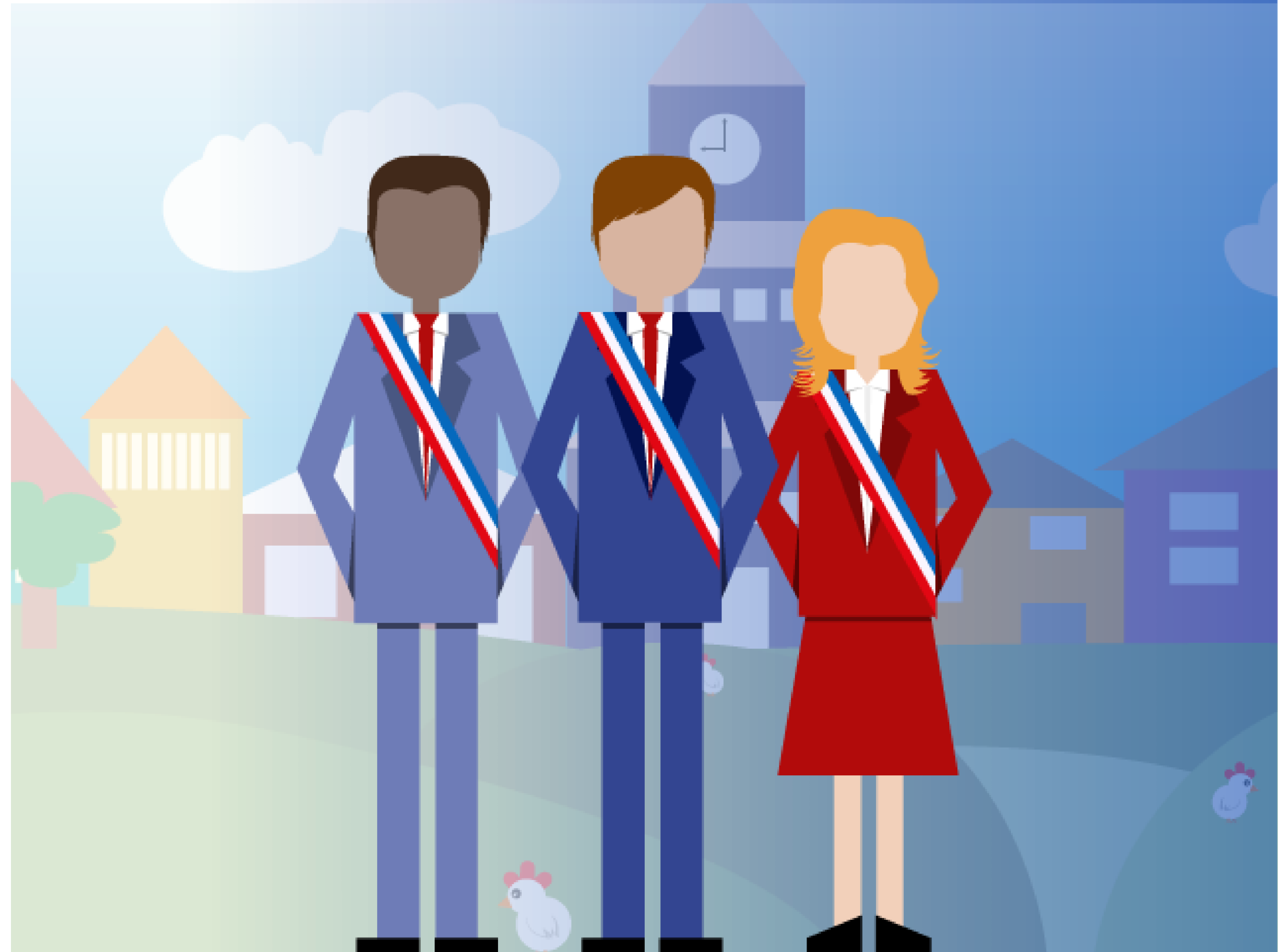


Maires et menaces cyber : prévenir et réagir



Comment s'y retrouver dans le « cyber bazar » ?

- Mme DUPONT est maire d'une commune
- Ses journées sont denses, beaucoup de sujets sont à traiter au quotidien et elle est régulièrement sollicitée sur de nouvelles thématiques : dématérialisation de l'urbanisme, désignation d'un référent déontologue, ...



- Depuis quelques mois maintenant un thème récurrent se manifeste tant dans son mandat politique que dans sa sphère personnelle :

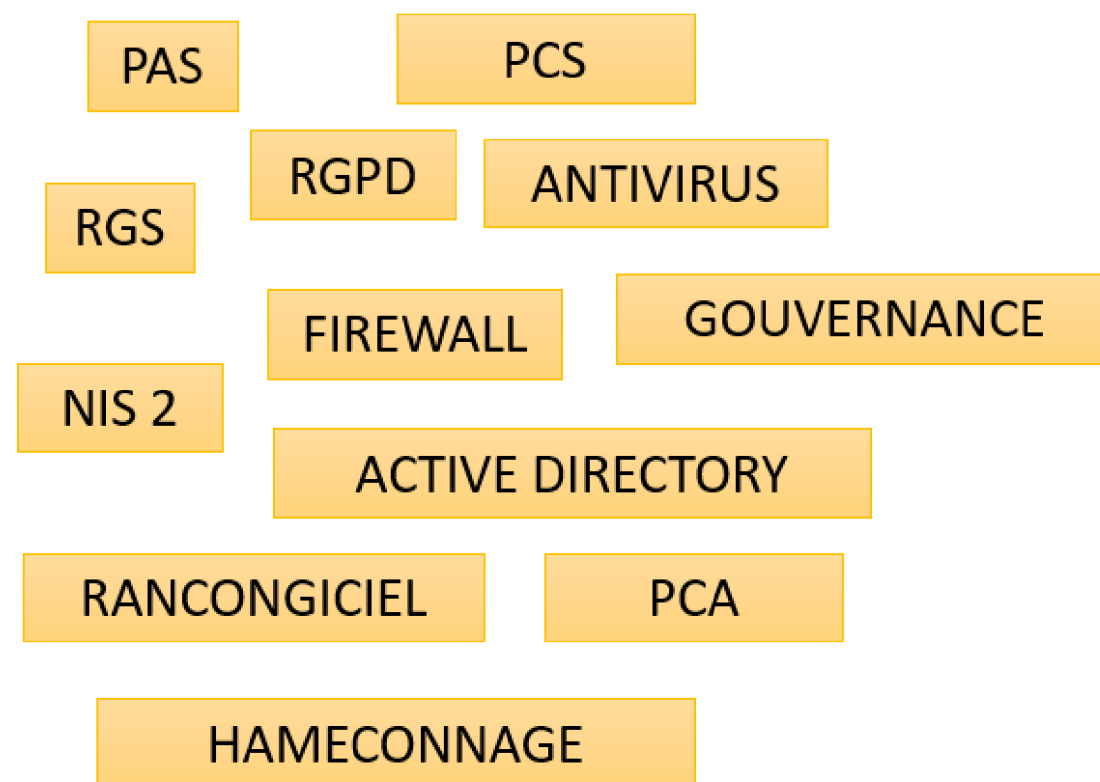
La Cybersécurité

- Elle est sollicitée quotidiennement par des partenaires qui lui proposent des sensibilisations, des webinaires, des réunions, des outils....





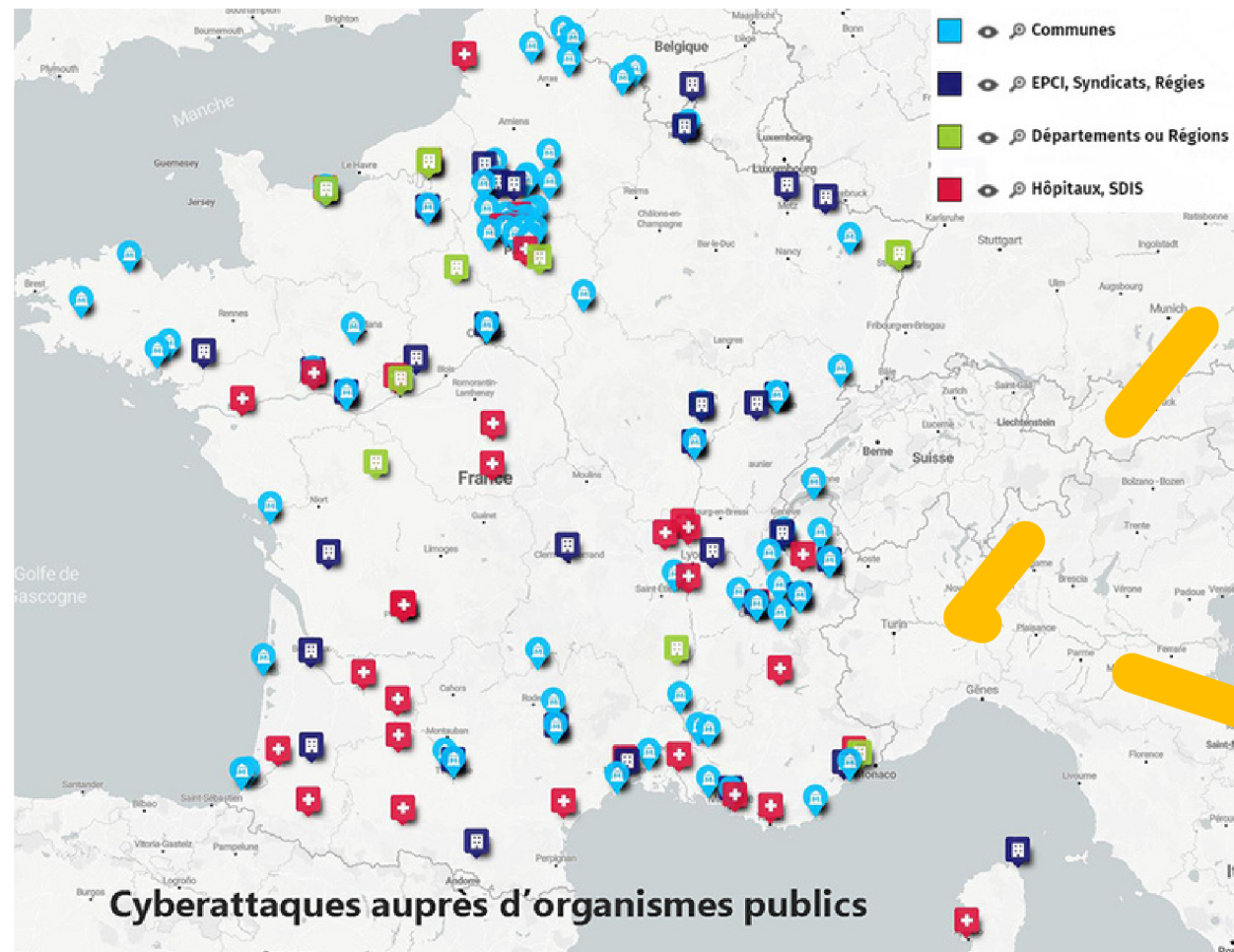
Ils semblent tous parler du même sujet mais elle a bien du mal à savoir qui contacter, par quoi commencer...



Les termes employés sont parfois très techniques et elle n'a pas d'informaticien dans son équipe.



Les acteurs à solliciter sont nombreux et elle ne sait pas à qui s'adresser.



• Elle voit par ailleurs que la situation semble grave, de nombreuses collectivités, de toutes tailles, et même des hôpitaux sont victimes de cyberattaques :

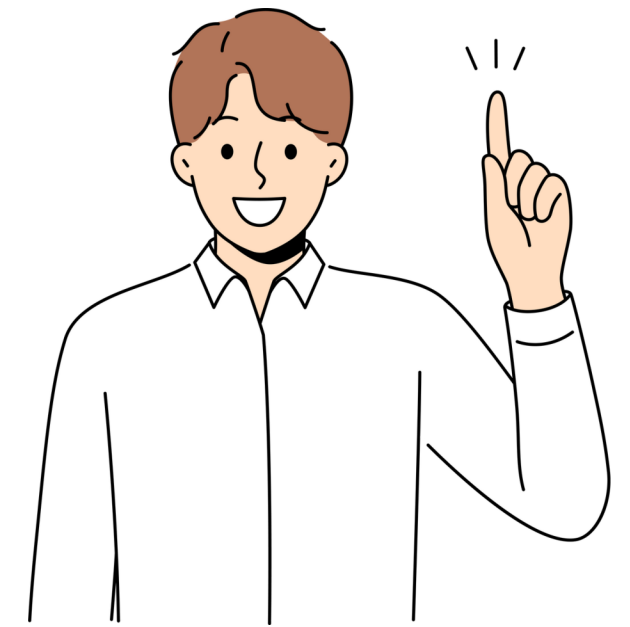
- leur fonctionnement et le service rendu à l'utilisateur sont perturbés pendant des jours / semaines / mois
- des données d'agents, d'élus sont volées et font l'objet d'un trafic
- les dépenses consacrées à la remise en route grèvent des budgets déjà tendus

Alors que faire ?

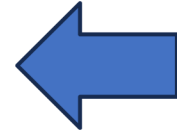


PREVENIR

Comment se préparer au risque cyber ?









3
2
1
0



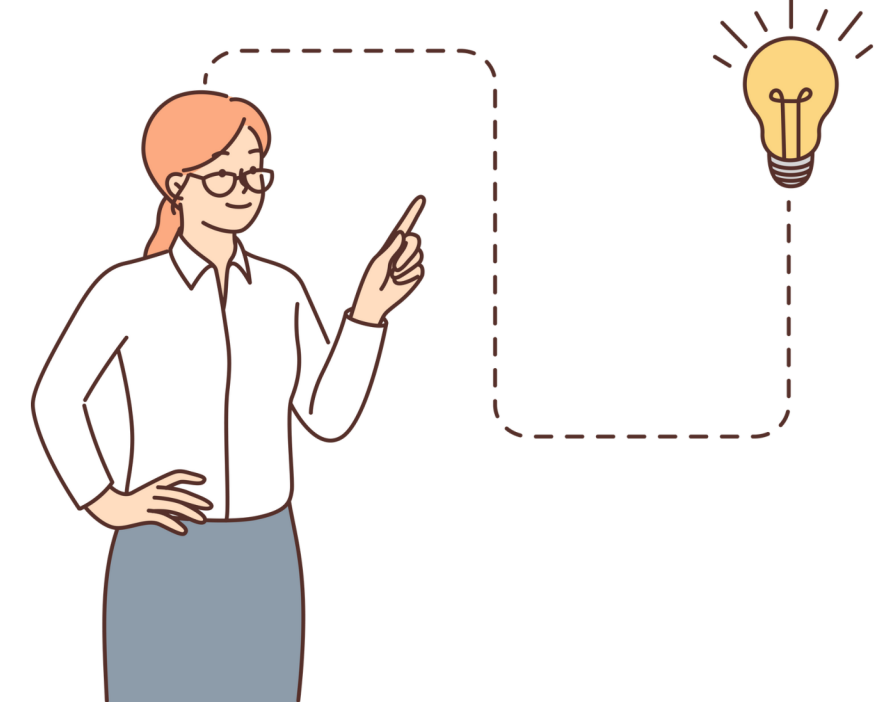
Niveau 0 : PRISE DE CONSCIENCE

Je n'ai mis aucune mesure particulière en place et souhaite me sensibiliser sur le sujet

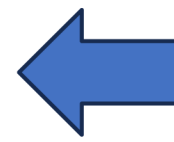
Qui peut m'accompagner ?	Comment ?
Cybermalveillance 	Programme e-sensibilisation
CDG 35 	Séances de sensibilisation à l'hygiène informatique
Mégalis 	Parcours d'accompagnement (sensibilisation)
Gendarmerie 	Diagnostic cyber « IMMUNITE » fruit d'une collaboration avec l'AMF et Cybermalveillance.gouv.fr + Réunion d'information
Recym 	Le réseau des experts cybermenaces (RECYM) de la police nationale sensibilise les PME, TPE et collectivités territoriales.
PEC 	Le PEC effectue un diagnostic pour les entités d'au moins 10 salariés, des entités de + 3500 habitants.

PREVENIR

Comment se préparer au risque cyber ?







- 3
- 2
- 1
- 0



Niveau 1 : PLAN D'ACTION

Je suis sensibilisé mais j'ai besoin d'assistance pour lancer une démarche de sécurisation

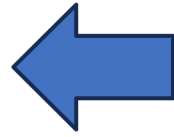
Qui peut m'accompagner ?	Comment ?
Cdg 35 	Accompagnement personnalisé (analyse de risque, plan d'actions et suivi)
Mégalis 	Parcours d'accompagnement n°2 sensibilisation avec pré-audit et plan d'actions (mutualisé au niveau de l'EPCI)
Gendarmerie 	Pré-diagnostic « Diagonal » – identification des chantiers prioritaires. Réunion d'information
ANSSI 	Mon Aide Cyber

PREVENIR

Comment se préparer au risque cyber ?








3
2
1
0



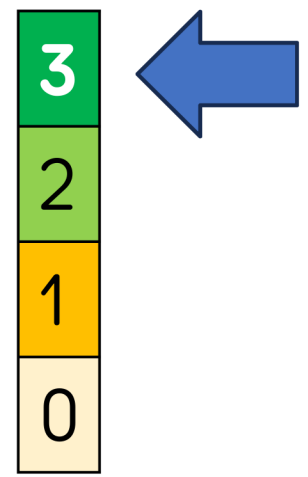
Niveau 2 : ACCOMPAGNEMENT

J'ai besoin d'accompagnement pour formaliser ma politique de sécurité et mettre en place des mesures techniques

Qui peut m'accompagner ?	Comment ?
CDG 35 	Modèles de documents pour formaliser une politique de sécurité (Charte informatique, inventaires...)
Mégalis 	Outils du bouquet de services numériques : Gestionnaire de mots de passe / Sauvegarde en ligne
Breizh cyber 	Services de détection et de surveillance via le Pack Breizh Cyber de Mégalis
PEC  	PACTE – EDIH – Essentiellement pour les EPCI – L'offre ne vise pas les petites communes. (structures de + de 10 employés)

PREVENIR





Comment se préparer au risque cyber ?



Niveau 3 : SIMULATION

J'ai besoin de me préparer et de simuler une cyberattaque



Qui peut m'accompagner ?	Comment ?
CDG 35 	S'entraîner à la gestion de crise Préparer un plan de continuité d'activité
Mégalis  <small>Syndicat mixte de coopération territoriale</small>	Formation à la gestion de crise cyber (DG des membres de Megalis)
Préfecture d'Ille-et-vilaine 	Campagne d'exercices prépa'risk en lien avec le Ministère de l'Intérieur et des outre-mer
ANSSI 	Mise à disposition de guides sur la gestion de crise d'origine cyber : Création du dispositif, entraînement, communication

PREVENIR
MENTION SPECIALE

Comment se préparer au risque cyber ?

3
2
1
0

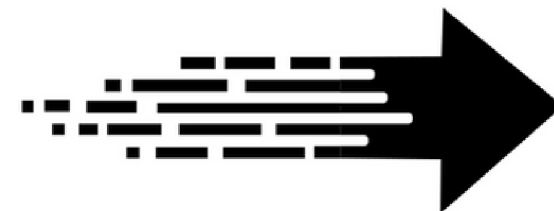
Tous les niveaux : J'ai besoin d'accompagnement pour maîtriser l'externalisation informatique dans ma commune

Dans le domaine informatique, le recours à l'externalisation est devenu une pratique courante qui présente un certain nombre d'avantages, mais aussi de risques qu'il convient d'évaluer.

Mise en place d'un document facilitant la gestion et la compréhension des enjeux liés à l'infogérance afin de vous assister dans une démarche de prévention à la demande de M. le Préfet.



Transmission par voie électronique après la conférence.



ÉDITORIAL DU PRÉFET D'ILLE-ET-VILAINE



Mesdames, Messieurs,

Si notre département était jusqu'à présent préservé des cyberattaques massives, 2023 a sonné le glas de cette période préservée. Nous assistons en effet à un véritable tournant dans les actions offensives visant nos institutions dans le cyberspace. Le CHU de Rennes et la ville de Betton ont ainsi été attaqués par des collectifs internationaux de cybercriminels.

Les impacts de telles attaques peuvent être majeurs à l'échelle d'une collectivité. Maillons essentiels de la relation entre l'État et les citoyens, les collectivités territoriales sont notamment dépositaires de données personnelles que nous devons protéger.

Dans le domaine informatique, le recours à l'externalisation est devenu une pratique courante qui présente un certain nombre d'avantages, mais aussi de risques qu'il convient d'évaluer. C'est pourquoi j'ai souhaité la mise en place d'un document facilitant la gestion et la compréhension des enjeux liés à l'infogérance afin de vous assister dans une démarche de prévention. Il est en effet apparu que ce type de guide n'existait pas. J'espère que cette innovation breillienne vous sera pleinement utile.

Je tiens à remercier chaleureusement les organismes impliqués dans ce travail : l'AMF 35, l'AMR 35, la gendarmerie nationale, l'agence nationale de la sécurité des systèmes d'information, le centre de gestion de la fonction publique territoriale, Mégalis Bretagne et le centre de réponse aux incidents de sécurité numérique de la région Bretagne, «Breizh cyber», qui renforce depuis novembre 2023 notre résilience numérique départementale.

La lutte contre les menaces d'origine cyber ne peut être menée individuellement : la sécurité du numérique est l'affaire de tous !

Philippe Gustin,
Préfet d'Ille-et-Vilaine

REAGIR

Comment gérer une crise cyber ?



Assistance et prévention
en sécurité numérique

Je suis cyberattaqué et je ne dispose d'**aucune compétences** ou
ressources suffisantes en sécurité numérique

The screenshot shows the website's navigation bar with the following menu items: LES MENACES ET BONNES PRATIQUES, L'ACTUALITÉ DE LA CYBERMALVEILLANCE, NOUS DÉCOUVRIR, and VICTIME D'UN ACTE DE CYBERMALVEILLANCE?. The main heading is 'Diagnostic en ligne'. Below it, the text reads: 'Vous pensez être victime d'un acte de cybermalveillance? Notre dispositif conseille et oriente les victimes de cybermalveillance.' A large image shows hands typing on a laptop keyboard. Below the image is a numbered list of three steps: 1. Répondez à quelques questions pour décrire votre problème; 2. Notre outil vous proposera un diagnostic et des conseils personnalisés; 3. Si besoin, vous pourrez être mis en relation avec un prestataire spécialisé susceptible de vous aider. At the bottom, there is a teal button that says 'DÉMARRER LE DIAGNOSTIC →'.

ESPACE PRESTATAIRE MON ESPACE

LES MENACES ET BONNES PRATIQUES L'ACTUALITÉ DE LA CYBERMALVEILLANCE NOUS DÉCOUVRIR VICTIME D'UN ACTE DE CYBERMALVEILLANCE ?

Diagnostic en ligne

Vous pensez être victime d'un acte de cybermalveillance ?
Notre dispositif conseille et oriente les victimes de cybermalveillance.

1. Répondez à quelques questions pour décrire votre problème
2. Notre outil vous proposera un diagnostic et des conseils personnalisés
3. Si besoin, vous pourrez être mis en relation avec un prestataire spécialisé susceptible de vous aider.

Si vous n'arrivez pas à résoudre votre problème, vous pourrez être mis en contact avec un professionnel.

DÉMARRER LE DIAGNOSTIC →

REAGIR

Comment gérer une crise cyber ?



Je suis une collectivité bretonne et je suis cyberattaqué !

Breizh Cyber

LE CENTRE DE RÉPONSE AUX INCIDENTS CYBER

Une initiative de



Soutenue par



RÉPUBLIQUE
FRANÇAISE

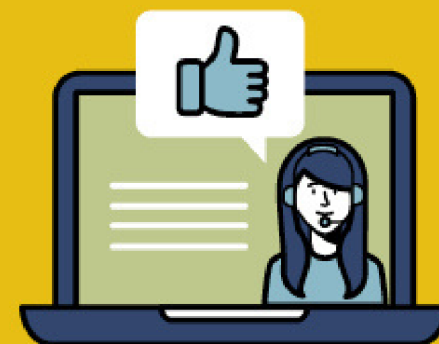
Liberté
Égalité
Fraternité



En cas de cyberattaque :

 **0 800 200 008** Appel gratuit

 **breizhcyber.bzh**



*Service d'assistance
gratuit*

Breizh Cyber est un centre de réponse aux incidents de sécurité informatique créé par la Région Bretagne, avec le soutien de l'État à travers l'ANSSI.

Deux grands volets :

1. **Accompagnement (gratuit) sur la réponse à apporter** : actions techniques immédiates, gestion de crise, questions juridiques, dépôt de plainte ;
2. **Mise en relation avec des experts référencés** dans le cadre de prestations de résolution de l'incident.

REAGIR

Comment gérer une crise cyber ?

Cyberattaque : Vous êtes une **administration**, un **opérateur d'importance vitale (OIV)** ou de **service essentiel (OSE)**

Contactez immédiatement le CERT-FR au **3218** ou **09 70 83 32 18**







Le CERT-FR n'est pas un service de justice ou de police recevant des plaintes.

REAGIR

Comment gérer une crise cyber ?



Je suis cyberattaqué et j'ai besoin d'aide



Qui peut m'accompagner ?	Comment ?
<p>Cyber Malveillance</p> 	<p>Diagnostic de cybermalveillance (questionnaire + mise en contact avec un prestataire spécialisé (prestation payante)).</p>
<p>Breizh cyber</p> 	<p>Service de réponse à incidents cyber dédié aux entreprises, associations et collectivités locales.</p>
<p>ANSSI</p> 	<p>Vous êtes un OIV, une entité régulée, le CERT-FR est joignable 7j/7, 24h/24. Le CERT-FR n'est pas un service de justice ou de police recevant des plaintes.</p>
<p>CDG 35</p> 	<p>Accompagnement violation de données personnelles</p>

REAGIR

Comment gérer une crise cyber ?

Je suis cyberattaqué, le réflexe 17 !



Qui peut m'accompagner ?	Comment ?
Gendarmerie 	Dépôt de plainte, recueil de la preuve numérique et enquête.
Police Judiciaire 	Dépôt de plainte + enquête numérique



PRÉFET
D'ILLE-
ET-VILAINE

*Liberté
Égalité
Fraternité*

Merci pour votre
écoute.

Vendredi 24 mai 2024



