Cybersécurité des collectivités en Centre-Val de Loire

En collaboration avec le **GIP-RECIA**, le Centre de Réponse aux Incidents Cyber **cybeRéponse** et la **Gendarmerie Nationale**.

Pourquoi, dans le cadre d'une politique de cyber sécurité sérieuse, une collectivité comme une MAIRIE, ne devrait JAMAIS utiliser de nom de domaine du type gmail.com, hotmail.fr ou wanadoo.fr ?

Principalement en raison de risques critiques pour la cybersécurité, la confidentialité et la légitimité institutionnelle.

1. Perte de contrôle sur les communications

Dépendance à un prestataire externe : avec un domaine tiers, la mairie n'a aucun contrôle sur le fonctionnement, les politiques ou les conditions d'utilisation imposées par le fournisseur. En cas de panne, de modification des conditions de service, ou de compromission, la mairie ne peut pas intervenir.

Aucune garantie sur les données : les messages transitent et sont stockés sur des serveurs appartenant à une entité privée. Si cette dernière décide de suspendre ou de clôturer le compte, la mairie perd accès à ses données.

2. Non-conformité avec les obligations légales et réglementaires

Violation du RGPD[1] [Règlement Général sur la Protection des Données] : les collectivités traitent des données sensibles [identité, santé, état civil, etc.]. Ces données doivent être protégées et rester sous juridiction européenne. Or, certains fournisseurs comme Gmail [Google] ou Hotmail peuvent héberger des données sur des serveurs en dehors de l'Union européenne, exposant la mairie à des sanctions légales.

Obligations spécifiques des collectivités : les administrations publiques françaises sont tenues de garantir la souveraineté numérique et d'utiliser des outils conformes aux recommandations de l'ANSSI [Agence nationale de la sécurité des systèmes d'information] relayées par le CSIRT cybeRéponse ou encore cybermalveillance.gouv.fr ainsi que celles de la CNIL afin d'héberger les données sur des infrastructures souveraines et conformes au RUT. L'utilisation d'un domaine générique viole ces principes.

3. Exposition accrue aux cyberattaques

Harneçonnage facilité : les adresses utilisant des domaines génériques [ex. : mairie.macommune@gmail.com] sont faciles à imiter, Les cybercriminels peuvent créer des adresses similaires pour tromper les citoyens ou d'autres partenaires.

Manque de sécurité avancée : les noms de domaine dédiés permettent de configurer des mécanismes de protection avancés comme SPF, DKIM et DMARC[1], qui authentifient les emails et empêchent leur usurpation. Ces options sont limitées ou absentes sur des services tiers.

1. Règlement Général à Protection des Données : https://www.cnil.fr/fr/reglement-europeen-protection-donnees
https://recia.fr/conseil-et-accompagnement/accompagnement-juridique-et-protection-des-donnees/

2. trois méthodes d'authentification du courrier électronique, empêchant les spammeurs, les hameçonneurs, et d'autres parties non autorisées d'envoyer des e-mails au nom d'un domaine dont ils ne sont pas propriétaires

Soutenu par

4. Les risques d'image

Image institutionnelle altérée : le fait pour une mairie d'utiliser une adresse générique [ex. mairie.macommune@gmail.com ou mairie.macommune@wanadoo.fr] peut nuire à la confiance des administrés et des partenaires.

Incohérence avec le rôle officiel : une collectivité doit être identifiable clairement via un domaine personnalisé [ex. mairie-macommune.fr] qui inspire confiance et reflété sen autorité.

5. Fragmentation et difficultés organisationnelles

Gestion dispersée des comptes : les adresses email sur des services tiers sont souvent utilisées de manière individuelle ce qui complique la centralisation et la gestion des communications, cela rend également la supervision difficile notamment pour le respect des politiques internes.

Pérennité compromise : si un élu ou un agent quitte la mairie, les accès à un compte tiers peuvent être perdus ou mal transférés, exposant potentiellement les informations à des risques.

NOTRE RECOMMANDATION

Une mairie ou une collectivité doit investir dans un nom de domaine propre [quelques dizaines d'euros par an] et l'hébergement associé, idéalement auprès d'un fournisseur spécialisé dans les services publics de proximité comme le GIP-RECIA.

Cela garantit

Sécurité accrue des données.

Confiance des administrés.

Conformité avec les obligations légales.

Maîtrise complète des systèmes de communication.

Exemple pour la mairie de "**Macommune**"

Domaine : mairie-macommune.fr

Adresses email : contact@mairie-macommune.fr

services@mairie-macommune.fr [privilégier des adresses génériques plutôt que nominatives]

Maintenant que vous êtes au courant, utiliser un domaine générique comme gmail.com, hotmail.fr, wanadoo.fr ou émanant d'autres opérateurs, expose une mairie à de nombreux risques : perte de contrôle, violations légales, cyberattaques, et perte de crédibilité. Il est impératif pour une collectivité d'avoir son propre domaine [ex. mairie-macommune.fr] et de mettre en place des infrastructures sécurisées pour garantir la souveraineté, la confidentialité, et la confiance.
Ce simple modèle renforce hautement la fiabilité et protège votre collectivité contre les risques liés aux services externes.

En collaboration avec le GIP-RECIA, **cybeRéponse** [information au 02 19 230 466 numéro d'urgence 0805 69 15 05] et la Gendarmerie Nationale [17], une assistance vous est proposée pour la création de votre nom de domaine auprès du GIP-RECIA, votre OPSN[3] régional mutualisant, en appelant le 02 38 42 79 60.

3. Opérateur Public de Services Numériques