LexisNexis®
RISK SOLUTIONS

When Attackers Log In

7 Steps to Help Reduce Account Takeover Risk for Higher Education Institutions

Higher education institutions have invested heavily in securing networks, applications, and data. Yet many of today's most damaging incidents don't begin with a system breach. They begin with a successful login.

Account takeover (ATO) is not simply the use of stolen credentials—it's the unauthorized control of a legitimate digital identity. In higher education environments, this often involves a combination of compromised credentials, session hijacking, or social engineering tactics that allow a bad actor to pass authentication checks and assume the privileges of a verified user. Once access is established, activity typically blends in with normal user behavior, making detection difficult and allowing misuse of systems, data, and institutional processes under the guise of legitimate access.

This tip sheet outlines **seven practical, non-disruptive steps colleges can make** to reduce account takeover risk, protect campus operations, and reinforce trust—without overburdening accessibility or the student user experience.

The Scope of the Risk

In the education sector, **86% of breaches** involve compromised credentials.[1]

More than **70% of successful breaches involve a human element such as phishing or credential misuse**—and nearly 60% of breached accounts are later used for internal phishing or impersonation.[2]

California community colleges reported **more than 1.2 million fraudulent applications** in 2024, including 223,000 suspected fake enrollments.[3]

1. Assume Valid Credentials Can Be Compromised

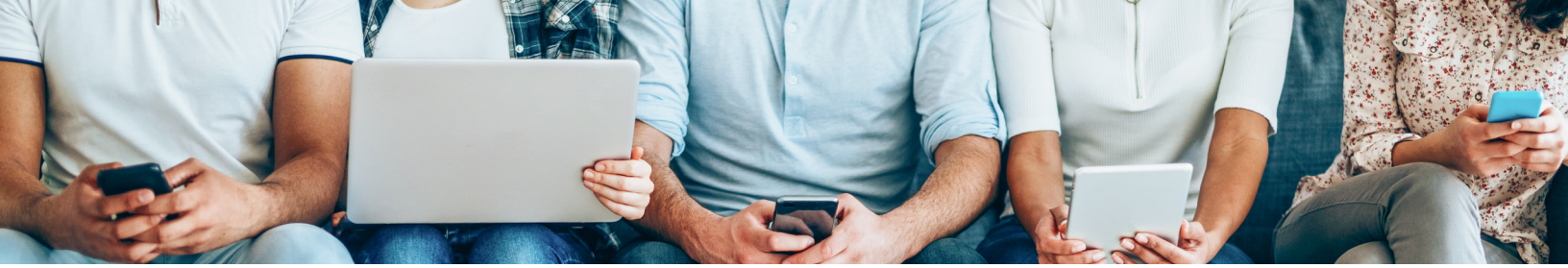
ATO isn't about bypassing security—it's about gaining access as a legitimate student, faculty, or staff member.

Many security models are still built around the idea that a successful login equals a trusted user. In reality, credentials are now one of the most commonly exploited attack vectors across higher education.

To reduce exposure:

- Treat stolen or misused credentials as a routine risk—not an exception
- Plan security strategies around the possibility that attackers may already have valid usernames and passwords
- Shift the focus from one time authentication to ongoing validation of trust

Why it matters: Once attackers log in, they can blend into normal campus activity, making detection far more difficult and increasing downstream impact.



2. Protect High Value Accounts First

Not every account carries the same level of risk.

In higher education, certain accounts and systems create outsized exposure if compromised. These environments often control access to funds, sensitive records, or administrative authority.

Consider prioritizing additional safeguards for:

- Financial aid, bursar, and refund processing systems
- Admissions, registrar, and student information platforms
- IT administrators, privileged users, and shared service accounts

By focusing protection where misuse would cause the greatest disruption, institutions can strengthen defenses without over burdening every user interaction.

3. Move Beyond "Checking the Multi-factor Authorization (MFA) Box"

MFA helps, but attackers increasingly target the human behind it.

MFA is an important control, but it isn't infallible—particularly when attackers rely on phishing, MFA fatigue, and social engineering rather than brute force.

Institutions should:

- Monitor for repeated or unusual authentication requests that may signal prompt bombing or coercion
- Pay attention to changes in login behavior, such as new devices, locations, or access patterns
- Combine MFA with contextual and behavioral indicators to better assess risk

Key takeaway: MFA reduces risk, but true identity assurance comes from understanding who is logging in and how that access compares to normal behavior.

4. Reduce the Risk of Internal Phishing and Impersonation

Trusted accounts are powerful once compromised.

When attackers gain access to legitimate campus accounts, they often turn those identities into tools for further fraud. Messages sent from known faculty or staff accounts are more likely to be trusted—and acted upon.

Common downstream risks include:

- Phishing campaigns sent from compromised campus email accounts
- Impersonation of IT, HR, financial aid, or academic offices
- Requests that pressure recipients into sharing information or approving actions

Detecting unusual messaging patterns or behavior early can help contain threats before they spread across departments or student populations.

5. Tame Identity Sprawl Across the Campus Lifecycle

Complex identity environments create blind spots.

Higher education institutions manage a constantly shifting population of users, including:

- New and departing students each term
- Adjunct faculty, visiting researchers, and seasonal staff
- Alumni, contractors, and third party service providers

Without consistent oversight, accounts can linger long after access is needed. Regularly reviewing privileges, retiring unused accounts, and aligning access with current roles helps reduce openings attackers are eager to exploit.

6. Use Risk Signals to Focus Staff Effort

Not every interaction warrants the same level of scrutiny.

Manual review and step up verification are valuable—but only when applied thoughtfully. Risk based approaches allow institutions to focus attention where it's most needed.

Effective strategies include:

- Applying additional checks only when risk indicators appear
- Allowing known, low risk users and interactions to proceed smoothly
- Reserving manual intervention for high confidence exceptions

This balance helps protect institutional resources while maintaining positive student and staff experiences.

7. Design Identity Controls That Can Adapt

Static controls struggle against evolving threats.

Fraud tactics change quickly, especially as AI and automation lower the barrier for attackers. Identity strategies that rely solely on fixed rules or templates are difficult to maintain over time.

Institutions benefit from identity controls that:

- Learn from new data and behavior patterns
- Adjust risk thresholds as conditions evolve
- Support multiple identity workflows across academic and administrative functions

Adaptability is essential in an environment defined by constant change.

How an Adaptive, Intelligence-Led Approach Can Help

As account takeover tactics grow more sophisticated, institutions often need to go beyond document-centric verification alone. A layered approach that incorporates identity intelligence, risk signals, and contributory data can help provide a more complete view of who is behind a digital interaction. This is where solutions like **LexisNexis EssentialID®** can play a role—helping institutions assess identity with greater context and confidence across a wide range of user journeys.

LexisNexis EssentialID applies advanced analytics and contributory data intelligence to help assess identities with greater confidence. By analyzing identity attributes, behaviors, and contextual signals in real time, institutions can identify potential risk indicators that may not be visible through traditional verification methods alone.

For higher education institutions, this approach can help:

- **Verify identities** using a broader set of trusted data points—not just credentials
- **Support automated decisioning** while reducing reliance on manual review
- **Strengthen identity assurance** across remote, hybrid, and digital-first interactions

By applying adaptive intelligence instead of rigid rules, institutions can reinforce trust across the campus identity lifecycle—without adding unnecessary friction for legitimate users.

LexisNexis® RISK SOLUTIONS

For more information,
scan QR code or call 1-888-216-3544

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions leverages the power of data, advanced analytics platforms and integrated AI solutions to provide insights that help businesses across multiple industries and governmental entities reduce risk and improve decisions to benefit people around the globe. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit LexisNexis Risk Solutions and RELX.

1 https://www.authx.com/blog/account-takeover-fraud-statistics-insights/

2 https://edscoop.com/how-account-takeover-is-reshaping-higher-ed-cyber-risk/

3 https://getnametag.com/newsroom/higher-ed-tech-breaches-student-identity-security