Importance of Multi-Factor Authentication (MFA)

A BRIEFING FOR K-12 LEADERS AND STAKEHOLDERS

Credential-theft and ransomware campaigns now rank as the #1 operational threat to U.S. school districts. Multi-Factor Authentication blocks more than 99% of password-based attacks. Failure to adopt MFA exposes districts to potential learning loss, districtwide outages, and personal data liability far in excess of the modest cost and effort to implement.

More often than not, hackers don't break in, they log in by utilizing active credentials, which are sold and traded on the dark web. In fact, Firestorm Global has found staff credentials located on the dark web for every assessed district. Once an adversary gains internal access, it activates a variety of potential threats.

In today's digital world, it's almost inconceivable to think that district staff do not utilize forms of Multi-Factor Authentication in their personal lives. Financial institutions, retailers, and similar industries commonly mandate MFA (both for customers and employees) as a method of safeguarding sensitive data. As custodians of sensitive student, staff and parent data, it's imperative that districts treat protected information with the same care as peer industries.

For employees unable or unwilling to utilize their smartphone, leading MFA platforms have options for staff to utilize alternative methods for authentication to ensure all staff are able to participate seamlessly. However, it's relevant to note that the supermajority of staff at other K-12 districts who have enrolled in MFA, opt to utilize their smartphone rather than alternative methods for purposes of ease and simplicity.

SAFER Cyber 6: Multi-Factor Authentication (MFA)

As members of SAFER JPA, the SAFER Board has set requirements for all member organizations to adopt six (6) leading cybersecurity controls as a mandated requirement.

Those six controls include: Multi-Factor Authentication, Firewalls and Antivirus, Security Awareness Training, Endpoint Detection and Response, Immutable Backups, and Vulnerability Scanning.

It's important for all members to implement these best practices to support the collective protection of the member pool.

Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency (CISA), which actively supports all K-12 organizations across the United States strongly encourages all districts to adopt MFA for their organization.

CISA advocates for organizations to adopt App-Based (mobile push notification) or FIDO (physical key) MFA methods.

Resource: https://www.cisa.gov/MFA

Why Passwords Alone Are Not Enough

- Passwords can be guessed, phished, or reused across dozens of sites
- Stolen passwords can circulate for years
- Artificial Intelligence (AI) is helping attackers generate likely password combinations

Recommendation to District Stakeholders

Implement district-wide Multi-Factor Authentication for all staff, contractors, and high-risk accounts on all critical applications and remote access methods. Standardize on app-based mobile push notification MFA with alternative authentication methods available, as required.

Provide clear, straightforward training to all staff on the importance of safeguarding district information and how to utilize available MFA methods.

Cybersecurity Questions?

Members receive advanced cybersecurity support at no additional cost including access to cybersecurity risk assessments, cyber awareness resources, external risk analysis, "ask an expert" help line and more.

If you have questions or would like to learn more, contact support@firestormglobal.com.