Bonjour,

Votre collectivité fait appel aux services du Centre Interdépartemental de Gestion de la Grande Couronne pour la gestion des ressources humaines et éventuellement d'autres prestations. Le 31 janvier 2022, le Centre de Gestion a été victime d'une attaque informatique par rançongiciel. Son Système d'Information a été atteint et son prestataire Orange Cyberdéfense vient de lui communiquer ses conclusions dans lesquelles il relève l'extraction de près de 270 Gigaoctets soit environ 3 % des données enregistrées sur nos serveurs.

En tant qu'administré, vos données personnelles renseignées dans le cadre de l'instruction d'un dossier d'urbanisme ont potentiellement été concernées par cette extraction.

Les investigations d'Orange Cyberdéfense ne permettant pas de déterminer les données concernées par l'extraction, nous vous invitons à la plus grande vigilance quant aux prochaines communications que vous serez amenés à recevoir. En effet, ces données peuvent être utilisées à des fins d'hameçonnage à votre encontre (*réception de messages trompeurs vous incitant à dévoiler vos données personnelles*) ou à des fins d'usurpation d'identité (*utilisation de vos informations personnelles à votre insu afin de vous tenir responsable d'actes frauduleux*).

Voici quelques indicateurs vous permettant d'identifier :

- **Une tentative d'hameçonnage :**
  - L'adresse mail de l'expéditeur paraît suspecte ;
  - Le contenu du mail présente des fautes d'orthographe, de frappe ou de grammaire ;
  - Le message du mail est alarmiste et vous demande d'agir rapidement (*fermeture d'un compte, colis non livré si absence de paiement, etc.*) ;
  - Le message est attractif (*montant gagné en attente, remboursement disponible, etc.*) ;
  - L'expéditeur vous incite à cliquer sur un lien ou à ouvrir une pièce jointe.

Si vous souhaitez plus d'information sur l'hameçonnage vous pouvez consulter le site https://www.cybermalveillance.gouv.fr/, rubrique « Les menaces et bonnes pratiques > Comprendre les menaces et agir > Que faire en cas de phishing ou hameçonnage ? » (*https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing*).

- **Une usurpation d'identité :**
  - Des notifications de modifications d'informations personnelles (*alerte concernant un changement de mot de passe par exemple*) ;
  - Des alertes de connexions inhabituelles ;
  - Une activité anormale sur vos comptes de réseaux sociaux (*difficulté de connexion, contact de vos proches à votre insu*) ;
  - La création de faux profils à votre nom (à vérifier avec une recherche de Google).

Si vous désirez en savoir plus sur le sujet de l'usurpation d'identité, vous pouvez consulter le site https://www.cybermalveillance.gouv.fr/, rubrique « Les menaces et bonnes pratiques > Comprendre les menaces et agir > Usurpation d'identité, que faire ? » (*https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/usurpation-identite-que-faire*).

Nous tenons à vous assurer que le CIG a mis en œuvre toutes les mesures techniques nécessaires afin de limiter l'étendue de l'attaque. Il a également mobilisé ses ressources internes et fait appel à des prestataires externes pour l'aider à rétablir son système d'Information.

Le service Gouvernance et Protection des données est disponible au 01 39 49 70 09 ou à l'adresse mail suivante dpd.cig@cigversailles.org

Le Centre Interdépartemental de Gestion de la Grande Couronne