

SPONSORED

School districts can drive an easy way to 100% MFA coverage, closing security gaps

Published June 21, 2022

iStock.com/AndreyPopov

SPONSORED CONTENT BY **yubico**

When the pandemic sent millions of workers to home offices, some gaping security holes were revealed. Legacy systems, budget constraints and a system unprepared to handle this new way of working and teaching only made those vulnerabilities even more obvious.

The federal government has been using smart cards for logging securely into workstations for decades, but smaller government and education entities with lesser security budgets have had to rely solely on usernames and passwords. A recent report logged 166 publicly disclosed cyber incidents affecting 162 school districts across 38 states. Ransomware was the most frequently disclosed incident, and data breaches (most of them coming through school vendors and suppliers) came in second.

The old username-password model clearly leaves critical information and records vulnerable to attack. Some schools moved to mobile-device-based multi factor authentication (MFA) as a response, a good step in the right direction. But even that move created its own problems – many employees can't, don't or won't use mobile devices for MFA. Here are just a few reasons why:

- They don't own smartphones or they live in low-connectivity areas.
- They don't want to give their IT departments admin access to a personal device (and they probably shouldn't be asked to).
- Compliance issues or union restrictions may prohibit using personal mobile devices for work.
- It's not cost effective for school districts with limited budgets to buy hundreds of mobile devices or reimburse faculty and staff for mobile-related costs.

Full multi-factor authentication coverage is best implemented through hardware-based security keys. These keys are physical, one-touch authentication devices users can plug into their computers or tap against their mobile phones to access critical systems and applications. Yubico's YubiKey, for example, is phishing-resistant and helps eliminate account takeovers. Many government agencies around the country have found YubiKeys fit well with a zero trust security architecture, allowing the agency to challenge a user with simple, one-touch authentication when the user's security posture must be reaffirmed.

Implementing 100% MFA for K-12 organizations is a multi-step process that should involve the following:

- Create a strategic plan and business justification for the cost is a critical first step
- Identify government grants that can help fund the MFA project if needed
- Ensuring successful grant applications is making sure they align with federal policies and standards – phishing-resistant MFA and zero trust

- Pick products that align with those policies, leveraging infrastructure in place today and solving the agency risk tolerances:
 - Unify the identity infrastructure to shrink the attack surface
 - Provide authenticator options dependent on risk tolerances, as not all MFA is created equal:
 - Legacy mobile-based MFA like OTP and push are frequently getting phished
 - MFA utilizing FIDO security keys such as YubiKeys stops phishing attacks
- Communicate with stakeholders and roll out the new system in a way that makes them feel heard and clearly explains what's happening

Phishing-resistant hardware keys for 100% MFA coverage

Before buying a hardware security key, check that it is compatible with the leading identity and access management (IAM) systems, including Microsoft, Okta, Duo Security and Ping. Flexibility and scalability will save on transition costs and make it easier for employees to adopt the new process. A hardware-based MFA solution should rely on the latest FIDO U2F and FIDO2 authentication protocols that provide strong two-factor and multifactor authentication. Organizations can defend against phishing attacks seeking to steal credentials, reducing the chance that a man-in-the-middle attack – when a hacker eavesdrops or alters communications between two parties – will be effective.

The pandemic permanently changed the way we do business and the way we work. It may take some time for education to catch up on the security front, but hardware-based security keys such as the

YubiKey, offer the quickest way to get to full MFA for our most vulnerable school districts.