ENJEUX

INFORMER

CONFORMITÉ

RGPD

PROCÉDURES

MATÉRIEL

Sensibilisation cybersécurité

À DESTINATION DES ÉLUS ET DES AGENTS TERRITORIAUX

COLLECTIVITÉS

MOTS DE PASSE

MISES À JOUR

RISQUES

GESTION

MOBILES

PARTENARIATS

PLANS

COMMENCER À METTRE EN PLACE LA CONFORMITÉ...

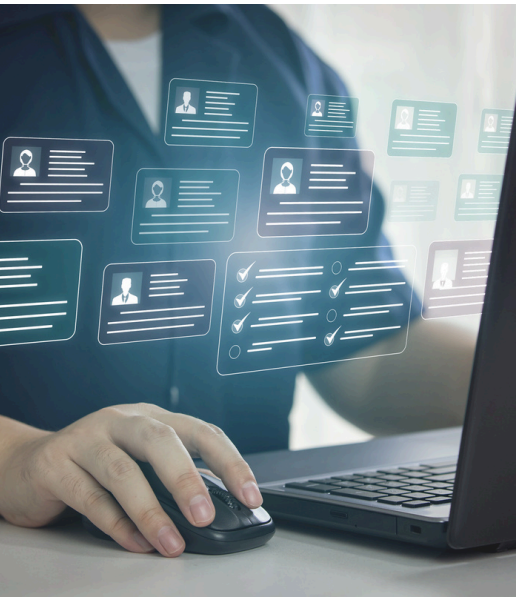
COLLECTIVITÉS

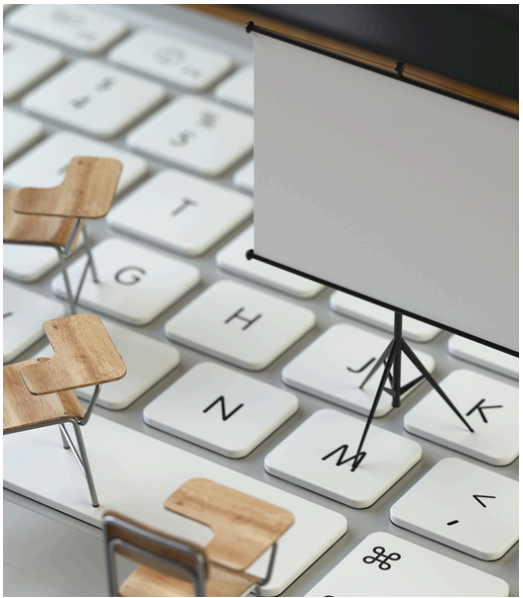
Quelques conseils de sensibilisation à la cybersécurité

Les collectivités gèrent de grandes quantités de données sensibles (données personnelles des administrés, informations fiscales, etc.), ce qui les rend particulièrement vulnérables aux cyberattaques.

Une cyberattaque peut paralyser les services publics, entraîner des pertes financières importantes et nuire à la réputation de la collectivité. La cybersécurité est donc essentielle pour assurer la continuité des services publics et la confiance des citoyens.

Il faut donc prendre du temps pour sensibiliser les membres du conseil, les agents territoriaux et tous les acteurs en lien avec la gestion des données des administrés.





COLLECTIVITÉS

Nos conseils pour les collectivités

Formation continue

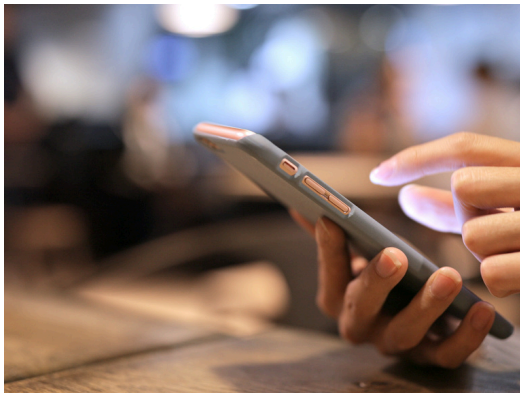
Les élus et les agents territoriaux doivent suivre régulièrement des formations sur les dernières menaces (phishing, ransomware, etc.), les bonnes pratiques et la réglementation en vigueur (RGPD, normes de cybersécurité, etc.).

Protection réseaux

Rappeler que les mises à jour des logiciels et systèmes d'exploitation sont essentielles pour combler les failles de sécurité. Les mises à jour doivent être appliquées dès qu'elles sont disponibles pour éviter l'exploitation des vulnérabilités par des cybercriminels.

Equipements mobiles

Les smartphones et tablettes doivent être protégés par des mots de passe ou des codes PIN. Les agents doivent être encouragés à ne jamais laisser leurs équipements sans surveillance et à utiliser des connexions sécurisées.



COLLECTIVITÉS

Nos conseils pour les collectivités

Identification risques

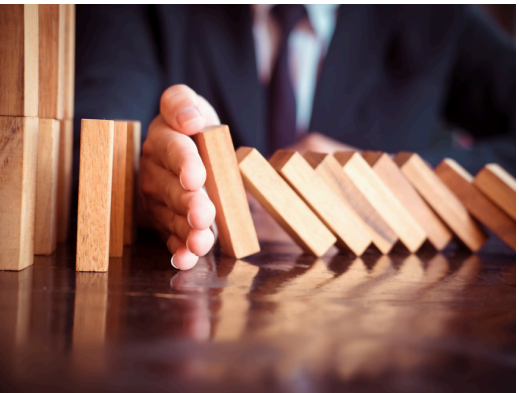
Expliquer l'importance de connaitre un grand nombre de techniques de phishing, où un hacker se fait passer pour un interlocuteur de confiance (banque, administration, ou collègue) afin d'obtenir des informations sensibles.

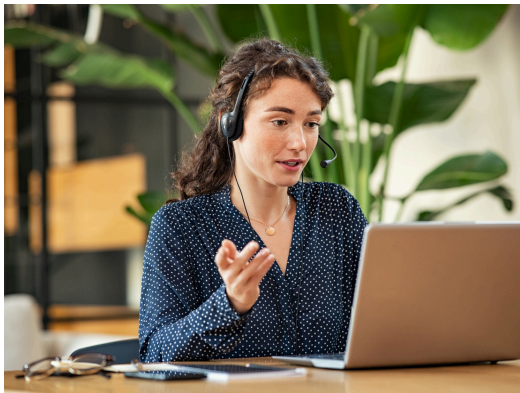
Gestion des accès

Expliquer l'importance de limiter l'accès aux informations sensibles. Seuls les agents qui en ont réellement besoin pour leur mission doivent y avoir accès.

Télétravail

Lors du télétravail, il est crucial d'utiliser des connexions VPN pour sécuriser les communications, surtout lorsqu'elles impliquent l'accès à des données sensibles de la collectivité. L'utilisation des réseaux Wi-Fi publics doit être évitée pour les accès sensibles.





COLLECTIVITÉS

Contact

SCHOETTEL Audrey
DPO externe / cybersécurité
Proche La Rochelle

www.revisium.fr

Mail : contact@revisium.fr

Tel : 0 805 035 135
ou 05 17 81 00 05

Revisium