

Paris, le 5 mai 2026
Communiqué de presse

Cybersécurité : une formation en ligne inédite pour préparer les élus et leurs agents aux crises cyber

Face à la montée en puissance des cybermenaces, les communes et intercommunalités se retrouvent en première ligne. En 2025, 293 revendications d'attaques cybercriminelles ciblant des collectivités territoriales ont été recensées¹. Les conséquences peuvent être lourdes : interruption des services publics, captations de données sensibles ou encore pertes financières significatives.

C'est dans ce contexte préoccupant que l'AMF et le Commandement du ministère de l'Intérieur dans le cyberspace (COMCYBER-MI) lancent aujourd'hui « CapCyber : crises & collectivités », un exercice de simulation en ligne innovant pour accompagner les élus locaux et leurs agents dans la prévention et la gestion du risque cyber.

Conçu pour anticiper les crises avant qu'elles ne surviennent, ce programme propose une immersion pédagogique dans une situation de cyberattaque simulée, afin de mieux comprendre les enjeux et adopter les bons réflexes.

Accessible à tous, « CapCyber ; crises & collectivités » propose une approche pédagogique et opérationnelle pour sensibiliser et former élus et agents. Le jeu de rôle est également ouvert aux citoyens, qui peuvent ainsi se mettre à la place d'un élu confronté à une crise cyber. Le programme s'articule autour de trois volets complémentaires :

- une formation théorique, composée de fiches pour se préparer à une crise cyber et constituer une cellule de crise ;
- une formation pratique, à travers un jeu de rôle évolutif, permettant de gérer une cyberattaque ;
- des témoignages de collectivités ayant vécu une crise ;
- une capsule vidéo de prévention contre les atteintes cyber concernant les élus par le Centre d'Analyse et de Lutte contre les Atteintes aux Elus (CALAE).

Hébergé sur le [site de l'AMF](#), ce module est présenté par David Lisnard, président de l'AMF, et le Général de division Patrick Touak, chef du COMCYBER-MI.

Avec ce dispositif, l'AMF et le ministère de l'Intérieur entendent renforcer la prise de conscience sur le risque cyber et doter les collectivités d'outils concrets pour améliorer leurs actions face à des menaces en constante évolution.

¹Source : Centre d'analyse et de regroupement des Cybermenaces (CECyber) du commandement du ministère de l'Intérieur dans le cyberspace (COMCYBER-MI). Lire le rapport annuel sur la cybercriminalité du ministère de l'Intérieur 2026 (<https://www.interieur.gouv.fr/sites/minint/files/medias/documents/2026-04/Rapport-cybercriminalite2026-WebA.pdf>)