



Cybersécurité dans les écoles

Protéger les étudiants
à l'ère numérique



Aperçu

Les écoles adoptent de plus en plus d'outils numériques tels que les plateformes d'apprentissage, les classes virtuelles et les appareils connectés, et la technologie devient un élément central de l'éducation moderne. Cependant, la transformation numérique rapide du 21^e siècle introduit également de nouveaux risques de cybersécurité que les enseignants ne peuvent pas se permettre d'ignorer.

Le rapport 2024 Keeper Security, issu d'une étude menée auprès de 6 000 personnes en Australie, en Nouvelle-Zélande, à Singapour, en Indonésie, au Japon, en France, au Royaume-Uni, aux États-Unis et dans la région DACH, réparties équitablement entre les étudiants âgés de plus de 16 ans, les parents et la population en général, met en évidence un écart critique entre la confiance et la réalité en ce qui concerne la capacité des écoles à protéger les étudiants à l'ère numérique.

Alors que de nombreux parents pensent que les écoles protègent les informations sensibles, les problèmes persistants tels que des mots de passe faibles ou réutilisés et une formation limitée en matière de cybersécurité exposent les élèves à des menaces persistantes, telles que les violations de données, l'usurpation d'identité et la fraude. Les résultats soulignent la nécessité urgente pour les écoles et les familles de collaborer à la mise en place de mesures de sécurité numérique plus strictes et de sensibiliser les élèves aux risques en ligne.



Les pratiques actuelles en matière de cybersécurité dans les écoles

L'enquête de Keeper Security met en évidence un paysage contrasté en matière de pratiques de cybersécurité dans les écoles. Si 74 % des parents font confiance à l'école de leur enfant pour protéger leurs informations sensibles, cette confiance ne correspond pas aux pratiques scolaires. Seuls 21 % des parents déclarent que leur école fournit des conseils sur la création et la gestion de mots de passe sécurisés, ce qui contribue à l'apparition d'habitudes dangereuses en matière de mots de passe. En effet, 19 % des personnes interrogées admettent qu'elles réutilisent les mots de passe de leurs comptes personnels et scolaires, ce qui accroît le risque d'une violation généralisée.

Taux de confiance dans les mesures de cybersécurité scolaires



18%
Confiance très forte



56%
Confiance moyenne



22%
Confiance faible



4%
Pas de confiance du tout

Pratiques actuelles de gestion des mots de passe

21%

Écoles fournissant des conseils sur les mots de passe sécurisés

19%

Réutilisation des mots de passe entre comptes

9%

Écoles offrant un accès à un gestionnaire de mots de passe

La disponibilité limitée de gestionnaires de mots de passe numériques sécurisés (seulement 9 % des écoles y ont accès), exacerbe encore ces risques. Les gestionnaires de mots de passe, qui sont essentiels pour générer et stocker en toute sécurité des mots de passe complexes, et qui sont recommandés par les organismes gouvernementaux et les experts en cybersécurité, sont notamment absents, ce qui constitue une opportunité évidente pour les écoles d'améliorer de manière significative leurs pratiques en matière de cybersécurité.

La nécessité d'améliorer l'éducation à la cybersécurité

L'éducation à la cybersécurité dans les écoles est dangereusement rare : seules 14 % des écoles rendent obligatoire la formation de sensibilisation à la sécurité, et 13 % la proposent à titre facultatif. Cette portée limitée de la formation obligatoire signifie que de nombreuses familles ne reçoivent pas les dernières informations sur la sécurité en ligne, ce qui rend les élèves vulnérables à l'évolution des cybermenaces. Une formation efficace à la cybersécurité ne doit pas seulement porter sur la manière d'identifier les escroqueries par phishing, les mesures de protection des appareils et l'importance des mises à jour logicielles régulières, mais aussi sur la gestion en toute sécurité de l'empreinte numérique des élèves.

Enseigner aux élèves les conséquences de leurs activités en ligne, telles que leurs publications sur les réseaux sociaux et leurs habitudes de navigation, est essentiel pour les aider à protéger leurs informations personnelles. Par exemple, l'éducation à la cybersécurité devrait souligner l'importance d'ajuster les paramètres de confidentialité sur les plateformes de réseaux sociaux afin de limiter l'exposition du public. Pour encourager un comportement responsable en ligne, il est essentiel d'expliquer aux élèves comment des acteurs malveillants peuvent exploiter leurs empreintes numériques pour commettre de futures usurpations d'identité ou des attaques ciblées.

Formation à la cybersécurité dans les écoles

21%

Méconnaissance des attentes de l'école en matière de cybersécurité

20%

Personnellement responsable de la cybersécurité

14%

Formation obligatoire

13%

Formation optionnelle

12%

Accès aux ressources de cybersécurité

Impact des cyberincidents sur les écoles

Les cyberattaques contre les établissements d'enseignement peuvent avoir des répercussions graves et profondes pour les élèves, les enseignants et les administrateurs, ce qui souligne la nécessité de mettre en place des mesures de sécurité robustes pour protéger les comptes et les données sensibles.

Selon l'enquête, si seulement 7 % des personnes interrogées déclarent que l'établissement d'enseignement de leur enfant, ou le leur, a été hacké, les conséquences ont été importantes. Interrogés sur les effets de ces violations, les répondants ont indiqué les impacts suivants:



32%

Vol de données



24%

Vol d'identité



26%

identifiants volés



27%

**Comptes
compromis**



16%

**Impact financier
pour l'école**



14%

**Impact financier
pour les étudiants/
le personnel**

L'importance du vol de données et d'identité met en évidence les graves implications pour la vie privée et la sécurité organisationnelle. La prévalence des identifiants volés et des comptes compromis illustre les dommages considérables que de telles violations peuvent infliger, entraînant souvent l'exposition d'informations

sensibles. Bien que les conséquences financières soient moins souvent signalées, elles restent importantes pour les écoles et les particuliers, ce qui montre que les cyberattaques peuvent causer des dommages qui vont au-delà des problèmes immédiats liés aux données et à l'identité.

Le rôle des familles dans la cybersécurité



Les parents et les tuteurs jouent un rôle essentiel dans le renforcement des bonnes pratiques de cybersécurité à la maison. Cependant, l'enquête de Keeper révèle que 19 % des familles réutilisent les mots de passe, une pratique dangereuse qui peut entraîner la compromission de plusieurs comptes par des attaques de bourrage d'identifiants. Alors que de nombreuses écoles ne fournissent pas de ressources en matière de cybersécurité, les familles peuvent contribuer à combler le fossé en utilisant des mots de passe forts et uniques et l'authentification multifacteur (MFA). La MFA ajoute une couche de sécurité supplémentaire aux comptes en ligne en exigeant au moins une forme de vérification supplémentaire pour se connecter.

Plus de la moitié (51 %) des personnes interrogées se disent très ou assez préoccupées par la cybersécurité à l'école, ce qui montre que les parents sont conscients des risques, même si les pratiques en matière de cybersécurité ne sont pas toujours à la hauteur. Pour faire face à ces risques, les familles doivent surveiller de manière proactive les activités en ligne de leurs enfants et respecter les bonnes pratiques en matière de cybersécurité à la maison. Il s'agit notamment d'apprendre à reconnaître les e-mails et les liens suspects, d'utiliser des mots de passe forts et uniques, d'activer le MFA sur tous les comptes qui la rendent disponible et de mettre à jour régulièrement les logiciels pour se protéger contre les vulnérabilités connues.

Aller de l'avant : Une approche unifiée de la cybersécurité

Relever le niveau de cybersécurité dans nos écoles nécessite un effort collectif et collaboratif de la part des institutions d'enseignement et des familles des élèves qui les fréquentent. Les écoles doivent améliorer leurs programmes d'éducation à la cybersécurité, intégrer des outils éprouvés tels que les questionnaires de mots de passe et étendre les initiatives de formation pour couvrir les bonnes pratiques en matière de cybersécurité. Les familles doivent soutenir ces efforts en renforçant les bonnes habitudes de cybersécurité à la maison et en participant activement à l'éducation numérique de leurs enfants.

En travaillant ensemble, les écoles et les familles peuvent créer un environnement en ligne plus sûr pour les élèves, en maximisant les avantages des avancées technologiques tout en minimisant les cyber-risques associés.

Méthodologie

Cette enquête en ligne auprès de 6 000 personnes en Australie, en Nouvelle-Zélande, à Singapour, en Indonésie, au Japon, en France, au Royaume-Uni, aux États-Unis et dans la région DACH a été réalisée par la société d'études de marché OnePoll, conformément au code de conduite de la Market Research Society. Cette enquête a été supervisée et éditée par l'équipe de recherche OnePoll. OnePoll est une société partenaire de MRS, membre d'ESOMAR et membre du British Polling Council.