

COMMUNIQUÉ DE PRESSE

MINISTÈRE
DE L'INTERIEUR

MINISTÈRE
DE LA JUSTICE

MINISTÈRE
DE L'ÉDUCATION
NATIONALE

CYBERMALVEILLANCE.GOUV.FR

CNIL

ASSOCIATION
E-ENFANCE
3018

GROUPE FRANCE
TÉLÉVISIONS

UNAF

Opération Cactus 2026 : renforcer durablement la sensibilisation de la communauté éducative aux cybermenaces

Lundi 30 mars 2026

Du 23 au 27 mars 2026, le ministère de l'Éducation nationale a conduit, en partenariat avec le ministère de l'Intérieur (COMCYBER-MI), le ministère de la Justice (section de lutte contre la cybercriminalité du parquet de Paris (J3) et direction des affaires criminelles et des grâces), Cybermalveillance.gouv.fr (GIP ACYMA) la CNIL ainsi que le groupe France Télévisions, l'UNAF et l'association E-enfance/3018, une opération nationale de prévention de grande ampleur reposant sur une simulation d'hameçonnage.

Cette initiative vise à renforcer la vigilance et la responsabilisation de l'ensemble de la communauté éducative face à l'une des formes de cyberattaque les plus répandues.

Une réponse éducative face à une menace croissante

Depuis 2017 les infractions d'atteintes aux systèmes de traitement automatiques de données (cyberattaques, introductions dans les systèmes informatiques, extractions frauduleuses de données etc.) traitées par le parquet de Paris qui a compétence nationale en matière de cybercriminalité, ont augmenté de 2 700% entre 2017 et 2025.

Face l'essor de ces affaires pour lesquelles la Justice est saisie, le parquet de Paris qui a créé une section spécialisée dans la lutte contre la cybercriminalité dès 2014 mène un grand nombre d'actions de prévention en lien avec les acteurs de l'État, comme l'Éducation nationale.

Lancée en 2025 sur l'ensemble du territoire, l'opération Cactus a pour objectif de **sensibiliser les élèves aux risques cyber et à leurs conséquences potentielles**, qu'elles soient économiques, psychologiques ou réputationnelles. **En 2026, les publics ont été élargis, en plus des élèves, aux enseignants, personnels éducatifs et aux parents.**

En effet, avec la généralisation des outils et services numériques, tant pour les apprentissages que pour la gestion administrative des établissements, les établissements scolaires sont confrontés depuis plusieurs années à de multiples attaques malveillantes ciblant les ENT et les outils numériques de vie scolaire. Les vols de mots de passe et campagnes d'hameçonnage massives ont parfois conduit à des fermetures temporaires de services, comme ce fut le cas dans la région des Hauts-de-France à la fin de l'année 2025. Ces incidents perturbent durablement le fonctionnement des établissements et exposent élèves, familles et personnels à des contenus frauduleux, voire parfois, choquants.

Par ailleurs, une enquête menée en septembre 2025 auprès d'élèves de CM1 à 6^e dans les [territoires numériques éducatifs](#) (TNE) met en évidence plusieurs constats structurants :

- **7 élèves sur 10** se déclarent sensibilisés à la cybersécurité. Un chiffre encourageant qui peut toutefois masquer des lacunes dans la compréhension concrète des risques ;

- **1 élève sur 3** indique avoir déjà été exposé à des actes de cybermalveillance (courriels ou SMS frauduleux, piratage de comptes, etc.) ;
- **1 élève sur 5** déclare ne pas encore avoir entendu parler des menaces cyber ou ne pas en avoir une connaissance suffisante.

Ces résultats soulignent la nécessité de renforcer et d'ancrer dans la durée l'éducation à la cybersécurité, dès le plus jeune âge, en associant étroitement les familles et l'ensemble des acteurs éducatifs.

Vers un renforcement de l'action d'éducation aux risques numériques

Fort de ces enseignements, le ministère de l'Éducation nationale affirme sa volonté de s'inscrire dans une stratégie pérenne d'éducation aux risques numériques et de citoyenneté numérique. Cette stratégie repose sur plusieurs piliers :

- une sensibilisation progressive et adaptée à chaque âge, du cycle 2 au secondaire, intégrée aux parcours scolaires ;
- l'association de l'ensemble des parties prenantes (élèves, parents, enseignants et personnels administratifs) afin de favoriser une responsabilité collective face aux cybermenaces ;
- la mise à disposition de ressources pédagogiques, d'outils d'accompagnement pour les équipes éducatives et de dispositifs de formation continue pour les professionnels ;
- le renforcement des collaborations avec les partenaires institutionnels et les autorités compétentes en matière de cybersécurité.

Pour **Édouard Geffray**, ministre de l'Éducation nationale, « À l'heure où les usages numériques s'imposent dès le plus jeune âge, notre responsabilité est claire : donner à chaque maillon de la communauté éducative – élèves, personnels et parents – les clés pour comprendre, anticiper et déjouer les menaces en ligne. L'opération Cactus constitue à ce titre une action pédagogique, concrète et ancrée dans le réel, pour former des citoyens éclairés, capables d'adopter les bons réflexes face aux cyberattaques. »

Cactus 2026 : une campagne massive qui a touché 1 français sur 6

9,2 millions de personnes réparties sur l'ensemble du territoire national, y compris en outre-mer, ont donc été impliquées dans l'opération Cactus 2026 :

- 3,5 millions collégiens et lycéens ;
- Près de 5 millions de parents d'élèves ;
- Plus de 500 000 personnels enseignants et administratifs.

Les participants ont reçu, via les espaces numériques de travail (ENT) ou de messagerie, un message frauduleux simulant une tentative d'hameçonnage et les incitant à cliquer sur un lien.

Parmi eux, 1 096 692 personnes ont cliqué sur ce lien, soit 12% du public cible. Elles ont été redirigées vers un message de sensibilisation comprenant une vidéo pédagogique. Cette vidéo, conçue dans un objectif d'intérêt public, vise à informer, responsabiliser et dissuader face aux pratiques illégales en ligne, en s'appuyant sur une communication claire et directe des autorités compétentes en matière de cybersécurité et de lutte contre la cybercriminalité.

Le contenu de cette vidéo, élaboré collectivement dans une démarche d'intérêt public, complète les actions déjà menées par le ministère de l'Éducation nationale en matière de sensibilisation à la cybersécurité, notamment via la [certification Pix+ Cybersécurité ou encore une étroite collaboration avec Cybermalveillance.gouv.fr](#).

Un [kit pédagogique](#) co-construit par les services engagés dans le projet, contenant tous les éléments d'explication et d'accompagnement de la campagne Cactus, est mis à disposition de chacune des académies pour permettre aux enseignants qui le souhaitent, de déployer cette action de sensibilisation.

En parallèle de cette opération ponctuelle, les pouvoirs publics s'engagent sur le long terme, en organisant des séances de sensibilisation animées par divers intervenants, directement dans les classes, au plus près des élèves.

NOS CONSEILS

Hameçonnage (extrait) :

- Ne pas cliquer sur les liens ou les pièces-jointes qui vous sont proposés dans un message non sollicité.
- Au moindre doute, lors de la réception d'un message inattendu ou alarmiste, contacter directement l'organisme concerné.

Retrouvez tous les conseils dans l'article dédié :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing>

Pour en savoir plus : <https://www.cybermalveillance.gouv.fr/>

Contacts presse

Ministère de l'Intérieur – ComCyberMI

Tél : 07 85 96 67 19

Mél : scrm.em.comcyber-mi@gendarmerie.interieur.gouv.fr

Ministère de la Justice

Bureau presse et veille du ministère

Tel : 01 44 77 65 54

Mél : presse-justice@justice.gouv.fr

Parquet du tribunal judiciaire de Paris

Tel : 06 07 18 42 28

Mél : scom.parquet.tj-paris@justice.fr

Ministère de l'Éducation nationale

Tél : 01 55 55 30 10

Mél : spresse@education.gouv.fr

Cybermalveillance.gouv.fr

Tél : 01 83 75 14 10

Mél : presse@cybermalveillance.gouv.fr

CNIL

Iris Le Gal

Tél : 06 80 71 51 25

Mél : presse@cnil.fr

Association E-Enfance/ 3018

Sandra Tricot

Tél : 06 65 85 85 65

Mail : s.tricot@e-enfance.org

Groupe France Télévisions

Jennifer ARMAND

Tél : 0610495374

Mél : jennifer.armand@francetv.fr

Unaf

Tél : 01 49 95 36 15

Mél : lmondet@unaf.fr