KEEPER®

Cybersecurity in Schools 2025

A Family and Educator Guide to Safer Digital Learning

Free resource from Keeper Security | Available at flexyourcyber.com

Overview

Classrooms are more connected than ever – and so are the threats against them. Ransomware attacks are disrupting districts, AI-generated scams are targeting students and phishing campaigns are becoming harder to detect. With digital platforms now central to homework, classroom collaboration and administrative operations, cybersecurity has become a fundamental requirement of education, and not an option.

This guide provides administrators, educators, parents and students with expert insights and actionable steps to strengthen digital safety. By combining awareness, best practices and open communication, schools and families can create secure learning environments that safeguard both academic continuity and personal data.

The 2025 Threat Landscape

Cyber attacks on education are accelerating – and the impact is hitting harder than ever.

- **Ransomware is rising:** In the first half of 2025, attacks on schools, colleges and universities surged 23% year over year (Comparitech)
- **Schools are prime targets:** 82% of U.S. K–12 schools experienced at least one cyber incident between July 2023 and December 2024 (Center for Internet Security)
- **Financial pressure is growing:** Average ransom demands now reach $556,000 (Comparitech)
- **Phishing is harder to spot:** AI-assisted malicious emails have doubled in the past two years (Verizon DBIR)

The takeaway: education is now one of the most targeted industries, and attackers are using AI to make their tactics more convincing than ever.

Top 5 Digital Risks Facing Students and Schools

Weak and Reused Credentials

Recycled or predictable passwords remain the easiest entry point for attackers.

Use a password manager to generate and store strong, unique credentials.

Shared Accounts and Poor Privilege Control

A single compromised shared login can expose entire classrooms, departments or even districts to attack.

Eliminate shared accounts and enforce least-privilege access.

Phishing and Social Media Scams

Cybercriminals exploit trust by impersonating staff, classmates or family members.

Verify identities through trusted channels before sharing information.

Unsecured Wi-Fi at Home or in Public

Open or poorly protected networks allow attackers to intercept sensitive data.

Use password-protected Wi-Fi or a VPN on school devices.

AI-Powered Misinformation and Deepfakes

Fake audio and video content can manipulate students and staff into sharing sensitive information or taking harmful actions.

Train users to spot red flags and encourage reporting when something feels off.

The Cybersecurity Playbook: Strategies and Tools

For Schools

- [ ] Enforce strong password policies and Multi-Factor Authentication (MFA)
- [ ] Implement Privileged Access Management (PAM) to secure critical systems
- [ ] Provide ongoing cybersecurity training for all staff
- [ ] Conduct regular vulnerability assessments and maintain a clear incident response plan
- [ ] Back up critical data regularly and test restoration processes
- [ ] Audit third-party vendors and partners for compliance and security practices

For Parents

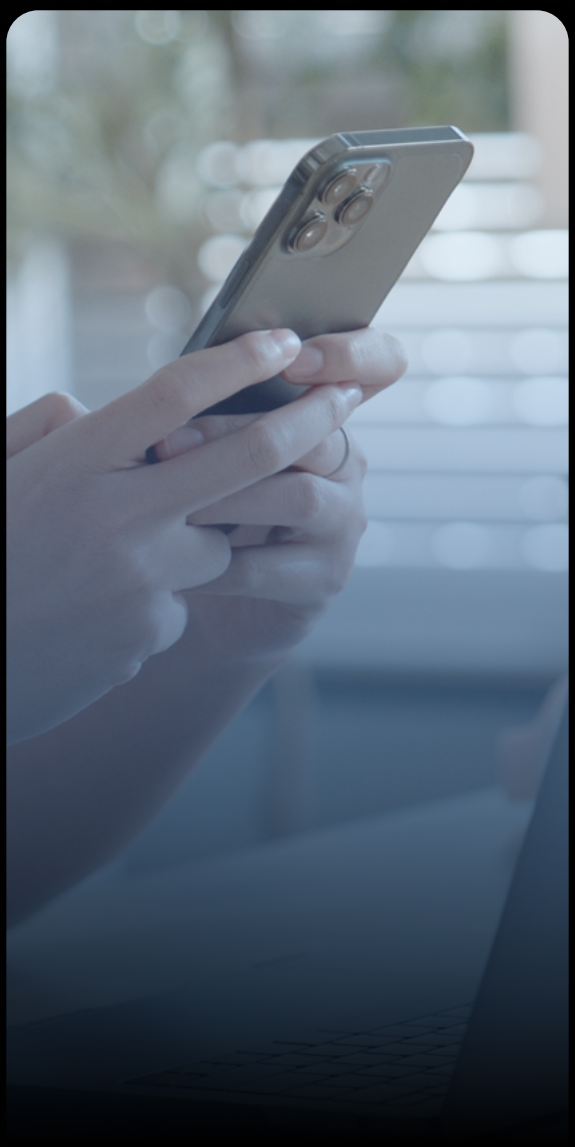
- [ ] Secure home devices with strong, unique passwords
- [ ] Enable automatic software updates
- [ ] Monitor online activity and encourage responsible browsing habits
- [ ] Use parental controls to limit risky content and downloads
- [ ] Model safe digital behavior by practicing good password hygiene

For Students

- [ ] Keep passwords private, even from friends
- [ ] Avoid clicking on unknown links or downloading unverified files
- [ ] Be cautious when sharing personal details online
- [ ] Speak up if something online feels suspicious or uncomfortable
- [ ] Don't ignore reminders to update software and devices

Parent-Child Cyber Conversation Starters

- [ ] “What would you do if someone asked for your password?”
- [ ] “How can you tell if a message or video is real?”
- [ ] “Why should you use different passwords for different accounts?”
- [ ] “What would you do if you saw something online that made you uncomfortable?”
- [ ] “Why is it important to ask before downloading a new app or game?”



The AI Factor
Scams Are the New Normal

AI tools now enable cybercriminals to scale attacks with alarming realism. Voice cloning and deepfakes can impersonate trusted individuals. AI-enhanced phishing emails are more convincing and harder to detect.

Red Flags of AI Scams

- Messages urging immediate action
- Requests for money, gift cards or personal information
- Strange phrasing, mismatched tones or unusual visuals
- A general sense that “something isn’t right”

How to Reduce Risk

- Use a family secret word or phrase to confirm identities
- End suspicious calls and reconnect using official numbers
- Limit public posting of videos and voice recordings

Build Cyber Confidence, Together

Digital learning is here to stay and so are the risks. But with awareness, preparation and the right tools, schools and families can stay ahead of cybercriminals. Practicing secure habits, keeping communication open and staying alert are key to creating safer classrooms and homes.

Cybersecurity is not just IT’s job – it’s everyone’s responsibility.

Key Takeaways

- **Education is now a top cyber target.** Attackers know schools often have limited budgets and IT staff, yet hold valuable sensitive data
- **Cybersecurity extends beyond the classroom.** Parents and students play just as critical a role as administrators in reducing risks through safe digital habits
- **AI is changing the game.** Deepfakes and AI-driven phishing are here to stay – making verification, skepticism and cybersecurity best practices essential skills for families and schools alike
- **Resilience depends on people, not just technology.** Strong defenses combine technical safeguards (MFA, PAM, secure networks) with training, communication and clear policies
- **Cyber confidence is built together.** Open conversations between educators, parents and students strengthen trust and create a shared culture of safety

Find more resources at flexyourcyber.com