KEEPER®

Cybersécurité à l'école 2025

guide pour les familles et les éducateurs pour un apprentissage numérique plus sûr

Ressource gratuite de Keeper Security | Disponible sur flexyourcyber.com

Présentation

Les salles de classe sont plus connectées que jamais – tout comme les menaces qui pèsent sur elles. Les attaques de ransomware perturbent les districts, les escroqueries générées par l'IA ciblent les étudiants et les campagnes de phishing sont de plus en plus difficiles à détecter. Les plateformes numériques étant désormais au cœur des devoirs, de la collaboration en classe et des opérations administratives, la cybersécurité est devenue une exigence fondamentale de l'enseignement, et non plus une option.

Ce guide offre aux administrateurs, aux éducateurs, aux parents et aux élèves des perspectives d'experts et des étapes concrètes pour renforcer la sécurité numérique. En combinant la sensibilisation, les meilleures pratiques et la communication ouverte, les écoles et les familles peuvent créer des environnements d'apprentissage sécurisés qui protègent à la fois la continuité académique et les données personnelles.

Le paysage des menaces de 2025

Les cyberattaques sur l'éducation s'accélèrent – et l'impact est plus fort que jamais.

- **Les ransomware sont en hausse:** au premier semestre 2025, les attaques contre les écoles, les collèges et les universités ont augmenté de 23 % par rapport à l'année précédente (Comparitech)
- **Les écoles sont des cibles privilégiées:** 82 % des écoles américaines de la maternelle à la 12e année ont été victimes d'au moins un incident cybernétique entre juillet 2023 et décembre 2024 (Center for Internet Security)
- **La pression financière augmente:** la moyenne des demandes de rançon atteint désormais 556 000 dollars (Comparitech)
- **Le phishing est plus difficile à repérer:** les courriels malveillants assistés par l'IA ont doublé au cours des deux dernières années (Verizon DBIR)

Ce qu'il faut retenir: l'éducation est désormais l'un des secteurs les plus ciblés et les attaquants utilisent l'intelligence artificielle pour rendre leurs tactiques plus convaincantes que jamais.

Les 5 principaux risques numériques pour les élèves et les écoles

Identifiants faibles et réutilisés

Les mots de passe recyclés ou prévisibles restent le point d'entrée le plus facile pour les attaquants

Utilisez un gestionnaire de mots de passe pour générer et stocker des identifiants forts et uniques

Comptes partagés et gestion inadéquate des privilèges

Une seule connexion partagée compromise peut exposer des salles de classe, des départements ou même des districts entiers à des attaques

Éliminez les comptes partagés et appliquez l'accès de moindre privilège

Phishing et escroqueries sur les réseaux sociaux

Les cybercriminels exploitent la confiance en se faisant passer pour des membres du personnel, des camarades de classe ou des membres de la famille

Vérifiez les identités par des canaux de confiance avant de partager des informations

Wi-Fi non sécurisé à la maison ou en public

Les réseaux ouverts ou mal protégés permettent aux attaquants d'intercepter des données sensibles

Utilisez un Wi-Fi protégé par mot de passe ou un VPN sur les appareils scolaires

Désinformation et deepfakes basés sur l'IA

Les faux contenus audio et vidéo peuvent manipuler les élèves et le personnel pour les inciter à partager des informations sensibles ou à prendre des mesures préjudiciables

Formez les utilisateurs à repérer les signaux d'alarme et encouragez-les à signaler lorsqu'ils ont un doute

Le guide de la cybersécurité: stratégies et outils

Pour les écoles

- [ ] Appliquez des politiques de mots de passe forts et une authentification multifactorielle (MFA)
- [ ] Mettez en œuvre la gestion des accès privilégiés (PAM) pour sécuriser les systèmes critiques
- [ ] Fournissez une formation continue en cybersécurité à l'ensemble du personnel
- [ ] Effectuez des évaluations régulières des vulnérabilités et maintenez un plan clair de réponse aux incidents
- [ ] Sauvegardez régulièrement les données critiques et testez les processus de restauration
- [ ] Auditez les fournisseurs et partenaires tiers pour vérifier leurs pratiques de conformité et de sécurité

Pour les parents

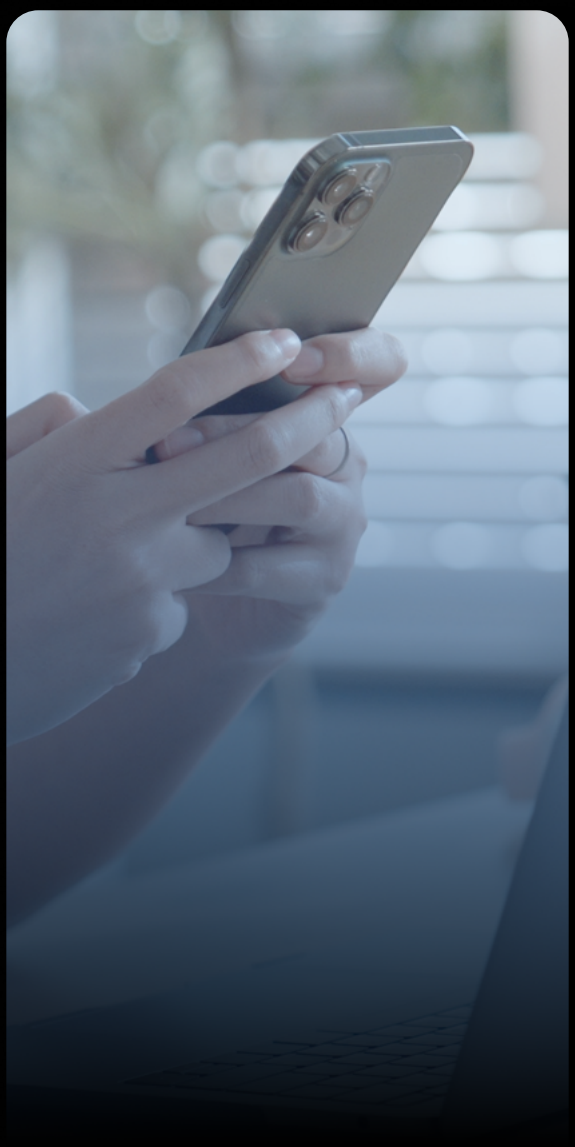
- [ ] Sécurisez vos appareils domestiques avec des mots de passe forts et uniques
- [ ] Activez les mises à jour logicielles automatiques
- [ ] Surveillez l'activité en ligne et encouragez des habitudes de navigation responsables
- [ ] Utilisez les contrôles parentaux pour limiter les contenus et téléchargements risqués
- [ ] Donnez l'exemple d'un comportement numérique sûr en adoptant une bonne hygiène des mots de passe

Pour les étudiants

- [ ] Gardez vos mots de passe privés, même de vos amis
- [ ] Évitez de cliquer sur des liens inconnus ou de télécharger des fichiers non vérifiés
- [ ] Soyez prudent lorsque vous partagez des informations personnelles en ligne
- [ ] Exprimez-vous si quelque chose en ligne vous semble suspect ou inconfortable
- [ ] N'ignorez pas les rappels de mise à jour des logiciels et des appareils

Démarreurs de conversation parent-enfant sur le cyberespace

- [ ] « Que feriez-vous si quelqu'un vous demandait votre mot de passe ? »
- [ ] « Comment savoir si un message ou une vidéo est authentique ? »
- [ ] « Pourquoi devriez-vous utiliser des mots de passe différents pour les comptes différents ? »
- [ ] « Que feriez-vous si vous voyiez quelque chose en ligne qui vous mettait mal à l'aise ? »
- [ ] « Pourquoi est-il important de demander avant de télécharger une nouvelle application ou un nouveau jeu ? »



Le facteur IA
les escroqueries sont la nouvelle norme

Les outils d'IA permettent désormais aux cybercriminels de lancer des attaques avec un réalisme alarmant. Le clonage vocal et les deepfakes peuvent usurper l'identité de personnes de confiance. Les e-mails de phishing améliorés par l'IA sont plus convaincants et plus difficiles à détecter.

Signes avant-coureurs des arnaques liées à l'IA

- Messages demandant une action immédiate
- Demandes d'argent, de cartes-cadeaux ou d'information personnelle
- Phrases étranges, tons mal assortis ou visuels inhabituels
- Le sentiment général que « quelque chose ne va pas »

Comment réduire le risque

- Utilisez un mot ou une phrase secret de famille pour confirmer les identités
- Mettez fin aux appels suspects et reconnectez-vous en utilisant les numéros officiels
- Limitez la diffusion publique de vidéos et d'enregistrements vocaux

Construisons ensemble la confiance en matière de cybersécurité

L'apprentissage numérique est là pour durer, tout comme les risques. Mais grâce à la sensibilisation, à la préparation et aux bons outils, les écoles et les familles peuvent garder une longueur d'avance sur les cybercriminels. Il est essentiel d'adopter des habitudes sûres, de maintenir la communication ouverte et de rester vigilant pour créer des salles de classe et des foyers plus sûrs.

La cybersécurité n'est pas seulement l'affaire des services informatiques, c'est la responsabilité de chacun.

Éléments clés

- **L'éducation est désormais une cible cybernétique de premier plan**
  Les attaquants savent que les écoles disposent souvent de budgets et de personnel informatique limités, mais qu'elles détiennent des données sensibles précieuses
- **La cybersécurité s'étend au-delà de la salle de classe**
  Les parents et les étudiants jouent un rôle tout aussi essentiel que les administrateurs dans la réduction des risques grâce à des habitudes numériques sûres
- **L'IA change la donne**
  Les deepfakes et le phishing piloté par l'IA sont là pour rester – ce qui fait de la vérification, du scepticisme et des meilleures pratiques en matière de cybersécurité des compétences essentielles pour les familles et les écoles
- **La résilience dépend des personnes, pas seulement de la technologie**
  Des défenses solides combinent des garanties techniques (authentification multifactorielle, PAM, réseaux sécurisés) avec une formation, une communication et des politiques claires
- **La confiance en cybersécurité se construit ensemble**
  Les conversations ouvertes entre les éducateurs, les parents et les élèves renforcent la confiance et créent une culture commune de la sécurité

Trouvez plus de ressources sur flexyourcyber.com