Vision ▶

Move Kentucky's K-12 school system closer to the Connected User Experience with a single secured cloud-based identity that allows users to connect to the information they need regardless of where they are or what device they have.

Project Goals ▶

- Increase program awareness and mission so all KY K-12 adults own the responsibility to **protect students' data.**
- **Provide licenses** to every district for Active Directory server CALs and to go *Beyond the Baseline* if they choose.
- **Simplify KY K12 staff logons** using Self-Service Password Reset, Single Sign On, and Password Expiration Notification.
- **Secure KY K12 staff logons** with MFA and Conditional access to combat account compromise, which can lead to data breaches, ransomware and other potentially crippling security incidents.
- **Provide Alerts to technology staff** about suspicious end-user account activity and security via meaningful canned/custom alerts and reports.
- **Setup a possible next phase** that focuses on endpoint and data security.
- Move KY K12 closer to the Connected User Experience.

Action items ▶

District EdTech Leaders

- Understand the KETS Security Baseline vision and goals and build rapport within district leadership and key stakeholders for implementation.
- Leverage the KETS Security Baseline to secure identity and provision access.
- Model the new ways of securing access and support others as needed.
- Use the enhanced security reporting capabilities to better inform users on security behaviors and risks.

School Staff

- Understand how to reset their own passwords.
- Understand how to use MFA to access sensitive data.

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

Sample Digital Content

Leverage individuals at all levels of the district to move the change effectively.

Staff Communication

KY District Examples
MFA Website - JCPS MFA Site Link
MFA Email Communication – Carter County Link
SSPR Email Communication – Pike County Link
SSPR/MFA/Passphrase Website – JCPS Site Link
Screen Shot Examples – Dayton Independent Link