SCHOOLSAFETY.GOV

Cybersecurity Resources

Be #CyberSmart. Defend Against Cybersecurity Threats to Your School.

Across America, kindergarten through grade 12 (K-12) educational institutions are experiencing a significant increase in cyberattacks, especially during the transition to remote and virtual learning as a result of the COVID-19 pandemic. Malicious cyber actors are targeting school computer systems, slowing access, and rendering the systems inaccessible to basic functions.

Our Nation's students are also spending more time online than ever before, using technology to complete homework, communicate with peers, and engage with teachers and school staff. Our growing dependence on technology systems - coupled with emerging, evolving, and increasingly deceptive cyber threats - demands enhanced awareness and vigilance when it comes to our online world. It is important for schools, parents, and students to stay safe online by taking proactive steps to defend against risks and strengthen cyber safety and security both at home and within schools.

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.

Resources

SchoolSafety.gov offers resources, programs, and tools school communities can use to prevent, respond to, and if needed, recover from cybersecurity threats and cyberattacks.

General Cybersecurity Resources

- Cyber Threats to K-12 Remote Learning Education: This fact sheet is a primer for non-technical educational professionals, and includes general cybersecurity best practices, video-conferencing best practices, and a list of available resources.
- Cyber Safety Considerations for K-12 Schools and School Districts: This fact sheet provides information to students, teachers, and administrators on identifying cyber threats, educating students on responsible online behavior, and learning how to prevent, prepare for, and respond to a potential cybersecurity incident.
- Cyber Safety Series: This series of short videos – centered around themes such as social media safety, ransomware, phishing, and making strong passwords – outlines tips and best practices to help schools, students, and educators stay safe online.
- Stop.Think.Connect. Parent and Educator Resources: These resources cover information on how to talk to your children and students about the importance of internet safety.
- Keeping Children Safe Online: This website offers guidance for teachers, parents, guardians, and caregivers on protecting children from becoming victims of online exploitation.
- Understanding Patches and Software Updates: This resource defines patches (software and operating system updates) and outlines best practices for software updates.

Ransomware and Phishing Resources

- StopRansomware.gov: This website is a one-stop resource where public and private sector entities can find U.S. government tools, information, and resources to help reduce the risk of ransomware attacks and improve resilience. The site includes a specific K-12 resource section, which includes information geared towards IT staff, students, parents, and administrators.
- Cyber Actors Target K-12 Distance Learning Education: This joint advisory details the threat of ransomware attacks, the theft of data, and the disruption of distance learning services to K-12 educational institutions.
- Protecting Sensitive and Personal Information: This fact sheet provides information for organizations to use in preventing and responding to ransomware-caused data breaches.
- Phishing (General Security Postcard): This postcard explains phishing and provides signs and tips to prevent attacks.
- Cyber Security Evaluation Tool - Ransomware Readiness Assessment (RRA): This tool is a stand-alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology. The RRA module is a self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend against and recover from a ransomware incident.