TIP SHEET

K–12 School Cybersecurity Tips and Best Practices

Private and independent K–12 schools are often low-hanging fruit for cybercriminals. As a whole, the industry is not spending the money and devoting the necessary resources required to mitigate risks. Schools tend to take a reactive vs. proactive posture, focusing on cybersecurity only after an incident has occurred. While protective technology is imperative, cybersecurity is primarily a people problem. Your school may have the best firewalls and technical protections in place, but attackers can get into your system if one employee makes one mistake. Here are some best practices to be proactive and reduce your school's risk of cyberattacks.

1 Restrict Access.

Your school software systems contain a great deal of sensitive data, from names, addresses, and contact information to credit card transactions and social security numbers. To protect your data, choose software solutions that allow role-segmented access levels. Each user's login should only give them access to the information they need to do their job. For example, an accounts payable clerk shouldn't have the same access as the Controller, and a helpdesk technician shouldn't have the same access as the IT director.

2 Enable Multifactor Authentication.

Ensure your school software uses multifactor authentication (MFA), which requires more than one way for users to identify themselves. For example, after entering their unique password in the system, a user may need to approve the login through a mobile app. Use MFA everywhere it is available in your school's tech stack.

3 Implement Single Sign-On.

Ideally, most of your software solutions should be integrated to allow single sign-on (SSO). SSO gives each user one set of login credentials for multiple systems, increasing access management security and providing a streamlined experience for faculty, staff, and families.

4 Train Your Faculty and Staff to be Security Aware.

People are your first line of defense from cyber threats that could impact your school. Studies show that 85% of data breaches are caused by human error. Ensure your people understand the threat landscape and how to protect themselves and your school from a breach. We recommend annual security training and education for all faculty and staff in addition to protective technology.

5 Beware of Unsolicited Communications.

If you or a staff member receives an email, phone call, or text message that feels odd, it probably is. Even if the origin of the contact seems authentic—a colleague or friend, your bank, or a trusted vendor—do not engage until you can validate it. Beware if the message includes poor grammar or spelling or if they ask for confidential information. Ensure your faculty and staff are aware of the various types of malicious behavior, including phishing (email), vishing (phone), and smishing (text). Most importantly, **do not click on links or attachments** in unsolicited emails or text messages.

6 Do Not Reuse or Share Passwords.

Savvy cyberattacks include credential mining and stuffing—stealing usernames and passwords from one location and then attempting to use them for other systems. Never use your work email address for non-work purposes like banking, shopping, contests, or other online logins. Keep work and personal accounts separate. Ensure your passwords are unique, long, and complex. Change passwords regularly.

7 Lock Your Devices.

Do not share your logins with coworkers, and do not give anyone the opportunity to use your computer surreptitiously. Log out of software when you aren't using it. Lock your computer screen when you leave your desk and set it to lock automatically after a brief period of inactivity. Keep your smartphone locked at work and home, and do not share your passcode. All it takes is a child accidentally clicking on a phishing link on your phone to infect it.

8 Review Your Cyber Insurance.

Cyber Insurance is more important than ever, yet insurance companies have tightened policies to mitigate their losses as claims have risen with ransomware payouts. Policies vary widely. Some have sub-limits or exclusions for ransomware attacks in the fine print, and schools only find that out when they need coverage the most. Work with a broker specializing in cyber insurance.

9 Update and Implement Security Policies.

Policies are critical to shaping a security culture within your school. Work with your IT director and software providers to set clear expectations of security best practices that are easily digestible to your faculty and staff. Include everything from password complexity to data management and training requirements. Ensure that any policies you implement are measurable and enforceable.

Blackbaud takes cybersecurity very seriously and the protection of our customers is paramount. Here are more resources with valuable information on mitigating risk and creating a cybersecurity program within your school:

Cyber Risk Management for the K–12 Business Office (video)

The U.S. Cybersecurity Infrastructure & Security Agency "Shields Up" program

The National Cybersecurity Alliance

Blackbaud's K–12 school solutions meet or exceed all federal, state, and industry privacy requirements. For more information, visit k12.blackbaud.com.

Learn more