Navarro ISD

Board Report

Technology Department

December 2024

Director

To enhance the security of our systems and protect sensitive information, we have implemented two-factor authentication (2FA) for all staff accounts. This additional layer of security requires users to provide two forms of identification when logging in: a password and a time-sensitive code generated by an authentication app or sent to a trusted device. This significantly reduces the risk of unauthorized access, even if a password is compromised. By enforcing 2FA, we are safeguarding our organization's data and ensuring the integrity of our operations. This proactive measure aligns with industry best practices and demonstrates our commitment to maintaining a robust security posture.

To bolster email security, we are looking to implement advanced phishing and malware protections. We are in the process of vetting a software that will scan emails, detonate any attachments or urls in a sandbox environment, and then determine whether the emails are safe before delivering it to the end user. This will add about a 30 second delay to email delivery, but should be relatively unnoticed by most users.

We have bolstered admin account security by requiring a more complex password, regular password changes, and required MFA for all Google and Classlink accounts. We are working to implement MFA into our other admin accounts, depending on the platform.

Systems Administrator

We also prioritized repairing GAM functionality to streamline the bulk management of Google users and devices. GAM is a critical tool in efficiently administering accounts and ensuring that user configurations align with organizational policies. Restoring this capability allows us to save time and minimize manual intervention when managing the ever-growing pool of Google accounts.

In addition, we are working on resolving issues with FOG, our imaging solution, to enhance its effectiveness in pushing devices back out to users. FOG plays an essential role in streamlining device deployment and ensuring uniformity across systems, and fixing this tool will help us better support staff and students.

Looking ahead, we have begun roadmapping a plan to improve password security for student accounts. This initiative aims to transition from a reactive approach to a proactive strategy, reducing vulnerabilities and enhancing overall account protection. By implementing stronger protocols and fostering best practices, we aim to provide students with a safer and more reliable digital experience.

Navarro ISD

Board Report

Network Administrator

1. **Network Optimization and Enhancements**: Continued improvements to the network have been implemented to optimize performance and enhance the overall user experience.
2. **New High School Network Planning**: The planning phase for the new high school network has been successfully completed, paving the way for enhanced connectivity and support for modern educational technologies.
3. **SEIM Solution Implementation**: Progress has been made toward the implementation of a Security Information and Event Management (SEIM) solution to bolster cybersecurity measures and ensure the safety of our digital assets.
4. **Secure Messaging Solution**: Steps are being taken to deploy a secure messaging system to facilitate the safe transmission of sensitive student information between staff and parents, ensuring compliance with data privacy standards.

Technicians

- The past month we have resolved 204/243 technology tickets. This leaves 39 that remain unresolved as we are waiting on parts, clarification, or responses from vendors and end users.
- We received and started setting up the 96 Staff devices that were approved by the board for purchase. These devices will be deployed the first workday back after the winter break.
- Three Cleartouch panels were installed at the JH to complete that campus ensuring that all teachers have access to an interactive touch panel.