DDFiP DE LA MEUSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

La sécurité informatique des collectivités locales

Introduction

Les collectivités locales sont régulièrement visées par des cyberattaques : services publics bloqués, données sensibles compromises, coûts financiers élevés et perte de confiance des administrés.

Face à ces menaces, il est crucial d'adopter une stratégie globale de cybersécurité pour garantir la continuité du service public et protéger les intérêts des citoyens.

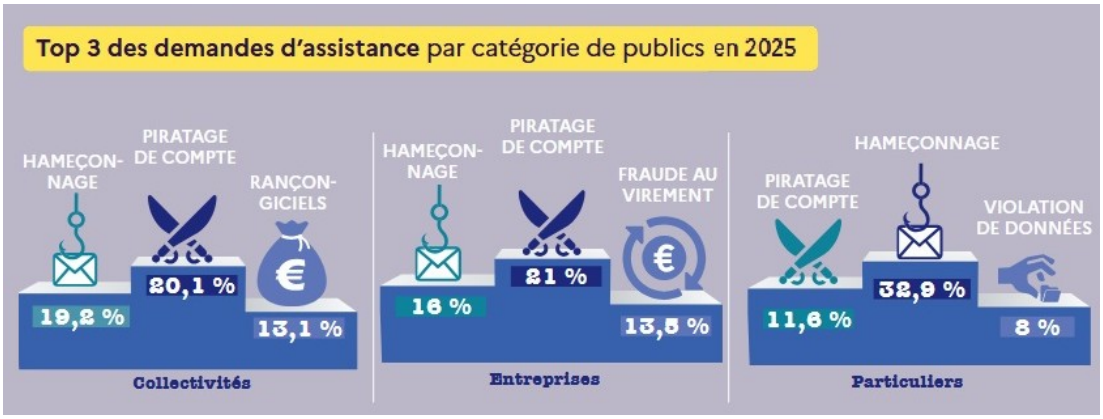
Face à la recrudescence des cyberattaques, la cybersécurité est un enjeu majeur pour les collectivités. En effet, une enquête réalisée en 2024 par la Banque des Territoires a relevé que 17 % des collectivités locales ont déjà été confrontées à une cyberattaque ayant entraîné des conséquences graves : interruption des services publics, compromission de données sensibles et impacts financiers considérables. De plus, 1/3 des communes de moins de 25 000 habitants, ayant subi une cyberattaque, a connu une interruption de ses services.

Face à la menace croissante, ces dernières doivent relever un double défi : protéger les informations sensibles de leurs administrés tout en assurant le bon fonctionnement de ses services publics.

Les collectivités locales particulièrement touchées par les cyberattaques

Les collectivités locales constituent une cible de choix pour les cybercriminels. En effet, elles récoltent et stockent de grandes quantités de données sensibles, qu'elles soient liées à l'identité des administrés, à leurs données bancaires, mais aussi à l'État. Tous ces éléments constituent une mine d'or pour les cyberattaquants : source de profit via leur revente pour permettre des attaques en cascade, très ciblées.
Les cyberattaques visant les collectivités locales sont motivées par plusieurs raisons, mais en pratique, la cybercriminalité de masse reste la menace la plus courante.

En **2024**, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a traité **218 incidents** concernant les **collectivités**, soit 18 incidents par mois. Cela représente **14 % de l'ensemble** des incidents portés à sa connaissance. Il convient de distinguer un signalement d'un incident. Un signalement est une notification ou une alerte reçue. Un incident est une attaque avérée. En **2025,** l'ANSSI a traité **2 209 signalements** pour **1 366 incidents**, pour les secteurs dont elle est en charge (santé, éducation, télécoms…).



Source : cyvermalveillance.gouv.fr – rapport d'activité 2025

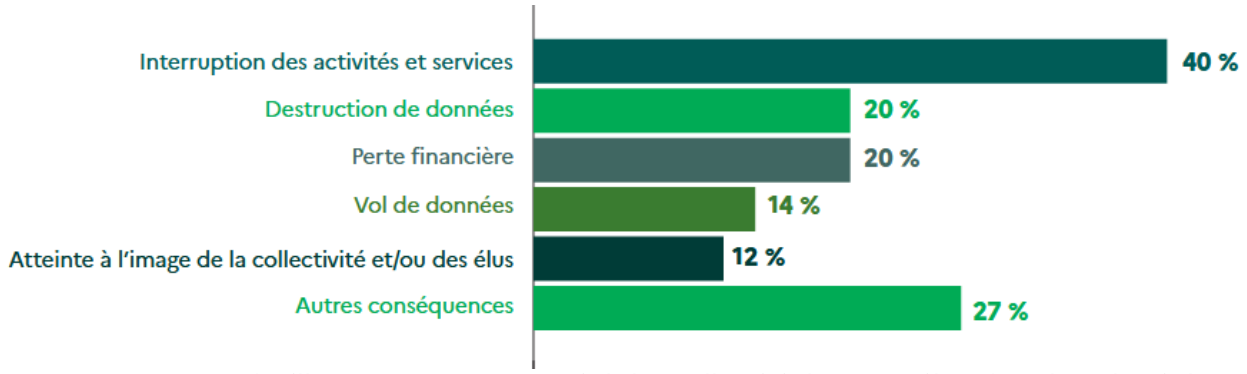
Source : cyvermalveillance.gouv.fr – rapport d'activité 2025

La fraude au virement enregistre une progression significative avec la 4e place (soit 8,5 % des besoins d'assistance) et un volume en très forte hausse de +262 %.

Les principaux types de cyberattaques

- **Hameçonnage :** Technique d'ingénierie sociale qui consiste à envoyer des messages frauduleux pour inciter la cible à divulguer des informations d'identification ou à cliquer sur des liens malveillants.
- **Fraude au président :** Escroquerie où l'attaquant se fait passer pour un dirigeant afin de demander un virement.
- **FOVI :** Détournement d'un virement attendu sur le compte bancaire d'un créancier, par usurpation de son identité.
- **Logiciel malveillant, Malware** (virus, cheval de Troie, ransomware, etc.) : conçu pour infiltrer, endommager ou exploiter un système informatique sans le consentement de l'utilisateur.
- **DDoS (Distributed Denial of Service)**: Attaque qui submerge un service en ligne avec un trafic massif provenant de multiples sources, le rendant indisponible pour les utilisateurs légitimes.
- **Rançongiciel**: Type de malware qui chiffre les données d'une victime et exige une rançon pour fournir la clé de déchiffrement.

Les conséquences d'une cyberattaque pour les collectivités locales



Source : cyvermalveillance.gouv.fr – maturité des collectivités en matière de cybersécurité 2025

Pour les collectivités locales, les cyberattaques ont des conséquences désastreuses. En effet, ces dernières peuvent provoquer :

- Un **blocage des services publics** qui touche directement la population (impossibilité d'accéder aux services en ligne, blocage des systèmes internes).
- Une **perte de données**, souvent accompagnée de leur compromission, car ces données peuvent être revendues ou réutilisées pour des attaques en cascade.
- Une **perte financière** importante (rançons, coûts de restauration des systèmes).
- Une **perte de confiance** de la part des administrés.

Garantir la sécurité informatique, c'est assurer la continuité du service public et protéger les intérêts de vos citoyens.

Comment renforcer la protection des collectivités locales face aux risques de cyberattaques ?

Pour se protéger des cyberattaques, les collectivités locales n'ont d'autre choix que de renforcer la protection de leur environnement SI (sécurité informatique). Il est important de distinguer 3 piliers de la cybersécurité :

- **Se préparer** : diagnostic de cybersécurité permettant d'identifier les faiblesses des environnements SI, actions de sensibilisation et d'entraînement face à la menace.
- **Se protéger** : déploiement de systèmes de protection des postes et des services, détection de la menace, renforcement des accès aux applications, sauvegarde sécurisée des données.
- **Réagir** : poursuite de l'activité en cas de cyberattaque, restauration des données.

<u>Diagnostic Cyber :</u>

MonAideCyber, initiative de l'ANSSI propose un diagnostic cyber **gratuit** destiné aux collectivités souhaitant mettre en œuvre une première démarche de cybersécurité.

Un échange en présentiel (ou à distance) est organisé autour des axes suivants :

- Gouvernance
- Sécurité des accès
- Sécurité des postes de travail
- Sécurité des infrastructures et données
- Sensibilisation des agents
- Réaction à une cyberattaque

Il identifie les vulnérabilités majeures et délivre un plan d'action structuré autour de six recommandations prioritaires pour mieux sécuriser la collectivité. La prestation dure environ **1h30** (diagnostic et recommandations).

https://messervices.cyber.gouv.fr/services/mon-aide-cyber.html

Si le risque zéro n'existe pas en matière de cybersécurité, il existe quelques conseils pour protéger votre structure :

- Mise en place d'une veille efficace : 45 % des collectivités déclarent que le manque de connaissances en cybersécurité est un frein important à l'acquisition d'un bon niveau de sécurité. Il est donc essentiel de se tenir informé.

- Faire les mises à jour : de nouvelles failles de sécurité sont découvertes tous les jours ; ainsi, appliquer les mises à jour dès leur publication réduit les risques.

- Ne pas mélanger les usages professionnels et personnels : qu'il s'agisse des boîtes mail ou des smartphones, il est indispensable d'avoir recours à des outils réservés à l'usage professionnel et spécialisés pour réduire la surface d'attaque.

- Un élu averti en vaut deux : avoir des plans de continuité/reprise d'activité en place vous permettra de gagner en sérénité, y compris en cas d'attaque. Savoir avant la crise qui contacter et quelles mesures d'urgence mettre en place vous fera gagner du temps et de précieuses ressources le jour J.

- **NE JAMAIS PAYER LA RANÇON** demandée lors d'une attaque : vous n'êtes pas certain de récupérer vos données, ni que les données potentiellement dérobées ne seront pas rendues publiques ou utilisées à des fins frauduleuses. De plus, vous encourageriez les cybercriminels à surenchérir et/ou à chercher à vous attaquer à nouveau.

https://cyber.gouv.fr/securisation/10-regles-or-securite-numerique/

Que faire en cas d'attaque ?

LE CENTRE D'ASSISTANCE
Grand Est Cybersécurité

Assistance : https://www.cybersecurite.grandest.fr/services-en-ligne/

Que faire en cas de FOVI ?

En cas d'escroquerie, réagissez vite !

1. **Informez immédiatement le comptable public de votre collectivité.**
   Lui communiquer :
   - les coordonnées bancaires présumées frauduleuses ;
   - les pièces (courriels, etc.) avec le nom de l'escroc présumé, son adresse de messagerie, son numéro de téléphone.
2. **Identifiez les paiements déjà réalisés, à venir ou en instance, pour effectuer les rejets et blocages nécessaires et en avertir le comptable.**
3. **Bloquez les coordonnées bancaires frauduleuses dans les applications informatiques de la collectivité locale.**
4. **Portez plainte auprès d'un service de police ou de gendarmerie, le plus rapidement possible.**
5. **Transmettre la plainte au comptable public**

collectivites-locales.gouv.fr cybermalveillance.gouv.fr

Il est essentiel de suivre cette démarche pour tenter de récupérer les fonds

Les signaux d'alerte

- lors d'une demande de **changement de RIB au profit d'une néo banque** ou d'une banque étrangère
- lors de toute transmission de factures ou de nouveaux RIB par courriel, hors Chorus Pro
- sur les **adresses mails d'envoi** :
  - adresses électroniques de type : @gmail.com, @servicecomptabilite.net par exemple
  - adresses quasiment similaires à l'adresse habituelle
- sur la **rédaction des courriels** : fautes d'orthographe, syntaxe, logo flou…

Les bons gestes de prévention

- LE CONTRE-APPEL au fournisseur ou à l'agent qui demande le changement de son RIB pour paiement de sa paye, à partir de coordonnées fiables (dossier, site internet de l'entreprise ou pages jaunes), et non à partir de coordonnées dans un mail ou dans les pièces justificatives jointes au paiement (factures…) ;
- LE RÉFLEXE CHORUS PRO pour la transmission des factures ou les changements de RIB ;
- Restez discrets sur le fonctionnement de la collectivité ou de ses fournisseurs ;
- Soyez vigilants pendant les périodes de congés et de forte charge de travail ;

Par ailleurs 2 autres indicateurs peuvent vous alerter :

- **la période de vacances**, pendant laquelle vos interlocuteurs habituels sont en congés, qui est un argument utilisé lorsque vous avez une nouvelle personne en relation ;
- **le caractère urgent du règlement** à faire sur un nouveau RIB.

Plaquette : https://www.collectivites-locales.gouv.fr/files/files/Ressources/D%C3%A9pliants%20LePointsur/depl-fovi_web.pdf

FOVI PAYE : Attention, saison à risque !

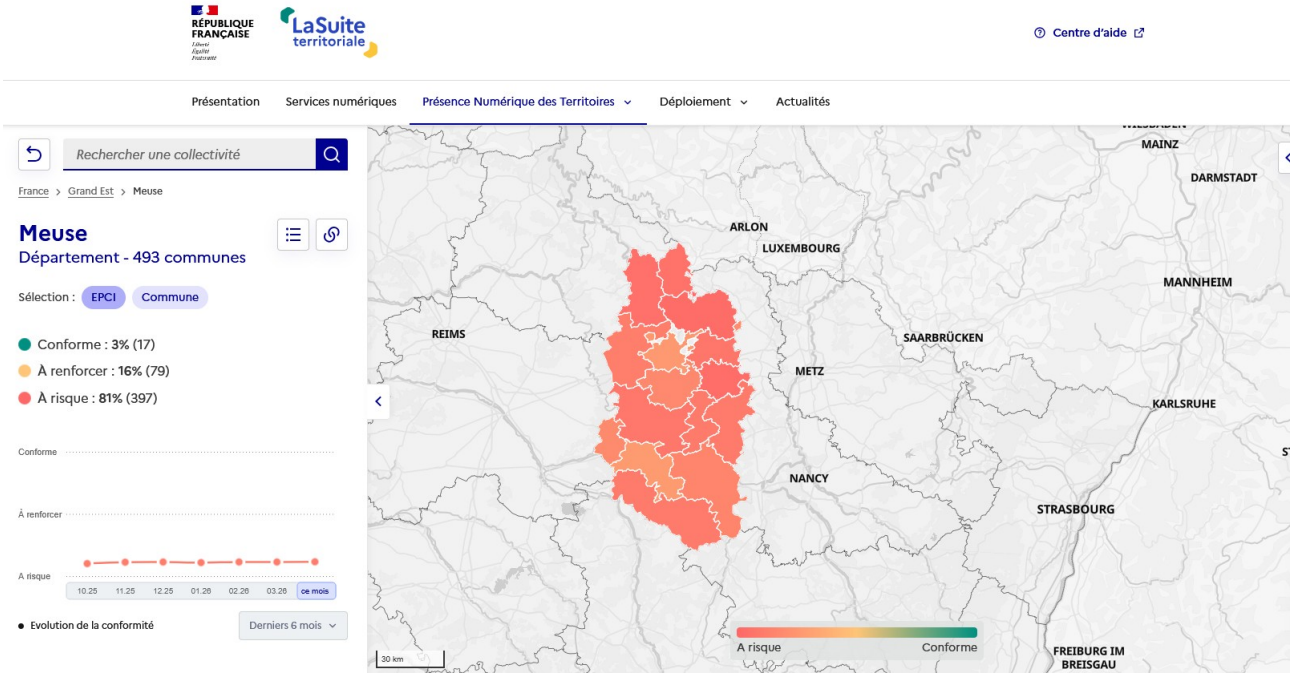
La demande de changement de coordonnées bancaires via **usurpation d'identité de l'agent** est aujourd'hui le mode de **fraude le plus utilisé.**
La prise de contact se fait :

→ par mail : via une messagerie frauduleuse (souvent très proche de celle donnée par l'agent), avec une formulation éventuellement inhabituelle, en envoyant un RIB frauduleux portant le nom de l'agent victime de l'usurpation ou en demandant le changement du RIB pour le versement de la paye.
→ par téléphone.

Outils utiles

- **Cartographie de conformité commune :**
  La Suite Territoriale met en ligne une carte interactive qui permet d'identifier les communes conformes ou non aux critères de sécurité dans leur communication en ligne en se basant sur les critères du site internet et de l'adresse de messagerie de la collectivité.

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



- **Mot de passe :**
  Le lien suivant permet à la fois de vérifier la robustesse d'un mot de passe et de s'assurer qu'il n'a pas été éventé :

https://www.ssi.economie.gouv.fr/motdepasse

⚠ rappel : **ne jamais divulguer son mot de passe à un tiers.**

- **Vérificateur d'IBAN :**
  Cet outil permet de confirmer la validité d'un numéro IBAN avant d'effectuer un virement ou un prélèvement. Il réduit ainsi le risque de fraude, notamment les faux ordres de virement (**FOVI**) :

  - Un escroc peut fournir un IBAN ou un RIB falsifié pour détourner un virement.
  - Il peut aussi créer des prélèvements frauduleux.

  - https://www.ibancalculator.com/

Témoignage : escroquerie au virement

En 2026, les arnaques au RIB restent une menace majeure, exploitant souvent l'usurpation d'identité via des comptes de messagerie piratés pour inciter les victimes à effectuer des virements vers des comptes frauduleux. Un élu local de la Meuse, victime de cette fraude nous relate les faits. Afin de garantir la confidentialité, ce témoignage a été présenté de façon anonyme.

Pourriez-vous nous raconter ce qui s'est produit ?
La mairie a fait appel à Monsieur X, pour qu'il réalise des travaux d'entretien de l'église de la commune. En septembre 2025, il nous envoie un mail contenant une facture ainsi qu'un RIB. Nous effectuons le virement. En janvier 2026, il appelle mon adjoint en disant que la facture n'était pas réglée. Nous lui avons dit que la facture avait été réglée en septembre. Nous lui avons retransféré le mail et c'est à ce moment qu'il nous indique que ce n'est ni son adresse mail ni son RIB.

À combien s'élève le préjudice ?
À plus de 11 000 €.

Quel est le RIB sur lequel vous avez effectué le virement ?
Il s'agit d'un compte de la BNP Paribas. Notre SGC a fait une recherche FICOBA avec laquelle nous avons eu des informations. Il s'agit en fait de Monsieur Y, domicilié en région parisienne.

Avez-vous déjà travaillé avec Monsieur X ?
Oui, nous avons fait appel plusieurs fois à lui, nous n'avons jamais eu de soucis avec lui.

Lorsque votre adjoint a eu Monsieur X au téléphone, quels échanges ont-ils eu ?
Monsieur X réclamait le paiement de la facture. Mon adjoint et moi-même lui avons envoyé un message en lui transférant le mail que nous avions reçu.

De quelle adresse avez-vous reçu le faux mail ?
nom.prénom1@gmail.com

Quelle est la vraie adresse de Monsieur X ?
prénom.nom@gmail.com

Aviez-vous déjà conversé avec Monsieur X par mail ?
Oui, à chaque fois, on passait par mail et c'est pour cela que nous n'avons pas trouvé cela bizarre.

Quel est le RIB sur lequel vous payiez habituellement Monsieur X ?
Un RIB appartenant au Crédit Agricole de Lorraine.

Qui a effectué le virement ?
La secrétaire de mairie a effectué le mandat et l'a envoyé au Trésor Public qui a effectué le virement.

Pouvez-vous nous fournir les dates et heures des contacts téléphoniques et d'échanges de mails ?
Nous avons été contactés le 08/09/2025 à 10h22. Or, Monsieur X nous a retransféré le vrai mail qu'il nous avait envoyé. Il nous l'avait envoyé à 6h11.

En comparant les deux factures, avez-vous remarqué des différences ?
Après coup, l'adresse mail sur les factures est différente et la signature numérique de la vraie facture a été remplacée par "mode de paiement : « virement ».

La boite mail de la mairie a-t-elle été piratée ?
Pas que je sache.

Sites utiles

https://www.cybermalveillance.gouv.fr/
https://cyber.gouv.fr/
https://www.francenum.gouv.fr/
https://www.cybersecurite.grandest.fr/services-en-ligne/
https://suiteterritoriale.anct.gouv.fr/