Beyond Identity for Educational Institutions

BEYOND IDENTITY

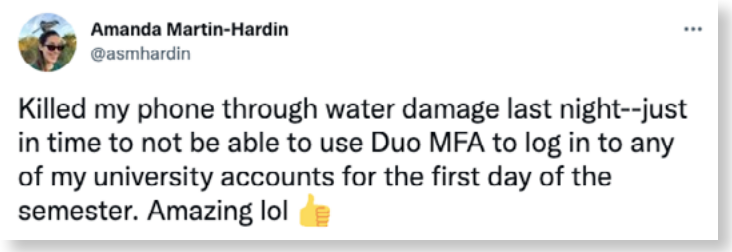
Overview

The number of cyberattacks continues to rise in all sectors, and education and research are the most targeted industries.

Recent studies show a 44% increase in targeted attacks against educational institutions in the first half of 2022. That's a 114% increase during the last two years (Check Point and CPR, Cyber Attack Trends: 2022 Mid-Year Report).

Protecting student, faculty, and staff data has become a priority for all educational institutions. However, the proliferation of cloud applications and the move to remote learning and working means that it is exponentially more difficult to control access to resources and sensitive data. Plus, users are overwhelmingly frustrated with the friction involved with mandatory multi-factor authentication (MFA) methods while attackers are increasingly successful in hacking traditional MFA.

Beyond Identity allows security and IT teams to easily roll-out unphishable MFA that users will actually enjoy with no passwords, one-time codes, push notifications, or second devices. Moreover, Beyond Identity provides immutable identity verification and allows for risk-based access control based on real-time user and device security signals.



The challenge: balancing security and usability in hybrid environments

Unlike previous generations, both on-campus and remote students, faculty, and staff are 100% reliant on digital resources to complete their education and work. With the move to cloud and mobile architecture as well as the transition to remote learning and work, traditional network perimeters are dissolving, leaving IT departments racing to mitigate the urgent threats of unauthorized access.

However, existing authentication solutions force a tradeoff between security and usability. Students, faculty, and staff complain about the friction of jumping through MFA hoops with second device requirements to get access to the resources they need to be successful. Making matters worse, attackers are now able to routinely exploit these traditional MFA methods.

The potential cost of remediation and damage to reputation can be devastating. In late 2021, a ransomware attack led to the closure of Lincoln College. In early September, Los Angeles Unified School District was also targeted in a ransomware attack that led to the disclosure of sensitive data, including Social Security numbers, as a consequence of not paying the ransom.

In May 2022, attackers breached Cisco's network and threatened to leak stolen files online if the company didn't meet their demands. If attackers can breach the security of a Fortune 500 company, one that owns a leading MFA software (Duo), then every educational institution using that software is at risk.

The solution: MFA built for the zero trust world

So how do you secure your organization now and in the future? You must adopt a zero trust security architecture that utilizes unphishable MFA, is completely passwordless, and actively uses zero trust authentication.

- Single-device MFA. Educational institutions using government funding or accepting government grants for research are under direction to adopt phishing-resistant MFA. Single-device MFA is part of a phishing-resistant MFA solution and can serve as another line of defense against exploitation of VPN technology.
- Passwordless. Passwordless authentication technologies, if architected properly, truly eliminate any use of passwords while avoiding push notifications and one-time codes. This type of technology is readily adopted by users and keeps password reset tickets to a minimum.
- Zero trust. Increasingly, educational institutions are pursuing zero trust security strategies to provide least privileged access to faculty, staff, and students while continuously enforcing access policies. Your authentication should adhere to and empower the achievement of zero trust by ensuring trust in the identity of the user as well as trust in the devices used.
- Built to serve on-premises and increasingly cloud-based apps and resources. Educational IT is a mix of traditional on-premise applications, storage, and data and cloud-enabled assets. Any technology employed must be built for the hybrid IT world and built for high availability.

Zero Trust Authentication Requirement	*Beyond Identity*	*Differentiation*
Frictionless: Easy for users to adopt and accelerates speed to resources	✓	Beyond Identity lowers MFA friction to zero by completely removing the need for second devices
Unphishable: No reliance on phishable factors including one-time codes, push notifications, and magic links	✓	Beyond Identity delivers unphishable MFA with: • Something you have - possession of private key within device secure enclave • Something you are - local device biometric
Passwordless: Eliminate threat of password-based attacks and also saves costs on help desk calls for password resets and lockouts	✓	Given our architecture, passwords can be fully eliminated from the user experience and database. What doesn't exist cannot be breached.
Zero trust compliance: Never trust and always verify every user and device, in real-time and continuously, that is requesting access	✓	Given our architecture, each device is cryptographically bound to a specific user identity to ensure that the right person, with a secure device, is accessing the right data Every authentication is also evaluated for real-time device risk continuously
Ease of deployment: Able to support on-premise and cloud-based apps and resources	✓	Beyond Identity is highly available, elastically scalable, and integrates with all major IDPs/IDaaS solutions while providing support for hybrid IT environments