Protecting against modern cyber threats across education

Cultivate phishing-resistant users to defeat modern cyber attacks

Cyber pressure keeps growing

Educational institutions are targeted for a number of reasons, primarily for the amount of personal student data, student loan information, confidential research data, and a lack of adequate cybersecurity. Over the last few years, ransomware attacks have become an increasing concern for schools and colleges worldwide, and with the advent of AI-driven phishing attacks, can have more frequent and costly consequences.

66%

63% of lower education and 66% of higher education organizations were hit by ransomware in 2024

Source

$3.76 million

The mean cost for lower education organizations to recover from a ransomware attack more than double than 2023

Source

$4.02 million

The mean cost for higher education organizations to recover from a ransomware attack was almost four times higher than 2023

Source

Not all MFA is created equal

Legacy authentication is not phishing resistant

While any MFA is better than a username and password alone, not all forms of multi-factor authentication (MFA) are created equal. Legacy mobile-based authentication such as SMS, OTP codes, and push notifications are highly susceptible to phishing attacks, malware, SIM swaps,and attacker-in-the-middle attacks. According to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-B4, **only two forms of authentication currently meet the mark for phishing-resistant MFA**: Smart Card/PIV and the modern FIDO2/WebAuthn authentication standard.

Legacy authentication creates MFA security gaps

Mobile-based authenticators create high-risk security gaps in an MFA strategy, when **users can't, don't, or won't use mobile authentication** due to union restrictions, personal preferences, cellular geographic inconsistencies, mobile-restricted locations, financial reasons and more.

yubico

Cultivating phishing-resistant users across faculty, staff and students

Modern, hardware security keys such as the YubiKey, are the only technology that offer phishing-resistant multi-factor and passwordless authentication that stops phishing attacks, account takeovers, and ransomware attacks initiated by compromised credentials, helping educational institutes stay protected, ensure compliance to regulations and cyber insurance MFA requirements. YubiKeys work with over 1,000 applications and services and are also highly suitable for users that can't, don't, won't use mobile authenticators and for mobile-restricted use cases. The YubiKey:

Helps **Reduce risk by 99.9%** and stops account takeovers with strongest phishing resistance Source

Is **FIPS 140-2 validated** (Overall Level 1 and Level 2) and meets Authentication Assurance Level 3 requirements (AAL3) of NIST SP800-63B

Helps **Bridge to modern FIDO passwordless authentication** with multiple authentication protocols on a single key—Smart Card (PIV/CAC), FIDO2/ WebAuthn, FIDO U2F, OTP, OpenPGP

Acts as a **Portable root of trust** that is ideal for shared workstations and devices

Reduces help desk costs by up to 75% Source with self-service password resets, and helps **lower cyber insurance premiums by 30%** Source

Discover how the YubiKey can help you drive phishing-resistant MFA at scale in our whitepaper, Graduating from legacy MFA to modern authentication

Contact us
yubi.co/contact

Learn more
yubi.co/edu

Yubico (Nasdaq First North Growth Market Stockholm: YUBICO) is the inventor of the YubiKey, the gold standard in phishing-resistant multi-factor authentication (MFA). The company is a pioneer in delivering hardware-based passwordless authentication using the highest assurance passkeys to customers in 160+ countries. For more information, visit: **www.yubico.com**.

yubico