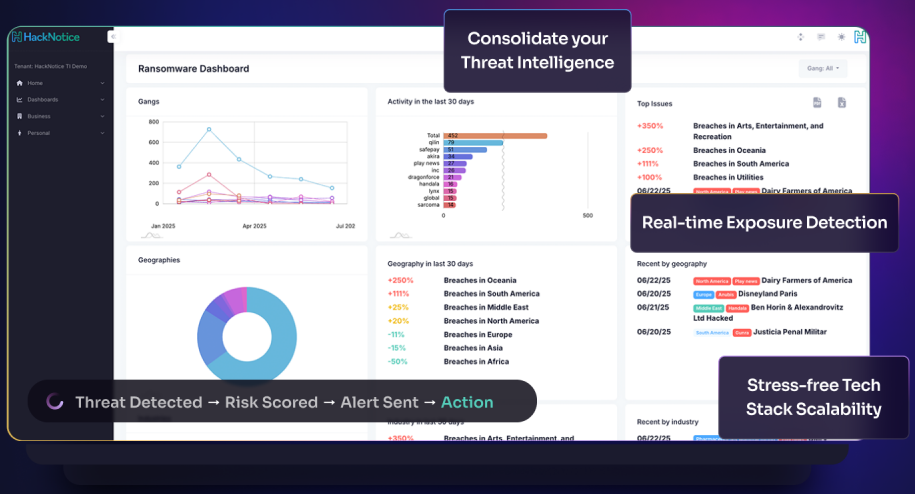
HackNotice

REAL TIME BREACHES & ATTACK DATA

Full-Spectrum Threat Intelligence For The Education Industry



Defend your workforce and students with continuous dark web intelligence tailored for educational services and school districts.

Educational institutions are prime targets for cybercriminals seeking to exploit exposed credentials, student and faculty data, and undersecured third-party platforms. With the surge in ransomware attacks across K–12 and higher education, protecting digital learning environments and sensitive records is more urgent than ever.

HackNotice delivers real-time, actionable intelligence to help IT and security teams identify risks early, reduce exposure, and respond quickly to emerging threats. Our continuous monitoring of the dark web and supply chain threats supports FERPA compliance and strengthens incident preparedness across your district or campus.

From safeguarding student information to protecting remote learning infrastructure, HackNotice provides always-on visibility to help education organizations stay ahead of evolving cyber risks.

Within days of onboarding, HackNotice will

- **Detect and monitor for compromised dark web attack data and users infected with infostealer malware.**
- **Provide continuous threat monitoring and real-time ransomware & data breach alerts for your supply chain.**
- **Protect students accounts from unauthorized access of commonly used educational platforms and applications.**

Proactively mitigate dark web and supply chain threats with AI-Powered Threat Intelligence

Protect Student Accounts

Monitor for student credentials leaked from platforms they use and interact with, enabling rapid response to prevent account takeover (ATO), fraud, and unauthorized access.

Monitoring Employee & Staff Assets

Identify leaked admin credentials, sensitive student data, and protected PII exposed on the dark web or paste sites—preventing unauthorized access and IP theft.

Mitigate Employee Account Take Over

Identify when employee credentials are stolen by infostealer malware, helping prevent Business Email Compromise (BEC), internal fraud, and unauthorized access to financial systems.

Supply Chain Threat Monitoring

Continuously track breaches, ransomware attacks, and trafficked data related to your third-party vendors and partners, enabling risk-based prioritization and remediation.

"We've been really happy with the service. Last month alone, **you provided us with 12 actionable alerts.**"

Empowering security teams with the intel they need to prevent compromise across their user base, workforce, and digital ecosystem—all in real time and at scale.