Centre de Gestion 14 Calvados

Cybersécurité

Pour les petites collectivités

Votre expert RH de la fonction publique territoriale

CENTRE DE GESTION DU CALVADOS
2 Impasse Initialis - CS 20052
14202 Herouville-Saint-Clair

02 31 15 50 20

cdg14@cdg14.fr

État de la menace

Apprenez à identifier les attaques !

Toutes les communes, même les plus petites, sont exposées au risque de cyberattaques.

1 collectivité normande par semaine :

Cyber attaquée selon la Gendarmerie Nationale pour la Région Normandie

1 collectivité sur 10 :

Victime de cyberattaque en 2024 au niveau national

Vous êtes une cible car :

Vous détenez des données personnelles de vos habitants, qui peuvent être revendues et améliorer les gains du pirate

Vous ne pensez pas être assez gros pour les intéresser

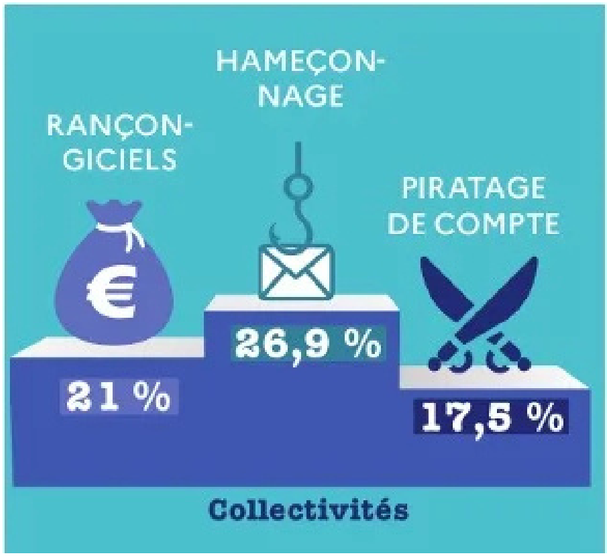
Vous êtes souvent sous équipés en solutions basiques de cybersécurité

Vous n’avez pas de service informatique interne pour vous épauler

Attaquants

TYPOLOGIE	OBJECTIFS
1 Étatique	Espionnage à des fins économiques, politiques ou militaires / déstabilisation / sabotage
2 Hacktivistes	Déstabilisation / porter atteinte à l'image de la collectivité
3 Cybercriminels	Recherche de gains financiers
4 Amateurs	S'entraîner / sabotage

Menaces les plus prégnantes pour les petites collectivités

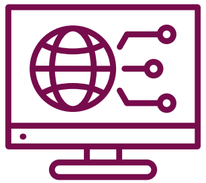


Source : cybermalveillance.gouv.fr

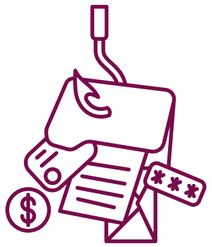
- Hameçonnage ou phishing
- Rançongiciels ou ransomwares
- Piratage de compte en ligne
- Arnaques au faux support technique

L'hameçonnage et/ou le piratage de compte sont utilisés pour réaliser des fraudes au Faux Ordre de Virement (FOVI).

Hameçonnage



Technique qui leurre l'internaute pour l'inciter à communiquer des données personnelles ou professionnelles (identité, adresses, comptes, mots de passe,données bancaires…)



1 hameçon – 1 appât – 1 victime
(sms, mail, téléphone, site frauduleux)

Usurpation de l'identité de l'organisme
(Administration, Banque, Fournisseur…)
Mots clés pour détourner votre attention
et jouent sur l'urgence

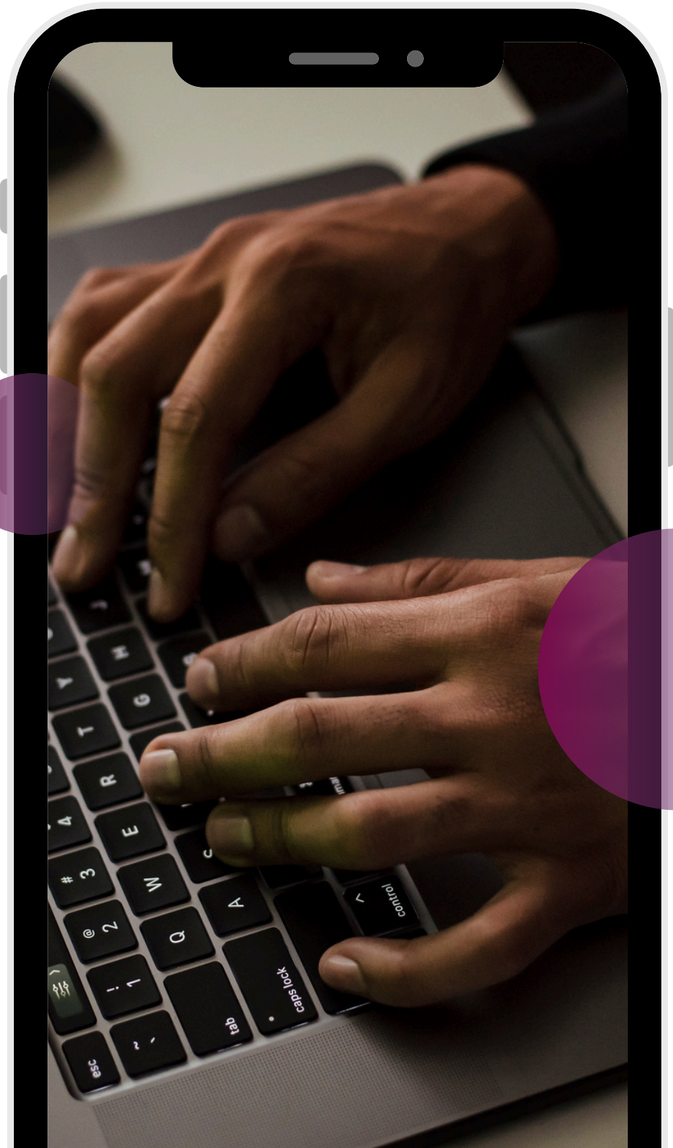
But poursuivi :
utilisation directe ou revente à des fins
d'escroquerie pour en faire
un usage frauduleux

Rançongiciels

Logiciel malveillant qui bloque l'accès à l'ordinateur et chiffre les fichiers

Comment ? L'infection passe par l'ouverture d'une PJ et/ou d'un lien malveillant dans un courriel, la navigation sur des sites compromis ou l'intrusion dans le système par l'exploitation d'une vulnérabilité connue

But poursuivi : extorsion de fonds ou encore endommager le système de la victime pour générer des pertes d'exploitation ou porter atteinte à son image



Piratage de compte

- Prise de contrôle d’un compte (messagerie, administration, banque, e-commerce, réseau social) par un individu malveillant au détriment de son propriétaire légitime

- **Comment ?** Mot de passe trop simple / communication de votre mot de passe lors d’un hameçonnage / utilisation du même mot de passe sur plusieurs sites

- **But poursuivi** : usurpation d’identité, transactions frauduleuses / escroqueries, reventes de données personnelles et/ou professionnelles, spam

Arnaque au faux support technique

Technique qui vise à vous effrayer prétextant un problème informatique grave et vous presse de rappeler un pseudo-service de dépannage

Comment ? Via une fenêtre pop-up, un sms, un tchat, un courriel ou par téléphone

But poursuivi : soutirer de l'argent pour un faux dépannage ou vous faire souscrire de faux abonnements, voire vous faire laisser prendre le contrôle de votre ordinateur.

Commune de -3500 habitants

Activités — Activités de service public diverses à mener (État Civil, Cimetière, Voirie, Espaces verts, cantines / distribution de repas , etc...)

Public — Chaque citoyen de la commune

Données — Ces activités conduisent au recueil de multiples données personnelles (administrés, agents, élus)

Objectif — Leur protection est un enjeu majeur, y compris pour le lien de confiance entre la collectivité et les citoyens

Une cyberattaque induit une déclaration à la CNIL en cas de violation de données → **RGPD**

Règlement Général sur la Protection des Données RGPD

Une obligation règlementaire en plusieurs étapes :

- Désigner un **Délégué à la Protection des Données** (sur le site de la CNIL)
- **Sensibiliser** les élus et agents
- Réaliser le **registre des traitements** de données personnelles
- **Mise en conformité :** sécurité informatique, contrats sous-traitants, mentions d'information, archivage

Le cas échéant :

- Répondre aux **demandes d'exercice des droits** (sous un mois)
- Alerter la CNIL en cas de **violation de Données Personnelles** (sous 3 jours)

Démarche continue :

Suivi conformité, mise à jour du registre, veille juridique...

Témoignage

Une commune du Calvados

Tendre vers une cybersécurité de qualité

- SOC (Security Operations Center)
- EDR (XDR)
- VPN (télétravail / double authentification)

- 1 identifiant par utilisateur
- Protection des mails (anti-phishing, antivirus, anti-spam)
- Sauvegardes (internes & externes)

- Antivirus
- Mises à jour systématique des OS (Windows)
- Verrouillage automatique de la session
- Mots de passe forts

Avez-vous des questions ?

CONTACT CYBERSÉCURITÉ :

Magalie LANDEMAINE
07 88 64 45 35 - cybersecurite@cdg14.fr

CONTACT RGPD :

Corentin PAUL & Alexandre LABBAY
02 31 15 50 49 - 02 14 99 04 07
rgpd@cdg14.fr

Merci de votre attention !

Le CDG 14, votre expert RH de la fonction publique territoriale.

02 31 15 50 20

cdg14@cdg14.fr

www.cdg14.fr

Centre de Gestion de la Fonction Publique Territoriale du Calvados

2 impasse Initialis
CS 20052
14202 HÉROUVILLE SAINT CLAIR

Horaires :

Du lundi au jeudi :
8h30 à 12h30 / 13h30 à 17h

Le vendredi :
8h30 à 12h30 / 13h30 à 16h30