Territoires, CoTer Numérique, Déclic, Régions de France, Région Pays de la Loire.

WWW.CYBERMALVEILLANCE.GOUV.FR

AMF
ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ