Dépliant

opentext™

# Les clés de la détection et de la prévention de la cyberintimidation

Les intimidateurs ont quitté la cour de l'école et sont désormais sur Internet. L'utilisation de la technologie chez les adolescents continue de se répandre, et les actes d'intimidation sont désormais perpétrés sur le Web et les réseaux sociaux. Retain Mobile et Retain Social aident les établissements à prévenir ces risques, grâce à des fonctions de monitoring, de filtrage et d'archivage sécurisé des communications issues des réseaux sociaux, des messageries électroniques et des périphériques mobiles.

OpenText offre une solution complète pour protéger vos élèves, votre établissement et votre personnel de situations potentiellement dangereuses, en vous fournissant des outils de détection et de prévention, y compris d'analyse par mot-clé, de filtrage des sites Web et des contenus et d'archivage pour les réseaux sociaux et les périphériques mobiles.

Depuis 2012 :

- 69 % des adolescents aux États-Unis possèdent un smartphone ou leur propre ordinateur.
- Parmi ces adolescents, 80 % sont actifs sur un ou plusieurs sites de réseaux sociaux.
- 81 % des jeunes disent qu'il est plus facile de ne pas être inquiété en intimidant en ligne qu'en intimidant en personne.
- 42 % des adolescents ayant accès aux technologies ont déclaré avoir été victimes de cyberintimidation au cours de l'année précédente.
- 34 % des étudiants interrogés ont déjà fait l'expérience de la cyberintimidation dans leur vie.
- 21 % des personnes interrogées ont déclaré avoir été victimes de cyberintimidation deux fois ou plus au cours des 30 derniers jours.
- 1 enfant sur 3 a déjà reçu des menaces en ligne, et 3 millions d'enfants sont absents de l'école chaque mois en raison d'actes d'intimidation.

Où peut mener ce type de harcèlement ?

- Les enfants victimes d'intimidation sont deux fois plus susceptibles de se suicider que les jeunes qui ne sont pas harcelés.
- 1 adolescent sur 5 victime de cyberintimidation pense au suicide, et 1 sur 10 fait une tentative.
- De 1985 à 2007, le taux de suicide des adolescents a augmenté de façon spectaculaire, parallèlement à la hausse de l'utilisation d'Internet et des technologies par ces adolescents.

## Deux solutions clés contre la cyberintimidation : la solution proactive et la solution réactive

Il existe deux approches principales pour prévenir la cyberintimidation : l'une est réactive, l'autre proactive. En mettant en oeuvre ces deux solutions, votre établissement disposera d'une double méthode pour faire cesser la cyberintimidation. Vous trouverez ci-dessous des solutions proactives et réactives à envisager.

1. **Solution proactive : filtrage du trafic Web et analyse de mots-clés**
   Le filtrage du trafic Web permet d'intercepter les messages avant leur livraison. Lorsqu'un élève, un enseignant ou un autre membre du personnel essaie de publier un message sur les réseaux sociaux ou d'effectuer des recherches sur le Web, vous devez avoir la possibilité de surveiller, de filtrer et de bloquer les contenus potentiellement dangereux. Le filtrage du trafic Web permet d'éviter que des publications, des recherches et autres contenus inappropriés entrent ou sortent de votre établissement. L'analyse des mots-clés dans les e-mails vous aide à lutter contre la cyberintimidation, le harcèlement sexuel et d'autres types de communication inappropriés, en signalant les mots-clés qui y sont associés et en prévenant les administrateurs et autres parties prenantes appropriées pour qu'ils puissent intervenir. Cela vous permet d'identifier et d'effectuer une analyse par mots-clés, tels que « arme à feu », « tuer », « mutiler », « détruire », « complot » et autres termes illicites ou nuisibles.

**Il existe deux approches principales pour prévenir la cyberintimidation : l'une est réactive, l'autre proactive. En mettant en oeuvre ces deux solutions, votre établissement disposera d'une double méthode pour faire cesser la cyberintimidation. Il existe plusieurs solutions proactives et réactives à envisager.**

**Communiquez avec nous**
Blog du PDG d'OpenText
Mark Barrenechea

Ces messages sont signalés de sorte qu'une situation potentiellement dangereuse puisse être désamorcée avant un incident, un désastre ou une tragédie. Bloquez ou supprimez des messages en fonction des règles que vous créez, empêchant ainsi les communications nuisibles d'être distribuées.

2. **Solution réactive : archivage des communications des réseaux sociaux et des périphériques mobiles**
La fonction d'archivage média d'OpenText™ Retain Social vous permet d'archiver les communications des réseaux sociaux au sein de votre réseau. Lorsque des élèves publient du contenu sur Facebook ou Twitter, vous devez être en mesure d'archiver ces communications dans une base de données centrale. Ces données doivent être accessibles et doivent pouvoir faire l'objet de recherches et de publications, ce en toute simplicité. Si un contenu inapproprié est publié par des élèves, des enseignants ou du personnel de votre réseau, vous devez être en mesure de le savoir. L'archivage des communications des périphériques mobiles vous offre la possibilité d'archiver les communications mobiles sur n'importe quel périphérique. L'archivage de ces données vous fournit un enregistrement de l'ensemble de la chaîne de communication, pour vous donner une image complète de ce qui a été dit et à qui, vous protégeant ainsi d'éventuels litiges. Ces données doivent être accessibles et doivent pouvoir faire l'objet de recherches et de publications, ce en toute simplicité.

## Commencez dès aujourd'hui à protéger votre établissement et vos élèves

OpenText™ offre une solution complète pour protéger vos élèves, votre établissement et votre personnel de situations potentiellement dangereuses, en vous fournissant des outils de détection et de prévention, y compris d'analyse par mot-clé, de filtrage des sites Web et des contenus et d'archivage pour les réseaux sociaux et les périphériques mobiles.

### FILTRAGE DES SITES WEB ET DES CONTENUS

OpenText vous propose une solution de monitoring, de filtrage et de blocage du trafic HTTP. Cette solution s'intègre aux systèmes ICAP compatibles pour fournir des fonctions de filtrage de contenu pour le trafic Internet entrant et sortant, avec filtrage des URL, des données de réseaux sociaux et des recherches. Elle intercepte les contenus inappropriés ou dangereux et alerte les responsables, les administrateurs et autres intervenants par e-mail ou via l'interface.

### ARCHIVAGE DES DONNÉES DE RÉSEAUX SOCIAUX ET MOBILES

Retain Social, OpenText™ Retain Mobile et OpenText™ Retain Email aident les établissements à prévenir ces risques, grâce à des fonctions d'archivage sécurisé des communications de réseaux sociaux, de messageries électroniques et de périphériques mobiles. Ces données archivées peuvent être immédiatement récupérées et examinées pour assurer la conformité, protéger les élèves, les enseignants et les autres membres du personnel de l'établissement, appliquer les stratégies de l'établissement et réduire les responsabilités liées aux communications électroniques dans les écoles.

Pour en savoir plus, rendez-vous sur **www.microfocus.com/opentext**

261-FR0054-001 | O | 05/23 | © 2023 Open Text

opentext™