DIGITAL THREAT REPORT

DIGITAL THREAT REPORT: ARKANSAS 2025

New Report from Proxyware's Digital Crime Database Reveals Rising Cyber Threats Against Arkansas Schools, Governments, and Universities

PROXYWARE

WWW.PROXYWARE.COM

EXECUTIVE SUMMARY

Proxyware's Digital Threat Report: Arkansas 2025 exposes how the Natural State has become a growing target for AI-driven phishing and malware campaigns. With more than 1.1 million digital attacks recorded this year, Arkansas ranks among the top 20 most targeted states in the nation; a sobering sign of how cybercrime increasingly impacts smaller states and rural communities.

In 2025 alone, K–12 schools have endured more than 250,000 attacks, local governments have faced over 265,000 incidents, and universities have recorded 360,000 targeted intrusions. The state of Arkansas itself has been hit by nearly 400,000 attacks, reflecting the widespread exposure of both public institutions and infrastructure providers.

Phishing remains the most common attack type statewide, followed closely by backdoor attacks. However, Arkansas's schools are unique in that backdoor attacks are the leading threat, allowing cybercriminals to embed malicious code within systems used daily by children and educators.

The state's average victim loss of $573,638 in 2024 illustrates the high economic and human toll of these persistent threats.

KEY FINDINGS

- Arkansas ranks 19th in the nation for total cyberattacks in 2025.
- Phishing is the most common attack vector across all sectors, while backdoor attacks dominate in K–12 schools.
- The Arkansas Public School Computer Network is among the most attacked education systems in the country.
- Municipal utilities and county governments are increasingly targeted for disruption and extortion.
- Universities face ongoing risks to research data, student records, and medical systems.

Sector-by-Sector Analysis

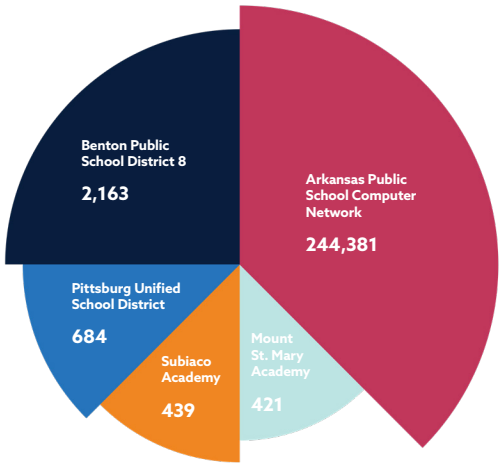
K-12 SCHOOLS

Schools are prime targets because they connect thousands of young users across shared systems with limited security oversight. Once infiltrated, these networks provide long-term access to sensitive student information and community records.

Arkansas' schools have faced more than 250,000 digital attacks in 2025, ranking the state 9th nationally for education-related incidents. The Arkansas Public School Computer Network, which connects multiple districts statewide, has endured over 244,000 attacks, making it **one of the most heavily targeted educational systems in the U.S.**

Children and educators have become collateral victims in a surge of backdoor attacks that compromise shared networks, giving hackers persistent access to devices, personal data, and online classrooms.

Top 5 K-12 Schools Attacked in 2025



LOCAL GOVERNMENT

Local governments in Arkansas have been targeted by more than 265,000 attacks in 2025, ranking 21st nationwide. The most targeted organizations are Paragould Municipal Utilities and Clay County Connect, both essential service providers critical to daily life.

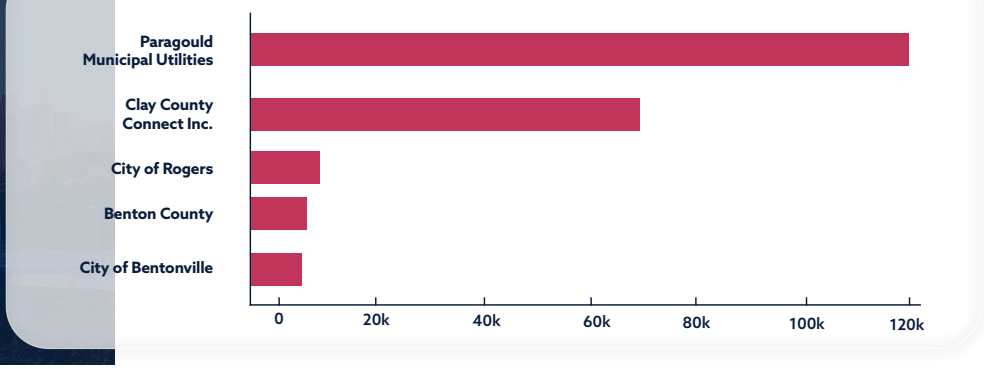
The attacks are heavily concentrated in smaller municipal utilities and county governments, which often lack the same cybersecurity infrastructure as larger cities.The high attack volume on Paragould Municipal Utilities and Clay County Connect reflects a growing trend: cybercriminals are exploiting essential community infrastructure (power, water, and connectivity) to pressure governments into ransom payments.

Many small municipalities still rely on outdated systems and limited IT staff, leaving them ill-equipped to respond to modern threats.

Municipal utilities have become a prime target, as threat actors attempt to exploit essential services like water, power, and broadband to extort payments or disrupt community access.

Top 5 Government Organizations Attacked in 2025

Source:
Digital Crime Index,
The Media Trust



HIGHER EDUCATION

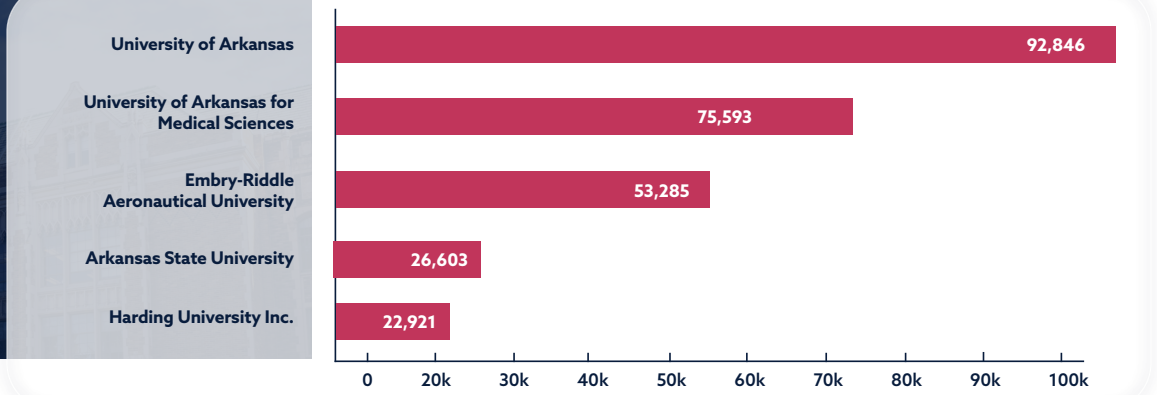
Universities sit at the intersection of research, healthcare, and student data, making them rich targets for phishing and credential theft.

In Arkansas, University research networks and medical systems face constant phishing and credential-harvesting attempts designed to gain long-term access for data theft or ransomware deployment. Attackers frequently impersonate faculty, deploy fake login portals, or embed malware in shared research platforms to steal sensitive intellectual property.

Arkansas universities have seen 360,000 attacks in 2025, ranking the state 31st nationally for higher-education targeting. The University of Arkansas leads the list with nearly 93,000 attacks, followed closely by the University of Arkansas for Medical Sciences and the University of Central Arkansas.

Top 5 Universities Attacked in 2025

Source:
Digital Crime Index,
The Media Trust



ATTACK PATTERNS ACROSS SECTORS

Arkansas's most attacked entities show the full range of its digital vulnerabilities, from education and healthcare to utilities and state government.

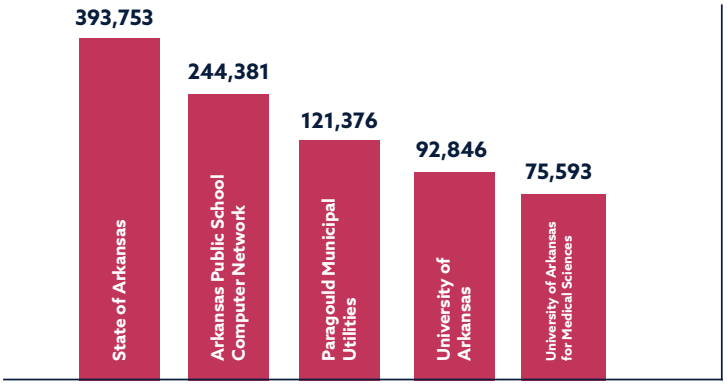
The concentration of attacks against state and education systems demonstrates how cybercrime has shifted toward smaller, less fortified institutions that manage critical data.

Phishing and backdoor attacks dominate Arkansas's threat landscape.

- **Phishing** is the primary method across most organizations, leveraging social engineering and AI-generated content to deceive users into sharing credentials or clicking malicious links.
- **Backdoor attacks** are especially prevalent in K–12 environments, where hackers exploit outdated devices and open networks to gain long-term access.

This combination creates a "dual threat" environment where social manipulation and technical infiltration work hand-in-hand.

Top 5 Most-Targeted Arkansas Organizations (all sectors)



CHRIS OLSON
CEO

EXPERT PERSPECTIVE

Arkansas is one of the most frequently targeted states for cyberattacks in the U.S., ranking **19th overall** *for total attack volume in 2025. This is a clear example of how cybercrime doesn't just target major cities or corporations, it goes where defenses are weakest.*

The state's mix of small governments, critical infrastructure, and growing digital migration among small businesses has made it a prime target for cybercriminals.

When local utilities, schools, and universities are under siege, it's not just networks that are disrupted, it's lives. When a local government's systems are locked, citizens lose access to essential services. When schools are breached, student safety and privacy are compromised.

Proxyware's mission is to detect and disrupt these attacks before they reach their targets, protecting the people of Arkansas from digital harm.

THREAT LENS SUMMARY

Arkansas's growing digital footprint has made it an increasingly attractive target for cybercriminals seeking vulnerable entry points. As local governments expand their online systems for tax collection, utilities, and public records, new gaps emerge that sophisticated actors are quick to exploit.

At the same time, small businesses accelerating their digital migration often lack the cybersecurity resources to defend against phishing and fraud. The state's critical infrastructure, spanning energy, logistics, and financial services, remains a high-value target for both financially motivated and state-sponsored attackers.

Compounding these risks, Arkansas experiences some of the nation's highest rates of phishing, which often serve as the initial gateway to more severe malware and ransomware infections.

Proxyware's technology helps stop these threats at the source—protecting not just systems, but the communities that depend on them.

DIGITAL THREAT REPORT

Powered by

PROXYWARE

WWW.PROXYWARE.COM