MÉMENTO SUR LA CYBERSÉCURITÉ POUR LES COMMUNES RURALES



Novembre 2026

ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en cybersécurité

Sommaire

Éditorial 3

1. Test « Où en êtes-vous en matière de cybersécurité ? » 4

2. Les principales menaces qui touchent les collectivités 5

3. 5 actions prioritaires pour se protéger 6

4. Comment réagir en cas de cyberattaque ? 8

5. Les services et solutions pour les communes rurales 10

6. Remerciements 12

Le présent memento n'a pas pour objet de couvrir de manière exhaustive l'ensemble des enjeux et mesures à appliquer pour assurer la cybersécurité des communes rurales. Il a été conçu pour présenter de manière synthétique des fondamentaux prioritaires et simples à mettre en œuvre pour déjà réduire une partie importante des risques auxquels elles sont exposées.

Éditorial

« Aucune commune n'est hélas à l'abri d'une rançon ou d'un vol de données sur internet. Même si vous n'avez que quelques ordinateurs et fichiers (cantines, état civil), les conséquences d'une attaque peuvent être très lourdes, allant jusqu'à paralyser le fonctionnement de la mairie et des services publics.
L'AMF aide les communes de toutes tailles à prévenir ces attaques et se former à la gestion des risques cyber. Ce mémento a ainsi pour ambition de vous aider à engager les actions prioritaires afin de garantir la continuité du service public, de protéger les données de la commune et de vos habitants.
Dans notre société marquée par une profonde transformation numérique, qui présente des opportunités immenses pour nos communes,
nous devons plus que jamais nous impliquer dans une démarche de cybersécurité associant les élus et les agents. C'est un enjeu de sécurité, d'efficacité et de confiance des habitants. »



© Arnaud Février pour l'AMF

David LISNARD,
Président de l'AMF

« Cybermalveillance.gouv.fr assiste des dizaines de collectivités victimes de cyberattaques chaque jour. Pourtant la cybercriminalité n'est pas une fatalité et des mesures simples à mettre en place mais essentielles pourraient déjà permettre à de très nombreuses communes de se prémunir des principaux risques. Chers élus et agents, vous n'êtes pas seuls et des solutions existent pour vous protéger. Ce mémento est là pour vous y aider. »



© Pierre Morel

Jérôme NOTIN,
Directeur Général de Cybermalveillance.gouv.fr

1. Test - Où en êtes-vous en matière de cybersécurité ?

Évaluez le niveau de cybersécurité de votre commune en répondant à ces questions :

1. Avez-vous une liste complète de tous vos équipements informatiques (PC, téléphones, serveurs, caméra de vidéosurveillance...) ?
❑ Oui ❑ Non ou Ne sais pas

2. Utilisez-vous des mots de passe complexes et différents pour chaque compte ?
❑ Oui ❑ Non ou Ne sais pas

3. Vos équipements informatiques sont-ils mis à jour fréquemment ?
❑ Oui ❑ Non ou Ne sais pas

4. Faites-vous des sauvegardes régulières des données, conservées sur un support déconnecté du réseau ?
❑ Oui ❑ Non ou Ne sais pas

5. Avez-vous sensibilisé vos agents aux risques numériques ?
❑ Oui ❑ Non ou Ne sais pas

6. Vos postes et serveurs informatiques sont-ils protégés par un antivirus ?
❑ Oui ❑ Non ou Ne sais pas

7. Êtes-vous en règle vis-à-vis du Règlement Général sur la Protection des Données* (RGPD) ?
❑ Oui ❑ Non ou Ne sais pas

8. Vos agents sont-ils équipés de matériels sécurisés pour le télétravail ?
❑ Oui ❑ Non ou Ne sais pas

9. Faites-vous réaliser régulièrement des évaluations de votre sécurité numérique par des audits techniques ?
❑ Oui ❑ Non ou Ne sais pas

10. Avez-vous un plan de secours face aux cyberattaques ?
❑ Oui ❑ Non ou Ne sais pas

Vous avez une majorité de « Oui » : Bravo ! Votre collectivité met en œuvre les mesures essentielles. Poursuivez votre démarche en découvrant et partageant ce mémento au sein de votre collectivité.

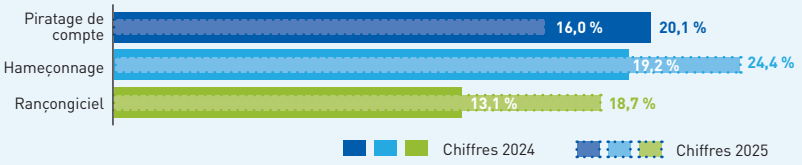
Vous avez une majorité de « Non ou Ne sais pas » : Attention, votre collectivité est vulnérable, découvrez les mesures essentielles pour la protéger dans ce mémento.

SOURCES



Adapté de « Immunité Cyber - *https://www.cybermalveillance.gouv.fr/medias/2021/09/immunite-cyber.pdf*
*RGPD : *https://www.cnil.fr/sites/default/files/2026-05/cnil_guide_securite_personnelle.pdf*

2. Les principales menaces qui touchent les collectivités



Principales menaces qui ont touché les collectivités et les administrations en 2025 selon Cybermalveillance.gouv.fr - https://www.cybermalveillance.gouv.fr/medias/2026/03/RA_2025_Cybermalveillance_gouv_fr.pdf

Le piratage de compte

Prise de contrôle d'un ou plusieurs comptes en ligne, à la suite d'un mot de passe trop simple, communiqué sans le savoir à la suite d'un message frauduleux ou utilisé sur plusieurs sites dont l'un a été piraté.

➜ **But recherché** :
Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

Pour plus d'informations, retrouvez la fiche « Le piratage de compte ».

L'hameçonnage ou *phishing* en anglais

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce…

➜ **But recherché** :
Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux.

Pour plus d'informations, retrouvez la fiche « L'hameçonnage ».

Une attaque de type rançongiciel, ou *ransomware* en anglais

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.

➜ **But recherché** :
Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

Pour plus d'informations, retrouvez la fiche « Les rançongiciels ».

3. 5 actions prioritaires pour se protéger

1. Choisir des mots de passe solides et différents pour chaque service

Vos mots de passe sont les clés d'accès à vos systèmes, services et aux données qu'ils contiennent. Une mauvaise gestion des mots de passe dans votre commune peut amener au vol, à la modification ou la suppression de vos données. Utilisez des mots de passe suffisamment longs (12 caractères minimum), impossibles à deviner, et surtout différents pour chaque service utilisé, afin que la divulgation ou le vol d'un de vos mots de passe ne puisse compromettre tout autre service sur lesquels vous pourriez l'utiliser. Pour renforcer la sécurité de vos comptes, activez également la double authentification sur tous les services qui le proposent.

Pour plus d'informations, retrouvez les bonnes pratiques à suivre pour la gestion des mots de passe.

2. Faire des sauvegardes régulières et déconnectées de vos données

Lors de certaines cyberattaques, les cybercriminels chercheront à détruire vos données et leurs sauvegardes en ligne pour vous faire chanter. Faire des sauvegardes fréquentes de vos données que vous garderez déconnectées du réseau sera votre meilleure assurance pour redémarrer votre activité avec un minimum de perte en cas d'attaque.

Pour plus d'informations, retrouvez les bonnes pratiques à suivre pour la gestion des sauvegardes.

3. Faire sans tarder les mises à jour de tous vos équipements et systèmes

Les mises à jour corrigent des failles de sécurité dans vos matériels et logiciels, qui peuvent être utilisées par des cybercriminels pour vous attaquer. Faire les mises à jour de l'ensemble de ses équipements (ordinateurs, serveurs, téléphones mobiles, tablettes...), applications et logiciels, dès qu'elles vous sont proposées, est donc indispensable pour se protéger.

Pour plus d'informations retrouvez les bonnes pratiques à suivre pour la gestion des mises à jour.

ACTION À RÉALISER PAR LA COMMUNE (ÉLUS ET AGENTS)

ACTION À RÉALISER PAR LA COMMUNE ET/OU PAR SON PRESTATAIRE

4. Être vigilant face aux messages d'hameçonnage (ou phishing)

Les messages d'hameçonnage par mail ou SMS sont l'un des principaux appâts des cybercriminels pour dérober des informations sensibles comme des mots de passe, vous faire installer un programme malveillant (virus…) ou encore vous faire réaliser un virement frauduleux.
Pour vous en prémunir, sensibilisez l'ensemble de vos collaborateurs à cette menace et aux réflexes à adopter en cas d'attaque ou au moindre doute.

Pour plus d'informations, retrouvez les bons gestes à adopter en cas d'hameçonage.

5. Utiliser un antivirus

En naviguant sur Internet, en cliquant sur un lien ou en ouvrant la pièce jointe d'un message, en branchant une clé USB… vos équipements peuvent être infectés par un virus informatique.
Un antivirus, régulièrement mis à jour, contribue à se protéger des menaces les plus usuelles.

Pour plus d'informations, retrouvez la fiche de Cybermalveillance.gouv.fr, « Les antivirus ».

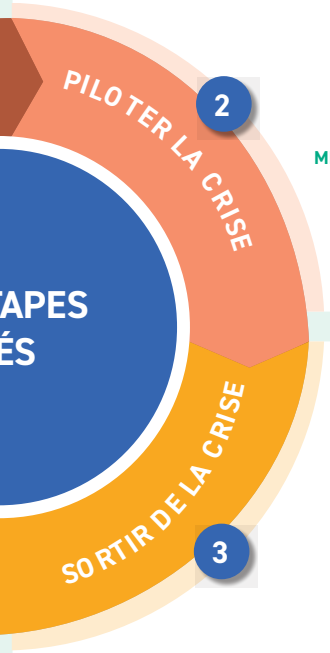
Un conseil :
Il est vivement recommandé que ce sujet soit porté par un élu, le maire et/ou un adjoint ou un conseiller municipal délégué.

ACTION À RÉALISER PAR LA COMMUNE (ÉLUS ET AGENTS)

ACTION À RÉALISER PAR LA COMMUNE ET/OU PAR SON PRESTATAIRE

4. Comment réagir en cas de cyberattaque ?





IDENTIFIEZ L'ORIGINE DE L'ATTAQUE ET SON ÉTENDUE

DÉPOSEZ PLAINTE

NOTIFIEZ L'INCIDENT À LA CNIL

METTEZ EN PLACE DES SOLUTIONS DE SECOURS

GÉREZ VOTRE COMMUNICATION

FAITES UNE REMISE EN SERVICE PROGRESSIVE ET CONTRÔLÉE

TIREZ LES ENSEIGNEMENTS DE L'ATTAQUE ET DÉFINISSEZ LES PLANS D'ACTION

ÉLU ACTION À MENER PAR L'ÉLU

TECHNICIEN ACTION À MENER PAR LE TECHNICIEN

5. Les services et solutions pour les communes rurales

1. Se sensibiliser et se former

➜ **Cybermalveillance.gouv.fr**
Ressources de sensibilisation et d'accompagnement pour les collectivités.

https://www.cybermalveillance.gouv.fr/

➜ **E-sensibilisation « SensCyber »**
Une sensibilisation interactive en ligne à la cybersécurité pour les agents et élus.

https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre

➜ **E-sensibilisation «SenCy-Crise »**
Une sensibilisation interactive en ligne à la gestion de crise cyber.

https://www.cybermalveillance.gouv.fr/gestion-de-crise/sency-crise

➜ **CapCyber crises & collectivités**
Exercice de simulation en ligne dédié à la gestion de crise cyber pour les collectivités.

https://www.amf.asso.fr/documents-cybersecurite-une-formation-en-ligne-inedite-pour-preparer-les-elus-leurs-agents-aux-crises-cyber/43158

2. Sécuriser sa commune

➜ **Mon ExpertCyber**
Faites appel à des prestataires labellisés pour de l'installation, de la maintenance et de l'assistance en cas d'incident.

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/label-expertcyber/decouvrir-le-label-expertcyber

➜ **MesServicesCyber**
Accédez aux services, ressources cyber et guides proposés par l'ANSSI et ses partenaires.

https://messervices.cyber.gouv.fr/

➜ **La Suite Territoriale**
Un ensemble de services numériques souverains et sécurisés pour outiller les collectivités territoriales.

https://suiteterritoriale.anct.gouv.fr/

3. Se faire assister en cas d'incident

➜ **17Cyber**
Bénéficiez d'une assistance en ligne 24/7 gratuite en cas d'incident.

https://17cyber.gouv.fr/

4. Déposer plainte

Déposer plainte rapidement au commissariat de police national ou à la brigade de gendarmerie la plus proche.

5. Notifier une violation de données

➜ **CNIL**

https://www.cnil.fr/fr/services-en-ligne/notifier-une-violation-de-donnees-personnelles

6. Accompagnement local

➜ **Associations départementales des maires**

https://www.amf.asso.fr/m/page/ad.php

➜ **Campus cyber national et territoriaux**

https://campuscyber.fr/

https://wiki.campuscyber.fr/Campus_Cyber_Territoriaux

➜ **Csirt territoriaux**

https://www.cert.ssi.gouv.fr/csirt/csirt-territoriaux/

➜ **Opérateurs de Services Numériques (OPSN)**

https://www.asso-declic.fr/

REMERCIEMENTS ET CRÉDITS

Ce mémento a été réalisé par l'Association des maires de France et des présidents d'intercommunalité, en partenariat avec Cybermalveillance.gouv.fr et avec la participation de :

Ce mémento est disponible sur le site de l'AMF (www.amf.asso.fr/BW43283) et de Cybermalveillance.gouv.fr

ASSOCIATION DES MAIRES DE FRANCE ET DES PRÉSIDENTS D'INTERCOMMUNALITÉ

41, quai d'Orsay
75343 Paris cedex 07
Tél : 01 44 18 14 14

amf@amf.asso.fr
www.amf.asso.fr
@l_amf