

→ **Lutter**
contre les atteintes cyber

→ **Communiquer**
sur la loi n° 2024-247
du 21 mars 2024 renforçant
la sécurité et la protection
des maires et des élus locaux

→ **Former / Sensibiliser**
un maximum d'élus

→ **Créer**
un guide « l' élu et la justice »

→ **valoriser**
les bonnes pratiques locales

→ **Renforcer**
les partenariats avec les
associations d'élus

En cas de danger n'intervenez pas seul mais avisez les services de police ou gendarmerie en composant le 17

 **Pour nous écrire**

Centre d'analyse
et de lutte contre
les atteintes
aux élus (CALAE)
Ministère de l'Intérieur
Place Beauvau 75 008 PARIS

 **Par messagerie
électronique**

calae@interieur.gouv.fr

 **Pour aller plus loin**

Missions et activités de CALAE, plan national de prévention
et de lutte contre les violences aux élus
<https://www.gendarmerie.interieur.gouv.fr/conseils/elus/centre-d-analyse-et-de-lutte-contre-les-atteintes-aux-elus>

Mais aussi de nombreuses informations et fiches réflexes
sur les applications pour smartphone

Ma sécurité 



GEND'élus 



Ce flyer a été conçu avec les organismes suivants

Comcyber MI
<https://www.gendarmerie.interieur.gouv.fr>

OFAC (Office anti-cybercriminalité)
Service interministériel en charge de la lutte
contre la cybercriminalité

ANSSI (Agence nationale de la sécurité
des systèmes d'information)
<https://cyber.gouv.fr>

Cybermalveillance
<https://www.cybermalveillance.gouv.fr>

UNC (Unité nationale cyber)
Service d'enquête gendarmerie

Cheffe CALAE: Madame Hélène DEBIÈVE, Administratrice de l'État
Chargé de mission CALAE: Capitaine Nicolas RIBON



La protection des élus

une priorité nationale

Centre d'analyse et de lutte
contre les atteintes aux élus (CALAE)

Mieux lutter contre les atteintes cyber avec vous!

→ Mieux se protéger:
améliorer la prévention

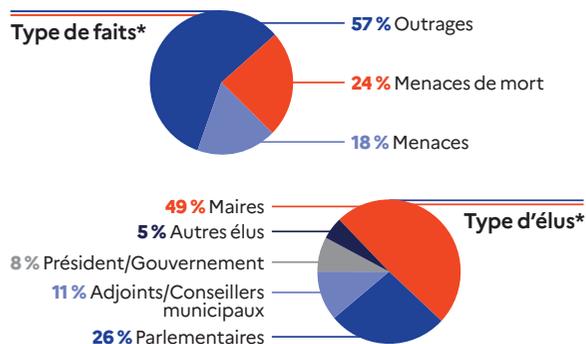
→ Être mieux accompagné
en cas d'atteinte

Les menaces et les violences ne sont pas une fatalité!
Signalez-les à la gendarmerie ou à la police

20 % des atteintes aux élus sont des atteintes cyber

Mieux se protéger Améliorer la prévention

Être mieux accompagné en cas d'atteinte



→ Atteintes cyber de quoi parle-t-on ?

Cybersécurité: état recherché pour un système d'information lui permettant de résister à des événements issus du cyberspace, susceptibles de compromettre la disponibilité, l'intégrité, ou la confidentialité des données stockées, traitées ou transmises, et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Cyberattaque: une cyberattaque consiste à porter atteinte à un ou plusieurs systèmes informatiques, dans le but de satisfaire des intérêts malveillants.

Cyberharcèlement: agissements malveillants répétés (intimidation, insultes, menaces, rumeurs) pour porter atteinte, et dégrader les conditions de vie de la victime.

Rançongiciel: virus informatique qui rend indisponible un système et des données, en réclamant une rançon pour obtenir à nouveau l'accès.

Hameçonnage (phishing): cyberattaque consistant à appâter une personne, pour lui faire exécuter une action nuisible, comme l'ouverture d'une pièce jointe corrompue, ou d'un lien pointant un site malveillant.

Déni de service: attaque contre un site ou serveur internet, consistant à saturer de requêtes, afin de le rendre indisponible.

→ Dans votre collectivité, les principaux risques sont :

- Le hameçonnage ou "phishing".
- Le piratage du compte en ligne.
- Le rançongiciel.

→ Pour votre collectivité: Mes Services Cyber

<https://messervices.cyber.gouv.fr>
Services et ressources cyber proposés par l'ANSSI et ses partenaires.

→ Mon Aide Cyber, pour un diagnostic

<https://monaide.cyber.gouv.fr>
Accompagnement et formations portés par l'ANSSI.

→ Pour sensibiliser les élus et agents de votre collectivité

- Réseau des experts cybermenaces (RECYM) de la police nationale: dnpj-ofac-recym@interieur.gouv.fr
- 250 référents cyber sécurité en gendarmerie, et 1 gendarme sur 10 formés aux méthodes d'investigation numérique: **contactez votre brigade locale.**

→ Pour vous en tant qu' élu, adoptez les 5 réflexes en matière d'hygiène numérique

- **Changez** tous les 6 mois votre mot de passe et **sécurisez-le** avec des contraintes fortes.
- **Veillez** à la sécurité de vos réseaux sociaux et **évit**ez les wifis publics.
- **Effectuez** régulièrement des mises à jour de sauvegarde et testez-les fréquemment.
- **Soyez vigilant** lorsque vous répondez à des messages ou postez des vidéos...
- **Séparez** vos usages professionnels et personnels.

→ Prévention du cyberharcèlement

- **Vérifiez** les paramètres de confidentialité de vos comptes.
- **Maîtrisez** vos publications et **ne renseignez votre profil** qu'avec les informations strictement nécessaires.
- **Ne répondez pas** en cas de message suspect.

→ Vos interlocuteurs

Formations gratuites CNFPT et Cybermalveillance dont **SensCyber:** <https://www.cybermalveillance.gouv.fr/sens-cyber/apprendre>
Programme d'e-sensibilisation gratuit et accessible à tous (comprendre les cyberattaques les plus courantes / agir pour s'appropriier les bonnes pratiques / Apprendre à transmettre ses connaissances...).

Pour vous informer: <http://www.interieur.gouv.fr/sites/minint/files/medias/documents/2025-04/2025-04-documentation-Cyber-combine.pdf>

Vous êtes victime ?

→ 17Cyber

<https://17cyber.gouv.fr>
Disponible 24h/24 et 7j/7, ce guichet unique permet de comprendre à quel type de menace vous êtes confronté, d'établir un diagnostic en ligne et de recevoir des conseils personnalisés, et, selon le besoin et le type de menace, d'être mis en relation avec un policier ou un gendarme, avec les téléservices opérés par le ministère de l'Intérieur, **les CSIRT territoriaux**, ou encore les associations d'aide aux victimes.

→ Vos interlocuteurs

Votre commissariat de police ou votre brigade de gendarmerie.

→ Vos outils

Le dispositif 17Cyber permet également d'être redirigé vers le service ou le téléservice approprié (exemple Pharos).

→ Vos outils du « pack sécurité élus »

- **Contactez votre référent « atteintes élus » (via votre commissariat de police ou votre brigade de gendarmerie):** pour chacun des élus sur tout le territoire.
- **Vous inscrire sur le système « alarme élu » (via votre commissariat de police ou votre brigade de gendarmerie):** vous êtes identifié par les forces de l'ordre en composant le 17.
- **Demander un bouton d'appel (via la préfecture):** en cas de menace, un bouton d'appel peut vous être octroyé par le préfet pour une durée de 3 mois renouvelable.