

→ Fiche 9

Sécuriser l'espace numérique scolaire

Signalement en cas de messages frauduleux dans les environnements numériques de travail (ENT) dans une école ou un établissement

L'usurpation des comptes ENT et la diffusion de messages menaçants doivent systématiquement faire l'objet d'un signalement immédiat :

- Aux autorités académiques (DASEN, cabinet du recteur et responsable académique de la sécurité des systèmes d'information-RSSI) ;
- Au procureur de la République sur le fondement de l'article 40 du code de procédure pénale ;
- Ils justifient également, lorsqu'ils ont causé à l'établissement ou à l'État un préjudice déterminé (matériel, financier, etc.), que l'établissement ou l'État se constitue partie civile dans l'instance engagée contre l'auteur des faits⁵⁷ ;
- Couper la messagerie ou restreindre son accès (par exemple, désactiver la messagerie pour les élèves) ;
- Réinitialiser les mots de passe des comptes usurpés voire plus largement des EPLE victimes ;
- Transmettre les traces techniques aux autorités et les partager avec le RSSI académique pour mutualisation des mesures de sécurisation au niveau national.

Les auteurs s'exposent à des sanctions pénales (peine d'amende et d'emprisonnement) et, s'il s'agit d'élèves, à des sanctions disciplinaires.

La réaction immédiate en cas de vagues massives de ce type, convenue entre le ministère et les collectivités, est de couper ou de fortement limiter le service de messagerie de l'ENT le temps d'identifier les comptes usurpés, de les remettre en sécurité en les réinitialisant, puis de rechercher et supprimer l'ensemble des messages menaçants transmis.

Mise en œuvre des mesures de prévention

La lutte contre le pirate informatique est l'affaire de toutes et de tous. Il convient de mettre en œuvre et de faire connaître à l'ensemble de la communauté éducative les indispensables règles de sécurité suivantes :

- Ne jamais saisir son mot de passe à la suite de la réception d'un lien dans un courriel (mesure anti-hameçonnage ou phishing) ;
- Ne jamais conserver des mots de passe de manière non sécurisée (fichier texte, post-it), ni dans un navigateur internet (les dérobeurs de mots de passe ou stealers utilisent souvent ces fonctions) ;
- Se méfier des logiciels dont l'origine n'est pas garantie, lorsqu'ils ne sont pas diffusés par leur éditeur officiel (ils peuvent servir de vecteurs pour installer des logiciels malveillants comme des stealers) ;
- S'assurer de disposer d'un anti-virus à jour et ne jamais le désactiver ;
- Mettre régulièrement à jour ses applications et équipements ;

57. Note SG-DAJ n° D2023-013066 du 14 décembre 2023 relative à la constitution de partie civile en cas d'alerte à la bombe.

- Ne pas télécharger de programmes ou modules (plug-ins) depuis des sites non officiels ;
- Se méfier des messages inattendus ;
- Ne pas utiliser le même mot de passe partout ; imaginer des mots de passe robustes et activer les authentifications renforcées quand c'est possible.

Chaque établissement diffuse, à chaque rentrée scolaire et à tout moment opportun, les règles de bonne hygiène en matière de sécurité numérique ainsi que [la fiche de sensibilisation aux dangers des dérobeurs de mots de passe](#) (ou stealers). Les élèves, parents et personnels sont ainsi sensibilisés aux bonnes pratiques permettant d'éviter les usurpations et vols de données.