RÉPUBLIQUE FRANÇAISE
*Liberté Égalité Fraternité*

Les Ressources Humaines FONCTION PUBLIQUE TERRITORIALE LOIRE-ATLANTIQUE

# Web Conférence Grand Témoin sur la Cybersécurité

**Animée par Nicolas Lagrange,**
rédacteur en chef au pôle Social-RH AEF Info

**INTERVENANT**
**Régis DUBRULLE**
Délégué régional sécurité numérique Pays de la Loire à l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

**Centre de Gestion**
**de a fonction publique territoriale**
**de Loire-Atlantique**

# ANSSI

## L’autorité nationale en matière de sécurité et de défense des systèmes d’information

Services du Premier Ministre

Secrétariat Général de la Défense et de la Sécurité Nationale

Agence Nationale de Sécurité des Systèmes d’Information

5 missions :

- Défense
- Connaitre
- Partager
- Accompagner
- Contrôle

Public prioritaire :

- Administrations,
- Organisme d’Importance Vitale (OIV) et Organisme de Service Essentiel (OSE)

~~ACTIONS OFFENSIVES~~ ~~RENSEIGNEMENT~~

# L’état de la menace

20 minutes

ELECTIONS Attaque informatique « massive » à la mairie de Marseille et à la métropole

## Municipales 2020 à Marseille : Attaque informatique « massive » à la mairie et à la métropole

ELECTIONS · Quelque 300 machines qui devaient créer les listes d’émargement des procurations ont été rendues inopérantes. La mairie assure que « les élections municipales auront lieu normalement »

20 Minutes avec AFP

Publié le 15/03/2020 à 03h43 • Mis à jour le 15/03/2020 à 07h28

MENU ouest france Presse Océan

Accueil › Pays de la Loire › Saint-Nazaire

Réservé aux abonnés

## La Ville de Saint-Nazaire, son agglo et d’autres communes victimes d’une cyberattaque

Depuis ce matin, mercredi 10 avril 2024, les deux collectivités ne peuvent plus utiliser leur réseau et le téléphone. D’autres communes sont touchées.

# L’état de la menace

Accueil › Société › Cyberattaque

Ouest-France
Yvan DUVIVIER
Modifié le 13/03/2025 à 17h44
Publié le 13/03/2025 à 17h10

## Cyberattaque à Lorient : 5 429 noms d’agents municipaux en vente à bas prix sur un forum

Une cyberattaque a touché fin février 2025 la mairie de Lorient (Morbihan). Des données strictement professionnelles d’agents municipaux sont aujourd’hui en vente sur un forum sur internet. Si la mairie en relativise l’impact, une plainte a été déposée et des recherches complémentaires diligentées.

# L’état de la menace

## Une commune du Morbihan victime d'une cyberattaque échappe in extremis à un préjudice de 150 000 euros

Des hackers ont accédé aux ordinateurs de la commune et ont essayé de passer de grosses commandes à des entreprises en se faisant passer pour le directeur général des services, révèle jeudi "ici Breizh Izel" (ex-France Bleu).

franceinfo, avec "ici Breizh Izel"
Radio France

Publié le 27/03/2025 08:44

Temps de lecture : 2min

# Q1 : Quel est le ratio de collectivités territoriales victimes d’une cyber attaque en 2024 ?

A)1 sur 2

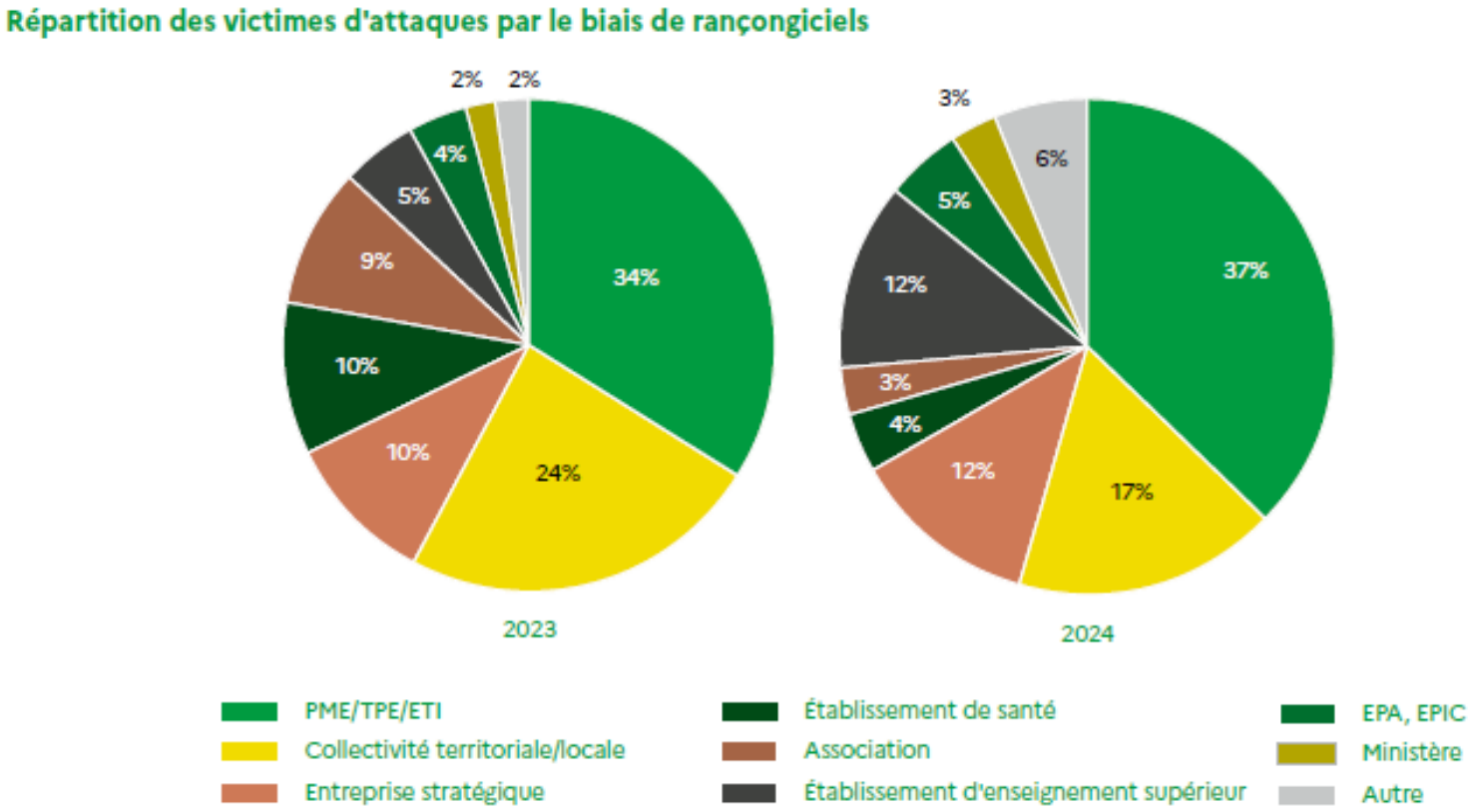
B)1 sur 10 ✅

C)1 sur 100

D)1 sur 1000

Étude 2024 conduite par OpinionWay pour Cybermalveillance.gouv.fr du 26 août au 4 octobre 2024 en ligne (CAWI) auprès d’un échantillon de 1710 élus de collectivités / agents communaux en charge de l’informatique et de la sécurité des communes de moins de 25 000 habitants en France métropolitaine et dans les départements et régions d ’Outre-Mer.

# Répartition des attaques par rançongiciel (source ANSSI 2024)



# L’état de la menace

MENU ouest france

## À Saint-Nazaire, la cyberattaque a déjà coûté 500 000 €

Un piratage informatique a ciblé la Ville et l’Agglomération de Saint-Nazaire, en avril 2024. Presque six mois plus tard, les services à la population ont été rétablis, mais des fonctionnements internes aux collectivités restent à reconstruire.

Ouest-France
Christophe JAUNET.
Publié le 27/09/2024 à 11h24

# DES CYBERMENACES EN HAUSSE

## CYBERCRIMINALITÉ

## ESPIONNAGE

## ACTIONS ÉTATIQUES

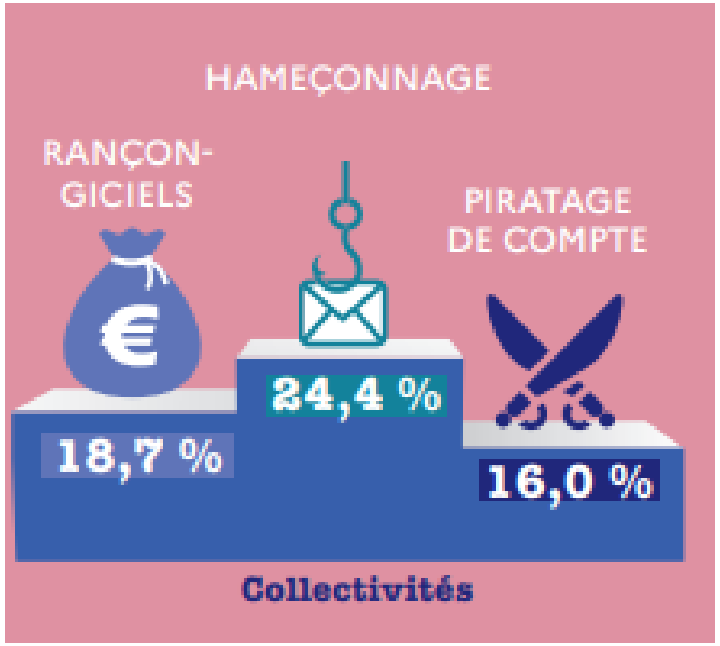
# Parmi les types de cyberattaques visant les collectivités territoriales, quelle est celle qui les touche le plus?

A) Piratage de comptes

B) Attaque par dénis de service

C) Rançongiciel

D) Hameçonnage ✅




Rapport d'activité 2024 de cybermalveillance.gouv.fr

# L’hameçonnage

# Mais aussi

**De :** Judith [redacted]etz.fr>
**Envoyé :** vendredi 26 avril 2024 09:03
**À :** David RICHARD - e-Collectivités <david.richard@ecollectivites.fr>
**Cc :** Pa[redacted]sn
<christ[redacted]
**Objet :** Piratage messagerie d'un agent - Mairie de[redacted]
**Importance :** Haute

Bonjour,

Je viens vous signaler qu'un de nos agents s'est fait pirater son adresse mail.
L'agent en charge de l'urbanisme a reçu un mail via une entreprise de travaux publics pour une demande de DICT.
Ce mail lui demandait de télécharger un lien via le site DropBox puis de renseigner son mot de passe pour pouvoir accéder à la demande de DICT.
Quand il s'est aperçu que la page téléchargée n'aboutissait sur rien, il a tout de suite pensée à un piratage.
J'ai fait intervenir notre prestataire informatique qui a bloqué son compte et lui en a créé un nouveau.

Restant à votre disposition pour tout renseignement complémentaire,

Cordialement,

P/O Le Maire

**Sujet :**Demande de règlement des factures a échéance et mise a jour de nos coordonnées bancaires
**Date :**Wed, 26 Mar 2025 14:27:04 +0100
**De :** COMMUNAUTÉ DE COMMUNES DE L'ERNÉE <11clarissemartin@gmail.com>

Bonjour chers clients,

Nous vous contactons aujourd'hui concernant les factures arrivant à échéance de règlement. En raison d'un problème technique rencontré sur nos serveurs, nous avons malheureusement perdu certaines données et n'avons pas pu retrouver l'historique complet des paiements à ce jour.

Nous vous serions reconnaissants de bien vouloir nous faire parvenir les informations relatives aux factures à régler.

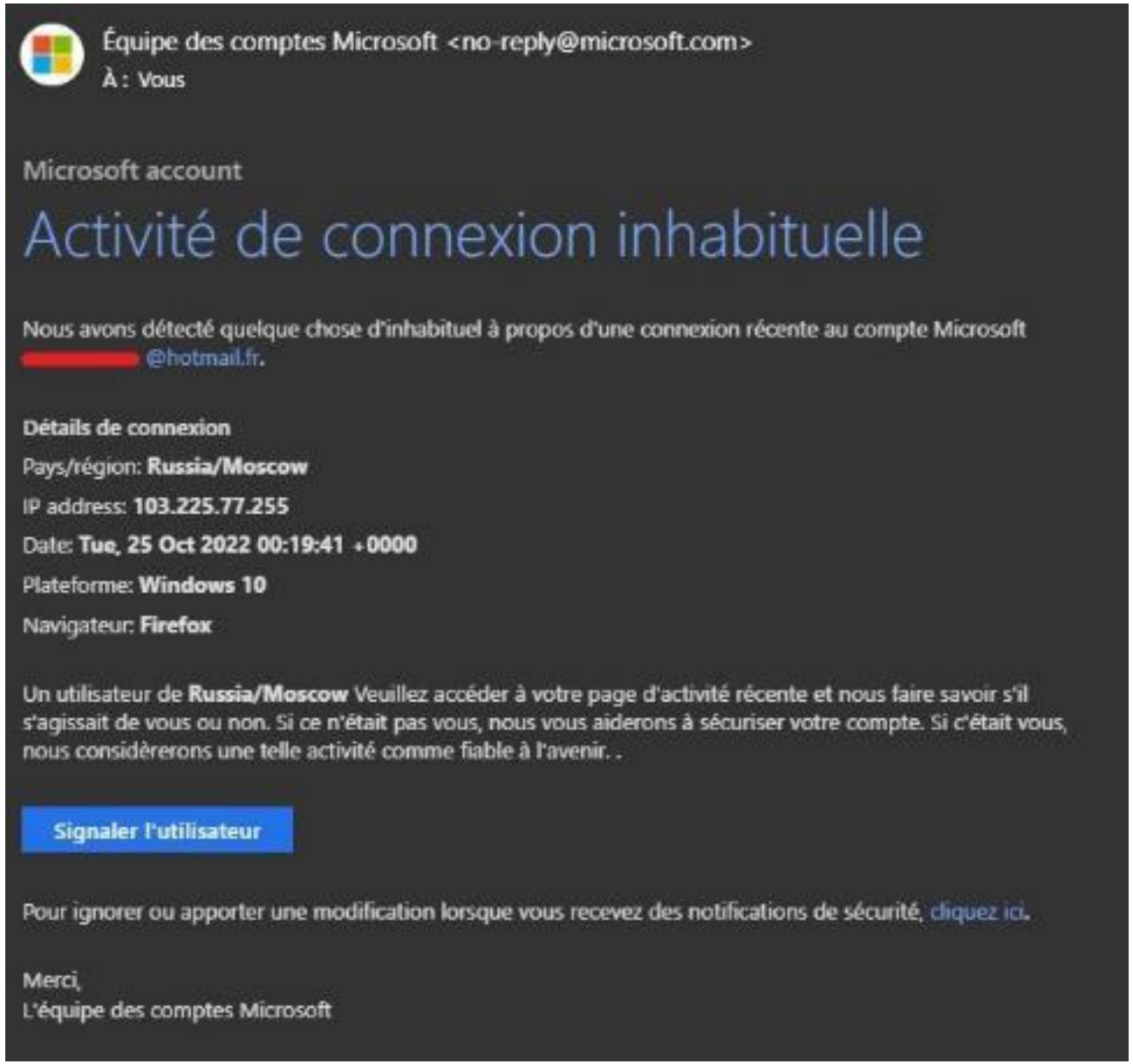
Nous profitons également de cette occasion pour vous informer d'un changement de nos coordonnées bancaires. Vous trouverez ci-joint notre nouveau relevé d'identité bancaire pour effectuer les paiements à venir.

Nous nous excusons pour la gêne occasionnée et vous remercions de votre compréhension et de votre collaboration.

Cordialement,

COMMUNAUTÉ DE COMMUNES DE L'ERNÉE
Parc d'Activités de la Querminais
53500 Ernée BP28
Tél. : 02 43 05 80 97
Fax : 02 43 05 45 26
www.lernee.fr

# Piratage de compte



Équipe des comptes Microsoft <no-reply@microsoft.com>
À : Vous

Microsoft account

## Activité de connexion inhabituelle

Nous avons détecté quelque chose d'inhabituel à propos d'une connexion récente au compte Microsoft [redacted]@hotmail.fr.

**Détails de connexion**

Pays/région: **Russia/Moscow**

IP address: **103.225.77.255**

Date: **Tue, 25 Oct 2022 00:19:41 +0000**

Plateforme: **Windows 10**

Navigateur: **Firefox**

Un utilisateur de **Russia/Moscow** Veuillez accéder à votre page d'activité récente et nous faire savoir s'il s'agissait de vous ou non. Si ce n'était pas vous, nous vous aiderons à sécuriser votre compte. Si c'était vous, nous considèrerons une telle activité comme fiable à l'avenir. .

**Signaler l'utilisateur**

Pour ignorer ou apporter une modification lorsque vous recevez des notifications de sécurité, cliquez ici.

Merci,
L'équipe des comptes Microsoft

# Et c’est l’avalanche….

**De :** [redacted]da.com>
**Envoyé :** mardi 10 août 2021 12:02
**À :** [redacted].com>
**Objet :** Sc da

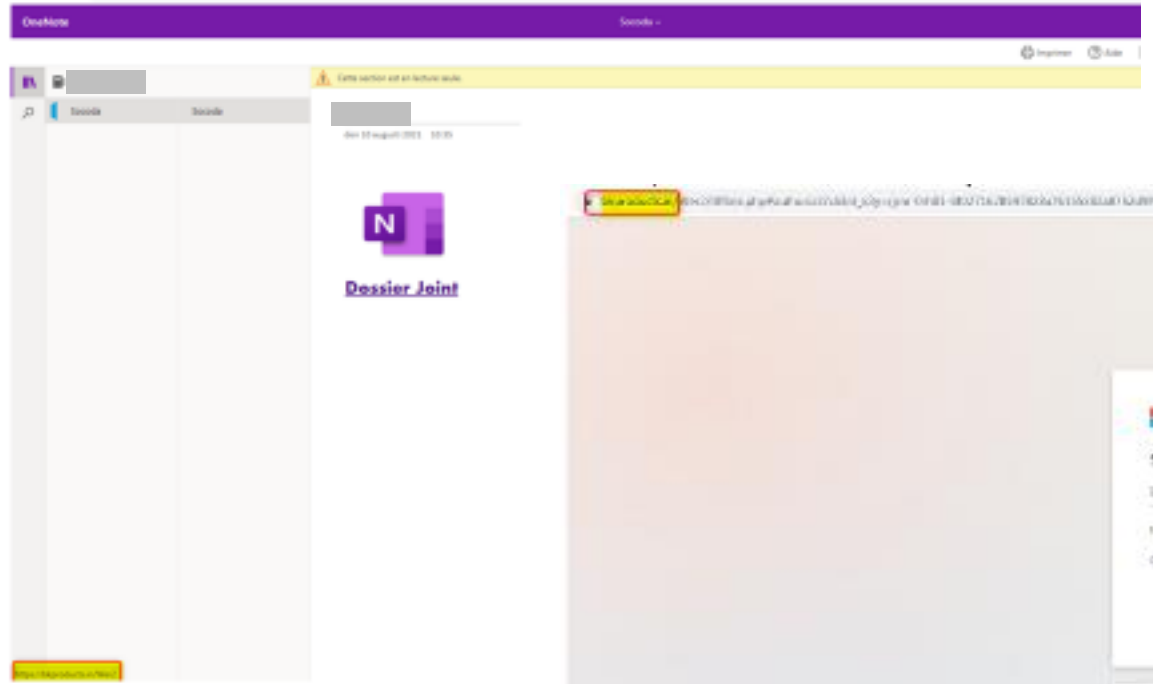
Bonjour,

Veuillez consulter le fichier que je vous ai partagé, fichier joint

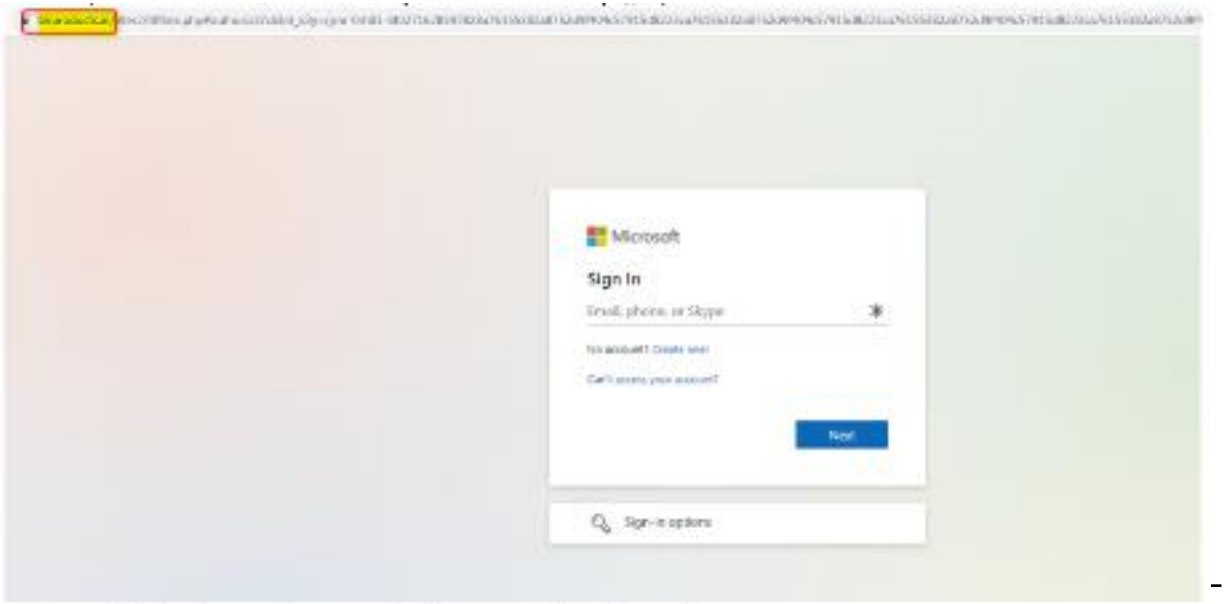
Cordialement,

[redacted]
Assistante Marketing et Commerciale
[redacted].com

https://[redacted]ny.sharepoint.com/:o:/g/personal/[redacted]/eux0mmf-61alz0mbpdiddobvzbeeyfsrr?pvw87f9d-vw7e-8bngy
Cliquez ou appuyez pour suivre le lien.




Quand on passe la souris sur le « Dossier Joint » ça affiche l’adresse « !



# Le rançongiciel ?

Logiciel malveillant qui rend les données inaccessibles

Le pirate réclame une rançon pour les  débloquer

# Dans le cadre d’une attaque rançongiciel dans une collectivité, quel service est le plus impacté ?

A) Le service informatique

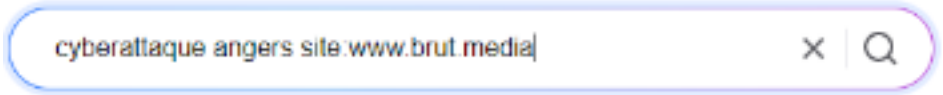
B) L’accueil

C) Les ressources humaines

D) L’ensemble des services ✅

# Un rançongiciel, une crise d’origine cyber !

- Arrêt du système d’information pendant plusieurs jours
- Mise en place d’une organisation de gestion de crise incluant l’ensemble des directions
- Réorganisation des services avec de lourds impacts humains
- Fuites et/ou pertes de données
- Atteinte à l’image
- Dépassement du budget informatique




# COMMENT FAIRE FACE ?

1. Prendre en compte le risque cyber
2. Sensibiliser
3. Protéger
4. Se préparer à la crise

# Quel est le pourcentage de collectivités qui s’estiment faiblement aux risques numériques ?

A) 1 %

B) 10 %

C) 46 % ✅

D) 75 %

Étude 2024 conduite par OpinionWay pour Cybermalveillance.gouv.fr du 26 août au 4 octobre 2024 en ligne (CAWI) auprès d’un échantillon de 1710 élus de collectivités / agents communaux en charge de l’informatique et de la sécurité des communes de moins de 25 000 habitants en France métropolitaine et dans les départements et régions d ’Outre-Mer.

#1

# Imaginez le pire !

## Que redoutez-vous le plus ?

- L'application REU indisponible 1 mois avant les élections
- Utilisation de la boite email générique de la commune pour **un envoi massif de spam**
- **Fuite des données personnelles** du portail famille
- ….

Etablir les scénarios de risques

Cartographier les données, applications et matériels

# #2 Sensibilisez les collaborateurs

Une grande partie des attaques n’auraient pas abouti du fait de la **sensibilisation** / implication / mobilisation des utilisateurs des systèmes d’information

Sensibiliser avec des campagnes des faux phishing

Innover avec des serious game

# Quel est le pourcentage d'entreprises ou collectivités qui pensent que leurs collaborateurs ou agents sont sensibilisés aux risques numériques ?

A) 100 %

B) 85 % ✅

C) 50 %

D) 27 %

"opinionway pour CESIN

## Baromètre de la cybersécurité des entreprises

Vague 10 – Janvier 2025

Echantillon de **401 membres du CESIN,** à partir du fichier des membres du CESIN.

Les interviews ont été réalisées **du 10 décembre 2024 au 7 janvier 2025**.

# #3 Bâtissez votre socle de sécurité numérique

La mise en place d'outils de protection doit être accompagnée de mesures permettant de respecter les **règles de bases** de la cybersécurité

Effectuez un diagnostic MonAideCyber

MonAideCyber
INNOVATION ANSSI

# Bénéficiez d'un accompagnement cyber dès maintenant.

**Inscrivez-vous sur le site !**

https://monaide.cyber.gouv.fr//

**Faites une demande** sur le site MonAideCyber pour être **mis en relation avec un Aidant cyber** de proximité.

1

**L'Aidant cyber** va mener avec vous, pendant 1h30, **un diagnostic adapté** aux enjeux cyber actuels.

2

À l'issue du diagnostic, une liste de **6 mesures prioritaires** sont proposées, complétée par **des ressources utiles**.

3

# Exemples de question

**21. Les mises à jour fonctionnelles et de sécurité des logiciels utilisés sont-elles déployées sur les postes de travail des utilisateurs et des administrateurs ?**

- ◯ Je ne sais pas
- ◯ Non
- ◯ Les mises à jour sont déployées systématiquement, il existe tout de même certaines exceptions non traitées actuellement
- ◯ Toutes les mises à jour sont déployées systématiquement dès que celles-ci sont disponibles et les exceptions font l'objet de mesures complémentaires

# Le rapport

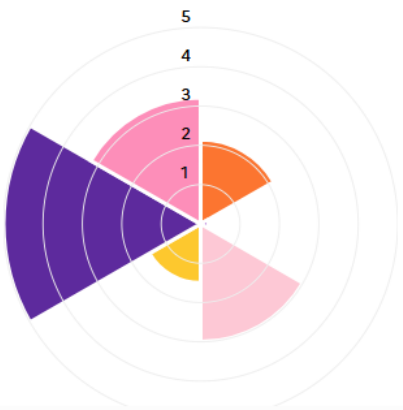
## Récapitulatif

### Informations

**ID 21a78f20-07cc-482f-b0c0-f7258b96271f**

Projet créé le **06.05.2025** à **10:00**
Dernière Modification le **06.05.2025** à **10:24**
Secteur géographique : **Loire-Atlantique**
Secteur d'activité : **Construction**

### Indicateurs MonAideCyber




| | |
|---|---|
| 2.1 | Gouvernance |
| 0.0 | Sécurité des accès au système d'information |
| 3.0 | Sécurité des postes |
| 1.5 | Sécurité des infrastructures |
| 5.0 | Sensibilisation des utilisateurs |
| 3.2 | Réaction à une cyberattaque |

0 - 1 = Critique 1 - 3 = Insuffisant

## 6 mesures prioritaires pour passer à l'action

- 1 . Limiter drastiquement le nombre d'utilisateurs disposant du privilège d'administration local sur leur machine +
- 2 . Établir la liste exhaustive et à jour des activités métiers et des informations à protéger en priorité +
- 3 . Mettre en œuvre des mesures de sécurité supplémentaires sur les serveurs, services et logiciels d'administration ne pouvant pas bénéficier des mises à jour +
- 4 . Traiter systématiquement les alertes générées par l'antivirus +
- 5 . Mettre en œuvre des mesures de sécurité supplémentaires sur les systèmes ne pouvant pas bénéficier des mises à jour +
- 6 . Utiliser des comptes d'administration dédiés à cet usage +

# Quel est le pourcentage du budget informatique à consacrer à la cybersécurité ?

A) 0 – 5 %

B) 5 – 10 % ✅

C) 10 – 25 %

D) Plus de 25 %

# 3ième baromètre de la maturité cyber pour les collectivités de moins 25 000 habitants

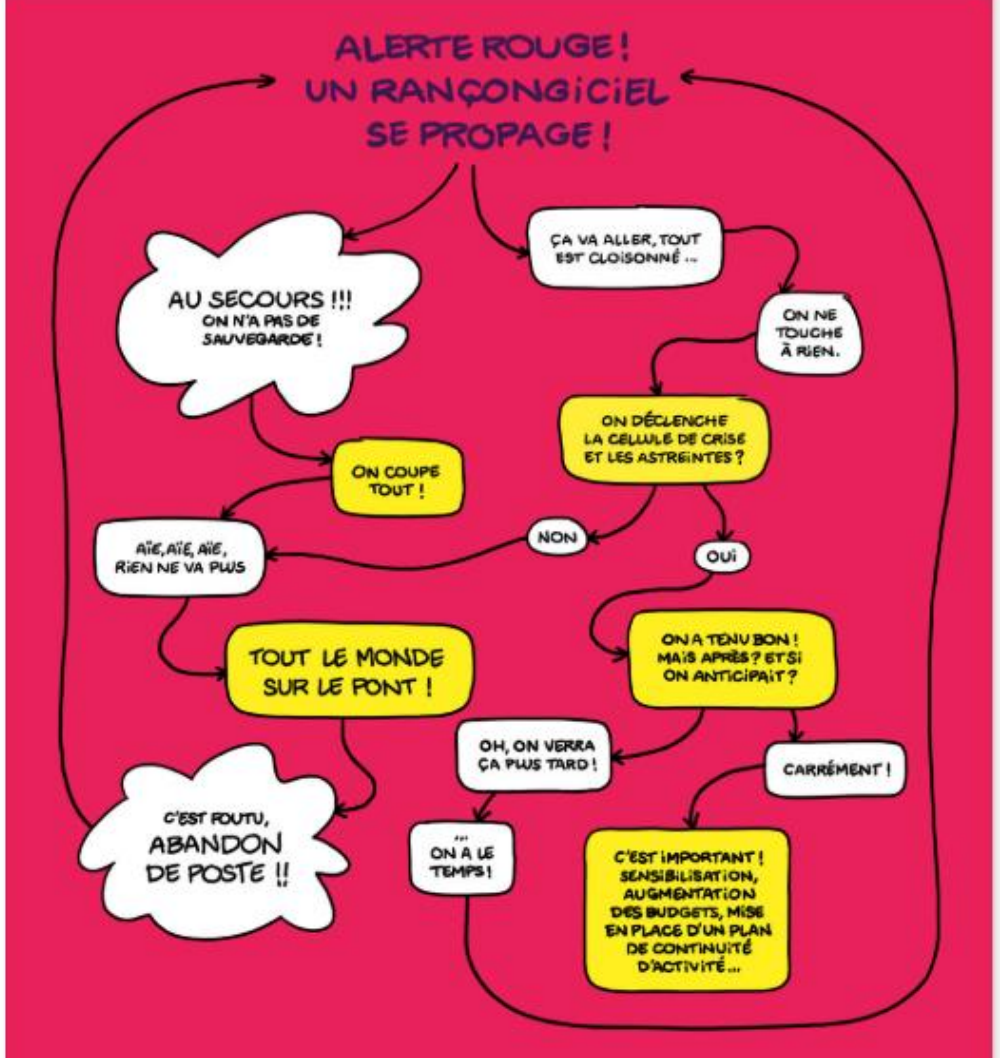
**77 %** Indiquent dépenser **moins de 2000 €** pour leur cybersécurité

# #4 Soyez prêt !

Il n’y a pas de crise cyber,

… il y a que des crises **d’origine cyber**

Mettre en place un dispositif de gestion de crise cyber dans le PCS



# Participer à l’exercice de crise Rempar25

Fort du succès de REMPAR22 et de ses enseignements, l’ANSSI, avec le soutien du Club de la Continuité d'Activité (CCA) et du CLUSIF, vous invite à participer à l'exercice massifié REMPAR25 le 18 septembre 2025.

REMPAR25 a pour fil conducteur de permettre aux organisations participantes de franchir une première étape en matière de maturité à la gestion de crise, en continuité d’activité cyber ainsi que de tester leurs dispositifs en place, pour ceux qui en disposent. Cette nouvelle édition, vous propose un fort ancrage territorial avec la possibilité de participer dans toute la France.

L'objectif ? Eprouver les capacités des organisations à faire face à une cyberattaque systémique. L’exercice se focalisera sur les besoins relatifs à l’anticipation, la préparation ainsi qu’à l’entrainement des dispositifs de gestion de crise et de continuité d’activité sur le plan cyber. Ce niveau de jeu stratégique et opérationnel, s'adresse à toutes les organisations, sur tous les territoires quels que soient leur maturité en gestion de crise cyber, leur taille et leur secteur d'activité. REMPAR25, est dédié aux différents métiers et compétences d’une organisation telles que : la communication, les ressources humaines, les métiers juridiques, ainsi que ceux du numérique jusqu'aux instances de décision.

https://www.evenements.cyber.gouv.fr/public/events/73921/website/home

# Avez-vous intégré une annexe attaque cyber dans votre Plan Communal de Sauvegarde (PCS) ?

A) Oui
B) En cours
C) Non
D) Je ne sais pas

# 0 800 100 200

## PAYS DE LA LOIRE
## CYBER ASSISTANCE

cyberassistance@paysdelaloire.fr

**Votre allié**
en cas de
cyberattaque

Soutenu par

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

RÉGION PAYS DE LA LOIRE


Virus,
chantage,
piratage...
17
CYBER
Ayez le nouveau
réflexe cyber :
rendez-vous sur le site
17Cyber.gouv.fr
Gratuit et sans abonnement