MENIFEE COUNTY *PUBLIC SCHOOLS*

440 Wynn Flat Rd Frenchburg, KY 40322
Phone: 606-768-8002

DATA SECURITY UPDATE:

- **Menifee County's previous and upcoming actions to protect and increase data security**

- **Kentucky Department of Education's vision, project goals, and action items, crimes that multi-factor authentication can prevent, and why the Kentucky Department of Education is taking these steps**

Menifee County's previous and upcoming actions to increase our data security:

The process of transitioning all staff email accounts to a Multi-Factor Authentication (MFA) framework has been executed to bolster security measures.

The authentication credentials for staff email, Google services, and computer logins have been updated to adhere to the recommended standard of employing single sign-on with passwords comprised of a minimum of 15 characters as stipulated by KDE guidelines.

Notifications are sent to raise awareness of phishing email attempts and what to look for to identify these types of emails.

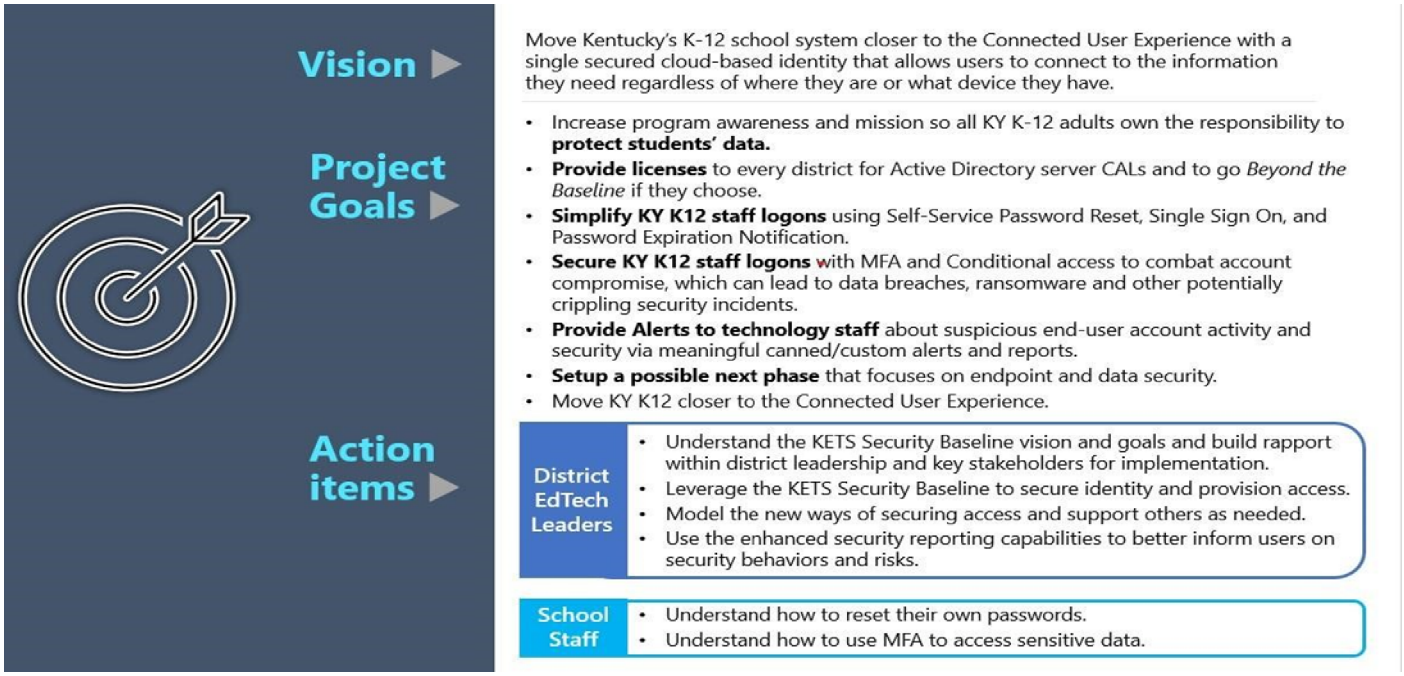
Network devices, firewall policy & cloud-based relay filtering systems were implemented and upgraded to protect our district staff and students.

During 2024-2025, our intentions encompass replacing 160 outdated access points throughout the school district. Active participation in recurring security training sessions and workshops.

MENIFEE COUNTY PUBLIC SCHOOLS

In the upcoming year 2024-2025, our initiative involves deploying Clever badge log-in on Chromebooks for K-3, specifically tailored to cater to our younger students. This strategic move aims to provide substantial assistance and support to our younger students.

Throughout the year 2024-2025, we plan to maintain a rigorous schedule for patching and updating software, operating systems, and applications to prevent vulnerabilities from being exploited.



MENIFEE COUNTY PUBLIC SCHOOLS

What sorts of Crimes Can MFA Prevent?

Multi-Factor Authentication (MFA) can prevent nearly every crime that starts with a criminal having your login name and password. **Here are several that have taken place in Kentucky K12:**

03/22/18 - A student **obtained the username and password** of a district staff member to access Infinite Campus. The credentials, which had been left unprotected, were used to alter attendance records and/or schedules of 5 students.

11/20/18 - Three district employees were **tricked via a phishing email** into giving their district login credentials to a crook, who then used their email accounts to request changes to their direct deposit information so those funds would be sent to the crook.

01/15/19 - Two students **utilized a teacher's logon cr**edentials, which the teacher had left posted on or near their workstation, to log on to the school network. The students found they had access to a shared network drive, which contained staff PII, resulting in a data breach.

05/03/19 - A school employee **was tricked by a phishing email** into sharing his password. The attacker used the stolen account to successfully have the employee's direct deposit information changed. Two pay periods were affected.

05/06/19 - A cyber-criminal **"cracked" the district CIO's password** and used the "Global Admin" permissions she had given her everyday user account to set up back-door dummy accounts and search through other users' files and folders for purchase order forms and information. The crook then submitted **fraudulent orders for approximately $250,000 of computers**. Despite being in the district's network for over 30 days, the plan was foiled when a vendor shipped the computers to the district anyway, not the attacker's provided address. This alerted the district to the crime, and over the course of several days of round-the-clock effort, the district and law enforcement were able to discover the plan, stop the orders and secure their network.

06/06/19 - District staff person **used co-worker's credentials** to look up relative's new teacher in the Kentucky Student Information System and while doing so, was able to access relative's PII but had no authority to do so, causing a data breach.

06/17/19 - A **KDE staff person's email account was compromised** by a cyber-criminal and briefly used to send spam email and malware/ransomware.

2/23/21 - One staff email account was **compromised by a cyber-criminal via a phishing email**. The cyber-criminal placed an auto-forward rule on the staff's mailbox and 2 emails containing unencrypted student data, including SSNs, were caught by the cyber-criminal before the compromise was discovered and remediated. This resulted in a data breach.

Why is Kentucky K12 Taking These Steps?

- Federal agencies predicted an **86% increase in cyber-attacks against schools** this year and research shows that **Education** is BY FAR the most aggressively attacked segment for multiple reasons
  - U.S. education community has been given significant funding over the past 2 years, which immediately drew the attention of cyber-criminals who want to steal it
  - K12 staff are very service-oriented and generally not as familiar with security controls as staff in other industries, which makes them easier targets
- **Ransomware increased 13%** - more than in the last 5 years combined
- **82% of breaches are due to people giving up/losing/being tricked out of passwords**
- Pandemic, Russian aggression and international reaction have caused an increase in the number and sophistication of cyber-attacks
- **Phishing is at an all-time high** and are becoming more sophisticated and better at *tricking people into sharing PII, passwords, clicking on ransomware, buying gift cards, and so on*
- Districts are being asked by their cyber-insurance providers to increase their security