

Threat Intelligence Brief:

Higher Education Under Attack

Thank you for your interest
in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through GSA, NASPO, The Quilt and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with KnowBe4, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.



To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com



Explore More Resources:
carah.io/KnowBe4Resources



Join Events & Webinars:
carah.io/KnowBe4Events



Discover Technology Solutions:
carah.io/solve

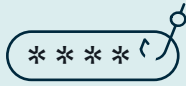


Learn About Procurement:
carah.io/KnowBe4Contracts



Connect With Our Team:
KnowBe4@carahsoft.com
(844) 445 5688

Threat Intelligence Brief: Higher Education Under Attack

**68.9%**

Built to Harvest Credentials

Two-thirds of phishing emails reaching higher education are designed to steal logins. Once compromised, stolen credentials can expose student records, research data and payment details.

35.9%

Designed to Evade Inspection

More than a third of analyzed phishing emails spoofed headers, obfuscated links and other evasions carried in the message itself. In 23% of higher education institutions, it is the single most common phishing characteristic.

~ 45%

Taking Advantage of Trust

Nearly 45% of phishing emails aimed at higher education rely on social engineering or business email compromise (BEC).

The Threat Intel the Education Sector Needs

More than two-thirds of phishing emails reaching higher education institutions are designed to steal credentials and give attackers access to valuable information.

The way in? Close to 45% rely on social engineering or business email compromise (BEC), while more than a third of the phishing reaching higher education is constructed to defeat inspection rather than to convince users. These technical tactics include spoofed headers, obfuscated links and other evasion built into the message itself.

Higher education infosec professionals are also defending against these campaigns with less to work with.

**Only 20%**

of higher education institutions in KnowBe4's own Defend platform data run a third-party email gateway,

versus 33% across all Defend customers.

Those that have a SEG still see 35.9% of phishing emails fitted with technical evasions, versus 27.4% for all Defend customers. The evasion is getting through the existing tooling.

KnowBe4 Defend Safeguards School and University Inboxes

That's the gap KnowBe4 Defend is built to close. Its behavioral AI reads linguistic patterns, urgency cues and historical communication context rather than just scanning for known-bad indicators, so it catches social engineering, BEC and attackers' technical tricks before an employee ever engages. Defend also pairs that detection with in-the-moment, localized teachable moments that turn every near-miss into lasting behavior change.

Turn the person who opens the email into a last line of defense supporting your educational institution's already overworked infosec team.

Education is a uniquely hard security awareness environment: multiple campuses, 50,000 inboxes, students, faculty and staff who all think about risk differently, and a security team that's usually five people, not 50. KnowBe4 is built for that reality. KnowBe4 combines automated email and collaboration security, AI-driven training that adapts to real click behavior and unified reporting so a five-person security team can protect a 50,000-person campus as effectively as a Fortune 500.

All data taken from the KnowBe4 Defend tool from April to September, 2026

[Learn More](#)