Microsoft

Meeting federal cybersecurity recommendations with Microsoft

New trends in cybersecurity

Congress enacted the K-12 Cybersecurity Act of 2021 in recognition of the heightened cyber risk for K-12 communities across the country. This act required the Cybersecurity and Infrastructure Security Agency (CISA) to report on and provide recommendations for the cybersecurity risks facing elementary and secondary schools. Microsoft can help you meet these recommendations and help secure your learning community.

Impact for Education

By the end of 2021, the public sector saw an **increase of 600% in cybercrime**[1]

Reported cyber incidents at schools between 2018–2021 have risen from 400 in 2018 to an accumulated total of **over 1,300**[2]

Microsoft reported **Education was the most targeted industry by malware** in February 2023[3]

For malware encounter data for the most recent month click here: https://www.microsoft.com/en-us/wdsi/threats

1. Cyber Resiliency Begins with People and Process, Not Technology | CompTIA
2. The State of K-12 Cybersecurity Report Series — K12 SIX
3. Cyberthreats, viruses, and malware - Microsoft Security Intelligence, 2023

Security and management solutions through Microsoft 365 for Education not only help meet the recommendations from CISA but also make the **most out of your district's time and resources.**

Help ensure everyone in your learning community can dedicate time to what matters most: creating engaging, inclusive, and meaningful learning experiences that empower every student to achieve their full potential.

Microsoft

Microsoft security solutions help protect people and data against cyberthreats to give you peace of mind

The Cybersecurity and Infrastructure Security Agency (CISA) created a report on cybersecurity risks facing K-12 institutions and provides recommendations designed to help schools face these risks. Highlighted below are what CISA has identified as the most impactful steps for prioritized investments and how Microsoft addresses each of them.

Recommendations	Microsoft's Solution
Deploy multi-factor authentication	• MFA is recommended for educators, staff, and admins at a minimum and is included with Azure AD including risk scoring to enforce MFA and more enhanced security controls. Azure AD supports the Microsoft Authenticator app, OATH TOTP and FIDO2. • Azure AD Password Protection using the Banned Password algorithm and corresponding requirements helps block weak or insecure passwords. **More info:** Azure Active Directory, Azure AD Multi-Factor Authentication, Azure AD Password Protection
Mitigate known exploited vulnerabilities	• Microsoft Defender for Endpoint and Defender for Cloud cover anti-virus and more with our EDR and automated response capabilities. Microsoft Defender for Cloud Apps as part of M365 Defender has malware detection capabilities. • Defender for Office 365, can provide email protection from target malware, phish, and email compromise attacks and can track attacks across Office 365 with advanced hunting capabilities that help identify, prioritize, and investigate threats. **More info:** Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps
Implement and test backups	• Microsoft 365 OneDrive PC folder backup automatically syncs folders on your PC to your OneDrive, helping keep files and folders protected and available. • Microsoft Purview Information Protection helps with flexible protection actions including encryption, access restrictions, and visual markings to help prevent data loss and enable users to better govern data in a compliant manner. **More info:** Microsoft OneDrive, Microsoft Purview
Prioritize patch management	• Patching can be managed with Endpoint Manager/Intune, and critical vulnerabilities can be found with Microsoft Defender for Endpoint, which also finds misconfigurations and assesses server security posture. • Microsoft Defender also covers next-generation antivirus for real-time protection and uses security updates to help ensure protection against the latest threats. **More info:** Microsoft Intune
Regularly exercise an incident response plan	• Microsoft Defender for Endpoint and Microsoft Sentinel delivers managed detection and response (MDR) and security information and event management (SIEM) capabilities, including endpoint detection and response (EDR). • Manage incident response retainers and plan requirements with Microsoft security services for incident response. **More info:** Microsoft Sentinel, Microsoft Defender for Endpoint
Implement a strong cybersecurity training program	• Attack Simulator in Microsoft Defender for Office 365 includes both phishing exercises and video trainings. • Microsoft offers additional incident response, technical support, escalation management, case management, proactive and reactive services. **More info:** Microsoft Defender

Questions? Contact your account team for more information and visit here for the CISA report

For the full list of CISA Cybersecurity Performance Goals (CPGs) visit: CPG Checklist \| CISA

Learn more about the current state of cybercrime at: Cyber Signals (microsoft.com)