Secure Passwords for Students

Defining the Issue: Secure Passwords for Students

- **Interactive Lessons and Games:** Use engaging, interactive activities to teach about password security. Create games where students build their strong passwords and explain why they're secure. This approach makes learning about cybersecurity fun and memorable.
- **Password Pictionary**: Students draw representations of a strong password without using letters or numbers, and their peers guess what it is. This encourages creativity in password creation and highlights the importance of using abstract concepts and symbols.
- **Cybersecurity Charades:** Here, students act out the principles of strong password creation (like avoiding common words, using a mix of characters, etc.) without speaking. This physical engagement helps cement the concepts in a fun, memorable way.
- **Real-World Scenarios**: Share stories (without causing alarm) about what can happen if passwords are weak. Relate these scenarios to their world, like social media accounts or personal data getting compromised.
- **Password Creation Workshops:** Host workshops where students create strong passwords for their school accounts. Teach them about password managers and the importance of not repeating passwords across different platforms.
  Use of Technology Leaders: Empower student tech leaders or a cybersecurity club to lead initiatives and spread awareness among their peers.

Tailoring Our Approach to Different Age Groups Within a School District

Kindergarten to Grade 2

- **Simple Concepts and Stories:** Use storytelling to introduce basic personal information and privacy concepts.
- **Interactive Activities:** Simple games and activities that teach them what a password is and the basic idea of keeping something secret.
- **Visual Aids:** Use cartoons and visuals to explain safe online behavior in a way that resonates with their understanding.

Grades 3 to 5

- **More Detailed Lessons:** Introduce the concept of strong passwords and why they're important.
- **Role-Playing Games:** Simulate scenarios where they must protect information with a password.
- **Creative Projects:** Encourage them to create posters or short presentations on safe online habits.

Middle School Students

- **Practical Workshops:** Hands-on workshops on creating strong passwords and using password managers.
- **Discussion and Debate:** Engage in discussions about real-world scenarios involving cybersecurity.
- **Online Safety and Ethics:** Introduce topics like social media safety, online etiquette, and the consequences of poor cybersecurity.

High School Students

- **In-Depth Curriculum:** Cover more advanced topics like data privacy, encryption, and cybersecurity careers.
- **Project-Based Learning:** Encourage projects that involve researching and presenting various cybersecurity threats and protection strategies.
- **Guest Speakers and Field Trips:** Introduce them to cybersecurity professionals and possibly organize visits to tech companies or cybersecurity labs.

Across All Ages

- **Regular Updates:** Keep the curriculum updated with the latest in cybersecurity trends and threats.
- **Parental Involvement:** Provide resources and workshops for parents to reinforce cybersecurity principles at home.
- **Empowerment Through Knowledge:** Focus on empowering students with knowledge, not scaring them with the consequences of poor cybersecurity.

National Institute of Standards and Technology (NIST) Guidance

The National Institute of Standards and Technology (NIST) last updated its password guidelines in 2017. This update was significant as it introduced several changes to the long-standing password security recommendations, focusing more on user-friendliness and practical security. These guidelines are detailed in NIST Special Publication 800-63B, which is part of a larger document, SP 800-63, Revision 3, entitled "Digital Identity Guidelines."

- **Length over Complexity:** NIST advises using long passwords, recommending a minimum of 8 characters for user-generated passwords and at least 6 characters for system-generated ones. Complexity (like mixing letters, numbers, and symbols) is less emphasized than length.
- **Avoiding Common Words and Phrases:** Passwords should not include easily guessable or common information like names, dates, or simple patterns.
- **Screen New Passwords Against Commonly Used Choices:** Organizations should check new passwords against lists of commonly compromised passwords to prevent users from picking easily hackable options.
- **Eliminate Periodic Resets:** NIST and Microsoft suggest doing away with routine password changes unless there's a known security issue. This counters previous advice, as frequent changes often lead to weaker password choices.
- **Encourage Passphrases:** Passphrases, which are longer and can be more memorable phrases, are recommended over traditional passwords for better security and usability.

- **Implement Multi-Factor Authentication (MFA):** MFA adds an extra layer of security, requiring a second form of identification beyond just a password.
- **User-Friendly Password Recovery:** Options for password recovery should be straightforward and secure, avoiding security questions with easily researchable answers.