RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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

ÉTUDE : LA SÉCURITÉ NUMÉRIQUE DANS LES COLLECTIVITÉS FRANÇAISES DE MOINS DE 3 500 HABITANTS

➤ LE CONTEXTE

Malgré une profonde transformation numérique des collectivités, l'angle de la cybersécurité reste un enjeu majeur face à la recrudescence des cyberattaques.

Les collectivités de toutes tailles sont devenues ces derniers mois des cibles d'actes de cybermalveillance de plus en plus nombreux (systèmes d'information bloqués, missions au service de leurs administrés interrompues, etc.). Un incident de sécurité numérique peut se produire à tout moment et dans n'importe quelle collectivité.

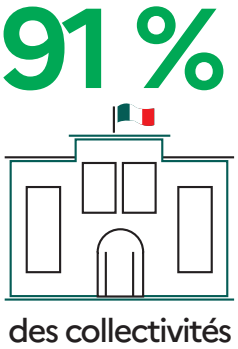
Dans ce contexte, le gouvernement a mis en place le plan France Relance avec un volet relatif à la cybersécurité des collectivités locales. C'est dans ce cadre que Cybermalveillance.gouv.fr a souhaité mener cette étude.

➤ L'ÉTUDE MENÉE

CIBLES

Cybermalveillance.gouv.fr a choisi de réaliser son enquête auprès des collectivités de moins de 3 500 habitants car elles représentent :

- **31 816** communes sur 34 965 collectivités* ;
- **91 %** des collectivités en France ;
- un Français sur trois.



OBJECTIFS

Cybermalveillance.gouv.fr a conduit une enquête visant les objectifs suivants :

1. Comprendre les **usages** numériques des communes de moins de 3 500 habitants ;
2. Identifier les **risques** numériques auxquelles elles sont exposées ;
3. Mieux connaître leurs **besoins** en matière de sécurité numérique ;
4. Leur apporter des **réponses** utiles, concrètes et adaptées.

*Source : Direction Générale des Collectivités Locales (DGCL), août 2021

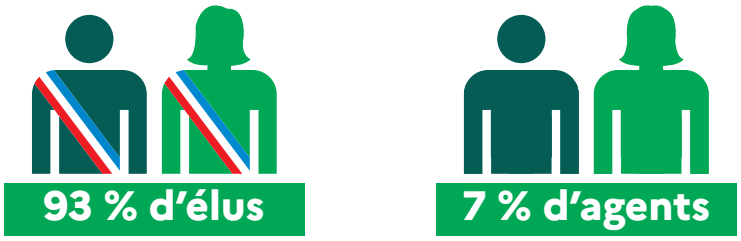
MÉTHODOLOGIE

Cette étude a été réalisée en 2 phases, dans le cadre du plan France Relance :

1. Approche **qualitative** (du 23 août au 15 décembre 2021) : interviews personnalisées avec guide d'entretiens différenciés auprès de 20 élus et agents de collectivités.
2. Approche **quantitative** (du 08 novembre au 15 décembre 2021) : enquête en ligne relayée par des associations d'élus et membres du dispositif Cybermalveillance.gouv.fr.

PANEL DES RÉPONDANTS

Au total, 524 répondants ont participé à l'étude, dont 93 % d'élus et 7 % d'agents.



Un échantillon de communes en adéquation avec la répartition nationale :

- **40 %** des répondants exercent dans les communes ayant entre 500 et 1 999 habitants ;
- **29 %** des répondants exercent dans les communes ayant entre 200 et 499 habitants.

Répartition des communes de moins de 3 500 habitants au niveau national et répartition des répondants par taille de commune :

Taille des communes en nombre d'habitants	% des répondants par nombre d'habitants	Nombre de communes en %
1 à 99	6,5 %	9,5 %
100 à 199	16 %	15,6 %
200 à 499	29 %	27,4 %
500 à 1 999	40 %	32 %
2 000 à 3 499	8 %	6,3 %

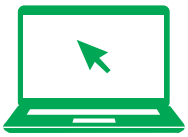
Source : Direction Générale des Collectivités Locales (DGCL), août 2021

➤ LES RÉSULTATS

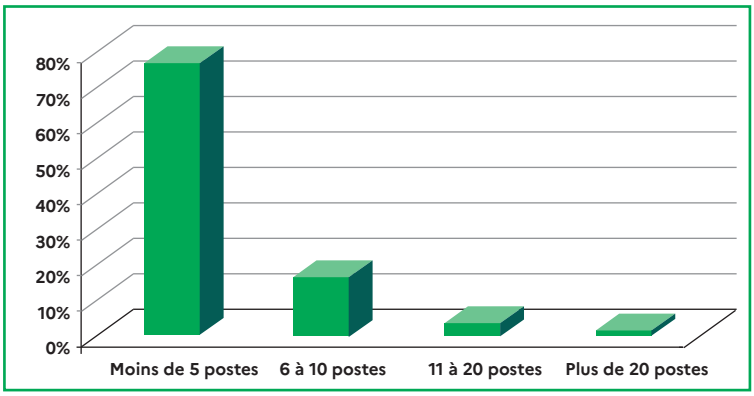
UN PARC INFORMATIQUE RÉDUIT

Il ressort de l'étude que **77%** des collectivités interrogées disposent de moins de 5 postes informatiques. Une des raisons évoquées est un faible budget dédié à l'équipement numérique.

77% **des collectivités ont moins de 5 postes informatiques.**



Répartition du parc informatique dans les collectivités interrogées :



UNE GESTION INFORMATIQUE EXTERNALISÉE

Il ressort de l'étude que **77 %** des collectivités interrogées n'ont pas de responsable informatique et externalisent la gestion de leur informatique.

Parmi eux :
- **64 %** ont recours à un prestataire externe ;
- **23 %** ont une gestion interne de leur parc informatique ;
- **10 %** font appel à des structures externes (mutualisation de services numériques ou associations d'élus) ;
- **2 %** externalisent au sein de la communauté de communes ;
- **1 %** externalisent chez un administré.

Quand elles externalisent, 64% d'entre elles s'adressent à un **prestataire informatique de proximité** qui gère l'ensemble du parc informatique de la commune :
- Installation des matériels ;
- Maintenance avec la mise à jour des logiciels ;
- Assistance en cas d'incidents informatiques ou actes de cybermalveillance.

En cas d'incident, les collectivités interrogées déclarent recourir en premier lieu à leur prestataire informatique de proximité :
- Parmi les collectivités ayant fait l'objet d'une cyberattaque, **61 %** déclarent avoir fait appel à leur prestataire ;
- Pour les collectivités n'ayant jamais été victimes de cyberattaques à ce jour, **41 %** affirment qu'elles contacteraient leur prestataire.

DES ORGANISATIONS PEU SENSIBILISÉES

- **65 %** des collectivités pensent que le risque numérique est faible, voire inexistant, ou ne savent pas l'évaluer.
- Seules **35 %** identifient un risque numérique élevé, voire très élevé, mais s'interrogent sur les moyens pour y pallier (budgets, outils, ressources humaines).
- **49 %** ont identifié des risques de perte de données et de blocage des services (état civil, école, social, urbanisme, financier).

Des publics peu voire pas du tout formés

Ces publics sont peu sensibilisés aux risques et bonnes pratiques en matière de sécurité numérique.

- **2/3 des publics** (maires, adjoints, agents, DGS*) n'ont pas été sensibilisés à la sécurité numérique.
- **57 %** des responsables informatiques interrogés ne sont pas formés à la sécurité numérique.

Des publics peu informés ou sensibilisés

Il ressort également de l'étude que les personnes interrogées n'ont pas connaissance du cadre juridique en vigueur, à l'exception du Règlement Général sur la Protection des Données (RGPD).

La majorité ne connait pas les dispositions relatives aux compétences et aux responsabilités des collectivités et des élus en matière de sécurité numérique. Ils ne sont pas familiers non plus de l'écosystème cyber et des acteurs étatiques impliqués (Cybermalveillance.gouv.fr, Agence Nationale de la Sécurité des Systèmes d'Information, ministère de l'Intérieur, etc.).

DES USAGES NUMÉRIQUES À RISQUES

Partage des mots de passe

Les collectivités interrogées déclarent partager l'usage d'ordinateurs, ce qui favorise l'échange des mots de passe entre agents et élus et implique une gestion non sécurisée.

Mélange des usages élus, professionnels et personnels

- En moyenne, **44 %** des élus, soit plus d'un tiers, utilisent leurs outils numériques personnels (**téléphone/ordinateur/messagerie**) dans un cadre professionnel, notamment lorsqu'ils exercent plusieurs mandats électifs ou une activité professionnelle en parallèle.
- En moyenne, **39 %** des agents déclarent mélanger leurs usages professionnels et personnels.

* Directeurs Généraux des Services

Détail de l'utilisation des outils numériques personnels dans le cadre de leurs usages professionnels :

Téléphones	Ordinateurs	Messageries
66% des élus 66% des agents	34% des élus 26% des agents	34% des élus 26% des agents

Méconnaissance du niveau d'expertise de leur prestataire

Les collectivités n'ont pas connaissance du niveau d'expertise en sécurité numérique de leur prestataire de proximité ou de leur sous-traitant le cas échéant. Elles se croient sécurisées et n'ont **pas le réflexe de contrôler ses compétences**, surtout lorsqu'il s'agit d'une relation contractuelle de longue date.

DES FREINS À LA SÉCURITÉ NUMÉRIQUE

Plusieurs préjugés ont pu être établis dans le cadre de l'étude en matière de cybersécurité.

Les principales objections des collectivités interrogées :

budget insuffisant	manque de temps	autres priorités	pas concernées

Pour les collectivités conscientes des risques :
- Elles ne savent pas vers qui se tourner ;
- Elles ont des difficultés à évaluer la maturité cyber de leur collectivité ;
- Elles estiment les communications non adaptées aux collectivités locales et aux élus ;
- Elles trouvent la réglementation complexe.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

FRANCE RELANCE

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

➤ UNE RÉPONSE UNIQUE : CYBERMALVAILLANCE.GOUV.FR

Un guichet unique accessible en ligne

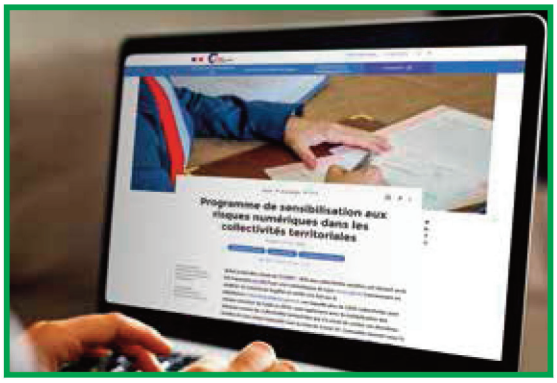
Des conseils adaptés aux collectivités locales

Un service de proximité grâce à un réseau de prestataires présents sur l'ensemble du territoire

Label ExpertCyber : un accompagnement par des prestataires de confiance, avec un niveau d'expertise et de compétences reconnu en cybersécurité

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Une sensibilisation des collectivités aux risques numériques avec des outils et un programme dédié



" I.M.M.U.N.I.T.É.Cyber " : un outil permettant à chaque élu ou responsable local de mesurer lui-même le niveau de cyberprotection mis en place au sein de sa collectivité

Pour toute information :
cybermalveillance.gouv.fr

GIP ACYMA
www.cybermalveillance.gouv.fr

Suivez-nous sur :

Retrouvez la synthèse de l'étude en infographie sur notre site.