FS-ISAC

Your Institution Logo

Security Tips Newsletter

8 April 2024 | Issue No. 9

Security is Everyone's Responsibility

Protecting Our Children

Summary

The surge in cyber attacks on K-12 schools, targeting vulnerable computer systems and exploiting the lack of cybersecurity experts, is causing widespread disruptions across the nation. With incidents doubling in 2023, these attacks, often involving ransomware and data theft, underscore the urgent need for enhanced cybersecurity measures to safeguard student records and maintain the continuity of education. (NPR)

Prevention Tips

At home and at school, protect your systems by performing the following:

- Deploy multi-factor authentication (MFA)
- Mitigate known exploited vulnerabilities
- Implement and test backups
- Regularly exercise an incident response plan
- Implement a strong cybersecurity training program

If you lack adequate resources, consider leveraging:

- The State and Local Cybersecurity Grant Program (SLCGP)
- Free or low-cost services to make near-term improvements in resource-constrained environments
- Technology providers enable strong security controls by default for no additional charge
- Minimizing the burden of security by migrating IT services to more secure cloud versions
- The Cybersecurity Infrastructure and Security Agency's (CISA) online toolkit provides additional free cybersecurity training and resources available for the K-12 community

Every K-12 organization—large and small—must be prepared to respond to disruptive cyber incidents. CISA is available to help you prepare for, respond to, and mitigate the impact of cyber attacks. When cyber incidents are reported quickly, they can use this information to render assistance and as a warning to prevent other organizations and entities from falling victim to a similar attack. CISA encourages our stakeholders to voluntarily share information about cyber-related events that could help mitigate current or emerging cybersecurity threats to critical infrastructure.

Sharing thwarted or actual cyber incidents with an information sharing organization could help mitigate current or emerging cybersecurity threats to critical infrastructure.

If you realize you clicked or responded to a phishing email involving your [Institution] account, contact us immediately. You will need to change your passphrase. Additionally, you can report the incident to the FTC at ReportFraud.ftc.gov or the Internet Crime Center at www.ic3.gov. Please remember, that *security is everyone's responsibility*.