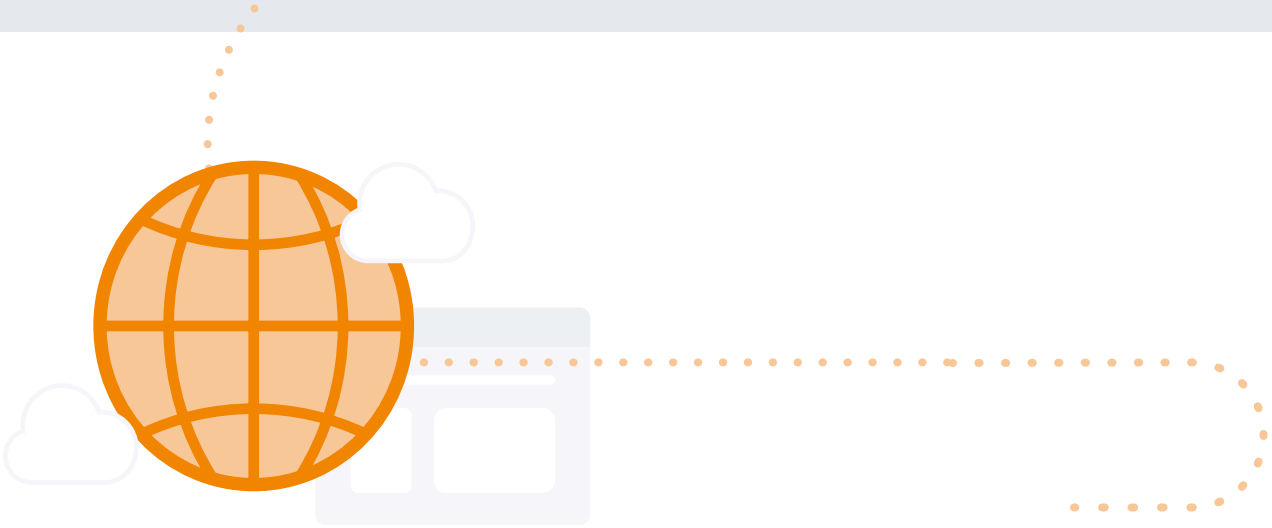
Le filtrage de contenu pour l'enseignement primaire et secondaire

jamf



Les écoles du monde entier s'efforcent de trouver le bon équilibre en matière d'Internet. Naturellement, elles veulent donner à leurs élèves l'accès aux incroyables possibilités de recherche et d'éducation offertes par le Web. Mais elles veulent aussi les protéger contre les contenus dangereux ou inappropriés, les tentatives d'hameçonnage et les prédateurs.

Chaque jour, des enfants tentent d'accéder à des contenus inadaptés ou dangereux à l'école. En Nouvelle-Zélande, les écoles ont récemment indiqué avoir bloqué 399 millions de tentatives d'accès à des contenus inappropriés en un mois.[1]

Désormais, les appareils fournis par l'école suivent les enfants à la maison, au-delà du pare-feu de l'établissement. Il faut donc un mécanisme de blocage basé sur l'appareil, pour protéger les élèves où qu'ils se trouvent.

Les écoles doivent donc aborder la sécurité des élèves sur plusieurs fronts. Ce guide est destiné à donner des repères aux écoles pour les accompagner dans cette démarche.

Dans ce guide, nous allons aborder :

- Les contenus en ligne qui mettent les élèves en danger, et pourquoi il est important de les protéger activement
- Les nuances et scénarios qui justifient une approche flexible et personnalisée du filtrage de contenu
- La sensibilisation des élèves à la citoyenneté numérique et leur autonomisation
- Et l'aide que nous, Jamf, pouvons vous apporter

Pourquoi filtrer ?

Pour mille raisons.

Protection des élèves

Les restrictions légales sur l'accès des élèves aux contenus en ligne varient d'un pays à l'autre, mais relèvent toutes de catégories similaires :

- Contenu pornographique ou obscène
- Discours haineux, sites violents ou radicalisants
- Sites encourageant l'automutilation, le suicide ou l'anorexie
- Hamçonnage et prédateurs
- Cyberharcèlement
- Suppresion des distractions telles que les réseaux sociaux et les jeux
- Sites de jeux d'argent

Selon l'Organisation mondiale de la santé, le suicide est la quatrième cause de décès dans le monde chez les 15-19 ans.[2] Et comme 47 à 60 % (selon l'âge) des élèves d'âge scolaire sont victimes de cyberharcèlement[3], protéger les élèves contre ce type de danger en ligne peut littéralement sauver des vies.

Concentration et productivité des élèves

Limiter l'accès aux réseaux sociaux à l'école ne contribue pas seulemeent à prévenir le cyberharcèlement : cela aide aussi les élèves à rester concentrés sur leurs études. Ils apprennent davantage, sont plus productifs et participent mieux en classe.

Bien souvent, une obligation légale

En 2000, le Congrès des États-Unis a adopté la loi sur la protection de l'Internet pour les enfants. Celle-ci assujettit les remises accordées par le programme E-rate à la politique de sécurité Internet d'un établissement.

En Angleterre et au Pays de Galles, le ministère de l'Éducation a publié en 2015 des directives statutaires. Intitulées « Keeping Children Safe in Education » (Assurer la sécurité des enfants dans l'éducation), elles obligent les écoles à mettre en place des systèmes de filtrage et de surveillance appropriés. Une règle similaire existe en Écosse.[4]

Des mesures similaires sont appliquées en tout ou en partie sur tous les continents (à l'exception de l'Antarctique, pour des raisons évidentes).

Sécurité du système

Un filtre qui bloque les logiciels malveillants, les logiciels publicitaires et les logiciels espions assure la sécurité des élèves. Mais il protège aussi le réseau de votre école.

Surveillance et rapports

Les parents doivent avoir l'assurance que leurs enfants n'ont pas accès à des contenus dont ils souhaitent les protéger. De leur côté, les écoles doivent surveiller leurs réseaux pour protéger les données et les élèves.

Mais cette surveillance doit se faire dans le respect de la vie privée : il n'est pas question de procéder à des inspections granulaires de chaque appareil. Cette démarche doit prendre la forme d'un processus transparent de collecte de données anonymes. Ces données seront ensuite présentées aux professionnels de la sécurité, aux parents et aux administrateurs.

Votre établissement doit s'équiper d'outils de sécurité qui assurent la protection des terminaux et la prévention des menaces sur le réseau, comme Jamf Protect et Jamf Safe Internet. Ces outils doivent remplir plusieurs fonctions : protection contre les virus connus, analyses comportementales pour trouver et isoler les nouveaux dangers, et production de rapports détaillés. Demandez-vous aussi s'ils s'appuient sur une communauté active, comme Jamf Nation ou Jamf Educator. Vous pourrez ainsi échanger des bonnes pratiques et obtenir les conseils d'autres personnes toutes aussi soucieuses que vous de la réussite de leurs élèves. Combinez-les avec une solution complète de gestion des appareils mobiles (MDM) comme Jamf School ou Jamf Pro, et vous serez paré.

Pourquoi ne pas simplement tout bloquer ?

Face aux statistiques sur les élèves vulnérables, parents et enseignants peuvent être tentés de verrouiller entièrement tous les accès. Mais cela peut être un problème à plusieurs égards.

Les enseignants et les élèves doivent avoir accès à des sites que l'établissement pourrait bloquer dans un excès de zèle, pour protéger les élèves et préserver l'attention en classe. Mais YouTube et les services Google, par exemple, ont leur place dans de nombreuses salles de classe. Sans eux, les enseignants désireux de travailler avec leurs élèves sur les événements de l'actualité, les mouvements sociaux et bien d'autres sujets se retrouvent privés de ce contenu éducatif. Et ils n'ont pas non plus la possibilité de recueillir facilement les travaux des élèves sous forme numérique.

Mais l'accès illimité à ces services peut également poser problème. La solution ? Un outil tel que Jamf Safe Internet, capable de filtrer selon des critères plus sophistiqués que le simple nom de domaine, pour protéger les élèves sans gêner leur apprentissage.

Aucun système de filtrage n'est parfait. Quelqu'un doit trouver les logiciels malveillants ou les sites d'hameçonnage et les ajouter aux listes de blocage. Malheureusement, de nouveaux sites sont créés chaque jour.

Pour cette raison, il est essentiel, dans le cadre de l'enseignement, de préparer les élèves à utiliser des appareils sans restriction. Les jeunes adultes qui comprennent déjà les dangers potentiels et savent comment les éviter seront plus en sécurité en ligne que ceux qui ont été complètement isolés d'Internet.

Les élèves, des citoyens numériques

L'éducation de tout élève devrait lui apprendre à se protéger de l'hameçonnage, des logiciels malveillants, des informations trompeuses et autres sur Internet – même après avoir quitté l'école et les filtres de contenu.

Les programmes d'études et la pédagogie devraient intégrer la nécessité d'éduquer et former des citoyens numériques avertis. Il s'agit notamment d'apprendre à reconnaître une source fiable, en faisant appel à la réflexion critique et à une sensibilisation à ce qui est ou non une source digne de confiance. Mais aussi de savoir éviter l'hameçonnage et autres escroqueries.

Aux enseignants qui cherchent un point de départ pour aider les élèves à s'approprier leur vie numérique, nous suggérons les leçons, programmes et idées prêts à l'emploi du programme Digital Citizenship de Common Sense Education – ils sont disponibles gratuitement. Common Sense est une organisation à but non lucratif basée aux États-Unis, qui se consacre à l'amélioration de la vie de tous les enfants et de leurs familles. Elle a créé ces leçons en partenariat avec Project Zero de la Harvard Graduate School of Education. Les leçons sont adaptées à différentes classes d'âge.

Comment trouver la bonne solution de filtrage et de sécurité ?

Comment déterminer quelle solution est la meilleure pour votre école ? Commencez par poser les six questions suivantes aux fournisseurs qu vous envisagez :

1 Est-ce que la solution filtre le contenu sur tous les appareils, iPad et Mac inclus ? Qu'en est-il des appareils personnels utilisés dans le cadre professionnel (BYOD) ?

Les solutions doivent offrir une couverture complète dans votre école. La qualité d'un système de filtrage est celle de son mur le plus fragile.

2 Comment se défend-elle face aux attaques inconnues ?

Le système que vous utilisez, quel qu'il soit, doit intégrer une analyse comportementale et des alertes en temps réel.
Sa mission est de détecter les sites et les logiciels malveillants inconnus, comme Jamf Protect ou Jamf Threat Defense.
Parce qu'elle reconnaît les opérations des logiciels malveillants et les phrases employées par les sites dangereux, l'analyse comportementale est capable d'arrêter des actions criminelles.

3 Peut-elle assurer un filtrage partiel des sites comme YouTube ou les services Google ?

YouTube et Google sont devenus de puissants outils d'apprentissage, mais ils ouvrent aussi la porte à des contenus inappropriés. Trouvez une solution de sécurité qui vous permette de filtrer l'accès au contenu de manière plus granulaire, sans limiter complètement l'accès à ces sites.

4 Comment cette solution favorise-t-elle la participation des parents ?

Si certains parents remettent en question la nécessité d'un filtrage, d'autres peuvent être très inquiets de toute perméabilité. Il peut être utile d'offrir aux parents la possibilité de suivre les activités de leur enfant pendant la journée grâce à une apps comme Jamf Parent.
Des rapports clairs et détaillés sur les problèmes de sécurité et de confidentialité, comme ceux offerts par Jamf, sont également précieux.

5 Comment filtrer les appareils des élèves hors site ?

Quelle que soit la solution choisie, vous devez vous assurer qu'elle intègre des filtres et une fonction de gestion des appareils des élèves, à la maison comme à l'école, comme le fait Jamf School. Et c'est encore mieux si les parents peuvent renforcer les filtres et la gestion dans une application facile à utiliser comme Jamf Parent.

6 Comment s'interfacera-t-elle avec mes autres solutions ?

Optez pour une solution de filtrage et de sécurité capable de fonctionner en toute simplicité avec un fournisseur MDM et de s'associer à des partenaires de confiance. Vous bénéficierez non seulement d'une sécurité de classe mondiale, mais aussi d'options pédagogiques plus large – autrement dit, d'une bien meilleure rentabilité.

Quels sont les avantages de Jamf ?

jamf SCHOOL

Des équipes informatiques et des enseignants autonomes grâce à une gestion Apple efficace.

jamf PROTECT

Protection des terminaux macOS spécialisée

Jamf Safe Internet

Filtrage de contenu et protection contre les menaces pour l'éducation

Jamf Teacher

Jamf School Student

Jamf Parent

Jamf Assessment

jamf EDUCATOR

L'éducation des clients au service de l'application Jamf Teacher

jamf MARKETPLACE

Des intégrations précieuses qui étendent la plateforme Jamf

Jamf et Jamf Safe Internet peuvent être précieux pour assurer la sécurité des élèves tout en protégeant leur vie privée :

- Tableaux de bord offrant une visibilité globale aux administrateurs
- Des rapports sur les tendances, qui donnent aux parents, aux enseignants et aux administrateurs un aperçu des tendances du comportement des élèves en ligne, pour les aider à élaborer leurs prochains cours.
- Des synthèses sous forme graphique pour un accès rapide et intuitif à l'information.
- Respect de la vie privée : outre toutes les règles et réglementations en la matière, Jamf a signé l'Engagement pour la protection de la vie privée des élèves. Nous manifestons par là notre volonté de protéger les informations des élèves, des parents et des enseignants de nos écoles.

jamf

L'expérience fluide et intégrée de Jamf Safe Internet peut apporter une valeur ajoutée aux workflows existants des apps Jamf Teacher, Jamf School Student et Jamf Parent.

Demandez une version d'essai

Ou contactez votre revendeur habituel de matériel Apple.