

Cybersecurity Considerations for School Nutrition Software

By Maximilian Draughn, Nutri-Link Technologies, Inc.

Drawing on over 20 years of experience supporting K-12 school nutrition programs, Nutri-Link Technologies combines operational insight with innovative technology solutions that help districts improve efficiency, compliance, and family engagement. This long-standing partnership with school administrators and nutrition professionals gives the company a unique perspective and positions it as a trusted voice on the future of school nutrition management.

Introduction

School nutrition software has become vital to the operations of K-12 meal programs. Today's systems manage transactions, student meal accounts, meal eligibility, online payments, inventory, and reporting. Many platforms integrate with district technologies such as student information systems to create a more connected and efficient nutrition program.

As schools continue to adopt these technologies, cybersecurity is becoming an increasingly important consideration. According to a report published by the Center for Internet Security (CIS) in 2025, about 82% of K-12 organizations experienced at least one cyber threat between July 2023 and December 2024.

While school nutrition software is only part of a district's technology system, it often contains private data, including information protected by FERPA and other laws, making protecting these systems a priority. In addition to federal privacy laws like FERPA, districts are often subject to state student privacy and data security laws, which further govern how student information is collected, stored, and protected. As school nutrition programs become increasingly dependent on connected software, maintaining a strong, secure network is imperative for the safety of student and family information as well as for avoiding potential legal and financial consequences.

Why Cybersecurity Matters for School Nutrition Software

School nutrition programs manage more than just meal transactions. Their software houses information such as student names, identifying information, meal eligibility status, account balances, dietary and allergy information, and payment records. Since these systems contain sensitive and protected information and streamline daily operations, they are increasingly becoming a target for cyberattacks.

A cybersecurity incident can have consequences beyond compromised information. Failure to prevent student data breaches from cyberattacks can disrupt essential services such as meal distribution, compromise privacy, and lead to costly restoration and legal expenses. In school districts where cafeterias serve hundreds or thousands of students each day, such incidents disrupt operations and meal service.

The U.S. Department of Education lists phishing attacks, compromised credentials, and unpatched software as the most common entry points for cyberattacks targeting K-12 schools. As school nutrition departments continue transitioning to cloud-based digital systems, practicing robust cybersecurity becomes extremely important to protect both student information and mealtimes.

Common Cybersecurity Risks

Many cybersecurity incidents begin with simple vulnerabilities, rather than sophisticated attacks. The 2025 CIS MS-ISAC report analyzed cybersecurity activities across over 5,000 K-12 schools and districts and found over 14,000 events and more than 9,300 confirmed incidents during the reporting period. Schools encounter cyber threats more frequently than one might expect, which is why every department relying on connected technologies must remain vigilant.

One of the most common cybersecurity threats is phishing. These tend to be fraudulent emails that appear to come from trusted organizations, coworkers, or software vendors and are designed to trick employees into clicking links or revealing sensitive information. Even a single compromised account allows attackers to gain widespread access to systems.

Weak and reused passwords also increase security risks. Sharing a password across several platforms or creating easy-to-guess passwords make unauthorized access much easier if credentials are compromised.

Outdated software can be a vulnerability as well. Security updates and software patches are often released to address newly discovered vulnerabilities before they are exploited by hackers. Putting off updates like these leave systems exposed, so it is important to keep them up to date.

Ransomware is one of the most disruptive cyber threats facing K-12 schools. These types of attacks often lock users out of critical systems and disrupt operations until systems can be restored. In the context of school meal operations, such attacks prevent staff from accessing critical software, such as student information and point-of-sale systems, potentially forcing schools to revert to less efficient manual processes until systems can be recovered.

Cybersecurity Best Practices

Technology by itself cannot prevent every cybersecurity incident. Staff diligence and consistent security practices are just as important.

Cafeteria and administrative staff help make their systems more secure by using strong passwords, enabling multi-factor authentication, locking devices when leaving their workstations, verifying the validity of emails before opening attachments or links, and reporting suspicious activity to IT staff.

Regular cybersecurity training helps employees recognize potential threats, like phishing emails, before they become incidents. Since about 68% of cyberattacks begin with human error, training

staff to recognize warning signs and actively working to keep systems safe significantly improves overall security.

By complementing secure technology with trained staff, school nutrition departments protect the data of families they serve while maintaining efficient operations. Continuous staff education is a necessity to ensure online system integrity. Technical safeguards are not enough to prevent human targeted threats, so ongoing cyber security training must be a priority.

Building a More Secure Future

Technology has and will continue to play a major role in K-12 school nutrition programs. From online payments to integrated student information systems, connected software helps school districts improve efficiency while enhancing services to students and families.

As digital tools become more interconnected, cybersecurity must remain a consideration when selecting and managing school nutrition software. A proactive approach to cybersecurity will help schools confidently embrace digital technologies that shape the future of school nutrition. Effective cybersecurity is crucial because investing in secure software and encouraging strong staff practices greatly reduces data threats while maintaining reliable daily meal service.

References

CIS Center for Internet Security. “2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience.” *CIS*, 6 Mar. 2025, www.cisecurity.org/insights/white-papers/2025-k12-cybersecurity-report.

Cybersecurity and Infrastructure Security Agency. *Cybersecurity and Infrastructure Security Agency*. U.S. Department of Homeland Security, <https://www.cisa.gov/>

“K-12 Cybersecurity.” *U.S. Department of Education*, www.ed.gov/teaching-and-administration/safe-learning-environments/school-safety-and-security/k-12-cybersecurity.