MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER

Liberté
Égalité
Fraternité

COLLECTIVITÉS - ÉTABLISSEMENTS DE SANTÉ - ENTREPRISES

diagNal

Évaluez votre niveau de cyber protection. Faites appel à la Gendarmerie et à son diagnostic cyber.

RÉPONDRE PRÉSENT

COMCYBERGEND

CYBERGEND
INVESTIGATION & CRIMINALISTIQUE

COLLECTIVITÉS TERRITORIALES

diagonal

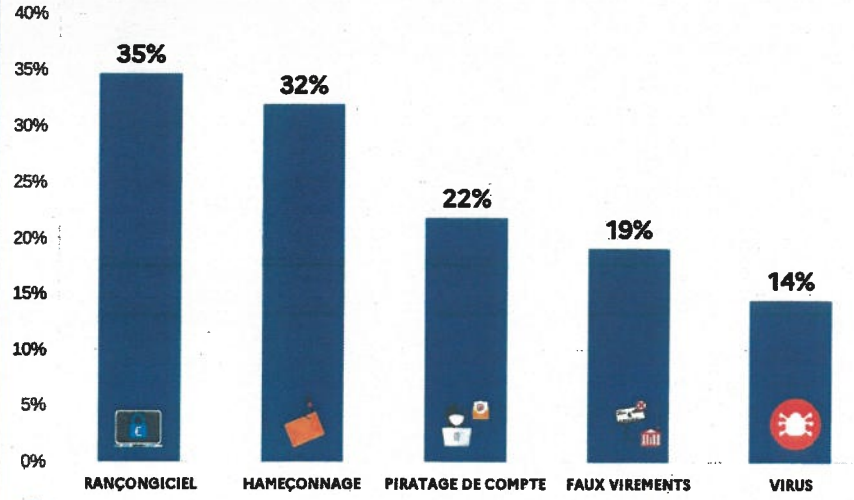
National — **8 juillet 2023**

1155 COLLECTIVITÉS DONT 22 ULTRAMARINES

- 3,1 % DES COMMUNES
- 925 communes de moins de 5000 habitants
- 54 EPCI/EPCL

- **41% N'ONT PAS DE DÉLÉGUÉ À LA PROTECTION DES DONNÉES**
- **55% DÉCLARENT NE PAS AVOIR DE RÉFÉRENT CYBERSÉCURITÉ**
- **74% N'ONT PAS DE PLAN DE GESTION DE CRISE CYBER**

TOP 5 DES CYBERMENACES PARMI LES VICTIMES



29% DES COLLECTIVITÉS SONT VICTIMES DE CYBERMENACES

1 COLLECTIVITÉ SUR 10 EST VICTIME D'UN RANÇONGICIEL

PLUS PETITE COMMUNE RECENSÉE : 200 HABITANTS

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

LES OBLIGATIONS ET RESPONSABILITÉS DES COLLECTIVITÉS LOCALES EN MATIÈRE DE CYBERSÉCURITÉ

FRANCE RELANCE

Les collectivités locales et leurs établissements publics sont tenus à 3 obligations en matière de cybersécurité, dans leurs relations avec les administrés et dans l'exercice de leurs compétences.

LES 3 OBLIGATIONS

	LA PROTECTION DES DONNÉES PERSONNELLES	LA SÉCURISATION DES TÉLÉSERVICES LOCAUX	LA SÉCURISATION DE L'HÉBERGEMENT DES DONNÉES DE SANTÉ
DÉFINITIONS	Une donnée personnelle est une information se rapportant à une personne physique identifiée ou identifiable : **nom, n° de téléphone, n° de sécurité sociale, photographie, etc.**	Un téléservice est un guichet d'accueil numérique permettant de procéder par voie électronique à des démarches administratives : **demande de permis de construire, inscription à la cantine scolaire, etc.**	Une donnée de santé est une donnée personnelle sensible. Elle est recueillie à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social : **radios, résultats de laboratoire, comptes rendus médicaux, etc.**
OBLIGATIONS	Dès lors que des données personnelles sont traitées (collecte, enregistrement, stockage, etc.), les collectivités sont soumises aux règles relatives à la protection des données personnelles.	Tout téléservice doit suivre au préalable un ensemble de règles de sécurité (réalisation d'une analyse des risques, définition des objectifs de sécurité, homologation du système d'information, etc.).	Les activités d'hébergement des données de santé sont soumises à des exigences de certification préalable.
TEXTES	• La loi Informatique et Libertés. • Le Règlement Général sur la Protection des Données (RGPD).	Le Référentiel Général de Sécurité : RGS.	Le Code de la santé publique.

LES RESPONSABILITÉS

En cas de cyberattaque, de dommages et/ou de méconnaissance de ces trois obligations, **la responsabilité des collectivités locales et/ou de leurs agents peut être engagée :**

Pour aller plus loin :
Cybermalveillance.gouv.fr
Cnil.fr

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT PILOTER SA CYBERSÉCURITÉ ? (DIRIGEANTS)

Pour vous informer sur les bonnes pratiques
et les principales menaces en matière de cybersécurité
rendez-vous sur :
www.cybermalveillance.gouv.fr

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMMENT PILOTER SA CYBERSÉCURITÉ ? (DIRIGEANTS)

Méthodologie synthétique de gestion de la cybersécurité pour les dirigeants des entreprises, associations, collectivités, administrations.

1 FAITES UN ÉTAT DES LIEUX

Dans un premier temps, il convient de dresser un inventaire le plus exhaustif possible de l'ensemble de vos actifs numériques (réseaux internes, sites Internet, messageries, réseaux sociaux, applications et services externalisés...), et de leurs responsables (support informatique interne ou externe).

2 PRENEZ CONSCIENCE DU RISQUE

Pour chaque système recensé, évaluez sa criticité pour le fonctionnement de votre organisation s'il venait à être piraté ou détruit ou si les données qu'il contient étaient dérobées par des cybercriminels.

3 ÉVALUEZ VOTRE NIVEAU DE PROTECTION

Interrogez votre support informatique interne et/ou externe sur la pertinence des mesures de sécurité techniques, organisationnelles et contractuelles appliquées au regard des enjeux, telles les politiques de mots de passe, de sauvegardes, de mises à jour ou encore de filtrage des accès externes.

4 DÉFINISSEZ UN PLAN D'ACTION

80 % des cyberattaques pourraient être évitées par l'application de mesures simples et à faible coût telles qu'une bonne gestion des mots de passe, des sauvegardes, des mises à jour de sécurité ou des droits d'accès. Priorisez les actions à entreprendre en fonction du rapport criticité/coût/efficacité.

5 FAITES-VOUS ACCOMPAGNER

Si aucun collaborateur n'est assigné à ce rôle, désignez une personne en charge de vous assister dans le pilotage du plan de cybersécurité de votre organisation. Pour l'évaluation technique du niveau de protection sur vos systèmes critiques, faites appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

6 SENSIBILISEZ VOS COLLABORATEURS

Vos collaborateurs sont un maillon essentiel de votre cybersécurité, qu'il s'agisse d'appliquer de bonnes pratiques de cybersécurité, de détecter ou de réagir à une tentative de cyberattaque. De nombreuses ressources gratuites de sensibilisation sont disponibles sur Cybermalveillance.gouv.fr.

7 PRÉPAREZ-VOUS AU PIRE

Il n'y a pas de cybersécurité absolue: le risque d'une cyberattaque réussie est malheureusement toujours possible. Il convient donc de préparer des plans de secours pour affronter une crise: annuaire de crise, fonctionnement dégradé, communication... Et de réaliser des exercices pour évaluer leur efficacité.

8 IMPLIQUEZ-VOUS

Pour vous assurer que le plan d'action cybersécurité est bien conduit, vous devez en tant que dirigeant vous impliquer, en le pilotant par des points de situation et d'avancement réguliers à votre niveau. Vous devez également montrer l'exemple et exiger de vos cadres et collaborateurs qu'ils ne dérogent ou ne contournent pas les mesures de sécurité décidées pour protéger leur organisation.

9 CONTRÔLEZ

Il est en effet important de vérifier que les décisions prises ont bien été mises en place. Pour les systèmes les plus critiques, un audit technique et organisationnel peut s'avérer nécessaire: il est recommandé de faire appel à un prestataire spécialisé en cybersécurité que vous pourrez trouver sur Cybermalveillance.gouv.fr.

10 ITÉREZ

Les services numériques des organisations évoluent en permanence, tout comme les moyens permettant de les attaquer. Pour en tenir compte, il est recommandé de « réappliquer » cette méthode pour tout nouveau service numérique, avant sa mise en œuvre, et de manière globale tous les deux à trois ans.

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

V230419

MINISTÈRE DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

GEND 20 24
AU PLUS PRÈS DE VOUS
PRÉSENT

Évaluez **la sécurité numérique de votre collectivité** en 10 points

AMF

CYBER MALVEILLANCE GOUV.FR

VÉRIFIER MON IMMUNITÉ CYBER

- I — INVENTAIRE COMPLET
- M — MOTS DE PASSE
- M — MISES À JOUR ET SAUVEGARDES
- U — UTILISATEURS SENSIBILISÉS
- N — NEUTRALISATION DES VIRUS
- I — INFORMATIQUE ET LIBERTÉS
- T — TÉLÉTRAVAIL EN SÉCURITÉ
- É — ÉVALUATION
- CYBER — ATTAQUES ANTICIPÉES

		OUI	NON ou NE SAIS PAS
1	Avez-vous un **inventaire complet** de tous vos systèmes numériques ?	☐	☐
2	Utilisez-vous des **mots de passe solides et différents** pour chaque service ?	☐	☐
3	Vos systèmes numériques sont-ils mis à jour en temps réel et faites-vous des **sauvegardes régulières** de toutes vos données ?	☐	☐
4	Avez-vous sensibilisé vos agents aux **risques numériques** ?	☐	☐
5	Vos postes et serveurs informatiques sont-ils protégés par un **antivirus** ?	☐	☐
6	Êtes-vous en règle vis-à-vis du Règlement Général sur la Protection des Données (RGPD) ?	☐	☐
7	Vos agents sont-ils équipés de **matériels sécurisés** pour le télétravail ?	☐	☐
8	Faites-vous réaliser régulièrement des **évaluations** de votre sécurité numérique par des audits techniques ?	☐	☐
9	Avez-vous un **plan de secours** face aux cyberattaques ?	☐	☐

10 ACTION À MENER

Vous êtes dans le VERT : Bravo ! Votre collectivité met en oeuvre les mesures essentielles. Pour aller encore plus loin et vous aider à perfectionner votre sécurité numérique, le réseau des cyber gendarmes est à votre service.

Vous êtes dans le ROUGE : Attention, votre collectivité est peut-être en danger. La gendarmerie peut vous aider à faire un état des lieux de votre sécurité numérique et à établir un plan d'actions pour renforcer votre protection.

UNE HÉSITATION ? UN DOUTE ?
Contactez votre GENDARMERIE pour un ACCOMPAGNEMENT DÉTAILLÉ