Introduction

Cybersecurity has become a critical part of every school's responsibility to protect students, staff, and institutional data.
While schools often operate with limited IT resources, they are frequently targeted by cybercriminals seeking access to personal information or to disrupt learning.
This guide provides practical steps to strengthen your school's cybersecurity posture, protect sensitive data, and maintain a safe digital environment for your community.

1. Common Cyber Threats in Schools

Schools face many of the same cybersecurity risks as large organizations, but with unique challenges such as shared devices, open networks, and a wide range of users.
Here are some of the most common threats:

- **Phishing emails** that trick staff or students into sharing passwords or clicking malicious links.
- **Ransomware attacks** that lock access to grading or student information systems.
- **Weak Wi-Fi configurations** or shared passwords that expose networks to unauthorized users.
- **Unsecured smart devices** such as cameras, printers, or classroom technology.
- **Lack of multi-factor authentication (MFA)** for administrative accounts.

Understanding these risks is the first step toward creating a safer, more secure environment.

2. Foundational Security Practices

Strong cybersecurity begins with disciplined, consistent practices:

- **Require Multi-Factor Authentication (MFA)** for all staff and administrative accounts.
- **Use strong password policies** and encourage regular password changes.
- **Segment networks** to separate student, staff, and guest access.
- **Apply the principle of least privilege,** giving users access only to the data they need.
- **Keep systems and firmware updated** to close known vulnerabilities.

- **Monitor network activity** for unusual logins, bandwidth spikes, or device anomalies.

These basic safeguards significantly reduce the likelihood of a successful attack.

3. Protecting Student and Staff Data

Educational institutions must comply with the **Family Educational Rights and Privacy Act (FERPA)** and relevant **Florida data protection laws**.
Maintaining compliance helps ensure that personal and educational records remain secure.
Recommended practices include:

- Encrypting all data in transit and at rest.
- Restricting access to sensitive systems to authorized personnel only.
- Keeping a detailed inventory of systems and services that store student information.
- Reviewing vendor contracts to confirm they meet privacy and security standards.

Protecting this data is not just a technical task, it is a moral and legal obligation to safeguard your community's trust.

4. Conducting a Basic Risk Assessment

Regular assessments help schools understand where vulnerabilities exist and how to address them effectively.
A simple annual review can include:

1. Identifying critical systems (SIS, Wi-Fi, backups, communication platforms).
2. Evaluating potential risks and prioritizing the highest-impact threats.
3. Reviewing access controls and updating permissions as staff roles change.
4. Testing backups and disaster recovery procedures.
5. Updating cybersecurity policies and documenting incident response steps.

Proactive reviews help prevent minor issues from becoming major disruptions.

5. Top 10 Cyber Hygiene Tips for Schools

1. Enable **MFA** for all accounts.
2. Keep **devices and firmware** fully updated.
3. Separate **student, staff, and guest** networks.
4. Limit **administrative privileges** to trusted personnel.
5. Use **endpoint protection and web filtering** across all devices.
6. Back up data daily and **test restorations** regularly.
7. Provide **cybersecurity awareness training** each semester.
8. Watch for **unusual login activity** or device behavior.
9. Secure **smart boards, cameras, and IoT devices** with strong credentials.
10. Maintain a **written cybersecurity plan** and review it yearly.

Small, consistent actions make the biggest difference in keeping systems resilient.

Conclusion

Cybersecurity in education isn't just about technology, it's about protecting people, ensuring continuity of learning, and upholding the values of trust and stewardship.
By applying these best practices, your school can minimize risk, meet compliance requirements, and build a culture of shared responsibility for safety in the digital classroom.