LesEchos.fr
URL :http://www.LesEchos.fr/
PAYS :France
TYPE :Web Grand Public
► 17 février 2017 - 11:38
Cliquez ici pour accéder à la version en ligne

Sécuriser les réseaux scolaires : comment protéger les enfants des menaces sur Internet ?

L'enseignement actuel demande un accès important à des informations et à des ressources sur Internet. À cet égard, les établissements scolaires doivent faire face à une forte pression de l'État, des parents et de groupes d'intérêts spéciaux, qui leur demandent de surveiller leurs réseaux afin de prévenir tout abus contre les enfants et adolescents dont ils ont la responsabilité.

Lorsque l'accès aux ordinateurs et aux réseaux sociaux n'était encore que très limité, les menaces en ligne contre les enfants ne concernaient que certains groupes vulnérables et souvent isolés. Cependant, avec la démocratisation des technologies et l'explosion des appareils mobiles chez les jeunes, le risque d'abus sur Internet a considérablement augmenté.L'adoption des réseaux sociaux à l'échelle mondiale a encore aggravé le problème en créant des opportunités supplémentaires de cibler les enfants par le biais de nouveaux canaux. Cette évolution a parfois donné lieu à des affaires très médiatisées de prédation sexuelle ou même de radicalisation, qui ont vu par exemple des étudiants partir pour la Syrie afin de rejoindre des groupes extrémistes. Jusqu'à présent, le principal obstacle à la lutte contre ces activités était l'absence de protocoles normalisés pour la protection des enfants sur Internet, mais aussi le manque de conseils aux enseignants, parents et autres membres du personnel encadrant sur la façon d'approcher les enfants vulnérables et de réagir en cas de découverte d'un abus. Pour faire face à ce déficit, le Ministère de l'Éducation nationale et de l'Enseignement supérieur donne accès à des outils et ressources pédagogiques pour favoriser les usages responsables d'Internet. En effet, les enseignants et les élèves peuvent s'appuyer sur le portail Internet responsable qui permet d'accéder à de nombreuses ressources sur ce thème, lequel contient des protocoles, recommandations et textes officiels.Le piège des réseaux sociauxLa plus grande difficulté pour les établissements tient souvent au fait que les enfants et adolescents connaissent en général bien mieux les réseaux sociaux comme Facebook, Twitter, Snapchat, Instagram et WhatsApp que les professeurs eux-mêmes. Selon le livre blanc Keeping Children Safe in Éducation - statutory guidance and changes to online safeguarding (Protection des enfants dans le cadre éducatif - Directives légales et nouveautés concernant la protection sur Internet), "un enfant sur quatre a déjà été confronté à du contenu perturbant sur les réseaux sociaux et un enfant sur trois a déjà été victime de cyberintimidation". Or, de nombreux établissements scolaires n'ont pas l'expertise nécessaire pour surveiller et sécuriser ces canaux, sans parler du fait que les coûts d'entretien d'une infrastructure et de services informatique peut amener certaines écoles à employer des solutions obsolètes et moins efficaces pour gérer leur écosystème. Même avec une sécurité renforcée et la mise en place d'un système de filtrage de contenu sur le réseau, il est en outre nécessaire de maintenir une vigilance constante sur la communauté afin de repérer les enfants vulnérables et d'intervenir.Cela nous amène à un autre problème important, à savoir l'extrême difficulté à reconnaître les victimes : les enseignants ayant peu d'expérience pour repérer les signes d'abus auront toutes les peines à apporter le soutien nécessaire aux enfants concernés. Aussi, l'absence de réseau de protection structuré ne permet pas aux établissements de surveiller chaque enfant individuellement, il est alors difficile de garantir qu'ils soient écoutés et que des mesures adaptées soient prises. Comme pour les cybermenaces, la lutte contre les abus en ligne requiert d'isoler chaque menace et chaque vulnérabilité afin d'assurer une sécurité constante et de protéger les utilisateurs vulnérables. Les écoles doivent ainsi adopter une double stratégie en vue de renforcer au maximum les dispositifs de protection autour des enfants confiés à leur garde.Combattre les abus sur Internet et dans les classesLa lutte contre les abus en ligne et la cyberintimidation demande d'abord de disposer des bons outils. Les écoles ne peuvent pas espérer créer un écosystème Internet sûr pour leurs élèves sans une stratégie unifiée de gestion des menaces.L'utilisation d'un pare-feu nouvelle génération doté de service de filtrage de contenus pour les enfants est un premier rempart indispensable pour contrôler la présence de contenu indésirable sur le réseau des établissements. Ces derniers doivent s'assurer que leurs logiciels de sécurité utilisent des filtres spécifiques visant à protéger les enfants. Ils doivent également veiller à ce que les filtres appliqués apportent une protection suffisante sans toutefois bloquer l'accès à des informations légitimes et nécessaires dans

le cadre des programmes scolaires.En outre, de nombreuses écoles ayant mis en place des points d'accès sans fil à Internet, il est aussi important d'établir des protocoles de sécurité mobile afin de gérer l'accès au réseau et d'assurer la sécurité de tous les appareils connectés. Dans la mesure où le budget informatique des établissements scolaires est souvent restreint, le recours à des services de sécurité infogérés et à un système de gestion simplifié de la sécurité peut également être avantageux, en ce qu'il permet de bénéficier des meilleurs niveaux de protection sans avoir besoin d'experts ou de techniciens sur place.Ceux qui se battent pour que les enfants restent des enfants sur InternetEn complément de l'installation d'outils adaptés, La Commission Européenne a initié le Safer Internet Day, événement mondial annuel organisé au moins de février, ayant pour but de promouvoir un Internet meilleur auprès des jeunes, leurs parents et la communauté éducative. Il a été lancé ce 7 février au ministère de l'Éducation nationale. Cette année encore, Internet sans Crainte mobilise tous les acteurs de la communauté éducative autour de la mise en place d'actions de sensibilisation sur la citoyenneté numérique et le cyberharcèlement. Plusieurs ressources sont disponibles sur le site, sous forme de vidéos et ateliers pédagogiques : initier les enfants aux bases de l'éducation au numérique ; comprendre le pouvoir des données à l'heure du big data ; parents : Agir face aux nouvelles formes de harcèlement, etc.L'association e-Enfance propose aux jeunes, aux parents et professionnels, des interventions en milieu scolaire et des formations sur les bons usages d'Internet et les risques éventuels comme le cyberharcèlement, le cyber sexisme et les autres formes de cyberviolence. e-Enfance apprend aux enfants et adolescents à se servir des nouvelles technologies de communication avec un maximum de sécurité. Ils ont mis en place une ligne d'appel gratuite, Net Ecoute, spécialisée dans les problématiques que rencontrent les enfants et les adolescents dans les pratiques numériques. Selon e-enfance, 10 % des élèves subissent du harcèlement sur Internet.La France est le deuxième pays hébergeur de contenus pédopornographiques en Europe. En effet, quelques chiffres alarmants sont à souligner. D'une part, le nombre de signalements de contenus inappropriés adressés à la plateforme Point de Contact, service de signalement en ligne de tout contenu choquant rencontré sur Internet, a augmenté de 144 % depuis 2014. 75 % de ces signalements concernent des images d'abus sexuels sur mineurs. D'autre part, les situations de cyberharcèlement et de discriminations en tout genre traitées par la ligne Net Ecoute ne cessent de croître et représentent aujourd'hui plus de 50 % de l'activité contre 25 % un an auparavant.Les technologies adéquates pour les établissements scolairesAfin de mieux contrôler la prolifération des réseaux informatiques et mobiles au sein d'un environnement sécurisé, sera-t-il nécessaire de faire appel à des auxiliaires tiers, aussi bien pour installer les nouvelles technologies requises que pour initier les enseignants et les tuteurs à des pratiques de sécurité modernes et efficaces ?Les fournisseurs de logiciels de sécurité sont bien placés pour les conseiller à cet égard, ainsi que pour doter les établissements de tout ce dont ils ont besoin pour se conformer aux dernières directives du département de l'Éducation, que ce soit en leur apportant des connaissances étendues en matière de protection des données sensibles et des utilisateurs, ou en leur faisant bénéficier de leur expérience pour gérer la transition vers des solutions de protection modernes. En mettant en place des mesures et des outils adaptés, les écoles peuvent permettre aux élèves de bénéficier de la mobilité offerte par les nouveaux appareils et d'explorer Internet sans craindre les risques d'abus.Vous aussi, partagez vos idées avec les lecteurs des Echos