DIGITAL THREAT REPORT

DIGITAL THREAT REPORT: OKLAHOMA 2025

New Report from Proxyware's Digital Crime Database Reveals a Surge in AI-Driven Scams and Cyberattacks Targeting Oklahoma's Students, Governments, and Universities

PROXYWARE

WWW.PROXYWARE.COM

EXECUTIVE SUMMARY

Proxyware's latest analysis across Oklahoma reveals that digital attacks across the state have reached unprecedented levels, with K–12 schools, universities, and local governments experiencing a wave of AI-driven scams and phishing attempts.

While Oklahoma ranks 38th nationally for total digital attacks, the intensity of targeted campaigns is rising, particularly in education and public-sector networks that form the backbone of daily community life.

In 2025 alone:

- K–12 schools were hit nearly 10,000 times,
- Local governments endured more than 66,000 attacks, and
- Universities absorbed nearly 280,000 attacks, placing Oklahoma among the top third of U.S. states for higher education targeting.

Phishing and backdoor intrusions account for the majority of these attacks, with phishing dominating statewide, and backdoor exploits more common in schools and local governments.

KEY FINDINGS

- Education remains the most targeted sector, with both K–12 school districts and universities facing high-volume, persistent threats.
- AI-generated phishing campaigns are increasingly sophisticated, using localized details and authentic-looking correspondence to deceive staff and students.
- K–12 school networks often serve as entry points for broader community attacks due to limited IT resources.
- Local governments, though ranking 32nd nationally, are experiencing sustained targeting that disrupts services and puts resident data at risk.
- Backdoor and phishing attacks each make up roughly 40% of total attempts, showing consistent tactics across sectors.

Sector-by-Sector Analysis

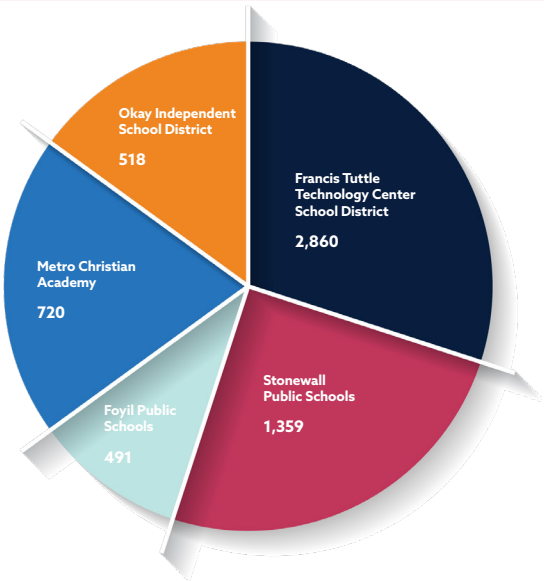
K-12 SCHOOLS

K–12 institutions are often targeted as "soft entry points." Their networks connect students, families, and local agencies—creating a broad digital footprint that attackers exploit.

Oklahoma schools have faced nearly 10,000 digital attacks so far this year, most of them phishing or backdoor intrusions. Smaller districts are not immune - cybercriminals are targeting students, educators, and administrators alike.

Source: Digital Crime Index, The Media Trust

Top 5 K-12 Schools Attacked in 2025



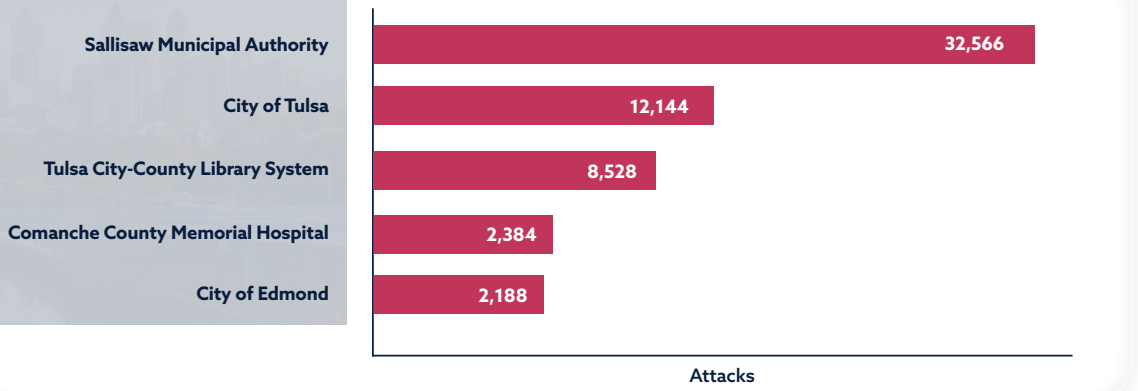
LOCAL GOVERNMENT

Oklahoma's local governments have collectively faced 66,000 attacks in 2025, ranking 32nd nationwide. Phishing and backdoor attempts dominate, with smaller municipalities increasingly in the crosshairs.

Sallisaw's surge in targeting, with over 30,000 attacks, shows how these small municipalities can become major digital battlegrounds. Local agencies hold vital personal and utility data, making them lucrative targets for ransomware and espionage campaigns.

Top 5 Government Organizations Attacked in 2025

Source:
Digital Crime Index,
The Media Trust

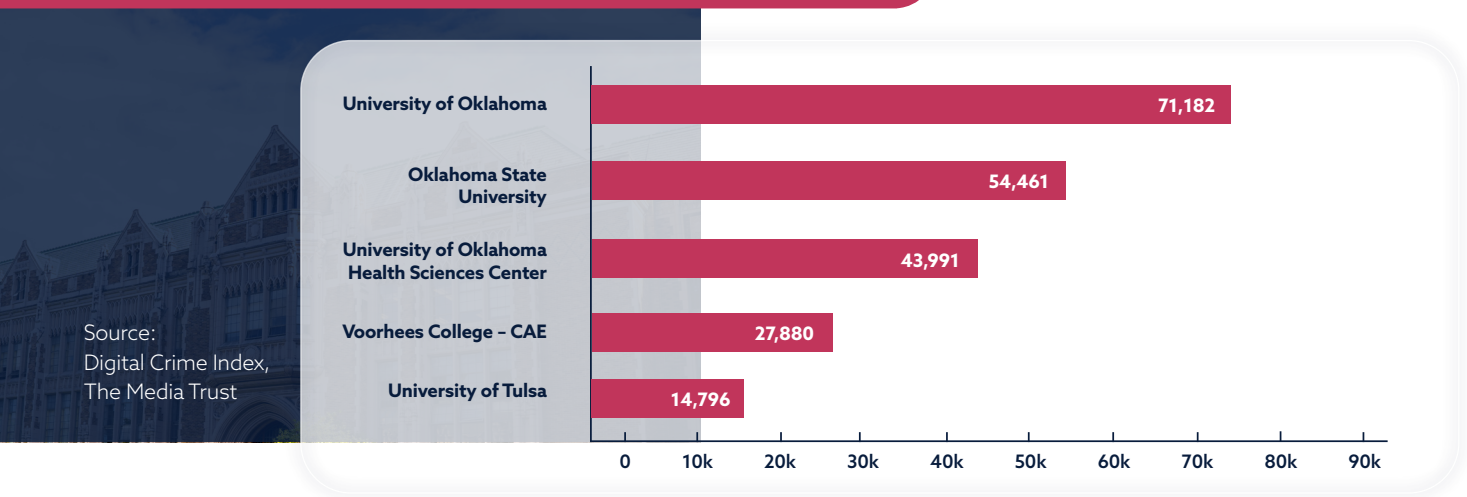


HIGHER EDUCATION

Students are the state's future leaders and are increasingly direct targets, with attackers seeking credentials, financial information, and access to institutional research systems.

Universities and colleges in Oklahoma have seen nearly 280,000 attacks in 2025, ranking 33rd nationally. The scale and persistence of these attacks underscore how institutions that combine personal data, research, and healthcare services attract cybercriminals.

Top 5 Universities Attacked in 2025



Source:
Digital Crime Index,
The Media Trust

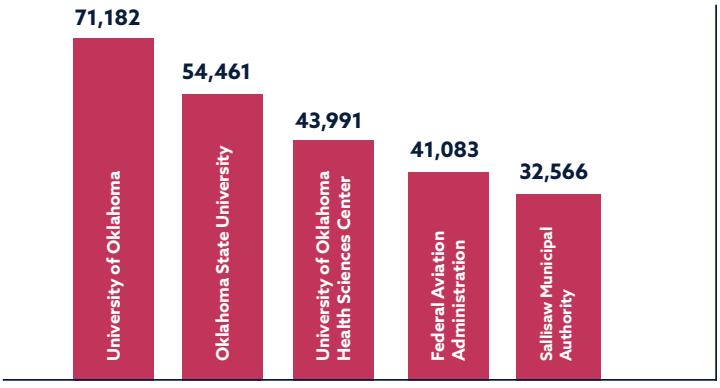
ATTACK PATTERNS ACROSS SECTORS

Phishing and backdoor attacks dominate Oklahoma's digital crime landscape, reflecting the same patterns seen across much of the nation. Phishing remains the most common tactic, accounting for the majority of attacks against the state's universities, hospitals, and federal facilities. These socially engineered campaigns often use convincing emails, text messages, or advertisements to trick victims into revealing credentials or downloading malicious files, methods that are increasingly enhanced by AI-generated language and visuals.

Meanwhile, backdoor intrusions are the preferred weapon against K–12 schools and local governments, where limited cybersecurity budgets and outdated infrastructure make systems easier to exploit. These attacks allow criminals to establish hidden access within networks, often remaining undetected for long periods while collecting sensitive data or preparing for ransomware deployment.

Together, phishing and backdoor attacks illustrate the dual challenge facing Oklahoma: defending people as well as systems in an environment where deception and persistence drive digital harm.

Top 5 Most-Targeted Oklahoma Organizations (all sectors)



CHRIS OLSON
CEO

EXPERT PERSPECTIVE

Phishing and backdoor attacks remain the most common entry points for criminals, and Oklahoma's schools, universities, and local governments are increasingly in their sights.

Through Digital Threat: Oklahoma 2025, we can see how digital harm is shifting from isolated incidents to sustained campaigns and how Proxyware's real-time intelligence helps communities fight back.

THREAT LENS SUMMARY

Oklahoma's digital threat landscape is evolving rapidly. Education and local governments—cornerstones of civic and economic life—are now primary targets for sophisticated cybercriminals. As Proxyware continues to expand its infrastructure across the United States, the insights from Threat Lens: Oklahoma 2025 will inform protection strategies that safeguard not just systems, but the people behind them.

DIGITAL THREAT REPORT

Powered by

PROXYWARE

WWW.PROXYWARE.COM