

CYBERACTU'

LE MAGAZINE DU SERVICE « PROTECTION DES DONNÉES » DU CENTRE DE GESTION DU GARD

Noël 2025



Spécial Noël



CENTRE ^{DE} GESTION

DU GARD



Contactez-nous

04 66 38 86 86
cdg30@cdg30.fr



CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous



CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous



CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

Contactez-nous



CENTRE DE GESTION
DE LA FONCTION PUBLIQUE TERRITORIALE
DU GARD

SOMMAIRE

Page 4

CONTE D'HIVER

Page 7

POURQUOI LES CYBERATTAQUES AUGMENTENT PENDANT LES FÊTES ?

Page 8

TOP 3 DES MENACES LES PLUS FRÉQUENTES EN DÉCEMBRE

Page 10

LE BON GESTE

« LA DISTRIBUTION DES CHÈQUES DE NOËL »

Page 15

LE MENU DE NOËL – VERSION SÉCURITÉ INFORMATIQUE RENFORCÉE

ÉDITO

Votre service « Protection des données » souhaite vous accompagner pendant cette période festive au travers de cette édition spéciale qui présente les stratégies les plus fréquemment utilisées par les cyber criminels, incarnés ici par le fameux « Grinchex ».

Dans le but d'assurer les données personnelles de vos agents, vous trouverez une nouvelle fiche de traitement à ajouter à vos registres « La distribution des chèques cadeaux ».

Un menu spécial qui vous permettra de partager un moment chaleureux et gourmand vous attend à la fin. Bonne dégustation!

Pierre BONANNI – Ana VEGA



Contacts

Service « Protection des données »

☎ : 04 66 38 86 86

@ : dpd@cdg30.fr



LE GRINCHEX ET LA GRANDE VEILLÉE DES DONNÉES

Conte d'hiver en trois grandes nuits

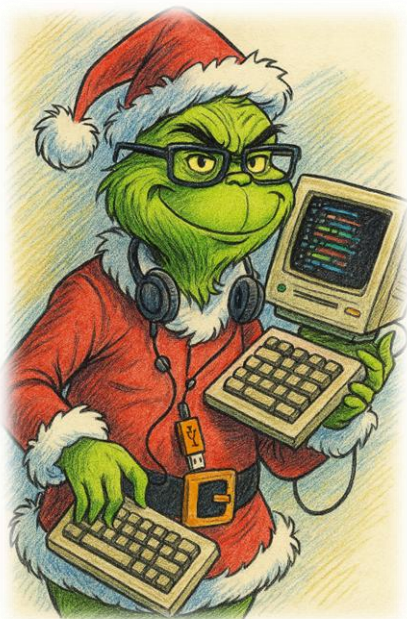
Là où souffle le Vent Hivernal

Il existait, au-delà des forêts de pins givrés et des plaines où la neige scintille comme un manteau de diamants, un petit bourg nommé Neige-sur-Réseau.

Ce village était réputé pour deux choses : la chaleur de ses habitants et la splendeur de sa Grande Veillée de Noël, célébrée chaque année avec des lanternes, des chants et des gâteaux si délicieux que certains prétendaient qu'ils pouvaient attendrir un cœur de pierre.

Mais au sommet du Mont Pare-Feu, dans une caverne creusée entre des rochers en forme de touches de clavier, vivait une créature étrange : le Grinchex.

Il ressemblait de loin au Grinch de contes plus anciens, mais celui-ci avait une obsession bien particulière : dérober les secrets, mots de passe et petites imprudences des habitants, non pas pour les faire souffrir... mais parce que, au fond, il rêvait de faire partie de leurs vies et d'être invité à leur fête. Seulement, n'ayant jamais appris la bienveillance, il ne savait que s'introduire dans les affaires d'autrui.



Et c'est ainsi que commence l'histoire de la Grande Veillée où tout changea.

Première Nuit : L'Hameçon d'Argent

Lorsque les premiers flocons tombèrent, Grinchex sentit que le moment était venu. Il avait passé des mois à élaborer un plan, griffonnant sur des parchemins couverts de schémas incompréhensibles et de dessins de cadeaux.

— Cette année, murmura-t-il, je serai au centre de la fête, et tout le monde remarquera enfin mon génie !

Il fabriqua alors ce qu'il appela son Hameçon d'Argent : une série de messages mensongers déguisés en invitations du Père Noël. Ils promettaient des cadeaux merveilleux, des réductions incandescentes, des paniers gourmands aussi gros qu'un renne.

Au matin, les villageois découvrirent dans leurs boîtes de courriel magique : « Cher ami, ton cadeau n'attend que toi ! Clique vite pour confirmer ton identité ! »

Certains s'exclamèrent :

— *Oh ! Quelle bonne nouvelle !*

— *Quel Père Noël attentionné !*

Mais au cœur du village vivait une vieille femme connue sous le nom de Mamie Filet-de-Sûreté. Son châle tricoté ressemblait à un pare-feu, et son regard, vif comme une alerte de sécurité.

En lisant le message, elle grogna :

— « *Ce Père Noël-là n'a ni style, ni orthographe. Et voilà une adresse mail bien curieuse !* »

Elle convoqua aussitôt la population sur la place, leur expliquant d'une voix grave :

— « *Méfiez-vous des hameçons d'argent, mes chers enfants. Noël rend les cœurs joyeux... mais parfois distraits.* »

Grâce à elle, plusieurs villageois annulèrent leur imprudence. Et déjà, le plan du Grinchex commençait à se fissurer.

Deuxième Nuit : Le Masque du Lutin Égaré

Déçu mais pas vaincu, Grinchex élaborait une seconde stratégie. Il se couvrit d'un costume de lutin rutilant, cousu de clochettes et de rubans trop brillants pour être honnêtes. Il descendit au village sous un prétexte plein de miel :

— « *Bonjour ! Je suis Lutin-Sécurion, envoyé spécial du Père Noël. Je viens vérifier vos accès magiques, vos mots de passe et vos coffres-forts numériques personnels pour... hum... assurer la sécurité des cadeaux !* »

Beaucoup d'habitants, naïfs ou trop occupés, manquèrent de peu de lui ouvrir leurs carnets ou leur coffres-forts numériques. Mais un enfant, Marcel, le regarda attentivement. Il remarqua une couture étrange derrière l'oreille du soi-disant lutin, ainsi qu'un badge mal contrefait.

— « *Monsieur... pourquoi votre badge dit-il Sécurion Officiel du Mont Pare-Feu et pas du Pôle Nord ?* » demanda-t-il.

Grinchex bafouilla. Les clochettes de son habit tintaient de peur.

Mamie Filet-de-Sûreté arriva à cet instant.

— « *Encore toi, petite fouine de montagne...* » lança-t-elle sévèrement.

Puis, s'adressant à la foule :

— « *Rappelez-vous : jamais un vrai envoyé spécial ne vous demandera vos secrets. Même sous un costume chatoyant !* »

Cette fois encore, Grinchex dut s'enfuir sous les huées... mais quelque chose en lui changeait. Car en voyant l'enfant le démasquer, il ressentit une émotion étrange : de la honte. Et une pointe... d'envie de faire partie d'eux.

Troisième Nuit : La Voix Métamorphosée

Pour sa dernière tentative, Grinchex utilisa une magie plus subtile, apprise dans de vieux grimoires numériques. Une magie capable d'imiter n'importe quelle voix : l'intelligence artificielle. Dans son antre, il grava dans un cristal vocal : la voix du maire, celle du boulanger, et même celle du Père Noël. Puis il appela la mairie en murmurant :

— « *Ho ho ho ! Je suis le Père Noël ! Donne-moi ton code secret pour libérer les cadeaux !* »

Mais le maire, homme prudent et formé aux mystères de la cybersécurité, demanda calmement :

— « *Très bien... mais alors, Père Noël, dis-moi : quel est le nom du renne que tu as blessé l'hiver dernier en glissant sur une comète ?* »

Le silence du Grinchex fut tel qu'on aurait entendu fondre un flocon. Il raccrocha, pris de panique. Le maire réunit tout le village :

— « *Mes amis, souvenez-vous toujours : la voix peut tromper, mais la vérification protège. Noël doit rester un moment de confiance, pas de naïveté.* »



Et sur le Mont Pare-Feu, Grinchex comprit que son dernier plan venait d'échouer. Il observait le village depuis sa grotte, sentant une lourdeur dans son cœur. Ces gens riaient ensemble, se protégeaient, se soutenaient... C'était ce lien qu'il envierait depuis tant d'hivers.

Le Réveil du Cœur Authentique

Le soir de la Grande Veillée arriva. Les lanternes éclairaient les rues, les chants s'élevaient, et l'air sentait la cannelle et le sapin. Grinchex, tremblant comme une fenêtre sous la neige, descendit néanmoins. Non pour voler. Pas cette fois.

Il avait un petit sac avec lui... non pas rempli de clefs USB infectées, mais de boules de Noël qu'il avait fabriquées de ses propres mains. Il avança timidement sur la place. Le maire se tourna vers lui. Les habitants se turent. Grinchex murmura :

— « *Je voulais... participer. Je ne savais pas comment... alors j'ai mal agi. Je suis désolé.* »

Mamie Filet-de-Sûreté posa sa main ridée sur la sienne.

— « *Il n'est jamais trop tard pour apprendre à protéger au lieu de tromper.* »

Le maire sourit :

— « *Grinchex... serais-tu prêt à devenir le Gardien de la Cybersécurité de Noël ? Nous avons besoin de quelqu'un qui connaît les pièges pour mieux les éviter.* »

Et alors, dans cette nuit glacée, le cœur du Grinchex se dilata si fort qu'on aurait cru entendre un antivirus se mettre à jour. Il fut invité au banquet. On lui donna un manteau rouge, un rôle officiel, et même une assiette de cookies encore tièdes.

Et depuis cette nuit-là, à Neige-sur-Réseau : aucun hameçon, aucune imposture, aucune voix trompeuse ne menaça plus jamais la fête, car le Grinchex, désormais leur allié, veillait sur eux.

La confiance est un cadeau précieux. Il se protège avec **vigilance**, se renforce avec **l'entraide**, et se partage avec **bienveillance**. Et surtout : Même les cœurs les plus maladroits peuvent apprendre à protéger ce qu'ils aiment.



POURQUOI LES CYBERATTAQUES AUGMENTENT PENDANT LES FÊTES ?

La période des fêtes de fin d'année est souvent un moment de ralentissement dans les administrations publiques : congés des agents, fermetures partielles, surcharge de sollicitations... Un contexte idéal pour les cybercriminels, qui profitent de cette baisse de vigilance pour multiplier leurs attaques.

Chaque mois de décembre, les collectivités territoriales enregistrent une hausse des incidents numériques, souvent plus complexes à détecter et à contenir que le reste de l'année.

Moins de personnel présent : une surface de risque élargie

Décembre est un mois où les équipes sont réduites. Une mairie qui fonctionne habituellement avec plusieurs agents peut se retrouver avec un seul agent ou même aucun agent pendant quelques jours. Les conséquences sont : moins de surveillance des systèmes, moins de disponibilité pour vérifier les alertes et une détection plus lente des comportements anormaux.

Dans de nombreuses attaques recensées, les intrusions ont eu lieu quelques jours avant Noël, lorsque les équipes commencent à s'absenter. Ce laps de temps donne aux cybercriminels une marge de manœuvre pour explorer le réseau sans être repérés.

Des délais de réaction longs

Lorsqu'un incident survient en semaine hors période festive, une équipe peut réagir en quelques minutes ou heures. Pendant les fêtes, ce délai peut se transformer en journée(s).



Une simple tentative de connexion suspecte, qui aurait été bloquée immédiatement en temps normal, peut se transformer en compromission majeure, faute d'intervention rapide.

L'accroissement des communications festives : une aubaine pour les attaquants

En décembre, les mairies et les administrations envoient des vœux institutionnels, des lettres d'information et des invitations à des événements. Les cybercriminels exploitent cette pratique pour envoyer de faux messages qui semblent parfaitement légitimes. La surcharge de communications crée un environnement où il est plus difficile de repérer un email frauduleux parmi les nombreux messages festifs.

Les "cartes de vœux numériques", les "invitations officielles" ou les "documents administratifs de fin de budget" sont aujourd'hui parmi les vecteurs de phishing les plus utilisés en décembre.

Il ne nous reste qu'à espérer que l'adage soit confirmé : « **Danger annoncé, malheur évité.** »

TOP 3 DES MENACES LES PLUS FRÉQUENTES EN DÉCEMBRE

Phishing déguisé en communication festive et usurpation d'identité du maire ou d'un élu

Il s'agit d'une attaque fréquente. Exemples courants :

- une fausse carte de vœux avec pièce jointe malveillante,
- une invitation à un événement municipal piégée,
- un email prétendant provenir d'un agent de la collectivité parti en congé.

Ces messages contiennent souvent des liens vers de faux portails intranet ou des pièces jointes infectées.



Ransomware : les attaques programmées avant les congés

De nombreuses campagnes de ransomware sont déclenchées fin décembre, à un moment où les agents sont moins disponibles.

Les attaquants :

1. infiltrent le réseau plusieurs jours/semaines avant,
2. attendent que les services ferment,
3. lancent le chiffrement lorsque la réaction sera la plus lente.

L'objectif : maximiser l'impact pour augmenter les chances de paiement, même si les collectivités refusent généralement de céder.



Faux bons de commande et arnaques au fournisseur

En fin d'année, les budgets sont souvent ajustés ou clôturés. C'est pour les cybercriminels un moment propice pour :

- envoyer de fausses factures,
- demander un virement urgent,
- se faire passer pour un prestataire informatique.

Ces attaques reposent sur le stress du "dernier délai", souvent difficile à vérifier en période de congés.





RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité



Assistance et prévention
en sécurité numérique

C'est parti pour le Calendrier de l'Avent Cybersécurité !

Pendant tout le mois de décembre, cybermalveillance.fr vous propose 1 action simple par jour pour renforcer votre sécurité numérique.

Objectif : protéger vos données, vos comptes et votre vie numérique... un petit pas à la fois.

Chaque jour, une nouvelle étape pour améliorer votre cybersécurité.

Si vous êtes prêts à relever le défi, rendez-vous sur leurs réseaux sociaux !



1 JOUR 1 ACTION



Change tes
mots de passe
pour qu'ils soient
ROBUSTES et UNIQUES

MOT DE PASSE

2

Les Mots de passe

- ✓ Un mot de passe différent pour chaque compte
- ✓ 12 caractères minimum
- ✓ Majuscules + minuscules + chiffres + caractères spéciaux

Le conseil extra :

- ✓ Utiliser un gestionnaire de mot de passe sécurisé pour n'avoir à retenir que le mot de passe qui permet d'en ouvrir l'accès.

Distribution des chèques de Noël

FINALITÉ

Gérer l'attribution, la distribution et le suivi des chèques de Noël destinés aux agents de la collectivité, dans le cadre de l'action sociale et des avantages facultatifs accordés au personnel.

BASE LÉGALE

Article 6(1)(e) RGPD – Mission d'intérêt public

PERSONNES CONCERNÉES

- Agents titulaires et contractuels de la collectivité.
- Eventuellement : retraités ou ayants droit si prévu dans le règlement social.

CATÉGORIES DES DONNÉES

Identité : nom, prénom, matricule RH.

Données professionnelles : service, grade, type d'emploi, statut (titulaire/contractuel).

Données nécessaires à l'éligibilité : présence effective, ancienneté, temps de travail.

Coordonnées professionnelles : adresse mail professionnelle.

Données relatives à la situation familiale (uniquement si le montant dépend du nombre d'enfants, selon le règlement social interne).

Distribution des chèques de Noël

DESTINATAIRES DES DONNÉES

- Service Ressources Humaines.
- Service Finances, si nécessaire pour la commande des chèques.
- Prestataire externe émetteur des chèques cadeaux (type: émetteur de titres cadeaux). Sous-traitant.

TRANSFERTS DES DONNÉES HORS UE

En principe aucun transfert hors UE.
Si le prestataire utilise des serveurs hors UE :
vérifier l'existence de garanties (clauses contractuelles types, décision d'adéquation...).

DURÉE DE CONSERVATION

- Données liées à l'attribution du chèque : 1 an (durée nécessaire à la gestion et au contrôle).
- Données comptables ou justificatives : 10 ans
- Liste des bénéficiaires à des fins statistiques internes : anonymisée dès que possible.

MESURES DE SÉCURITÉ

- Accès restreint aux agents habilités du service RH.
- Transmission sécurisée des listes au prestataire (chiffrement ou espace sécurisé).
- Contrat de sous-traitance conforme à l'article 28 RGPD.
- Authentification forte dans les systèmes RH.
- Archivage sécurisé et suppression à échéance.

BLACK FRIDAY

**Attention
aux bonnes
affaires !**

7 CONSEILS POUR ÉVITER LES
ARNAQUES EN LIGNE





-20%

1

Méfiez-vous des
offres trop alléchantes qui
peuvent cacher des pièges

-50%



-20%

2

Ne vous précipitez pas !
Prenez le temps de vérifier la
réalité de l'offre et la
notoriété du vendeur



3

Assurez-vous que vous n'êtes
pas sur une **copie frauduleuse**
d'un site de vente officiel

-40%



-30%

4

Vérifiez la réalité de la
promotion sur le site officiel
du commerçant ou en
contactant par téléphone
son service commercial





-50%

5

Prenez garde aux **faux messages de livraison**, vérifiez toujours sur le site officiel de votre transporteur



6

Ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes des messages douteux

-20%



-40%

7

Pour vos achats comme pour toute autre activité en ligne, utilisez un **mot de passe solide et différent** pour chaque application ou site Internet



Plus d'informations sur :
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)





MENU *de Noël*

VERSION SÉCURITÉ
INFORMATIQUE RENFORCÉE

APÉRITIFS « ANTI-INTRUSION »

Bouchées pare-feu croustillantes

Mini feuilletés sélectionnés avec soin pour bloquer toute tentative d'intrusion culinaire non autorisée.

Verrines MFA (Multi Factor Appétit)

Combinaison double de saveurs : validation gustative indispensable en deux étapes.

ENTRÉES « PRÉVENTION DES MENACES »

Saumon fumé chiffré au citron vert

Mariné sous protocole SSL pour garantir fraîcheur et intégrité.

Velouté de potimarron patché

Recette mise à jour pour corriger les failles de gourmandise détectées l'an passé.

PLATS « HAUTE DISPONIBILITÉ »

Dinde farcie « Protection des données »

Cuisson maîtrisée, farce confidentielle, accès réservé au personnel habilité.

Ragoût végétarien compatible RGPD

Transparence sur l'origine de chaque ingrédient, aucune donnée personnelle collectée.

DESSERTS « ANTI-PHISHING »

Bûche de Noël « Anti Usurpation de recette »

Impossible à confondre avec une fausse bûche : authentique, signée et délicieuse.

Mousse au chocolat en « bac à sable »

Isolée pour éviter tout débordement gourmand incontrôlé.

