SCHOOLSAFETY.GOV

Cybersecurity Action Steps

Take proactive steps to defend against cybersecurity threats to your school.

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. All educational institutions are at risk of falling victim to a cyberattack, and in recent years, K-12 schools have been an increasingly frequent target. These attacks can impact a school's ability to carry out its educational obligations, protect sensitive student and staff data, and provide a safe and secure learning environment for our nation's youth.

Defending against cyber threats takes teamwork, and every individual in the school setting, no matter their role, can play a part. Students, educators, administrators, and school personnel should 'see themselves in cyber' by taking simple, proactive steps to better protect themselves and their school systems online.

School communities can take four simple action steps to reduce their cybersecurity risk posture.

Enable Multi-Factor Authentication

Adversaries are increasingly capable of phishing or harvesting passwords to gain unauthorized access to information systems. Multi-factor authentication (MFA) is a layered approach to securing online accounts and the data they contain that requires users to provide two or more authenticators to verify their identity. Users who enable MFA are significantly less likely to be hacked because even if a password is compromised, unauthorized users will not be able to meet the second authentication requirement, stopping them from gaining access to online systems and data.

Use Strong Passwords

Passwords are the most common means of authentication, and many systems have been successfully breached because of non-secure and inadequate passwords. Tips for creating a strong password include applying a combination of varying character types; avoiding common words, numerical patterns, and personal information; and using the longest password or passphrase permissible. School staff can also consider using a password manager program, which stores randomly generated passwords across multiple accounts and is only accessible with a master password.

Recognize and Report Phishing

Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. Common signs of a phishing attempt include suspicious sender addresses, generic greetings and signatures, spoofed hyperlinks and websites, misspellings, poor grammar and sentence structure, and suspicious attachments. Schools can reduce the risk of phishing emails by enabling strong spam filters and implementing a cybersecurity awareness and training program to educate students and staff on the ways to recognize and report suspicious activity.

Update Your Software

Outdated software can contain vulnerabilities that can be exploited by threat actors. When vendors become aware of vulnerabilities in their products, they often issue patches. Schools and districts should install updates as soon as possible to protect their systems, as well as enable automatic software updates whenever possible.

Sources: cisa.gov/ | schoolsafety.gov/cybersecurity/

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.

Follow   Sign up

SchoolSafety.gov