merlin cyber

DATA SHEET

Zimperium Mobile Threat Defense (MTD) for Higher Education

COMPREHENSIVE MOBILE SECURITY FOR THE MODERN CAMPUS

ZIMPERIUM®

Mobile Device Ecosystems are Universities' Largest Attack Surface

Mobile devices are the gateway to your university's data, classrooms, health clinics, and critical IT systems, and cyber adversaries know it. Education is quickly becoming a prime target for mobile-based threats, with phishing, smishing, rogue Wi-Fi, and third-party apps driving credential theft and session hijacking across both university-owned and BYO devices. Zimperium delivers privacy-first, on device defense that protects students, faculty, administrators, and clinical staff without adding friction to teaching, research, or executive operations.

Recent reports from Microsoft Threat Intelligence and Zscaler show that the education sector now accounts for nearly one in five mobile malware targets (18%)[1], and phishing aimed at campuses surged 224% in 2024 as cybercriminals timed attacks to coincide with admissions and financial aid cycles[2]. Meanwhile, attackers are exploiting new channels like QR codes ("quishing"), with 15,000+ malicious QR-codes aimed at education daily[3], as well as using instant messaging and collaboration tools to bypass traditional defenses.

The result is that universities face increasing threats to sensitive data, intellectual property, and patient records—yet their students, faculty, and administrators require seamless digital experiences that ensure privacy. Protecting the modern mobile campus now requires an adaptable security approach that prioritizes striking the right balance between security and operational continuity.

Why Higher Education is Increasingly at Risk

Higher-ed institutions face unique, multifaceted challenges in mobile cybersecurity:

BRING YOUR OWN DEVICE (BYOD):
With thousands of students and faculty using personal devices, traditional visibility and control are limited. University security teams lack standardized device security protocols and cannot rely on invasive monitoring that risks academic freedom or trust.

ROGUE NETWORKS AND RISKY APPS:
Attackers increasingly use malicious Wi-Fi hotspots and malicious third-party apps to harvest credentials and install malware. Without the right mobile defense and risk prevention, faculty and students often do not realize they have been targeted until it is too late.

HEALTHCARE AND RESEARCH EXPOSURE:
Universities with teaching hospitals or major research grants and programs must protect sensitive data without disrupting patient care or research collaboration.

PHISHING SUCCESS RATES ON MOBILE:
Research shows users are 6–10 times more likely to fall for phishing on mobile than email, with 82% of breaches involving the human element originating from phones and tablets[4].

Mobile-based threats not only put sensitive data at risk, but they also threaten the trust, continuity, and reputation of academic institutions. Considering these complex pain points facing universities, it is critical to future-proof mobile cybersecurity for education with automated defenses.

Comprehensive, Always-On Mobile Threat Defense for Higher Education

Zimperium is purpose-built to defend the mobile ecosystem without disrupting how people teach, learn, and work. Unlike bolt-on tools, Zimperium runs directly on the device, delivering real-time protection even when users are offline. This privacy-first approach ensures both university-owned and personal devices remain secure while respecting the user experience.

Zimperium's MTD platform protects against the most critical mobile threats facing higher education:

PHISHING AND QUISHING

On-device detection instantly blocks connections to malicious domains across SMS, iMessage, QR codes, browsers, and collaboration apps—even when attackers evolve their tactics, techniques, and procedures through new attack vectors.

DOCUMENT & FILE ATTACKS

Advanced PDF scanning identifies malicious files and embedded phishing links, protecting admissions, research, clinical, and financial aid workflows from compromise via novel techniques targeting mobile devices.

MALICIOUS OR RISKY APPS

Automated detection identifies vulnerable or unauthorized apps, eliminating risk exposure from third-party app stores or sideloading. This protects students, faculty, and executives from targeted mobile malware with policy-driven application security and rapid response.

ROGUE WI-FI AND NETWORK ATTACKS

Zimperium identifies unsafe networks before users connect, blocking attackers from harvesting faculty, student, and administrator credentials. This prevents compromise of sensitive data and ensures sensitive records and PII remain safe from session hijacking.

University cybersecurity and incident response teams also gain visibility that was previously unattainable. With scalable integrations, contextual telemetry flows seamlessly into existing UEM, SIEM, SOAR, and XDR tools, empowering SOCs to investigate incidents quickly and automate responses. These unmatched forensics enable rapid identification and prevention of compromised device outbreaks through analysis of key IoCs, risk indicators, and vulnerable devices.

A Frictionless Experience for the Campus

Security is only effective if it works in practice. Zimperium is designed with the campus experience in mind:

Privacy-first	Protects sensitive data without intrusive monitoring—segregating university resources, apps, and data from personal information is critical for BYOD.

Invisible to users	Runs quietly in the background, ensuring students, faculty, and clinicians are never interrupted by pop-ups, slowdowns, downtime, or remediation workflows requiring end-user input.
Operationally Friendly	Integrates with existing IT and security workflows so institutions can strengthen defenses without downtime, retraining staff, or overhauling infrastructure.

A Secure, Resilient, and Trusted Outcome for Universities

By adopting Zimperium, higher-education institutions can:

- Protect student and faculty accounts from credential theft and session hijacking.
- Safeguard intellectual property and research data from compromise, exfiltration, and mobile-based malware.
- Secure academic healthcare environments and enforce HIPAA compliance without disrupting patient care or clinician workflows.
- Ensure operational continuity by reducing costly downtime and minimizing the propagation and impact of cyber incidents.

Universities are not only protecting devices; they are protecting the trust of their students, faculty, and alumni, as well as the integrity of their research and the resilience of their healthcare systems.

ZIMPERIUM®

merlin cyber

Future-Proof Security for the Mobile Campus with Zimperium and Merlin Cyber

Zimperium is the global leader in mobile device and application security, trusted by public-sector organizations and enterprises around the world. Merlin Cyber is here to help your university plan, pilot, and scale Zimperium MTD to integrate with your existing IT infrastructure, align mobile device security practices and controls with the university's mission, and protect students, staff, and sensitive data from sophisticated mobile threats.

[1] Zscaler, *2024 ThreatLabz Phishing and Malware Report*, based on data from the Zscaler Security Cloud (June 2023 – May 2024).
[2] Zscaler ThreatLabz, *Beyond the inbox: 2025 Phishing Report reveals how phishing is evolving*, January 14, 2025.
[3] Microsoft, *Cyber Signals, Issue 8: Education under siege—How cybercriminals target our schools*, October 10, 2024.
[4] Verizon, *Mobile Security Index 2022.*

About Merlin Cyber

Merlin Cyber is the go-to-market and Zero Trust Modernization affiliate of Merlin Group, a network of companies that invests in, enables, and scales technology companies with disruptive cyber solutions. Through Merlin Cyber, the U.S. Government can access innovative, public sector-ready cybersecurity solutions that are designed to meet government requirements and mission priorities. Merlin does this by selectively partnering with best-in-class cybersecurity brands, investing in visionary emerging technologies, and enabling the U.S. Government to successfully keep ahead of today's critical threats, accelerate Zero Trust modernization initiatives, and defend our nation.

703.752.2928 info@merlincyber.com merlincyber.com

merlin cyber