https://france3-regions.francetvinfo.fr/normandie/seine-maritime/rouen/menaces-d-attentat…

Écrit par Manon Loubet

4 min read

Menaces d'attentat dans des établissements scolaires de l'agglo de Rouen

Des établissements scolaires ont reçu des menaces de commission d'attentats dans la matinée du mardi 19 septembre 2023, dans l'agglo de Rouen (Seine-Maritime). Tous les établissements ont été évacués.

MISE À JOUR, mardi 19 septembre, 17 heures. Au collège Fontenelle de Rouen, les mesures de prévention et de protection ont été mises en oeuvre. "L'activité est maintenant revenue à la normale", indique l'établissement aux parents d'élèves, vers 17 heures. Les cours reprendront normalement dès mercredi 20 septembre.

Des établissements scolaires ont fait l'objet de meances de commission d'attentats dans la matinée de ce mardi 19 septembre 2023, dans l'agglo de Rouen (Seine-Maritime).

Des menaces ont été reçues dans le lycée des métiers Grieu à Rouen, le lycée Gustave-Flaubert à Rouen, le collège Fontenelle à Rouen, le lycée Marcel-Sembat à Sotteville-lès-Rouen, le lycée Fernand-Léger à Grand-Couronne et le CFA Simone-Veil à Rouen. "Aucune menace n’a à ce stade été confirmée", indique la préfecture dans un communiqué.

> Il a toutefois été décidé en lien étroit entre le rectorat de Normandie et la direction des services départementaux de l’Éducation nationale de la Seine-Maritime d’évacuer les établissements scolaires concernés, afin de permettre à la police nationale d’engager un protocole de levée de doute.
>
> *Préfecture de Seine-Maritime*

Dans ce cadre, une visite approfondie des locaux des établissements scolaires va être organisée. Toutes les dispositions sont prises afin que les élèves puissent réintégrer leur établissement dans les meilleurs délais.

En parallèle de ce protocole de levée de doute, le procureur de la République près le tribunal judiciaire de Rouen a ouvert une enquête, qu'il a confiée à la direction territoriale de la police judiciaire.

Ce n'est pas la première fois que des établissements seinomarins font l'objet de menaces de ce type. En avril 2023, le lycée Flaubert de Rouen mais aussi Jules Siefried au Havre avaient été la cible de messages de menaces.

Ces messages ont également été envoyés dans d'autres établissements de France depuis début septembre, notamment à Mérignac.

Lors des investigations, plusieurs logiciels malveillants de type "stealer" ont été retrouvés sur des ordinateurs personnels d'élèves.

"Les virus informatiques de type stealer sont spécialisés dans le vol d'identifiants (mots de passe…), de portefeuilles de cryptomonnaies, de cookies de session et autres données stockées notamment dans les navigateurs Internet. Une fois exfiltrées, ces données sont utilisées par les cybercriminels à des fins frauduleuses ou malveillantes", indique le site du gouvernement Cybermalveillance dans un communiqué à destination des parents d'élèves.

Dans le cadre du dossier des fausses alertes à la bombe, les stealers ont été introduits intentionnellement dans des logiciels contrefaits non validés par les éditeurs originels. Le virus a plus précisément été diffusé via des liens postés sur différentes plateformes grand public comme, par exemple, les réseaux sociaux.

Cybermalveillance prodigue plusieurs conseils pour éviter ces messages de menaces :

- Ne pas télécharger, ni utiliser de logiciels, d'applications et de vidéos piratés ou d'origine douteuse qui peuvent souvent contenir un virus;
- Ne jamais désactiver votre antivirus à la demande d'un logiciel.
- Face à un message suspect (inattendu, alarmiste, aguicheur…), ne pas ouvrir les pièces jointes ou cliquer sur les liens.

- Mettre régulièrement à jour vos appareils, logiciels et applications.
- Utiliser des mots de passe forts qui ne disent rien sur vous et différents pour chaque accès afin d'éviter des piratages en cascade.
- Deux sécurités valent mieux qu'une : activer la double authentification lorsque cela vous est proposé.
- Ne pas stocker vos mots de passe de manière non sécurisée : post-it, fichiers textes, messages brouillons, notes sur votre smartphone…
- Utiliser un gestionnaire de mots de passe ou un trousseau d'accès sécurisés, stockés de préférence en local, pour conserver vos mots de passe en sécurité. Vous n'aurez ainsi à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes.
- Ne jamais sauvegarder vos mots de passe dans le navigateur d'un ordinateur partagé.
- Se déconnecter systématiquement de votre compte après utilisation, pour éviter que quelqu'un puisse y accéder après vous.