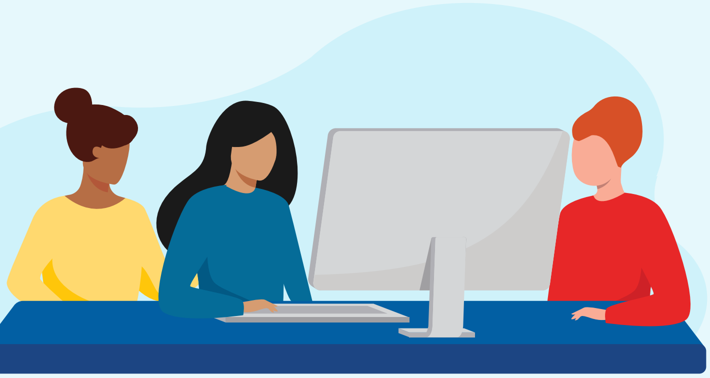
SCHOOLSAFETY.GOV

Cybersecurity Resources

Minimize exposure to cyberattacks and build secure and resilient systems.



Cyberattacks and online threats are an increasingly significant and widespread problem for K-12 schools and school districts. Educational institutions can be a lucrative and vulnerable target for malicious cyber actors because they maintain extensive amounts of sensitive student and staff data and personal information, utilize multiple forms of networking technologies and systems to facilitate learning, and often lack resources to put in place a comprehensive cybersecurity program.

K-12 cyber threats can include unauthorized disclosures or data breaches, ransomware attacks, phishing attacks, and denial-of-service attacks. These incidents can have significant impacts, making critical systems inaccessible, exposing sensitive personal information of students and school personnel, putting confidential school plans and data at risk, and disrupting school operations. Cyberattacks can also result in high financial costs for school districts and the loss of learning for students, as well as jeopardize the safety and security of our educational system.

As new, evolving, and increasingly sophisticated cyber threats materialize, it is important that schools and school districts take proactive steps to:

- Minimize exposure to common attacks
- Protect sensitive data and critical systems and
- Enable safe, secure, and accessible learning experiences for all students.

Impacts of a Cyberattack

According to a 2022 U.S. Government Accountability Office report, the loss of learning following a cyberattack ranged from three days to three weeks, and recovery time can take anywhere from two to nine months.

The monetary losses to school districts following a cyber incident ranged from $50,000 to $1 million.

Adapting Cybersecurity Measures

Cybersecurity should be approached as a continuous process of managing risk. As new technologies are adopted within a school environment, schools and districts can proactively implement thoughtful and well-informed processes to reduce exposure to cyber threats. These include investing in the most impactful security measures while building towards a more mature cybersecurity program for the future.

SchoolSafety.gov Disclaimer

The U.S. Department of Homeland Security (DHS), U.S. Department of Education (ED), U.S. Department of Justice (DOJ), and U.S. Department of Health and Human Services (HHS) do not endorse any individual, enterprise, product, or service. DHS, ED, DOJ, and HHS do not mandate or prescribe practices, models, or other activities described in this communication. DHS, ED, DOJ, and HHS do not control or guarantee the accuracy, relevance, timeliness, or completeness of any information outside of those respective Departments, and the opinions expressed in any of these materials do not necessarily reflect the positions or policies of DHS, ED, DOJ, and HHS.

Strategies to Strengthen K–12 School Cybersecurity

There are several strategies school communities can implement to strengthen their cyber posture and protect against current and future digital threats. Some of these strategies include:

Practice and Provide Training on Good Cyber Hygiene

While cybersecurity threats are complex and wide-ranging, there are relatively simple actions that every K–12 organization can take to significantly reduce the risk of a damaging intrusion. This includes recognizing and reporting phishing attempts, using strong passwords, turning on multifactor authentication, and keeping software updated. Each of these fundamental, low-cost steps can significantly minimize exposure to common cyberattacks. Schools should also consider creating an education and awareness program to train staff at all levels on these and other actions that can reduce cybersecurity risk.

Establish and Exercise a Cyber Incident Response Plan

Similar to planning for physical or natural emergencies, schools should develop a cyber incident response plan outlining what should be done before, during, and after a cyber incident. Cyber incident response plans may include information about key roles and responsibilities, how a cyber incident may be declared, when to mobilize the incident response team, and plans to alert leadership and other important stakeholders should an incident occur. Schools should also consider integrating this plan into broader school or district emergency operations management efforts and test and exercise their plans regularly with key personnel to validate, update, and strengthen policies and procedures critical to managing an incident.

Stay Informed and Connect with K–12 Cyber Partners

Situational awareness of the risk environment and access to timely resources can help K-12 organizations take strategic and cost-efficient actions to strengthen cybersecurity. Information sharing and analysis centers (ISACs), nonprofit organizations specific to the K-12 education sector, and public-private partnerships are often available to join at little to no cost and can provide information on evolving threats and tactics, high-impact actions or best practices, and opportunities to discuss specific challenges or approaches unique to school environments. K–12 organizations also should establish a relationship with their regional Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity advisor and local Federal Bureau of Investigation (FBI) field office. These officials can provide cyber preparedness services and resources, as well as coordination and support during cyber disruptions or attacks.

Sources: SchoolSafety.gov Cybersecurity | Cybersecurity Action Steps | Protecting Our Future: Partnering to Safeguard K-12 Organizations from Cybersecurity Threats | 4 Easy Ways to Stay Safe Online | CISA Blog | Cybersecurity Considerations for K-12 Schools and School Districts | Building Technology Infrastructure for Learning | K-12 Digital Infrastructure Brief: Defensible & Resilient | SchoolSafety.gov Cybersecurity Resources | Cybersecurity for K-12 Education | K-12 Cyber Incident Map

Resources

SchoolSafety.gov offers resources, programs, and tools school communities can use to prevent, protect against, and respond to cybersecurity threats and attacks. These resources include:

Guides, Briefs, and Fact Sheets

- K-12 Digital Infrastructure Brief: Defensible & Resilient: This brief highlights cybersecurity recommendations and promising practices from states and districts across the country. It is designed to help schools build solutions for their own contexts and offers examples from the field of those who faced challenges to connectivity, accessibility, cybersecurity, data privacy, and other infrastructure issues and designed solutions for their challenges. Other briefs available on these topics include Adequate and Future-Proof and Privacy-Enhancing, Interoperable and Useful.
- Partnering to Safeguard K-12 Organizations from Cybersecurity Threats: This report provides recommendations and resources to help K-12 schools and school districts address systemic cybersecurity risks. It also provides insight into the current threat landscape specific to the K-12 community and offers simple steps school leaders can take to strengthen their cybersecurity efforts.
- Phishing Infographic: This infographic provides a visual summary of how threat actors execute successful phishing operations. It provides detailed actions organizations and individuals can take to prevent successful phishing attacks, from blocking phishing attempts to teaching individuals how to report successful phishing operations.
- #StopRansomware Guide: This guide serves as a one-stop resource to help organizations, including schools, reduce the risk of ransomware incidents through best practices to detect, prevent, respond, and recover, including step-by-step approaches to address potential attacks.

Trainings, Videos, and Webinars

- Cybersecurity Considerations for K-12 Schools and School Districts: This training course is designed to help K-12 schools and districts understand cybersecurity considerations needed to inform school emergency operations plans and safety, security, emergency management, and preparedness programs.
- Cybersecurity and Incident Response: This recorded webinar provides best practices for schools and districts that are looking to build or enhance their cyber incident response capabilities.
- K–12 Education Leaders' Guide to Ransomware: Prevention, Response, and Recovery: This recorded webinar focuses on the steps K-12 schools can take to prevent, respond to, and recover from ransomware attacks, as well as free services that administrators can utilize to protect their schools.

Websites and Additional Resources

- Cyber Resources Hub: This webpage offers a range of cybersecurity assessments that evaluate operational resilience, cybersecurity practices, organizational management of external dependencies, and other key elements of a robust and resilient cyber framework.
- Cybersecurity for K-12 Education: This webpage provides tools, information, and resources to help K-12 schools be more cyber secure and resilient.
- Privacy Technical Assistance Center: This program provides information and assistance on privacy, confidentiality, and security practices related to student-level data systems and other uses of student data.
- StopRansomware.gov: This website is a one-stop hub for ransomware resources for individuals, businesses, and other organizations to help private and public organizations mitigate their ransomware risk.

Learn more and find additional cybersecurity resources on SchoolSafety.gov.