SECRET DOUBLE OCTOPUS

CASE STUDY

Passwordless MFA Helps University Bolster Security with a Better Student and Faculty Experience

Octopus Platform Stops Phishing, Facilitates Matriculation, and Preserves Academic Freedom

Institutions for higher education rank among cyber criminals' top targets for phishing campaigns that lead to modern ransomware attacks. To stay out of the headlines, IT and security leaders at large colleges and universities have rolled out multi-factor authentication (MFA) to verify user identity—only to find that it doesn't stop phishing.

Customer

Industry: 100+-year-old state university consisting of multiple schools

Headquartered: USA

Size: Approximately 7K users

Such was the case at one state university prior to adopting passwordless MFA from Secret Double Octopus. **"We started out using extremely lengthy username/password combinations to verify identity,"** the project leader recalls. **"Then we added the step of sending one-time passcodes via SMS messages and emails, and we still had a security incident with all that in place."**

The university's cyber insurance provider attributed a recent breach that impacted university systems to the failure of traditional MFA to prevent users from being phished for working credentials. The incident led the security team to begin exploring other options that would deliver stronger user authentication while at the same time meeting the unique security challenges of higher education.

Cyberattacks Hit Higher Education Harder than Most

With security staffs routinely understaffed, universities face more dire consequences as a result of cyberattacks than other industries:

79%

of higher education providers reported being hit by ransomware

Sophos

25%

Higher rate of insider threats (student, staff) reported in 2022

Verizon DBIR

40%

of schools say fewer insurance providers are offering them coverage

Sophos

Passwordless MFA satisfies diverse user expectations

The potential impact of ransomware and other cyberattacks continues to rise as many schools offer remote learning and access to shared assets on a permanent basis. In addition, the ideal MFA solution keeps things simple for users and IT.

> **"You need to build stronger security — traditional controls are just too vulnerable — but you can't make the process of logging in too cumbersome to the end-user,"** the IT leader says. **"You can't have MFA that creates overkill or users won't be able to utilize it."**

Once they concluded a passwordless approach was essential to stop phishing, the team evaluated multiple solutions, including ones they had in place or had access to through other products in their infrastructure. The need to curtail "MFA push fatigue" led identity managers to rule out the use of hardware keys and physical tokens to verify identity.

At one point they had used smartcards to support an off-campus facility and found it proved too complicated. Users quickly grew frustrated with having to carry around tokens and IT concluded the solution wouldn't scale to a campus with thousands of users.

Security professionals also needed a solution that supported convenient push notifications and biometrics (face, voice, fingerprint scanning) to verify identity from any device to satisfy universities' other user base—faculty members that aspire to maintain their academic freedom. Like many enterprises, the university wished to balance the flexibility for employees to use their own devices with the need to secure shared resources and protect data.

After considering several passwordless approaches, the team **conducted a proof-of-concept (PoC) demonstration with Double Octopus.** The platform delivered phishing-resistant MFA while supporting remote access, high device turnover among students, and the faculty's academic freedom.

> **"SDO was definitely the best all-around fit for our needs,"** the team leader recalls. **"It does what we need it to do — stops phishing and keeps the process of authenticating simple for users — and the rollout was easy to manage with a limited staff."**

Passwordless improves ROI while keeping the phish out of school

By removing the vulnerable user password from the local and remote login process, Octopus passwordless MFA **stops phishing that leads to ransomware attacks and other breaches.** The platform also improves the business case for FA by removing user passwords without forcing the team to overhaul applications or its backend directory infrastructures.

Stronger authentication helps satisfy evolving regulatory requirements including NIST 800-171 as well as mounting pressure from cyber insurance carriers to fortify defenses against ransomware.

In the end, upgrading to the Octopus solution lets the university balance compliance and user experience with the pressing need to avoid phishing attacks and improve security posture quickly and well into the future.

SECRET DOUBLE OCTOPUS