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

K12 Cybersecurity Toolkit - Authentication Management
Strategy 1: Leverage Single Sign-On (SSO)

This is the first in a series of CoSN member publications outlining recommendations for a comprehensive password management approach in K12 schools and districts.

User credentials are both the first line of defense protecting information systems from unauthorized access and an easy point of compromise. In education environments, passwords are not only vulnerable to phishing attacks that trick employees into providing their credentials but are subject to inquisitive students who seek out passwords hidden under keyboards, stored in desk drawers, or taped to the bottom of pencil holders.

Getting Started with SSO

One of the first strategies for reducing end-user complexity is to leverage single sign-on. SSO solutions allow a user to use the same set of credentials across multiple systems. This allows users to establish and memorize one really strong set of credentials, instead of having to remember different passwords for each system. This reduces the burden on the users, increases operational efficiency and minimizes instructional time lost due to forgotten passwords.

The most common form of SSO leverages a platform that integrates with multiple technology systems. Setting up SSO involves the following steps:

1. Identify which SSO technology to leverage in your organization. Look for a tool that integrates with your existing applications and architecture.
2. Test the SSO technology on either a test system or an application with a relatively small footprint to minimize the potential impact on school operations and classroom activities..
3. Clearly communicate the impact and benefits of SSO to all users. Develop a transition plan and train employees and students how to utilize SSO.
4. Plan the rollout. Select the applications and systems to which SSO will first be applied. Utilize a phased approach to SSO implementation to minimize risk and user confusion.

One challenge with SSO is that younger students, in particular, may have trouble remembering long or complex passwords. This can lead teachers to utilize unsafe security practices, such as writing down student passwords and storing them in one place. Encourage the use of passphrases, which may be easier for students to remember. *(See Authentication Management Strategy 4 - Transition From Traditional Passwords to Passphrases)*

Another SSO approach is to utilize a product that supports QR code or RFID scanning of an identification badge to login. QR code logins rely on the use of device cameras to facilitate the login process. The user holds their identification badge up to the camera to be scanned. RFID chipped cards rely on scanners attached to devices and are less convenient than the QR code approach. This approach may add some overhead to the SSO environment setup due to the additional technology involved.

SSO Implementation Challenges

One of the biggest challenges of implementing SSO is that not all applications will integrate with different SSO platforms. When selecting an SSO tool, it is important to first identify all applications that must be connected to the SSO solution and select the tool that best meets organizational needs. In some cases, it may be necessary to utilize a second SSO platform to accommodate systems unable to integrate with the primary SSO tool. There may still be some systems outside the SSO implementation that require a separate set of authentication credentials.

SSO Implementation Risks

It is important to be thoughtful when deciding which systems to connect through SSO. Because exposure of a single user password can grant access to a wide range of systems, SSO can increase the risk to sensitive data assets. This risk can be mitigated by combining SSO with the use of passphrases, training staff and students to create strong passwords and adopting multi-factor authentication to protect critical systems.

Regardless of the approach selected, SSO implementation will significantly reduce the number of account credentials school system employees and students must remember, increasing efficiency and improving system security.

K12 Cybersecurity Toolkit - Authentication Management
Strategy 2: Implement Multi-Factor Authentication (MFA)

This is the second in a series of CoSN member publications outlining recommendations for a comprehensive password management approach in K12 schools and districts.

The practice of requiring only one category of credentials to access a protected system, such as a username and password, is considered single-factor authentication (SFA). Although this has been a standard IT policy approach for many years, it now puts organizational assets at risk. 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. These sensitive data types are at significant risk of unauthorized access, theft and exploitation due to compromised user credentials.

User credentials are commonly exposed either through phishing attacks, where the user is tricked into revealing their credentials; by users writing down and storing their passwords on or near their devices; or through password reuse. In the latter case, when a password has been compromised elsewhere, a hacker can easily research the user to identify other systems to which they have access and leverage the compromised credentials.

Benefits of Implementing Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) introduces 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 implementing 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 for mitigating the risk of password compromise. Because an additional piece of information is required to authenticate, MFA effectively eliminates most phishing attack risk.

Disadvantages of MFA

MFA can present some disadvantages. Because MFA requires access to an additional factor, such as a cell phone or physical token, users may be unable to log in if they forget, lose or damage their secondary authentication device. Examples may include leaving a cell phone at home or washing physical tokens in the laundry. However, this risk can be mitigated by providing backup MFA alternatives. Examples include using SMS text message authentication as a backup to a physical token, or developing an identity verification system that provides users with a temporary authentication code.

MFA Implementation

As outlined above, MFA can be implemented using a variety of technologies as the authentication key. Each approach provides varying levels of security, with hardware tokens being the most secure.

At a minimum, school systems should consider requiring MFA for employees with administrative account access to critical systems, including:

- Business systems (financial/banking accounts and software, payroll, and student information systems)
- Communication and IT systems (telephones, servers, firewalls, switches, etc.)
- Security systems (alarms, security cameras, etc.)

School systems looking to implement MFA should start with a tiered approach. For example, they might initially require a hardware key for IT administrators, financial officers, and other critical employees with access to sensitive data. Offering a voluntary early adoption option for staff with lower level privileges can help drive acceptance of MFA more widely.

Extending a MFA implementation school or district-wide requires IT leadership to actively engage with other department leaders and employees. Investing in these conversations and building support for the change in advance will make the transition much easier. Be sure to communicate how employees can personally benefit from the added security of MFA. For example, one education organization made employees aware that criminals had attempted to re-route an employee paycheck using a compromised username and password. Because employees were invested in protecting their paychecks from theft, they embraced MFA adoption as a process improvement.

MFA can be a powerful tool for districts seeking to improve their cybersecurity posture. Thoughtful implementation practices that include comprehensive user training can increase employee buy-in and help keep system data safe.

K12 Cybersecurity Toolkit - Authentication Management
Strategy 3: Implement password management

This is the third in a series of CoSN member publications outlining recommendations for a comprehensive password management approach in K12 schools and districts.

While single sign on (SSO) is often the preferred solution for providing streamlined access to information systems, it may not be available for all applications. There may be data systems that do not use SSO, cannot integrate with the organization's selected SSO, or for which SSO is not a secure solution. In these cases, staff and students still have to remember multiple usernames and passwords. A password management tool can greatly improve the security of passwords used for standalone systems.

What is a password manager?
Password managers are software applications that securely store passwords in an encrypted format. They can also assist users in creating passwords and simplify the process of retrieving them on demand. Like SSO solutions, password managers reduce the number of passwords and passphrases that users are required to remember. Most password managers require users to set a single strong passphrase to access the password manager/locker, where multiple login credentials are stored.

Benefits

Password managers offer significant benefits to both organizations and end users. First, they support increased password complexity. Because a password manager stores the password(s) in a secure environment, users can create extremely long and complex passwords without having to memorize them, reducing the risk of password reuse.

How password management tools work

Password managers store all of a user's different login credentials in an encrypted database which requires a single, strong master passphrase to access. Most password managers are web based and are accessible on a variety of end user devices. Many come with the ability to create or recommend complex passwords on behalf of the user.

Selecting a password management tool

There is a wide range of password managers on the market and it is important to select one based on your organization's needs.Consider the following requirements during the evaluation and selection process:

- **Centralized or enterprise management:** Select a password manager with centralized or enterprise-grade management capabilities, including the ability to assist users who lose or forget their master password. This requirement distinguishes individual user/home use password managers from enterprise-grade products and can support disaster recovery if the district needs to retrieve a password locked in someone's vault.
- **Known product with good reputation:** Candidate products should have a history of high quality service and security. Do your research to ensure they have not previously fallen victim to cybersecurity attacks.
- **Easy and intuitive password updating:** Ensure that users can easily update their stored passwords.
- **Ease of use:** Transitions easily with users from device to device and can support single users on multiple devices.
- **Strong encryption:** Password managers should support and provide 256-bit AES encryption.
- **Recommends/creates strong passwords:** Consider password managers that can create strong passwords on behalf of the user.
- **Web browser integration:** The vast majority of passwords are used for web applications and sites. Products should integrate seamlessly with multiple web browsers and be able to autofill web-based login forms.
- **Cloud or on premises:** Password management tools can be hosted in the cloud or on premises. Determine which option will best support the school system's business model.
- **Backup and recovery:** Confirm that password databases are backed up and can be restored in the event of an emergency.

Implementing password management

Regardless of the password management tool selected, it is important to have a well-defined implementation strategy. Consider deploying the tool within the IT team first and testing the product thoroughly before launching a larger rollout. Next, provide password management tools to staff with access to highly sensitive data systems, such as finance/accounting, payroll, and student information. Finally, rollout the tool to all end users, training them both on how to use the tool and the rationale behind it.

K12 Cybersecurity Toolkit - Authentication Management
Strategy 4: Transition From Traditional Passwords to Passphrases

---

This is the fourth in a series of CoSN member publications outlining recommendations for a comprehensive password management approach in K12 schools and districts.

Historically, information technology departments have directed users to create complex, eight character passwords that contain letters, numbers and special characters. In part, this approach was employed due to the technological limitations of older systems; unfortunately, it frequently resulted in easy-to-guess passwords like Pa$$w0rd, or in numbers and letter combinations that were difficult for users to remember. As a result, passwords often ended up being written down and stuck under the keyboard, on the monitor, or on the back of an employee ID badge.

The eight-character complex password is no longer considered the best approach to password creation. Organizations are now encouraged to transition to passphrases, which are easier to remember and harder to break.

What's a passphrase?

Passphrases are a sequence or words or text used to verify identity. Much longer than the traditional eight character password, passphrases may use a variety of letters, numbers and special characters including spaces. A passphrase can be any phrase, quote, statement, etc. that is easy for a person to remember. For example, the passphrase "MaytheF0rc3Bewithyou!" is easy to remember, relatively easy to type, and much more difficult to break than a traditional eight character password like StarW@rs. The most recent digital identity guidelines from the National Institute for Standards and Technology (NIST) encourage organizations to transition to passphrases The NIST blog: Easy Ways to Build a Better P@$5w0rd provides additional recommendations for building passphrases.

Benefits of using passphrases

Implementing longer passphrases - best practice is at least 14-16 characters - is a cost-effective approach to improving authentication security. Combining passphrases with

multi-factor authentication (MFA) is a highly effective way to protect systems and data resources.

Disadvantages

The key disadvantage of passphrases is they require users to type more characters to log into systems. Although some users may balk at the increased password length, reducing the complexity requirements and training users how to create passphrases can help ease the transition.

Implementing passphrases

Transitioning to longer passphrases requires these essential steps.

1. Determine the changes needed to the existing password requirements.
    - Identify minimum passphrase length (recommend **at least** 14 character minimum passphrase length).
    - Identify any changes that need to be made to password complexity requirements. Determine if capital and small letters, numbers, and special characters are still required, or if the complexity can be reduced in favor of length.
2. Review legacy systems to ensure they will support longer passphrases and special characters. Remember to test all special characters, because some systems will accept most but not all of them.
3. Communicate the timing of the change to users. Let them know what to expect and when. Explain why the change is necessary and how they will benefit.
4. Train users how to create a passphrase that is easy to remember. Once users are confident in their ability to create and use passphrases, they will generally find this an easier method to use.

Transitioning to passphrases is a simple but effective way to improve system security and reduce the burden on end users.

Additional resources:

- 3 Easy Ways for Educators to Keep Online Accounts Secure https://ferpasherpa.org/bearden1/
- 3 Easy Steps for Educators to Create a Secure Passphrase: https://ferpasherpa.org/bearden2/

LEADING EDUCATION INNOVATION

K12 Cybersecurity Toolkit - Authentication Management
Authentication Strategy 5: Cybersafety and Student Account Provisioning

---

This is the fifth in a series of CoSN member publications outlining recommendations for a comprehensive password management approach in K12 schools and districts.

While authentication management initiatives often focus heavily on employees, student accounts also need protection. Although student accounts don't have access to employee systems, they usually have digital access to individual student grades and schoolwork, including projects, papers, and test results. School systems must both protect student information and teach students how to protect it.

Student account setup

Student accounts are frequently set up in conjunction with an email address. Depending on how they are set up (which may vary according to age and grade level), student email accounts may be restricted to internal organization use, or they may be allowed to communicate with external accounts. Consider the following when setting up student accounts:

1. Determine if your school system considers student email addresses to be personally identifiable information (PII) or directory information (as defined by the Family Educational Rights and Privacy Act, or FERPA). This will impact how you design and protect access to student email addresses. If email addresses are considered PII in your locality, protect it like you would any other PII.

2. Develop a naming convention that **does not** use the student's name, any part of the student's name, or their student ID number. For example, avoid account names such as pat.doe@school.edu. Using student names for account credentials and email addresses makes them easier for hackers to guess and target with phishing attacks.

3. Create a naming strategy that will prevent account credentials and email addresses from being reused in the future. Recycling accounts can result in students inheriting a previously compromised account.

Student passwords

Student accounts are not exempt from needing strong passwords. Student accounts are frequently compromised by other students, especially when they are set up using a standard formula. For example, setting up student accounts using a student name as the username and their student ID number as the password is a poor security practice. Including personally identifiable and easily accessible information in user credentials teaches students poor cyber hygiene habits and leaves student account vulnerable to compromise, in violation of FERPA.

Because students don't usually arrive at school with the cybersecurity knowledge needed to protect their personal information, password management and basic cyber hygiene skills should be integrated into the curriculum. Teaching these skills doesn't necessarily require a significant time investment, and password management is a good place to start.

- Introduce students to best practices in setting up and protecting their user credentials. Develop and communicate clear policies and expectations regarding the use of student accounts and train students accordingly. Remind them never to share their login credentials with other students.
- Teach students how to make strong passwords, preferably using passphrases that are easy to remember and manage. A few minutes spent helping students set up memorable but secure passphrases can significantly reduce password reset requests and help minimize lost instructional time.
- Consider providing students access to a password locker or password management tool that streamlines and supports the utilization of strong passwords.

Successfully securing student accounts requires shifting the focus from convenience to cyber safety and life skills. Although in the short term teachers and system administrators may find it easier to set up and manage simple passwords for student accounts, this approach puts student data at risk and sends students the wrong message. Cybersecurity training is an area in which an ounce of prevention is worth several pounds of cure.

Today's students need to be prepared for a personal life that is increasingly integrated with technology and a modern workplace requiring the careful management of access credentials. Strong cyber hygiene skills are essential to help protect their privacy and personal safety.