YubiKey

Achieve 100% MFA across education to protect against modern cyber threats

Lack of an MFA strategy puts you at risk
Multi-factor authentication (MFA) is becoming a critical aspect of cyber defense strategies and cyber insurance mandates across the higher education and K-12 school landscape. According to the 2021 IBM Security Cost of a Data Breach Report, the average cost of a data breach in education is $3.79 million. While MFA can be a strong first-line of defense against modern cyber attacks such as phishing and ransomware, not all forms of MFA are created equal. Legacy authentication such as usernames and passwords can be easily hacked, and mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to modern phishing attacks, malware, SIM swaps, and man-in-the-middle (MiTM) attacks.

Safeguard faculty, staff, and students with the YubiKey
To protect against modern cyberthreats, Yubico offers the YubiKey—a hardware security key for phishing-resistant two-factor (2FA), MFA, and passwordless authentication at scale. It is the only solution proven to completely eliminate account takeovers in independent research.

The YubiKey is simple to deploy and use—a single YubiKey can be used across legacy and modern applications, services, and devices, with multi-protocol support for Smart Card, OTP, OpenPGP, FIDO U2F and FIDO2/WebAuthn on a single key, and doesn’t require a battery or internet connection.

YubiKeys are highly suitable for users that can’t, won’t, or don’t use mobile authentication due to teacher’s union restrictions, personal preferences, cellular geographic inconsistencies, and more, helping you achieve 100% MFA coverage across your institution.

Risk of account takeovers

- **FIDO Security key (YubiKey)**: 0%
- **On-device prompt**: 10%
- **SMS code**: 24%
- **Secondary email**: 21%
- **Phone number**: 50%

Research by Google, NYU, and UCSD based on 350,000 real-world hijacking attempts. Results displayed are for targeted attacks.

How the YubiKey can help you secure your technology, data, and users:

1. **Meet your cyber insurance requirements**

Higher education and K-12 schools can face a shortage of cybersecurity insurance capacity and increased cost for coverage if MFA isn’t satisfactorily deployed across the entire ecosystem. Restrictions could include reduced sublimits, higher deductibles, and narrower coverage terms. Cyber policy non-renewals may also be a potential outcome, which can expose a school to significant risk if targeted by hackers, phishing attacks, or ransomware attacks. YubiKeys offer the strongest MFA protection across the industry, ensuring compliance to your cyber insurance mandates.
2. Secure access to data from anywhere, and from any device
Cloud-based SaaS applications such as Google GSuite and Microsoft Office 365, accelerated adoption of online learning platforms, and user mobility have accelerated digital transformation across the academic sector. Faculty, staff, and students need secure and quick access to email, applications, and data from any location—on or off-campus, and from any device.

YubiKeys offer phishing-resistant MFA, ensuring only authorized users have access to the right applications and data. YubiKeys integrate seamlessly with existing identity and access management (IAM) and identity provider (IDP) solutions such as Microsoft, Okta, DUO, Ping, and more than 700 applications and services out-of-the-box, including Google Suite, Microsoft Azure, Microsoft Office 365, Box, Jamf, and identity and credential management (ICAM) solutions, eliminating rip and replacement of existing solutions.

3. Secure shared workstations
With the YubiKey you can secure access to shared workstations and devices with highest-assurance MFA and passwordless authentication, and deliver a convenient user experience—even for remote access. A single YubiKey works across multiple devices including desktops, laptops, mobile, tablets, notebooks, and shared workstations, enabling

Palo Alto Unified School District (PAUSD) Protects Student Data with YubiKeys
PAUSD, located in Silicon Valley, had an incident where student grade information was being exposed on a third party website related to compromised credentials of a teacher’s account.

Today, all PAUSD staff use YubiKeys in their daily computing activities. Student information databases are protected by the YubiKey at the staff level, as well as personal data at the parent and guardian level.