FAQ – Reprise d'activité après la cyberattaque
À destination des enseignants et personnels administratifs des lycées

Version 31/10/25

LA CYBER ATTAQUE

Qu'est-il arrivé exactement ?

Le 10 octobre 2025, une cyberattaque liée au rançongiciel Qilin a touché le système d'information des lycées publics des Hauts-de-France. La totalité des établissements ont été impactés, rendant les serveurs et postes informatiques inaccessibles.

Qui est mobilisé pour gérer la situation ?

Une cellule de crise conjointe réunit le conseil régional Hauts-de-France, les académies de Lille et d'Amiens, la DRAAF, ainsi que des experts en cybersécurité.

Des plaintes ont été déposées par le conseil régional et par les académies. Un signalement CNIL a été fait. Une enquête est en cours.

Des experts de la cyber sécurité ont été mandatés par le conseil régional et les académies bénéficient de l'expertise de l'ANSSI et du fonctionnaire de sécurité des systèmes d'information du Ministre de l'Education nationale.

Les données personnelles ont-elles été compromises ?

Les premières analyses menées par le conseil régional ont mis en évidence un accès non autorisé à certaines données personnelles qui ont pu être exfiltrées des serveurs. Une notification a donc immédiatement été faite à la CNIL. Ces données concernent notamment les services administratifs des lycées (intendance, secrétariat, gestion de la vie scolaire) et peuvent inclure des informations relatives aux élèves et à leurs familles. Afin de limiter tout risque, il est donc recommandé :
• de rester attentif à toute utilisation inhabituelle de vos données personnelles (relevés bancaires, courriels suspects, démarchages anormaux) ;
• de signaler sans délai à votre banque ou à votre assurance toute anomalie constatée ;
• de faire preuve de prudence vis-à-vis de courriels ou de messages sollicitant des informations personnelles ou financières.
L'enquête judiciaire se poursuit.

QUESTIONS TECHNIQUES GENERALES

1. Dois-je changer mon mot de passe académique ?

Il est impératif que tous les agents en lycée procèdent au renouvellement de leur mot de passe académique depuis Eduline (Lille) ou Intranet (Amiens : clé orange en haut à droite de l'accueil), si cela n'a pas été fait depuis le 10 octobre et avant le 5 novembre, délai de rigueur.

2. Puis-je allumer mon ordinateur en arrivant au lycée ?

Vous êtes enseignant : le conseil régional déploie actuellement un logiciel de sécurité sur tous les postes informatiques pédagogiques des lycées. Ce logiciel doit être installé par le conseil régional avant toute utilisation du poste afin de protéger les systèmes d'information. Il est installé à distance sur certains établissements, mais impose une installation sur site pour d'autres.

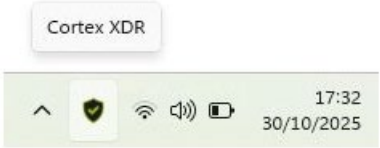
Dans le premier cas, un mail du conseil régional indiquera la possibilité d'utiliser les postes pédagogiques ; dans le second cas, le technicien en informera l'établissement après son intervention.

La souche de ce rançongiciel a été identifiée et est désormais utilisée par tous les anti-virus actualisés de manière automatique.

Ne pas allumer votre ordinateur sans validation.

Vous êtes personnel administratif : le conseil régional a déployé un logiciel de sécurité sur plus de 7000 postes administratifs. Ils sont de nouveau utilisables. Ils disposent d'un accès à Internet, mais restent déconnectés du réseau informatique du conseil régional.

Dans tous les cas : quand le PC est protégé, l'icône suivant apparaît en bas à droite de l'écran sur les postes protégés :



3. Situation actuelle : quels services informatiques fonctionnent à ce jour ?

Les ordinateurs administratifs ont été réinstallés et sont de nouveau utilisables. Ils disposent d'un accès à Internet, mais restent déconnectés du réseau informatique du conseil régional.

Ce qui fonctionne parfaitement :

- ENT,
- Pronote si hébergé par Index éducation,
- toutes les applications informatiques hébergées par l'éducation nationale ou les applications WEB (hors GFC, voir ci-dessous),

- tous les communs numériques (Visio-agents, M@gistère, Tribu etc.)
- la messagerie @ac,
- l'accès aux intranets académiques (Eduline et intranet),
- les systèmes autonomes utilisant le réseau informatique de l'établissement (ex : contrôle du chauffage, téléphonie, vidéo-protection, contrôle des accès, PPMS etc.),
- l'annuaire technique permettant aux 250 000 utilisateurs de s'authentifier pour utiliser les ordinateurs.

4. Quels services ne fonctionnent pas encore ?

Ce qui est en cours de rétablissement : ~80 000 postes pédagogiques, les serveurs administratifs et pédagogiques des établissements non migrés sur le domaine edu.hdf, les impressions en mode dégradé, les équipements de gestion de passage à la restauration. GFC, Pronote dans 4 établissements.

Ce qui ne fonctionne pas pour le moment : Les serveurs des établissements migrés sur le domaine edu.hdf et donc les fichiers accessibles depuis les lecteurs réseaux, les logiciels installés sur les serveurs des lycées, les imprimantes ou copieurs, ni pour imprimer, ni pour numériser des documents (voir point 7).

5. Le wifi interne du lycée fonctionne-t-il ?

Non, pas pour le moment. Le conseil régional y travaille.

6. Je ne retrouve plus mes fichiers habituels sur le serveur de l'établissement. Que faire ?

Les serveurs sont indisponibles pour le moment. En attendant leur remise en fonction :

- Enregistrer vos documents sur l'ENT ou utiliser les outils de l'éducation nationale tels que Nuage (https://nuage.apps.education.fr).
- Dès lors que l'usage d'un poste est autorisé, vous pouvez utiliser un support amovible (ex. clé USB) ; si celui-ci contient des données à risque, il sera bloqué par le logiciel de sécurité.
- Il est possible que vos fichiers enregistrés sur les serveurs de l'établissement aient été chiffrés et ne puissent être récupérés. Le conseil régional reviendra vers vous ultérieurement.

7. Puis-je imprimer ou numériser des documents ?

Une solution d'impression en mode dégradé via le réseau est en cours de mise en œuvre. Dans ce mode dégradé, il ne sera pas possible dans un premier d'utiliser les options de type agrafage, recto-verso et scan.

L'impression et la numérisation sont possibles si l'équipement est connecté en local ou s'il permet l'usage direct d'un périphérique amovible.

8. Puis-je utiliser mon ordinateur personnel ou une clé USB pour travailler ?

Dès lors que l'usage d'un poste est autorisé, vous pouvez utiliser un support amovible (ex. clé USB) ; si celui-ci contient des données à risque, il sera bloqué par le logiciel de sécurité installé par le conseil régional.

Votre ordinateur personnel ne doit en aucun cas être connecté au réseau informatique de l'établissement. L'ENT, nuage (cf. point 3) ou une clé USB peuvent être utilisés pour le stockage des fichiers devant être accessibles tant depuis, que hors de l'établissement.

La vigilance est également de rigueur dans l'usage des postes personnels, à utiliser exclusivement hors réseaux informatiques des établissements, notamment sur les points suivants :

- Le système d'exploitation doit être à jour : Windows 11, version à jour du système d'exploitation pour les Mac ou PC sous linux …
- L'ordinateur doit disposer d'un anti-virus à jour. C'est essentiel ;
- Sauvegardez les données importantes sur une clé USB ou un support de sauvegarde externe.
- Ne connectez pas votre ordinateur personnel au réseau informatique du lycée.

9. Puis-je utiliser un vidéo projecteur ou le tableau interactif ?

Oui en vous connectant directement sur le vidéo projecteur avec câble type HDMI ou VGA, ou via une clé USB ou depuis un poste dont l'usage est autorisé par le conseil régional.

10. J'ai utilisé mon PC personnel sur les réseaux de l'établissement récemment, peut-il être contaminé ? J'ai partagé une clé USB entre mon ordinateur personnel et un ordinateur de l'établissement, y-a-t-il un risque ?

Pour lever les doutes, vérifier que votre antivirus est à jour et lancez une vérification complète de votre ordinateur et des périphérique externes : clés USB, disque externe.

PERSONNELS ADMINISTRATIFS – précisions :

1. Où trouver le kit de reprise administrative ?

Un kit de reprise élaboré avec les établissements et les services académiques est disponible sur la page d'accueil d'Eduline (Lille) et de l'intranet (Amiens).

Il recense les applicatifs accessibles, les procédures alternatives et les ressources utiles pour la reprise.

2. Les paies sont-elles assurées ?

Oui. Les établissements mutualisateurs de la paie et les services académiques ont sécurisé la situation administrative et financière de tous les personnels, AED et AESH :

- les paies et versements de rémunérations ont été maintenus ;
- les contrats et affectations ont été pris en compte normalement.

3. Les campagnes sont-elles maintenues ?

Oui, avec quelques aménagements :

- Campagne de bourses : traitement possible au format papier ;
- Élections et procédures disciplinaires : maintenues avec des outils sécurisés.

4. Et les inscriptions aux examens ?

Les dates de clôture des inscriptions aux examens ont été décalées au 21 novembre, hors BTS (date nationale : 12 novembre).

5. Les données administratives sont-elles perdues ?

Certaines données enregistrées sur les serveurs du lycée peuvent être inaccessibles ou perdues. Les accès aux fichiers partagés ne seront pas rétablis immédiatement.

PERSONNELS PEDAGOGIQUES – précisions :

1. Les enseignants pourront-ils reprendre leurs activités numériques à la rentrée ?

Oui, mais de manière progressive. Les ordinateurs pédagogiques sont en cours de restauration. Les mots de passe utilisateurs seront réinitialisés à la reprise. Des plans de continuité pédagogiques ont été produits par les corps d'inspection (voir point suivant).

2. Un accompagnement est-il prévu pour les enseignants ?

Oui. Les corps d'inspection des académies de Lille et d'Amiens ont préparé deux guides de continuité pédagogique :

- Voie générale et technologique
- Voie professionnelle

Ces documents proposent :

- des conseils techniques et de sécurité,
- des ressources par discipline,
- des repères pour adapter les pratiques pendant cette période.

Ils sont disponibles sur la page d'accueil d'Eduline (Lille) et de l'intranet (Amiens).

Les inspecteurs référents et inspecteurs disciplinaires seront présents à la reprise pour accompagner les équipes et répondre à leurs questions.

3. Les données pédagogiques sont-elles perdues ?

Certaines données enregistrées sur les serveurs du lycée peuvent être inaccessibles ou perdues.
Les accès aux fichiers pédagogiques partagés ne seront pas rétablis immédiatement.

ET POUR LA SUITE ?

1. Quand tout sera-t-il complètement rétabli ?

Le rétablissement complet prendra encore du temps.
Une phase de fonctionnement partiel sécurisé est déjà en place pour les réseaux administratifs, et la reconstruction du réseau pédagogique est en cours.

2. Comment serons-nous informés de la suite ?

Restez attentif aux informations transmises par :

- Votre établissement ;
- Les académies et le conseil régional;
- Les canaux officiels : ENT, messagerie académique, l'intranet (Amiens), Eduline (Lille), e-lycée.

Cette FAQ sera régulièrement actualisée sur l'intranet (Amiens) et Eduline (Lille).

Soyez **très vigilant sur les mails que vous recevez**. De nombreux spams élaborés circulent en se faisant passer pour une académie, la DRASI, un collègue.

✗ ***Ne relayez pas sur les réseaux sociaux d'informations non confirmée***

3. Les bons réflexes à adopter au quotidien :

- Verrouiller votre session lorsque vous vous absentez temporairement de votre poste de travail et éteignez votre ordinateur avant de quitter votre poste pour une longue période (soir, vacances…).
- Ne sauvegarder aucun mot de passe dans les navigateurs internet et supprimer et modifier les mots de passe qui y seraient déjà enregistrés.

4. Comment protéger mes comptes et mes données ?

- Utiliser des mots de passe forts (12 caractères minimum) et changer les régulièrement.
- Ne jamais partager ses identifiants, même temporairement.
- Ne jamais réutiliser le même mot de passe sur plusieurs services.
- Distinguer les usages professionnels et personnels.
- L'utilisation de supports de stockage amovibles (clé USB, disque dur externe, etc.) pour la sauvegarde ou la consultation de données doit se faire uniquement à partir de matériel vérifié et sécurisé.
- Ne pas télécharger de fichiers dont le contenu est incertain ou inconnu et/ou provenant d'une source non identifiée.

- Rester vigilant lors de la réception de courriel (cohérence globale du courrier, vérification de l'adresse de l'expéditeur, liens suspects, pièces jointes douteuses…).
- Ne sauvegarder aucun mot de passe dans les navigateurs internet et supprimer et modifier les mots de passe qui y seraient déjà enregistrés.
- En cas de doute, signaler immédiatement toute anomalie.

5. Quelles mesures sont prévues pour éviter qu'une telle attaque ne se reproduise ?

Un retour d'expérience complet est engagé avec le conseil régional et les autorités académiques. Des mesures de durcissement et de prévention sont en cours par le Conseil régional pour renforcer la cybersécurité du système d'information des lycées.

6. À qui m'adresser ?

- Pour les consignes générales : à la direction ou au référent numérique de l'établissement;
- Pour toute question informatique : au centre de service informatique via l'Intranet (Amiens) ou Eduline (Lille) ;
- Pour les questions pédagogiques : aux corps d'inspection ;

Et pour les bonnes pratiques numériques consultez : cybermalveillance.gouv.fr