Introduction au spam dans l'enseignement primaire et secondaire

jamf

Introduction au spam dans l'enseignement primaire et secondaire

Notre série d'e-books nous a fait découvrir les cybermenaces courantes auxquelles les établissements primaires et secondaires sont confrontés chaque jour. Au cours de cette classe verte, nous avons rencontré :

- **Les logiciels malveillants**
- **Le phishing**
- **Le cryptojacking**

Cette fois-ci, nous allons parler du spam. Il n'est pas toujours malveillant, mais il peut laisser un goût amer et devenir un véritable obstacle à l'apprentissage.

DANS CET E-BOOK, NOUS ALLONS NOUS PLONGER DANS LE SPAM QUI CIBLE LE DOMAINE DE L'ÉDUCATION EN ABORDANT SPÉCIFIQUEMENT :

1. Qu'est-ce que le spam ?
2. Ses différentes formes ?
3. Son impact sur les utilisateurs dans l'enseignement primaire et secondaire ?
4. Comment l'éviter ?

Qu’est-ce que le spam ?

En règle générale, le spam est un contenu indésirable et non sollicité, envoyé pour diffuser de la publicité, obtenir des informations ou propager des logiciels malveillants. Il circule sur différents canaux : e-mail, appel téléphonique, SMS, message sur les réseaux sociaux, etc. Le spam n’est pas toujours malveillant, mais lorsqu’il l’est, il peut être particulièrement néfaste pour son destinataire.

Vous avez peut-être entendu parler des SMS racistes ciblés envoyés à des étudiants américains. Dans la mesure où l’intention de voler des informations, ces messages ne constituent pas nécessairement des cybermenaces, mais ils peuvent blesser et créer des conflits.

Ce n’est pas la première fois que le spam perturbe des étudiants. En 2020, des collégiens et lycéens de Floride ont reçu « des millions d’e-mails de spam au contenu offensant et inapproprié » : il s’agissait de messages racistes et sexuellement explicites à propos d’une employée de l’école.

Le spam peut également avoir pour but de tromper pour obtenir des données personnelles (comme dans le cas du phishing), de l’argent ou autre.

On imagine facilement l’impact négatif que le spam peut avoir sur les étudiants, que ce soit :

- En attaquant certaines populations
- En exposant les enfants à des contenus perturbants ou inappropriés devant lesquels ils peuvent être démunis
- En perturbant les cours à cause des discussions déclenchées par le contenu
- En encombrant les boîtes de réception de messages inutiles
- En exploitant la naïveté des élèves à des fins financières ou autres

Les différentes formes du spam

Le spam se présente sous toutes sortes de formes et évolue constamment pour faire le plus grand nombre de victimes. Vous pouvez recevoir du spam :

Par e-mail | **Par SMS** | **Sur des forums de discussion** | **Par téléphone** | **Sur les réseaux sociaux**

Malgré la diversité de ces formes, le spam a tendance à suivre certains schémas, comme nous allons le voir.

Contenu inapproprié ou agressif
Comme on l'a vu, le spam peut avoir pour but de blesser ou de choquer le destinataire. Si la motivation de ces messages n'est pas toujours claire, les perturbations qu'ils provoquent sont bien réelles. Leurs destinataires peuvent être blessés, et leur bien-être psychique peut être durablement affecté. Ces messages peuvent également perturber les cours en suscitant des discussions entre les élèves, par exemple.

Publicité
Même s'ils proviennent d'une organisation légitime, les messages promotionnels non sollicités sont considérés comme du spam. Imaginons qu'un étudiant reçoive un message lui expliquant qu'il peut « bénéficier de réductions exclusives en faisant des achats avant minuit ». Le message n'est pas nuisible en soi, mais il fait perdre du temps à l'étudiant et prend de la place dans sa boîte de réception.

Logiciels malveillants et phishing
Certains spams sont créés dans l'intention d'inciter leur destinataire à faire quelque chose qui finira par lui porter préjudice. Un e-mail peut, par exemple, inviter l'utilisateur à télécharger et ouvrir une pièce jointe qui va installer un virus sur son ordinateur. Il peut aussi le pousser à agir dans la précipitation en laissant planer des menaces en cas d'inaction, et le rediriger vers un site web de phishing.

Des offres « trop belles pour être vraies »
Le spam se présente souvent sous la forme d'une offre « trop belle pour être vraie » pour inciter l'utilisateur à cliquer sur un lien et à donner des informations personnelles. Quelques exemples :

- Pour recevoir une forte somme d'argent, le destinataire doit donner son adresse ou faire un versement.
- Le destinataire a gagné une console de jeu et doit donner ses informations personnelles
- Le destinataire a été sélectionné comme influenceur et doit cliquer sur un lien où ses informations seront collectées.

Les étudiants, et en particulier les jeunes, sont plus sensibles à cette tactique.

Le spam dans l'enseignement primaire et secondaire

Dans le pire des cas, le spam est malveillant et provoque une violation des données de votre école. Au mieux, mais ce n'est toujours pas idéal, c'est une nuisance mineure.

Le meilleur des scénarios ? Des outils de sécurité qui font en sorte que les utilisateurs ne voient même pas passer ces messages.

Quoi qu'il en soit, le spam ne doit pas être négligé, car il peut avoir un impact réel sur l'apprentissage des étudiants. Par exemple, des écoles californiennes ont reçu des e-mails menaçants évoquant la présence d'une bombe. Une enquête a révélé qu'il s'agissait d'une fausse alerte, mais plusieurs écoles ont décidé de fermer leurs portes par prudence.

Heureusement, ces e-mails n'ont pas entraîné de catastrophe. Mais ils ont nui à l'apprentissage des élèves et à leur sentiment de sécurité. Des cours ont été annulés. Les élèves ont besoin de se sentir en sécurité à l'école pour s'épanouir et apprendre, et le spam compromet la confiance.

Les spams qui contiennent des liens ou des logiciels malveillants peuvent également avoir des conséquences destructrices. Les établissements d'enseignement sont des cibles de choix pour les pirates. Le spam peut même être le point de départ d'une attaque de ransomware. En effet, selon le rapport Sophos sur l'État des ransomware dans l'enseignement en 2024, les e-mails malveillants et le phishing étaient respectivement impliqués dans 26 % et 8 % des attaques de ransomware. Les conséquences peuvent être très lourdes :

- Heures de cours annulées en raison du blocage des systèmes
- Violation et fuites de données des élèves et des enseignants
- Coût et durée du processus de restauration

Prévention du spam

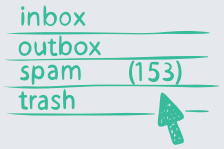
Heureusement, la lutte contre le spam n'a rien d'une cause perdue. Voyons maintenant quelques outils et tactiques pour empêcher le spam de faire des ravages.

Gestion des appareils mobiles

La gestion des appareils mobiles (MDM) est un socle qui garantit que les appareils de votre établissement sont correctement configurés et sécurisés. Avec une solution MDM, vous pouvez :

- Effectue le suivi des appareils, des utilisateurs et des applications
- Enregistrer les incidents liés aux appareils
- Déployer des applications à la demande des enseignants
- Appliquer des configurations sécurisées aux appareils

En d'autres termes, une solution MDM offre aux administrateurs la visibilité nécessaire pour assurer le bon fonctionnement et la sécurité des appareils, sans porter atteinte à la vie privée des élèves.



Filtrage des e-mails

L'e-mail est un vecteur majeur de spam : il faut donc le cibler en priorité pour empêcher les messages indésirables d'arriver jusqu'aux utilisateurs. Les filtres d'e-mail interceptent les spams en fonction de leur contenu, de leur expéditeur et d'autres critères.

Filtrage de contenu

Mais le spam ne passe pas toujours par l'e-mail, et aucun filtre antispam ne peut tout arrêter. D'où l'importance du filtrage du contenu, qui constitue la ligne de défense suivante : il empêche les utilisateurs d'accéder à des sites web malveillants ou dangereux. Si un élève clique sur une lien de phishing, le filtrage du contenu bloquera l'accès au site web qui a été créé pour voler ses informations. Le filtrage du contenu peut également interdire l'accès aux réseaux sociaux ou aux forums connus pour diffuser du spam.

Logiciels de sécurité

Que se passe-t-il si un utilisateur télécharge un logiciel malveillant après avoir reçu un spam par e-mail ? Votre logiciel de protection peut détecter sa présence, l'empêcher de s'exécuter et prendre des mesures de sécurité. Il pourra notamment se coordonner avec votre solution MDM pour corriger le problème.

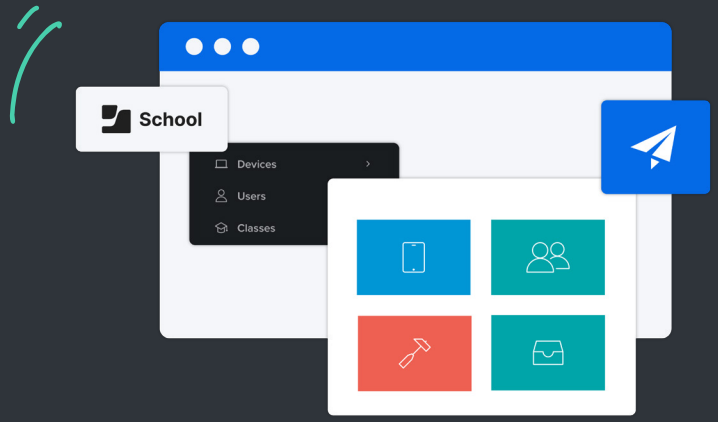
Sensibilisation des utilisateurs

L'éducation des utilisateurs est essentielle pour empêcher le spam d'entraver l'apprentissage. Pour renforcer la sécurité de l'établissement, il est crucial d'apprendre aux élèves, aux enseignants et au personnel les indices qui trahissent le spam et la marche à suivre s'ils en reçoivent.

MISE EN ŒUVRE : JAMF SCHOOL ET JAMF SAFE INTERNET

Nous avons évoqué plusieurs stratégies pour lutter contre le spam. Voyons maintenant comment les mettre en œuvre.

Jamf propose un logiciel puissant pour bloquer les spams et bien d'autres menaces.



Jamf School

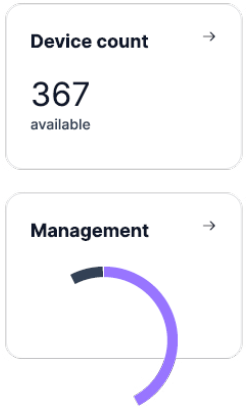
Jamf School est une solution MDM spécifiquement conçue pour les établissements scolaires. Elle est entièrement pensée pour soutenir l'apprentissage, du service d'assistance informatique à la salle de classe. Comme on vient de le dire, la MDM est la pierre angulaire de la sécurité, et la MDM Jamf School répond aux exigences du monde de l'éducation.

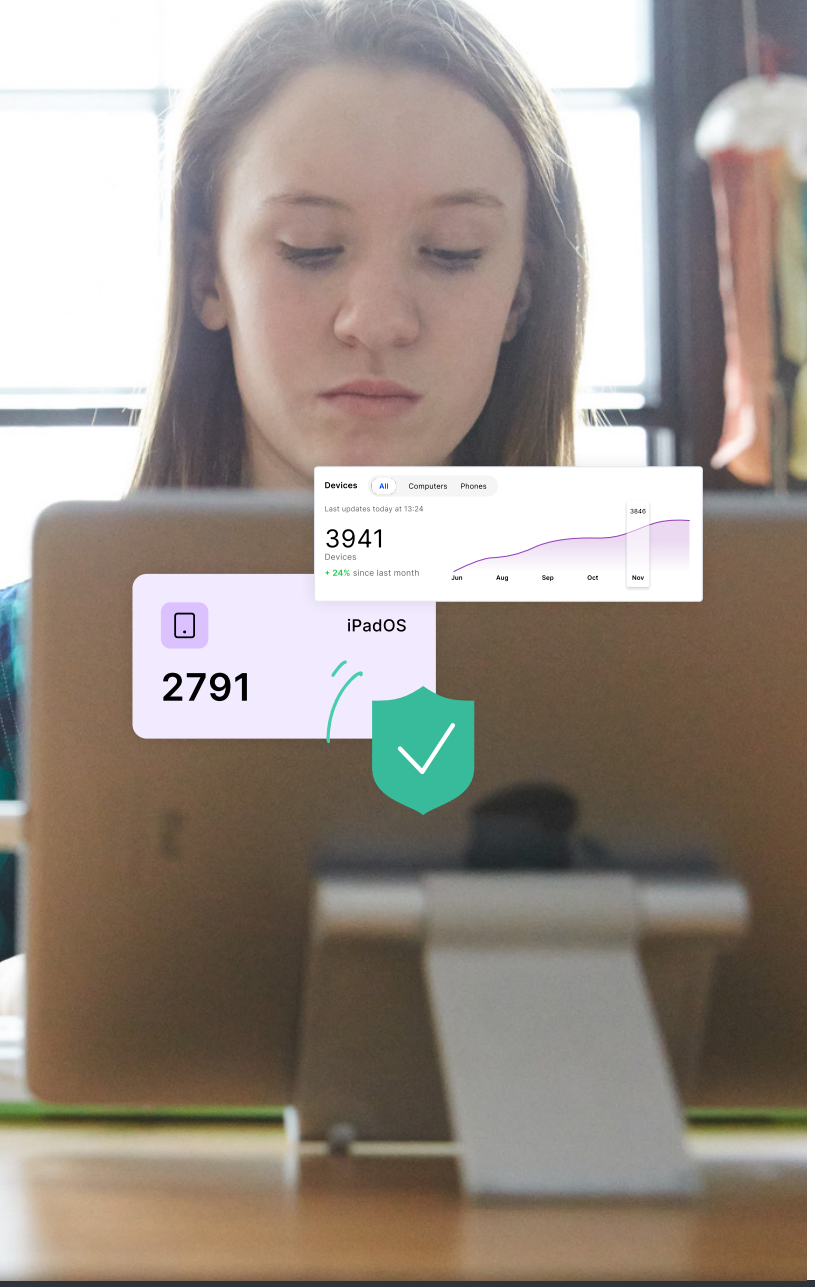
Jamf School offre de nombreux outils pratiques pour gérer les appareils :

- Des tableaux de bord clairs et lisibles pour effectuer le suivi des appareils gérés, des applications et des utilisateurs
- La diffusion d'applications, de contenus et de restrictions par simple glisser-déposer
- Le suivi des dommages et des incidents liés aux appareils

Elle s'accompagne d'applications gratuites comme Jamf Teacher, destinée à être utilisée en classe. Un élève est distrait ? Il veut poser une question ? Il a reçu du spam ou rencontré un contenu perturbant ? L'enseignant peut rapidement réagir :

- En affichant une notification sur l'écran de l'élève
- En échangeant des messages avec lui
- En limitant l'accès à certains sites web et applications.





Jamf Safe Internet

Internet a beaucoup à offrir, mais il est aussi truffé de menaces : spam, logiciels malveillants et phishing, entre autres. Jamf Safe Internet est une puissante solution de prévention des menaces réseau et de filtrage du contenu qui protège les élèves contre ces menaces. Le filtrage de contenu est exercé sur l'appareil : les élèves n'ont pas besoin d'être connectés au Wi-Fi de l'école pour être protégés.

Outre les sites web malveillants, les administrateurs peuvent bloquer des catégories précises de contenu, comme les divertissements, les jeux et les réseaux sociaux. Jamf Safe Internet active automatiquement Google SafeSearch et le mode limité de YouTube pour que les élèves n'aient pas accès à des contenus néfastes.

Jamf Safe Internet empêche les acteurs malveillants de voler des données personnelles, qui doivent impérativement rester privées. C'est pourquoi Jamf Safe Internet respecte la vie privée des élèves et ne surveille pas leurs faits et gestes.

jamf

Découvrez comment Jamf peut enrichir votre solution de gestion de la technologie, de sécurité et de filtrage de contenu.

Lancez-vous !

www.jamf.com/fr