K12 Cybersecurity Toolkit - Authentication Management
Executive Summary

Controlling access to organizational systems and resources is an essential element of cybersecurity. The traditional approach to access control has been to assign usernames with complex password requirements, generally a combination of up to eight letters, numbers and special characters. However, in an era of sophisticated hackers and cybercriminals, this cybersecurity approach is no longer adequate.

Relying solely on a username/password combination for access control opens organizations up to a number of risks:

- Username/password combinations are routinely and easily compromised through
- successful phishing attacks.Passwords created using the traditional requirements described above are often difficult for end-users to create and to remember. This results in passwords that are weak, which iterate with a single number change, are often re-used and/or are written down and stored near or on the device.
- Inquisitive students often seek out and use passwords hidden under keyboards, stored in desk drawers, or taped to the bottom of pencil holders.

Districts seeking to improve their security stance are advised to use a combination of the following strategies to better support the use of authentication credentials:

Strategy 1: Single Sign-On (or Simplified Sign-On)

Single sign-on (SSO) solutions allow a user to use the same set of credentials across multiple systems. This allows users to establish and commit to memorizing one really strong set of credentials, instead of having to remember different passwords for each system. This significantly reduces the number of passwords employees and students have to remember, increasing operational efficiency and minimizing lost instructional time.

Strategy 2: Multi-Factor Authentication (MFA)

Username and password combinations alone are not enough to protect the most sensitive data, including employee and student personally identifiable information (PII) and financial data such as bank accounts and payroll.

Multi-factor authentication (MFA) improves security by introducing an additional factor into the login process, such as a randomly generated code, an identification card that must be scanned, or biometric data such as a fingerprint scan. Most school systems considering multi-factor authentication opt for systems that deliver randomly generated codes to a user's cell phone via text message or an authentication app, or that require a fob-type device or identification card.

Multi-factor authentication is an extremely effective strategy to reduce the risk of a password compromise. Because an additional piece of information is required to authenticate, MFA effectively eliminates most of the risk of phishing attacks.

Strategy 3: Leverage Password Management Tools

While single sign on (SSO) is often the preferred solution for streamlined system authentication, school districts often have a number of important systems that do not support SSO or cannot integrate with the district's selected SSO. As a result, even when SSO is implemented, staff and students may still have to remember multiple usernames and passwords.

For these situations, selecting and implementing a password management tool or password locker and training users to use it can improve system security.

Strategy 4: Transition to Passphrases

The eight-character complex password is no longer considered the best approach to password creation. The most recent digital identity guidelines from the National Institute for Standards and Technology (NIST) encourage organizations to transition to passphrases which are easier to remember and harder to break. This NIST blog post highlights their updated user recommendations.

While this approach may be technically simple to implement, it is often a significant departure from previous policy. This requires IT departments to clearly communicate the "why" and "how" of the change to employees and students and train users accordingly.

Strategy 5: Cybersafety and Student Account Provisioning

While authentication management initiatives often focus heavily on employee access and use, schools have a large population of non-employee system users - students. Student account provisioning should be managed to help protect students from cybercriminals and teach

students basic cyber hygiene skills. Key strategies include creating student accounts and email addresses without using student names and training them to create strong passphrases.

Leveraging some or all of these approaches enhances security and reduces the burden on end-users. For example, implementing passphrases and multi-factor authentication can allow an organization to safely extend the password lifecycle.

Conventional wisdom used to be that passwords should be changed every 30, 60, or 90 days, however, this approach is dated and NIST guidelines now recommend organizations not require passwords be changed unless there is a user request or evidence that the password has been compromised.[1] While frequent password changes may reduce the window for leveraging compromised passwords, the benefit is often offset by the unsafe security practices users practice as a result, such as writing down passwords and storing them near their device. Training system users to create a single, complex passphrase to use in conjunction with MFA and limiting required password changes to once a year can incentivize users to embrace IT policy changes.

The Future: Prepare to leave passwords behind

The next step in authentication management will be to leave passwords behind and control access with multiple verification factors such as biometrics or authentication devices. Once the technology has matured and become mainstream, this will require a significant redesign of existing authentication processes. In the meantime, developing and maintaining a comprehensive password management strategy remains relevant and necessary.

For more information…

A deeper analysis of each of these approaches is available to CoSN members in the following briefing papers, which you can access in the toolkit folder in your account downloads:

- Leverage single sign on
- Multi factor authentication
- Implement a password management tool
- Transition to passphrases
- Set up student accounts to support cyber safety

[1] NIST Special Publication 800-63B Digital Identity Guidelines, June 2017