CSNP
CYBERSECURITY NON-PROFIT

Teacher Cybersecurity Training

Equipping educators with essential knowledge to protect students in our digital world

PROFESSIONAL DEVELOPMENT

CSNP WORKSHOP

Why Cybersecurity Education Matters Now

Student Vulnerability

Students spend 6+ hours daily online, often without understanding digital risks. Their personal data, identity, and wellbeing depend on digital literacy.

Teacher Responsibility

Educators are the frontline defense in protecting student digital safety. Your awareness can prevent incidents before they escalate.

Institutional Risk

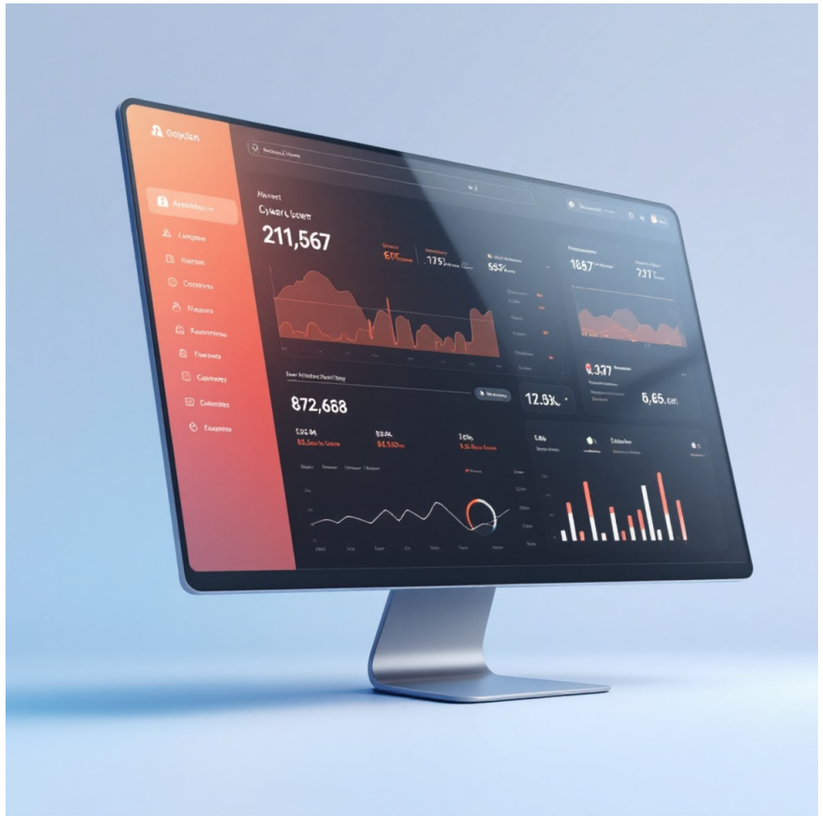
Schools face increasing cyberattacks targeting student records, financial data, and operational systems. K-12 attacks increased 200% in recent years.

The Current Threat Landscape for Schools

Rising Attacks

School districts experience cyberattacks weekly, from ransomware to data breaches. These incidents disrupt learning, compromise student records, and drain limited budgets.

K-12 schools are now the #1 target for ransomware attackers due to limited security resources and valuable student data.



1,200+

School Cyberattacks

Reported incidents in U.S. schools last year

$3.6M

Average Cost

Per incident for school districts

92%

Email-Based

Attacks starting with phishing emails

Understanding Student Digital Behaviors by Age

Elementary (K-5)

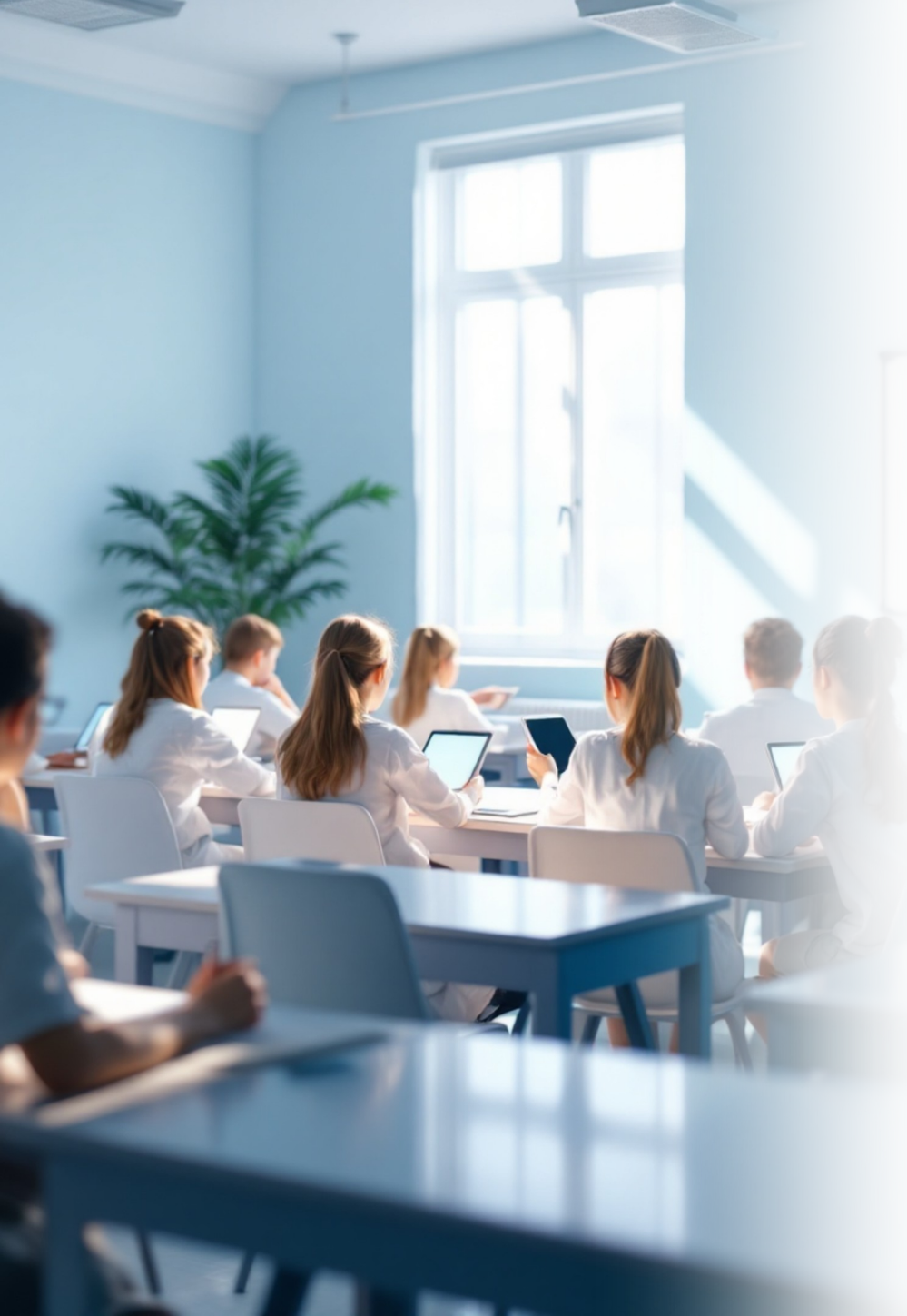
Heavy app and game usage, often sharing devices. Limited password awareness and easily influenced by pop-ups. Vulnerable to inappropriate content exposure.

Middle School (6-8)

Social media emergence, password sharing with friends, peer pressure to join platforms. Increased cyberbullying risk and digital reputation concerns.

High School (9-12)

Sophisticated online presence, multiple platforms, financial app usage. Risk of identity theft, online scams, and permanent digital footprint mistakes.



Classroom Technology Risks You Should Know

Shared Device Dangers

Students forget to log out, leaving accounts accessible. Previous users' saved passwords and browsing history create privacy vulnerabilities and potential embarrassment.

Unsecured Networks

Public Wi-Fi in schools can expose student activity to monitoring. Guest networks without proper segmentation allow unauthorized access to educational systems.

Third-Party Apps

Educational apps often request excessive permissions and may share student data with advertisers. Many free tools monetize through student information collection.

BYOD Challenges

Personal devices on school networks create security gaps. Students may access inappropriate content or download malware that spreads across the network.

Teaching Password Safety That Actually Works

Beyond "Make It Strong"

Students need practical, age-appropriate password strategies they'll actually use:

Passphrases: Teach memorable phrases instead of complex symbols (e.g., "MyDog8PizzaOn Tuesday!")

Unique passwords: Different passwords for each account, especially email and school platforms

Password managers: Introduce secure tools for older students

Two-factor authentication: Add this extra layer whenever possible

> Never share passwords with friends, even your best friend. Accounts are personal responsibility.

1

Create

Long, unique phrases

2

Store

Use secure methods

3

Protect

Never share access

4

Update

Change if compromised

Recognizing and Responding to Cyberbullying

Recognize Signs

Sudden withdrawal, device anxiety, reluctance to go to school, emotional distress after screen time, declining grades

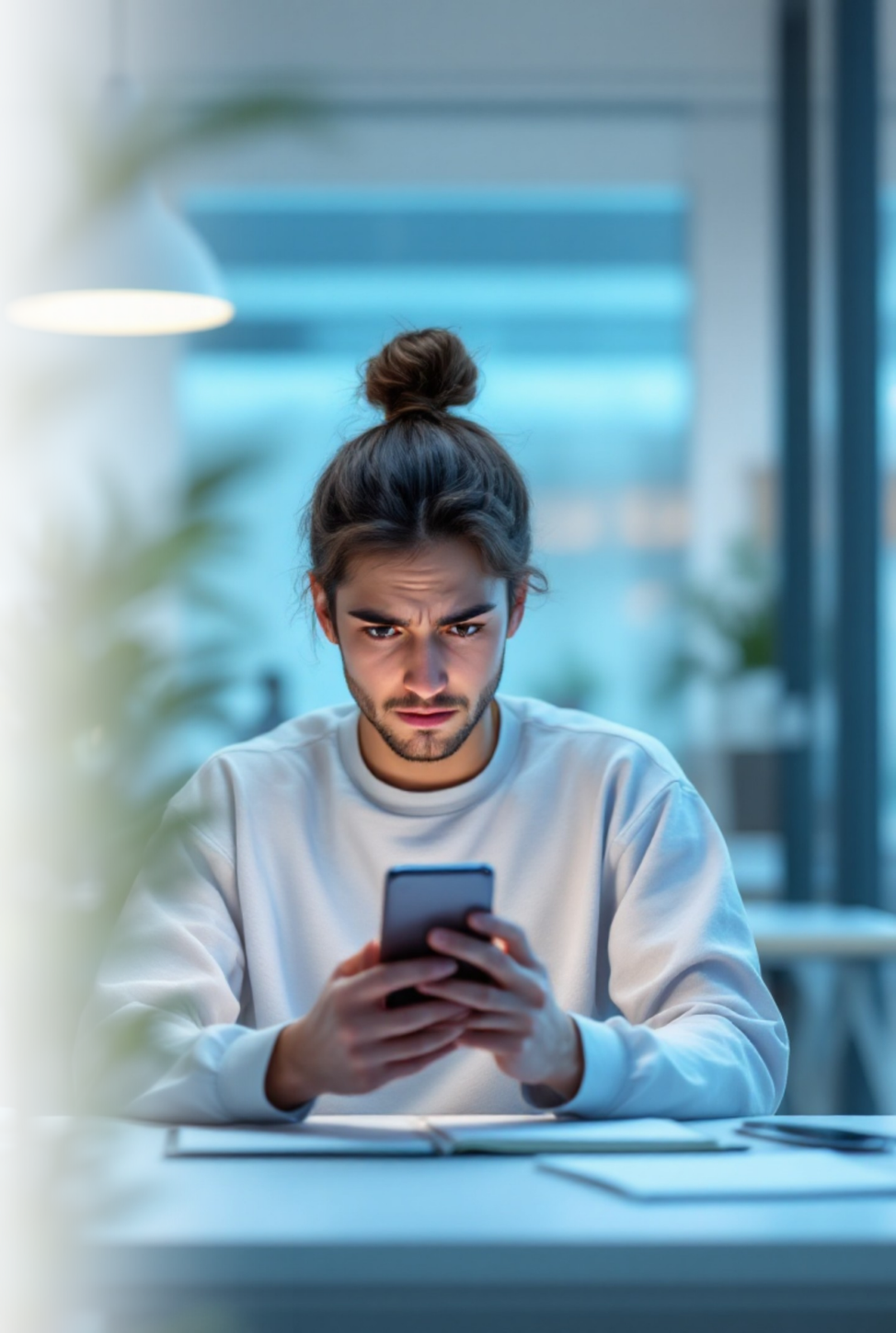
Create Safety

Establish classroom culture of digital respect, make reporting easy and anonymous, validate student concerns seriously

Take Action

Document evidence immediately, involve counselors and administration, contact parents of all parties involved, follow school protocol

Key insight: Cyberbullying is not "just kids being kids online." It has real psychological impacts and requires immediate intervention. Students need to know you take digital harm as seriously as physical harm.



Privacy in Educational Technology

Your Role in Protecting Student Data

Every educational tool you introduce collects student data. Understanding privacy implications is part of professional responsibility.

Before using any new platform:

- Review the privacy policy and data usage terms
- Verify FERPA and COPPA compliance for K-12 use
- Understand what data is collected and shared
- Check if parental consent is required
- Ensure school IT has approved the tool

FERPA Protected

Student educational records require strict confidentiality and secure handling

COPPA Compliance

Students under 13 need parental consent for data collection online

School Policy

Follow district guidelines on approved tools and data sharing

When and How to Report Security Incidents

1

Recognize the Incident

Suspicious emails, unauthorized access attempts, student data exposure, malware infection, lost devices with student information, unusual network activity

2

Immediate Actions

Do not click suspicious links. Disconnect affected devices from network. Preserve evidence (screenshots, emails). Document what happened with timestamps.

3

Report Promptly

Contact IT department immediately. Notify school administration. Complete incident report form. Do not attempt to fix security issues yourself.

4

Follow Through

Cooperate with investigation. Change passwords if compromised. Inform affected students/parents as directed. Participate in post-incident review.

Remember: Reporting quickly prevents bigger problems. There's no penalty for reporting potential threats, even false alarms. Early detection is key.

Integrating Cybersecurity Across Subjects

English & Language Arts

Analyze persuasive techniques in phishing emails, research digital citizenship essays, discuss online reputation in character studies

Mathematics

Calculate encryption strength, analyze data breach statistics, explore probability in password cracking, budget for cybersecurity costs

Social Studies

Examine privacy laws across cultures, study cyber warfare history, debate surveillance vs. freedom, explore digital rights movements

Science

Investigate encryption algorithms, explore biometric security technology, study network infrastructure, analyze cyber forensics methods

Arts

Create cybersecurity awareness posters, design secure password infographics, develop digital citizenship campaigns, produce PSA videos

Health & PE

Address mental health impacts of cyberbullying, discuss online relationship safety, teach digital wellness and screen time balance

Grade-Level Resources for Every Classroom

K-2: Digital Foundations

- Picture-based internet safety stories
- Simple privacy rules (don't share real name/address)
- Recognizing safe vs. unsafe websites
- Asking adults before clicking

3-5: Building Awareness

- Password creation activities and games
- Understanding personal information value
- Identifying trustworthy online sources
- Basic digital footprint concepts

6-8: Critical Thinking

- Social media privacy settings tutorials
- Phishing email identification exercises
- Cyberbullying prevention workshops
- Digital reputation management

9-12: Advanced Skills

- Secure online financial practices
- Career-focused cybersecurity paths
- Legal implications of cyber activities
- Advanced privacy protection strategies

Access all resources: Visit csnp.org/resources for free, ready-to-use lesson plans, activities, and materials for every grade level.

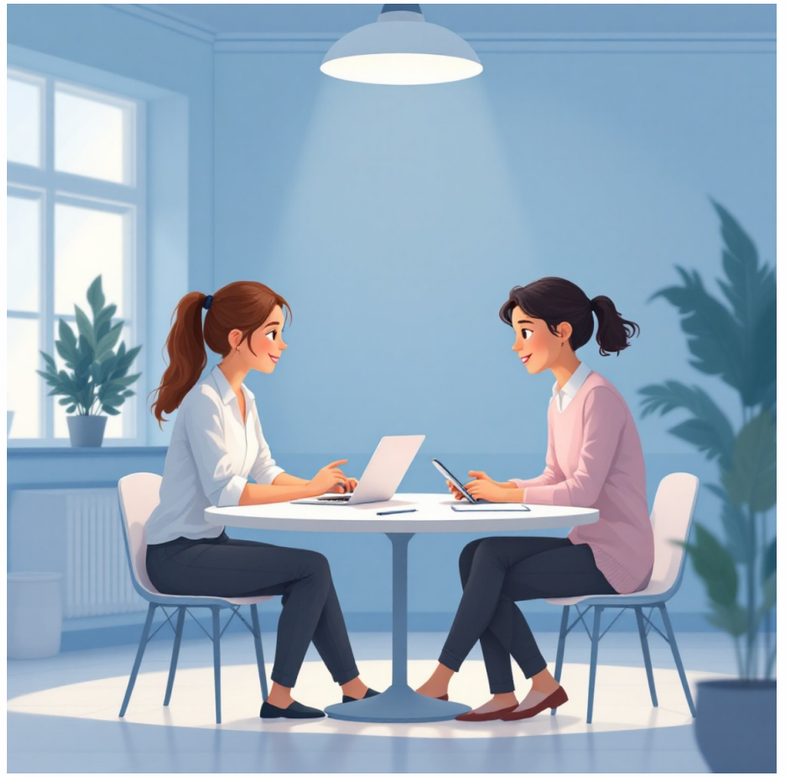
Effective Parent Communication Strategies

Building Home-School Partnerships

Parents are essential partners in student digital safety, but many feel overwhelmed by technology. Your communication can empower them.

Communication approaches that work:

- Monthly newsletter section on digital safety tips
- Quick parent guides for specific tools you use
- Family cybersecurity night events
- Simple tech tutorials in multiple languages
- Open door policy for technology questions



> "Don't assume parents understand the technology. Explain it simply and provide specific action steps they can take at home."

CSNP offers free family cybersecurity resources you can share with parents at csnp.org/resources

Your Cybersecurity Action Plan

This Week

- Review your current classroom technology for privacy compliance
- Update your own passwords using strong passphrase methods
- Identify one cybersecurity topic to integrate into upcoming lessons
- Bookmark csnp.org/resources for quick access to materials

This Month

- Conduct a classroom discussion on digital citizenship
- Send home parent communication about online safety
- Review school incident reporting procedures with IT
- Attend or organize a faculty cybersecurity discussion

This Semester

- Implement cybersecurity concepts in at least three lessons
- Host a family digital safety night or contribute resources
- Evaluate all educational apps for privacy compliance
- Mentor a colleague in digital safety teaching strategies

Ongoing

- Model good digital citizenship daily in your teaching
- Stay informed about new threats and student platforms
- Maintain open communication with students about online concerns
- Share successes and challenges with your teaching community

Key Takeaways for Educators

You Are the First Line of Defense

Your awareness and action directly impact student safety. Every teacher plays a crucial role in creating a secure digital learning environment.

Integration, Not Addition

Cybersecurity doesn't require new curriculum—weave it into existing subjects. Small, consistent conversations build lasting awareness.

Partner with Parents

Digital safety is most effective when reinforced at home. Clear, jargon-free communication empowers families to protect their children.

Resources Are Available

You don't need to be a tech expert. Free, accessible resources at CSNP support your efforts every step of the way.

Start Small, Build Momentum

Choose one action from today's session and implement it this week. Progress compounds—small steps lead to significant cultural change.

About Cybersecurity Non-Profit (CSNP)

"Making cybersecurity knowledge accessible to everyone through education, community, and practical resources."

Our Free Programs for Every Community

- **Business & Non-Profit Security**

  Practical cybersecurity guidance for organizations of all sizes, helping protect operations and stakeholder data

- **Family Cybersecurity**

  Comprehensive resources to help families navigate digital safety together and build healthy online habits

- **Kids Safety**

  Age-appropriate education empowering children to make safe choices in their digital interactions

- **Senior Digital Safety**

  Specialized support helping older adults protect themselves from targeted scams and fraud

- **Women's Security**

  Addressing unique digital safety challenges and providing tools for personal security online

- **Parents & Educators**

  Everything you need to teach and reinforce cybersecurity at home and in the classroom

Everything We Offer Is Completely Free

Because everyone deserves access to cybersecurity knowledge and protection.

Visit csnp.org

Access Resources