CDG 67
fonction publique territoriale

Mars 2020

Covid-19 : protéger les données et le SI[1] face à l'augmentation de la cybermenace

Dans ce contexte de crise sanitaire du Covid-19 ainsi que du développement du télétravail, les cybermenaces se sont développées (attaques informatiques, telles que virus, ainsi que les vols de données).

Ainsi, les quelques bonnes pratiques suivantes sont à respecter pour s'assurer de la protection des données personnelles et du système d'information de votre collectivité :

- **Faire attention aux mails, sms ou appels téléphoniques** qui pourraient utiliser le contexte de crise concernant le coronavirus pour vous inciter à réaliser notamment les points suivants :

  – **Ouverture de pièces jointes et de liens présents dans un mail ou sms** : possibilité de télécharger un virus caché dans une pièce jointe ou dans un lien
  – **Transmission de données illégitimes** : possibilité de faire l'objet d'un hameçonnage, c'est-à-dire de communiquer les données à une personne se faisant passer pour quelqu'un de légitime (demande de saisie de votre identifiant et mot de passe, demande de communication d'un RIB ou d'autres informations personnelles, paiement d'une facture, etc.)

⇨ Avant l'ouverture d'une pièce jointe, d'un lien, ou de la transmission de données à un tiers, vérifiez l'expéditeur de ce message et si ce message était attendu de cette personne (si un doute persiste, téléphonez à cette personne). Sachez tout de même que les cybercriminels peuvent vous envoyer un message de la part d'un expéditeur légitime. Ainsi, il faut porter son attention sur le contenu du message (style d'écriture du message et cohérence du contenu) pour s'assurer qu'il s'agit bien de la bonne personne qui a écrit ce message.

- **Faire attention aux sites internet** qui pourraient utiliser le contexte de crise concernant le coronavirus pour vous inciter à réaliser notamment les points suivants :

  – **Transmission de données illégitimes** : possibilité de faire l'objet d'un hameçonnage, c'est-à-dire de communiquer les données à une personne se faisant passer pour quelqu'un de légitime (demande de saisie de votre identifiant et mot de passe, demande de communication d'un RIB ou d'autres informations personnelles)

[1] SI signifie système d'information, c'est-à-dire l'ensemble de l'organisation permettant de collecter, stocker, traiter et distribuer de l'information (à travers notamment des ressources informatiques, organisationnelles et humaines)

CENTRE DE GESTION DE LA FONCTION PUBLIQUE TERRITORIALE DU BAS-RHIN
12 avenue Schuman – CS 70071 – 67382 LINGOLSHEIM CEDEX
Tél. 03 88 10 34 64 – Fax : 03 88 10 34 60
www.cdg67.fr

- **Téléchargement :** possibilité de télécharger un document contenant un virus caché

- **Eviter l'utilisation des plateformes telles que Google drive, Dropbox ou Wetransfer ainsi que la transmission par mail de documents contenant des données personnelles :** ces méthodes ne garantissent pas la sécurité et la confidentialité des données stockées.

- **Chiffrer[2] les documents avant de les mettre en pièces jointes ou de les déposer sur des plateformes de partage de documents en ligne,** avec l'outil présent sur tous les ordinateurs, **7zip.** Le mot de passe choisi devra être transmis, soit par téléphone, soit dans un second mail a minima.

- **Protéger vos mots de passe :**

  - Ne les communiquer à personne, sauf le service informatique le cas échéant (mais il faut bien s'assurer qu'il s'agisse d'une demande du service informatique et non d'une personne se faisant passer pour le service informatique)
  - Ne pas les stocker sur votre ordinateur dans un fichier Word ou Excel non protégé (a minima, il faudrait chiffrer ce document et ne pas le nommer « mots de passe »)

- **Ne pas utiliser les ressources professionnelles à des fins personnelles et inversement**

À NOTER

A contacter en cas de constatation, ou de doutes, sur un évènement malveillant :

- **Si vous avez fait l'objet d'une cyberattaque, ou que vous avez des doutes, ou que vous remarquez des choses inhabituelles, contactez au plus vite votre service informatique ou votre prestataire**

[2] Utilisez l'outil 7zip présent sur tous les postes, clic droit sur le fichier que vous souhaitez chiffrer puis cliquez sur 7zip, puis cliquez sur ajouter à l'archive, puis ajouter un mot de passe dans l'espace en bas à droite de la fenêtre.