THE COMPROMISED CAMPUS

From impersonated faculty emails to stolen research data, account takeovers are striking at the heart of the academic mission. Here is how IT leaders can fight back.

A Scoop News Group Report

Higher education has spent decades fortifying the digital perimeter by modernizing identity systems, securing cloud platforms and building digital "moats" around sensitive data. Yet today's most damaging cyber incidents rarely involve breaching those defenses with advanced malware. Instead, attackers are exploiting something far more basic: **trust.**

Account takeover (ATO) attacks — in which criminals hijack legitimate credentials through phishing or social engineering — are accelerating across the academic landscape. The consequences are widespread and often invisible at first. Faculty email accounts are weaponized to spread internal phishing links. Student accounts are mined for financial aid data. Administrative credentials become a skeleton key to sensitive research, donor records and health care systems.

In higher education, the risk is not just technical; it strikes at the core of the academic mission. Universities are designed for openness, collaboration and ease of access. Attackers have learned how to turn that culture of trust into an attack surface.

"Attackers don't have to break in anymore; they just log in," says Paul Chavez, Senior Product Marketing Manager at Proofpoint. "Once they control a trusted account, every system downstream assumes that activity is legitimate."

A perfect storm: Why campuses are targets

Universities are uniquely vulnerable because they operate more like small cities than centralized enterprises. Highly mobile populations, decentralized IT environments and constant onboarding and offboarding create ideal conditions for credential-based attacks.

Proofpoint research shows that more than 70% of successful breaches involve a human element, such as phishing or credential misuse, rather than malware alone. Several factors make the campus environment a goldmine for credential-based attacks:

- **A REVOLVING DOOR OF USERS:** Every semester brings a wave of new students and adjunct staff. Many arrive with poor "password hygiene" and access sensitive systems from unmanaged personal devices.
- **A CULTURE OF OPENNESS:** Higher education thrives on sharing research and data across departments and borders. This makes lateral movement easy for an attacker once they have a foothold.
- **HIGH-VALUE TARGETS:** From federally funded research and intellectual property to sensitive healthcare data and financial aid records, universities hold the kind of data that fetches a premium on the dark web.
- **FEDERATED GOVERNANCE:** Unlike a centralized corporation, security policies often vary wildly between a university's medical school, athletic department and liberal arts college.

"These environments are built for access and collaboration," says Chavez. "Attackers understand that, and they take advantage of it."

Red flags for campus IT

Keep an eye out for these common indicators that an account has been compromised and an attacker is attempting to establish persistence.

MFA Fatigue & Spamming	Users reporting unexpected or endless login prompts; attackers often use a victim's stolen password to trigger repeated authentication requests until the user hits "yes" out of frustration.
Hidden Mailbox Rules	The sudden appearance of new rules designed to auto-forward sensitive emails to external addresses or automatically delete messages to hide the attacker's tracks.
Unauthorized OAuth Applications	The installation of third-party applications with broad access permissions, which allow attackers to maintain persistent access without needing a password.
Weaponized Internal Documents	Legitimate files within SharePoint or OneDrive that have been modified to include malicious scripts or lures to compromise other users across the institution.
Anomalous Behavioral Signals	Large-scale downloads of research files, unusual login locations, or access to sensitive cloud storage folders at atypical hours.
"Urgent" Internal Impersonation	Emails from leadership or faculty — often sent as part of an existing thread — requesting wire transfers, sensitive data, or payment rerouting.

> "Attackers don't have to break in anymore; they just log in. Once they control a trusted account, every system downstream assumes that activity is legitimate."
>
> —Paul Chavez, Senior Product Marketing Manager, Proofpoint

From phishing to full-scale compromise

Most account takeover incidents in higher education begin with phishing — but today's attacks are far more sophisticated than generic spam. Proofpoint data shows that nearly 60% of compromised accounts are later used for internal phishing or impersonation, enabling attackers to spread laterally using trusted identities. On a campus, that often means one compromised account quickly becomes many.

"The initial click is just the beginning," says Chavez. "The real damage happens once the attacker can operate as a legitimate user."

Modern campaigns rely on highly targeted lures that mimic financial aid notices, research updates or learning management system alerts. Increasingly, attackers exploit compromised internal accounts to send malicious links from trusted senders, abuse OAuth permissions to maintain persistent access, and layer multi-stage tactics that escalate privileges before exfiltrating data.

Once inside, attackers move fast. They create inbox rules to hide security alerts, modify multifactor authentication (MFA) settings or use stolen session cookies to bypass additional controls. By the time suspicious behavior surfaces, the compromise is often well established.

Anatomy of an attack

While higher-education security leaders often view account takeover as a singular event, such as a stolen password or a clicked link, modern attacks follow a calculated lifecycle that exploits the "frictionless" nature of campus digital environments:

RECONNAISSANCE:
Cybercriminals are opportunistic and often target a university's partners or suppliers to exploit trusted relationships. By breaching a third-party account, they can use that existing trust to bypass institutional security perimeters.

INITIAL COMPROMISE:
Beyond standard phishing lures, attackers use MFA bypass techniques such as session hijacking and OAuth abuse. A typical campus tactic is MFA spamming, where a user is bombarded with push notifications until they approve the request out of sheer frustration.

PERSISTENCE:
Once inside, attackers entrench themselves by creating hidden mailbox rules, adding rogue authentication methods or installing third-party applications with broad permissions.

IMPACT:
With a foothold secured, they impersonate the victim, inject malware into active conversations, redirect payments or exfiltrate research and student data. Because the activity originates from legitimate accounts, it frequently evades traditional security controls designed to filter external threats.

Understanding this lifecycle is critical. Focusing only on how attackers get in obscures how they stay in and how far they spread.

The limits of traditional defenses

Higher-education institutions have invested heavily in identity security. Single sign-on, MFA and email filtering are now standard.

Yet these controls were designed for perimeter-based threats, not trust-based compromise.

Proofpoint research indicates that more than 90% of phishing attacks leading to compromise now bypass basic email filters, often because they originate from trusted accounts or legitimate cloud services.

MFA remains essential but not infallible. Push fatigue, social engineering and token abuse can all undermine it. "MFA is critical, but it's not a silver bullet," says Chavez. "If teams focus only on the login event, they miss the behavioral signals that show an account has already been compromised."

Email security cannot prevent abuse once a legitimate account is under an attacker's control, and static detection rules struggle to distinguish normal academic collaboration from subtle misuse.

The result is a widening gap between compromise and detection — precisely the window attackers exploit to establish persistence, move laterally and amplify impact.

Reframing ATO as a people-centered problem

One of the most important shifts underway in higher-education security is the recognition that account takeover is fundamentally a human-centered threat. Proofpoint's Human Factor research shows that users interact with malicious content in roughly 1 out of every 5 attacks, underscoring how central human behavior has become to modern cyber risk.

"People aren't the weakest link: They're the most targeted," says Chavez. "Defenders need visibility into how real users behave so they can tell when something is off."

Addressing ATO, therefore, requires more than tightening technical controls. It demands deeper insight into user behavior, context and intent. Security leaders are increasingly focused on the ability to:

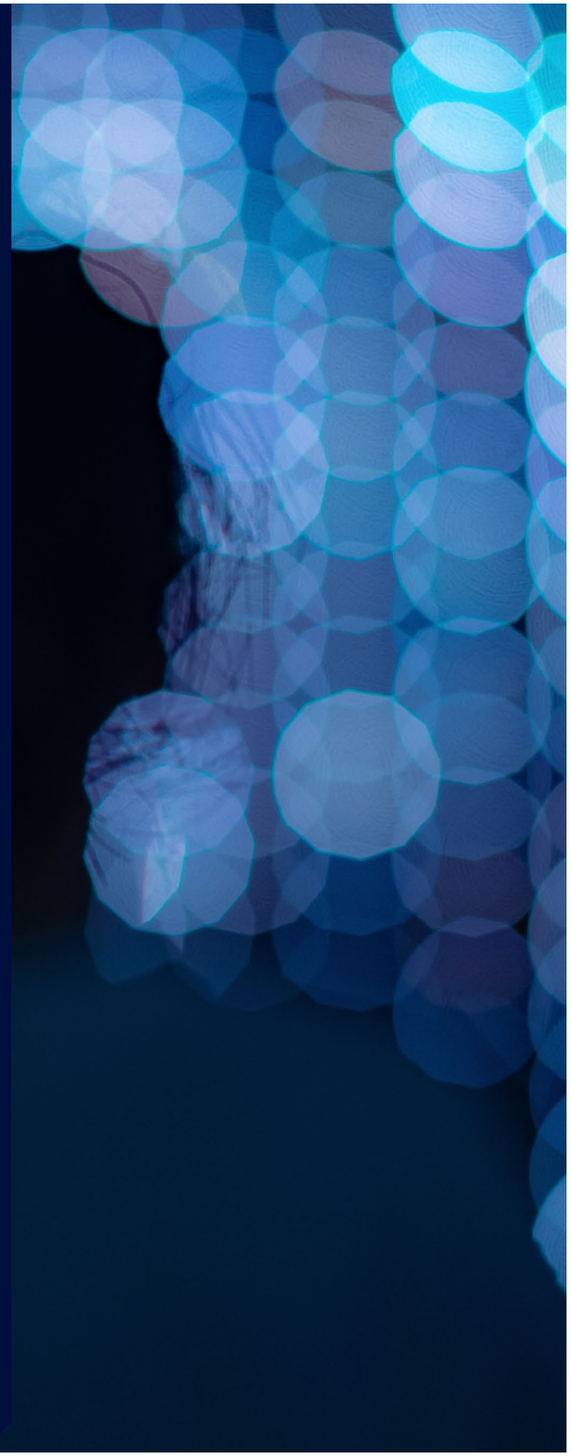
- Establish behavioral baselines for students, faculty and staff.
- Detect anomalous activity even when credentials appear valid.
- Identify high-risk accounts based on role, access and exposure.
- Respond to post-compromise behavior — not just suspicious logins.

This approach shifts institutions from perimeter-based defense toward continuous protection of trusted identities throughout their lifecycle.

Closing the gap with Proofpoint

How Proofpoint's integrated platform stops the ATO lifecycle.

Solution	Key Functionality
Collaboration Security Prime	A unified platform that stops human and AI agent-centric threats with 99.999% efficacy. It extends protection beyond email to analyze messages across Teams, Slack, Zoom and other channels.
Nexus AI & Relationship Graph	Uses an "ensemble" of AI models — including Nexus RG — to identify subtle behavior changes and anomalies in user communication even when credentials appear valid.
Cloud App Security Broker (CASB)	Provides full visibility into post-compromise activity by monitoring mailbox rule changes, MFA modifications and unauthorized file access in platforms like Microsoft 365.
Targeted Attack Protection (TAP)	Identifies "Very Attacked People" (VAPs). It uses the Attack Index to score threats based on actor sophistication and attack volume, allowing teams to prioritize high-risk users.
Threat Response Auto-Pull (TRAP)	Reduces attacker dwell time by more than 50%. It automatically expands to follow forwarded mail and distribution lists to quarantine malicious messages post-delivery.



Building a modern ATO defense strategy

According to Chavez, a comprehensive approach to reducing account takeover risk in higher education typically spans four core pillars.

01 Strengthen Identity Protection:

Institutions should continue to mature identity foundations, including phishing-resistant MFA, adaptive authentication and least-privilege access.

02 Detect Compromise through Behavior:

Behavioral analytics can surface early signs of compromise (e.g., unusual login locations, atypical data access or abnormal email-sending patterns) even when credentials appear legitimate.

03 Reduce Post-Compromise Blast Radius:

Proofpoint data shows that organizations with automated containment capabilities can reduce attacker dwell time by more than 50%, sharply limiting lateral movement.

04 Educate and Support users:

Security awareness remains essential, but it must be timely and contextual — moving beyond annual training to real-time prompts and in-the-moment guidance for high-risk users.

Proofpoint is focused on protecting the full lifecycle of account takeover, from initial credential theft to post-compromise abuse.

"What matters is context," says Chavez. "When teams can correlate identity, email and behavior, they can stop one compromised account from becoming a campus-wide incident."

Modern platforms increasingly combine:

- Advanced threat detection across email and cloud environments.
- Identity-centric analytics that surface risky behavior.
- Automated response capabilities to contain threats.
- Human risk insights that help institutions prioritize protection.

For resource-constrained IT and security teams, this integrated visibility can be the difference between a contained incident and a campus-wide disruption.

Looking ahead

The impact of account takeover extends well beyond cybersecurity metrics. Repeated compromises erode institutional trust, disrupt teaching and learning, and strain IT teams already operating with limited resources.

The scale of this threat is further highlighted by Proofpoint data showing that attackers lurk undetected in compromised accounts for an average of 233 days before discovery. This extended "dwell time" provides a massive window for data exfiltration and lateral movement across the campus ecosystem.

Furthermore, the financial stakes are higher than ever; research indicates that the average cost of an account compromise involving a third-party supplier is $4.76 million. Given that 80% of organizations face attacks from compromised supplier accounts every month, the "culture of openness" in academia is now under constant financial and operational siege.

As higher education's digital transformation accelerates, the attack surface will only expand. With cloud adoption, remote learning and external collaboration now permanent, protecting identities is synonymous with protecting the institution itself. The institutions that succeed will be those that recognize account takeover as an ongoing, human-driven threat and respond with greater visibility, adaptability and speed. By combining strong identity controls, behavioral detection and user-centric risk management, colleges and universities can move from reactive cleanup to proactive defense. This shift may prove to be one of their most consequential security investments.

Learn how Proofpoint takes a human-centered approach to meet the compliance needs of higher-education institutions and improve their cybersecurity posture.

This report was produced by Scoop News Group for EdScoop and underwritten by Proofpoint.

EDSCOOP proofpoint.