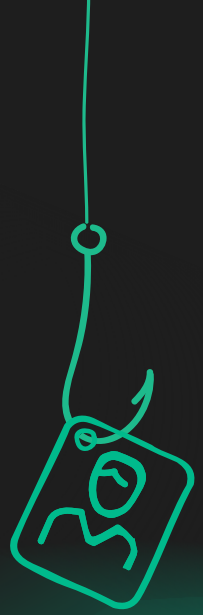
L’ingénierie sociale dans l’enseignement primaire et secondaire : introduction

jamf



Les enfants vont à l'école pour apprendre, mais pas seulement. L'école leur enseigne aussi les interactions sociales, la confiance en soi et l'appui de leurs camarades et d'adultes. C'est une période tumultueuse, qui n'est pas toujours caractérisée par un grand discernement.

Les pirates le savent ; c'est précisément la raison pour laquelle ils utilisent l'ingénierie sociale pour cibler les écoles.

En misant à la fois sur le sentiment d'urgence et la naïveté des élèves, ils ouvrent la porte à d'innombrables malveillances.

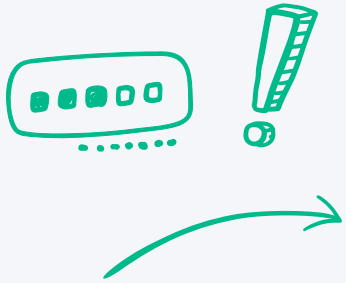
Dans cet e-book, nous abordons :

- **Ce qu'est l'ingénierie sociale**
- **Les tactiques courantes**
- **Ses manifestations dans les établissements d'enseignement primaire et secondaire**
- **Les outils et les techniques pour prévenir les attaques**

Qu’est-ce que l’ingénierie sociale ?

L’ingénierie sociale utilise des tactiques psychologiques pour inciter les utilisateurs à divulguer des informations sensibles. Elle peut être utilisée seule : c’est le cas, par exemple, lorsqu’un site web malveillant imite une page de connexion familière pour dérober des identifiants. Mais elle peut également être couplée à d’autres vecteurs, notamment en implantant des logiciels malveillants.

L’ingénierie sociale cible l’élément humain de votre posture de sécurité. Ce phénomène est extrêmement courant ; il **dépasse même les autres vecteurs d’attaque d’au moins 45 %**, selon le **Rapport 2025 du CIS MS-ISAC sur la cybersécurité dans l’enseignement primaire et secondaire : l’alliance de l’éducation et de la résilience communautaire.**



Pourquoi l'ingénierie sociale est-elle un enjeu pour les équipes informatiques ?

Pour dire les choses simplement, elle rend votre école vulnérable aux attaques.
Quelques sujets de réflexion :

Contournement des contrôles :

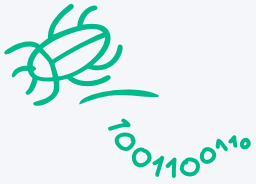
si vos configurations informatiques et vos mesures de protection ne tiennent pas compte de l'ingénierie sociale, elles pourront être contournées. En effet, lorsqu'un pirate dispose d'identifiants légitimes, son infiltration ne déclenchera aucune alerte en l'absence d'outils dédiés.

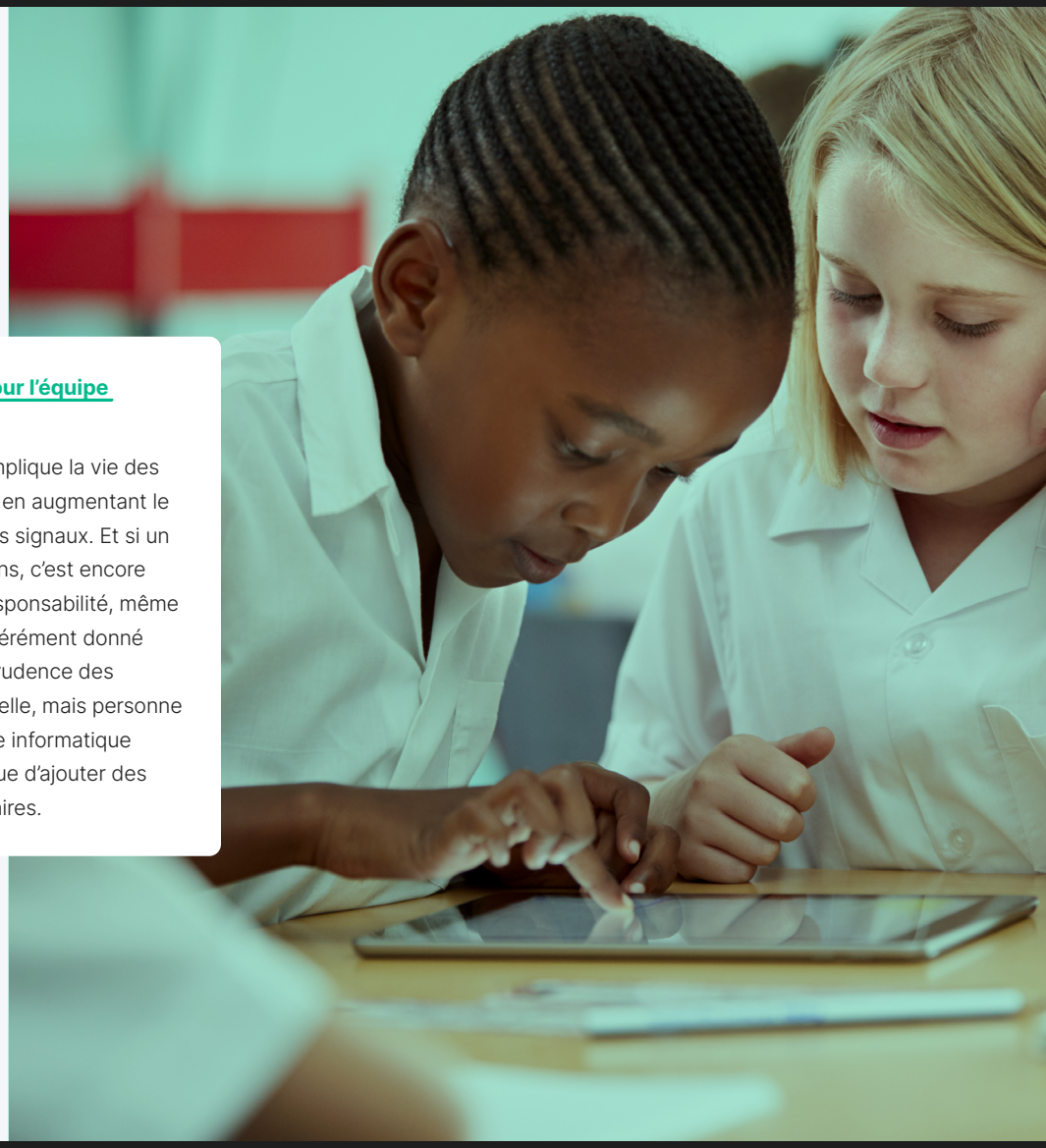
Danger des mouvements latéraux :

un seul compte compromis peut ouvrir la porte à tous vos systèmes, y compris les plus sensibles, et ainsi augmenter l'ampleur des perturbations.

Une lourde charge pour l'équipe informatique :

l'ingénierie sociale complique la vie des équipes informatiques en augmentant le bruit et en brouillant les signaux. Et si un pirate parvient à ses fins, c'est encore sur elle que pèse la responsabilité, même si un utilisateur a délibérément donné ses informations. La prudence des utilisateurs est essentielle, mais personne n'est parfait. Le service informatique n'a pas d'autre choix que d'ajouter des défenses supplémentaires.





Tactiques courantes d'ingénierie sociale

Hameçonnage

L'hameçonnage est une forme courante d'ingénierie sociale. Les pirates se font passer pour des membres du personnel ou des services de l'école, imitent des sites web légitimes et suscitent un sentiment d'urgence pour amener les utilisateurs à donner leurs informations.

Publicité malveillante

La publicité malveillante, ou malvertising, prend la forme d'annonces en ligne trompeuses qui incitent l'utilisateur à télécharger des logiciels malveillants ou à livrer ses identifiants.

Faux SMS

Les faux SMS revêtir plusieurs formes, mais ils servent généralement à gagner la confiance d'un utilisateur. Les attaquants peuvent se faire passer pour une figure d'autorité ou un collègue pour le rassurer et l'amener à divulguer ses informations.

Appât

L'appât attire les utilisateurs avec des propositions irrésistibles : argent facile, reconnaissance, contenu exclusif, etc. Mais en cliquant sur le lien qu'on leur indique, les utilisateurs installent des logiciels malveillants ou sont redirigés vers des sites d'hameçonnage.

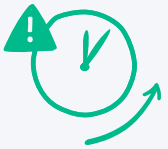
Empoisonnement du référencement

Les attaquants achètent des encarts publicitaires sur les moteurs de recherche pour mettre leurs sites contrefaits en tête des résultats de recherche et attirer les utilisateurs peu méfiants.

Avalanche de notifications

Les attaquants envoient une série de demandes d'authentification multifacteur pour user la patience de l'utilisateur et l'inciter à céder.

Ces techniques existent depuis longtemps. Ce qui est nouveau, en revanche, c'est l'impact de l'IA. Cette technologie change totalement la donne. Dans son **Rapport sur le coût d'une violation de données 2025,** IBM a observé qu'une violation de données sur six impliquait des attaques pilotées par l'IA.



Grâce à l'**IA générative**, les attaquants peuvent ***« faire passer le temps nécessaire à la création d'un e-mail d'hameçonnage convaincant de 16 heures à 5 minutes seulement ».***

L'IA permet d'élaborer rapidement des attaques d'hameçonnage et des deepfakes particulièrement convaincants. Les établissements scolaires doivent impérativement tenir compte de ces avancées, d'autant plus efficaces lorsqu'elles visent de jeunes utilisateurs.

Manifestations de l'ingénierie sociale dans les établissements d'enseignement primaire et secondaire

L'ingénierie sociale est employée dans toutes sortes de cyberattaques. Selon le **Rapport sur les enquêtes relatives aux violations de données 2025 de Verizon**, des techniques d'ingénierie sociale étaient utilisées dans **17 % des attaques ciblant le secteur de l'éducation**.

Les techniques elles-mêmes peuvent varier, car l'ingénierie sociale prend de nombreuses formes et évolue constamment.
Voici quelques scénarios possibles :

Les jeux en ligne ? Ils cachent parfois des pièges.

Un collégien navigue sur Internet à la recherche de jeux après avoir terminé ses devoirs. Il visite un site web qui lui propose de la monnaie gratuite pour son jeu en ligne préféré. La tentation est irrésistible : il clique sur le lien et arrive sur une page qui lui promet une belle somme virtuelle en échange de ses identifiants de connexion.

Il y a parfois du bon à regarder les dents du cheval qu'on veut vous donner

Votre nouvel enseignant tient à démontrer sa bonne volonté aux administrateurs de l'école. À tel point que lorsque son « principal » lui envoie un e-mail pour lui demander des codes de cartes-cadeaux, il n'hésite pas un instant. Il n'a pas assez d'expérience dans l'établissement pour reconnaître que son principal ne s'exprime ***pas tout à fait*** comme l'auteur de cet e-mail.

Vrai ou faux : ce téléchargement est sûr

(spoiler : c'est faux)

Une lycéenne se prépare à passer des examens d'entrée pour une grande école. Elle se met en quête de ressources pour mieux se préparer. En haut des résultats de recherche, un lien sponsorisé propose des tests d'entraînement gratuits. Il lui suffit de télécharger l'application de préparation, qui – ô surprise – contient un logiciel malveillant.

Ta popularité va grimper en flèche… quand tes données auront fuité.

Un groupe d'élèves de primaire reçoit un e-mail au sujet d'un concours de popularité : « Vote pour l'élève le plus populaire et tente de gagner la première place ! Nous avons simplement besoin de vérifier que tu es bien un élève de ton école ; peux-tu nous fournir quelques informations personnelles ? »

Neutraliser l'ingénierie sociale

Que pouvez-vous faire pour empêcher l'ingénierie sociale d'exploiter vos utilisateurs et de menacer la sécurité de vos données ? Vous devez l'aborder sous deux angles : **vos utilisateurs et votre infrastructure technologique.**

Sensibilisation des utilisateurs

Vos utilisateurs, en particulier les plus jeunes, n'ont pas encore découvert tous les bons et mauvais côtés d'Internet. Ils n'ont pas encore pris l'habitude de remettre en question ce qu'ils voient en ligne. Idéalement, les enjeux de citoyenneté numérique devraient faire partie du programme scolaire de votre école. La citoyenneté numérique vise à donner aux élèves les compétences nécessaires pour utiliser Internet de manière responsable et sûre.

Elle englobe plusieurs aspects :

- Fournir des **explications adaptées à l'âge** sur les cybermenaces courantes
- Proposer des **exemples** de sites web et de contenus suspects
- Encourager un **comportement** éthique et responsable en ligne

Naturellement, le corps enseignant et le personnel administratif ont, eux aussi, besoin de formation. Quelques pistes :

- Simulations d'e-mails **d'hameçonnage**
- **Formation** de conformité régulière et obligatoire
- **Culture de la transparence** : les utilisateurs doivent se sentir libres de parler à l'équipe informatique s'ils craignent d'avoir été victimes d'une attaque d'ingénierie sociale.

Les outils technologiques et les règles, une autre ligne de défense

Les attaquants ciblent l'élément humain pour une bonne raison : il demande moins d'outils techniques et le taux de réussite est plus élevé. Et comme nous sommes tous faillibles, nous avons besoin d'une protection supplémentaire.

Filtrage de contenu

Le filtrage de contenu bloque les contenus malveillants, même si l'utilisateur final clique sur un lien malveillant. Vous pouvez filtrer le contenu à l'aide de listes d'autorisation et de blocage, qui définissent explicitement les sites web autorisés ou non. Mais cette pratique a ses limites. Il est impossible d'autoriser tous les sites utiles, comme de bloquer tous les sites malveillants. Et ce n'est pas dans cet Internet que navigueront les élèves une fois qu'ils auront quitté l'école.

Le filtrage par catégorie s'avère plus efficace. Il ne s'agit plus de dresser une liste de domaines. Ce filtrage classe les sites web par catégorie, et c'est sur cette base qu'il décide de le bloquer ou non. Les sites pour adultes, les sites de jeux d'argent, les partages de fichiers, les réseaux sociaux, les sites violents ou offensants, etc., peuvent ainsi être bloqués en fonction de votre configuration. Vous pouvez même ajouter de l'IA et de l'apprentissage automatique pour un filtrage intelligent et optimisé.

Authentification multifacteur

L'authentification multifacteur, ou MFA, ajoute une couche supplémentaire de protection au moment de la connexion. Si les identifiants d'un utilisateur sont compromis, l'authentification MFA réduit le risque qu'un attaquant accède effectivement à son compte. La MFA exige au moins deux méthodes d'authentification parmi les catégories suivantes :

- **Une information que vous connaissez,** comme un mot de passe, un code PIN ou une question de sécurité
- **Une caractéristique de ce que vous êtes,** comme votre empreinte digitale ou votre visage
- **Un objet que vous possédez,** comme un autre appareil ou une clé de sécurité

Les outils technologiques et les règles, une autre ligne de défense

Authentification par signature unique (SSO)

Ajoutez un fournisseur d'identité (IdP) à votre infrastructure technologique pour mettre en place une véritable authentification par signature unique : un seul mot de passe indique à votre IdP qu'il peut ouvrir l'accès à ***tous*** les comptes d'un utilisateur. Comme les utilisateurs ont moins de mots de passe à retenir, le risque de compromission est plus faible. Mais est-ce que cela ne signifie pas aussi que les attaquants n'ont besoin que d'un seul mot de passe pour se connecter à tout ?

Ce n'est pas le cas, fort heureusement : l'authentification SSO s'appuie généralement sur la MFA. Vous pouvez la configurer de manière à demander des données biométriques, comme l'empreinte digitale de l'élève. En plus d'éviter la lassitude liée à la multiplication des mots de passe et de réduire le nombre de points d'entrée possibles, l'authentification SSO contribue aussi à prévenir le vol d'identifiants. Supposons qu'un utilisateur final se retrouve sur un site contrefait : comme votre IdP ne reconnaît pas le nom de domaine, il n'autorisera pas l'utilisateur à se connecter ni à exposer ses identifiants.

Gestion des appareils

Tous les outils que nous avons mentionnés sont très performants. Mais ils sont difficiles à mettre en œuvre sans gestion des appareils mobiles (MDM). Avec une solution MDM, les administrateurs informatiques peuvent :

- Obtenir une visibilité sur la posture de sécurité de leurs appareils
- Définir des règles de sécurité et des configurations sécurisées
- Configurer les paramètres et les restrictions de l'appareil, pour imposer un code d'accès obligatoire ou installer certaines applications.
- Maintenir les appareils et les applications à jour
- Déployer des solutions de filtrage de contenu

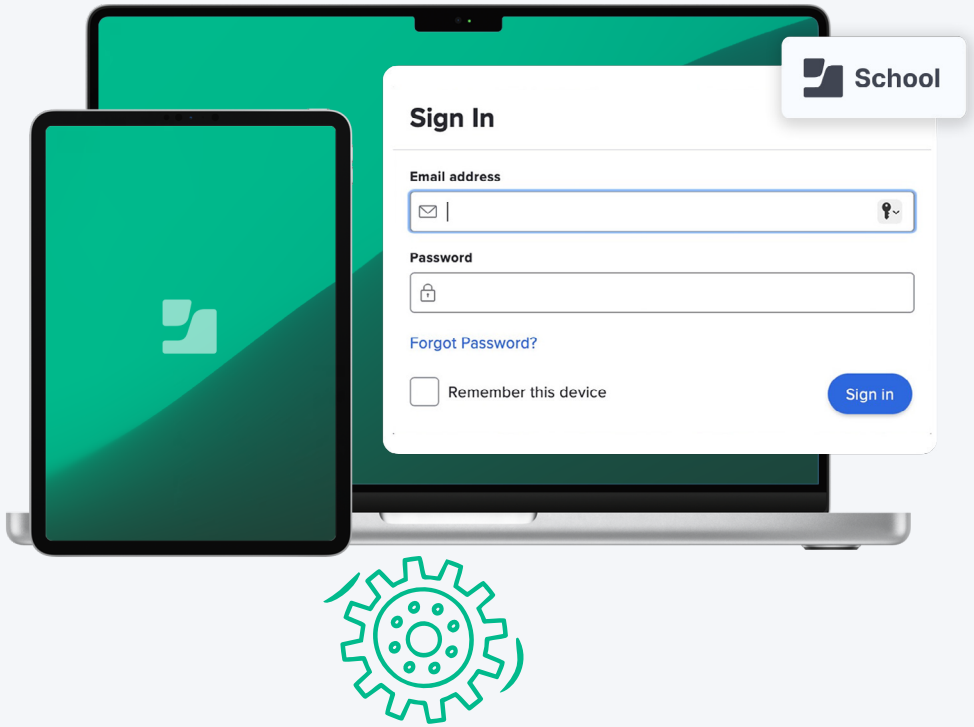
Mise en œuvre : Jamf School et Jamf Safe Internet

Jamf School

Jamf School est une solution MDM conçue pour les écoles.
Elle offre de nombreuses possibilités :

- **Configuration de l'appareil à l'aide de modèles** qui tirent parti de la gestion déclarative de l'appareil
- **Inventaire des appareils** qui indique aux administrateurs sachent quels appareils sont connectés aux ressources de l'école
- **Visibilité totale** sur l'état des appareils, afin de résoudre rapidement le moindre problème
- Possibilité de **définir des restrictions** et d'appliquer des **réglages** sur un appareil, notamment pour exiger la création d'un code secret
- **Compatibilité avec l'authentification SSO** (avec un fournisseur d'identité supplémentaire)
- **Un moyen simple** pour les enseignants de demander des applications au service informatique
- Et bien plus **encore** !

Avec Jamf School, votre établissement dispose d'une base d'appareils sécurisés qui peuvent être configurés pour résister aux attaques d'ingénierie sociale.

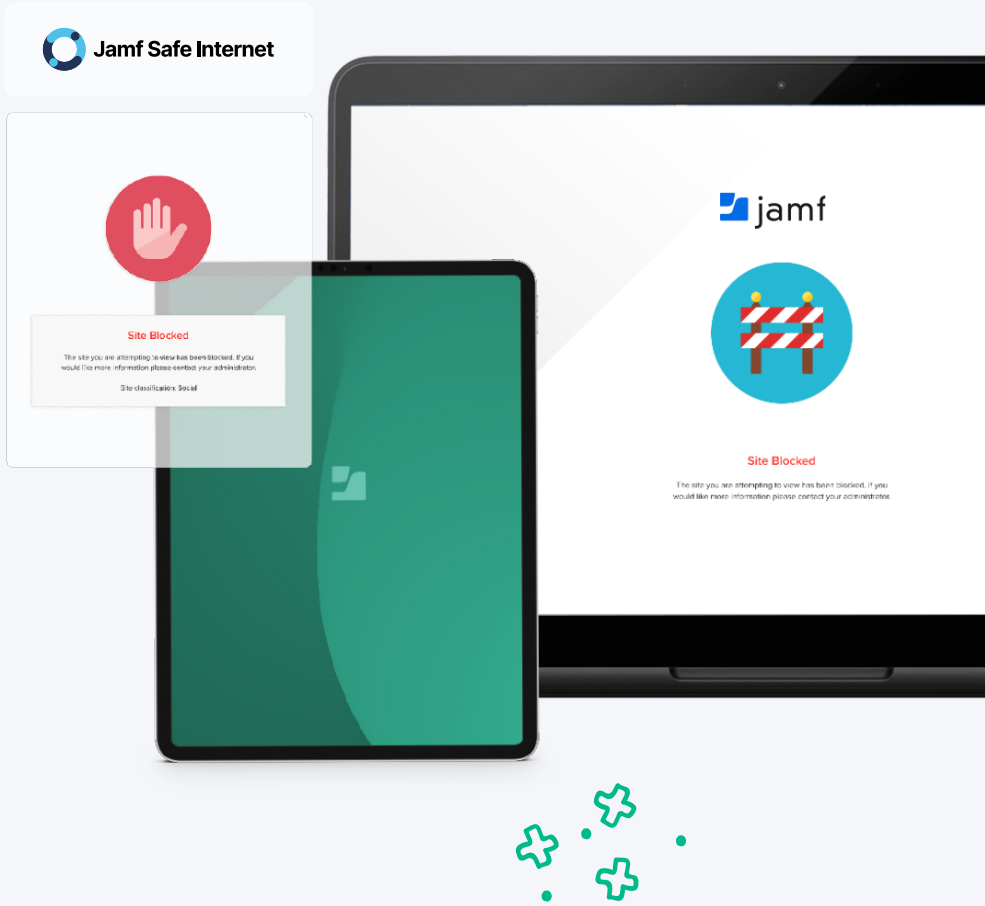


Jamf Safe Internet

Jamf Safe Internet apporte une couche de sécurité supplémentaire et est compatible avec les appareils Apple, Chromebook et Windows. Entièrement personnalisable, Jamf Safe Internet permet de définir et de modifier facilement des règles qui vont s'appliquer à différents groupes d'appareils en fonction de leur localisation, de leur type ou d'autres critères. Cet outil fonctionne avec tous les types d'appareils : appareils partagés, appareils individuels et appareils personnels utilisés à l'école.

Pour se défendre contre les menaces telles que l'ingénierie sociale, **Jamf Safe Internet offre** :

- **Un filtrage de contenu puissant** enrichi par IA et ML, qui bloque l'accès aux sites web d'hameçonnage avant même qu'ils ne soient identifiés comme malveillants.
- **Le blocage des DNS** et des **noms de domaine** pour se défendre contre l'usurpation de DNS
- **Le filtrage de contenu sur l'appareil** (iPad) pour un filtrage effectif partout
- **La protection sur le réseau** qui bloque les sites Web malveillants avant qu'ils ne puissent nuire aux appareils.
- L'utilisation obligatoire de **Google SafeSearch** et **Google Safe Browsing** pour empêcher les sites malveillants ou inappropriés d'apparaître dans les recherches.



Sécurité sans surveillance : les élèves sont libres de naviguer sur Internet et de développer leur citoyenneté numérique sans exposer leur vie privée. Avec une technologie fiable et sécurisée dans la salle de classe, tout le monde est gagnant :

Les enseignants
peuvent se concentrer sur leurs cours sans rencontrer de problèmes de connexion ni de perturbations.

Les élèves
sont libres d'explorer et d'apprendre en toute sécurité.

Les administrateurs informatiques
peuvent se consacrer à d'autres tâches en sachant que les données sont à l'abri.

Vous voulez savoir ce que la technologie peut apporter à votre école ?

Essayez Jamf