DIGITAL THREAT REPORT

DIGITAL THREAT REPORT: MISSOURI 2025

New Report from Proxyware's Digital Crime Database Reveals Missouri as a Strategic Target for Cybercrime and State-Sponsored Attacks

PROXYWARE

WWW.PROXYWARE.COM

EXECUTIVE SUMMARY

Proxyware's Digital Threat Report: Missouri 2025 reveals a sharp rise in targeted cyber activity across the state's education, government, and research sectors. With more than 1.6 million attacks recorded this year, Missouri ranks as the 14th most targeted state in the U.S. This is a reflection of both its digital importance and the vulnerabilities within its expanding infrastructure.

Missouri's K–12 schools have endured nearly 120,000 attacks, local governments over 373,000 incidents, and universities nearly 1.1 million targeted intrusions—the 7th highest total among higher education systems nationwide. This surge underscores how the state's concentration of research networks, agriculture operations, and military installations has made it a prime target for phishing and backdoor attacks.

At the center of Missouri's cybersecurity challenge are entities like Morenet, the Missouri Research and Education Network, which alone has faced more than 440,000 attacks in 2025, and the City of St. Louis, which has surpassed 108,000 incidents.

The strategic importance of Whiteman Air Force Base and the University of Missouri system adds further pressure, as foreign and domestic cyber actors seek to compromise institutions tied to national defense, research, and economic stability.

KEY FINDINGS

Missouri ranks 14th nationally for total cyberattacks in 2025.

Phishing remains the top attack vector statewide, followed by backdoor intrusions.

K–12 schools and local governments are primarily targeted through backdoor attacks exploiting open networks and shared systems.

Universities face persistent, large-scale attacks, ranking 7th in the nation for higher-education targeting.

The University of Missouri was named in a **2023 Russian ransomware attack** (Cl0p) that exposed student and faculty data, highlighting the long-term threat to research institutions.

Sector-by-Sector Analysis

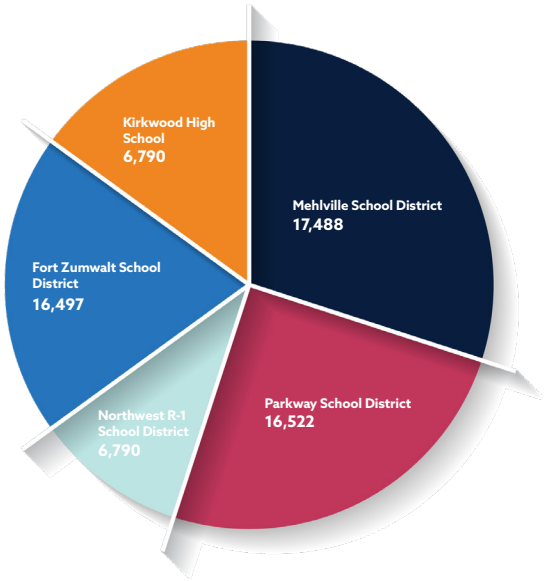
K–12 SCHOOLS

Missouri's K–12 schools have experienced nearly 120,000 digital attacks in 2025, ranking 22nd nationally for school-related cyber incidents.

Large suburban districts such as Mehlville, Parkway, and Fort Zumwalt have each faced more than 16,000 attacks, illustrating how public education systems remain frequent entry points for cybercriminals.

Backdoor attacks dominate Missouri's education sector, targeting administrative systems and online learning platforms. The Fort Zumwalt School District, which provides free statewide access to online career development programs, represents a unique vulnerability; serving as a digital hub for students across Missouri and a potential conduit for wider network compromise.

Top 5 Schools Attacked in 2025



Source: Digital Crime Index, The Media Trust

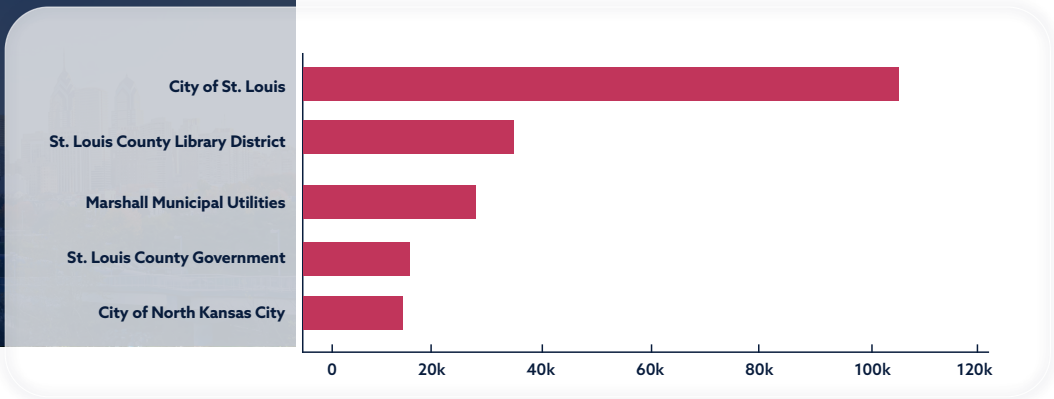
LOCAL GOVERNMENT

Local government entities remain under constant threat due to their interconnected digital systems and essential services. Municipal utilities, libraries, and public offices are being exploited for data theft and ransomware. As cybercriminals leverage phishing and backdoor malware to gain persistence, even small city networks are facing enterprise-level threats.

Missouri's local governments have been targeted by more than 373,000 attacks in 2025, ranking 15th in the nation for public-sector threats. The City of St. Louis continues to be the epicenter of attacks, with more than 108,000 incidents recorded this year alone.

Top 5 Local Government Organizations Attacked in 2025

Source:
Digital Crime Index,
The Media Trust

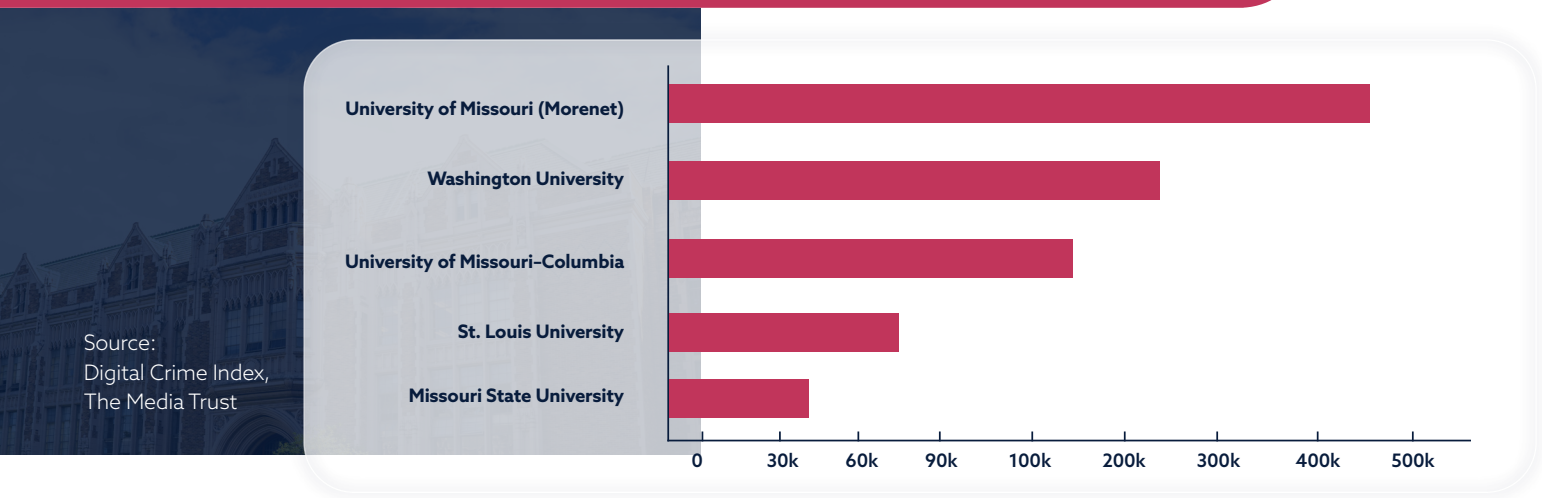


HIGHER EDUCATION

Missouri's universities have long been a target for both financially and politically motivated cyber actors. In 2023, the University of Missouri was named as a victim in a Russian ransomware campaign (Cl0p) that compromised sensitive student and staff data, including Social Security numbers, salary records, and financial information. The incident demonstrated the scale and persistence of attacks on Missouri's research ecosystem, especially as AI, medical, and agricultural technologies become higher-value targets.

Missouri's higher education institutions have faced nearly 1.1 million digital attacks in 2025, ranking the state 7th nationwide for university and research targeting. The Missouri Research and Education Network (Morenet) alone has absorbed more than 440,000 attacks, reflecting its critical role as a shared infrastructure backbone for universities and public institutions across the state.

Top 5 Universities & Research Organizations Attacked in 2025

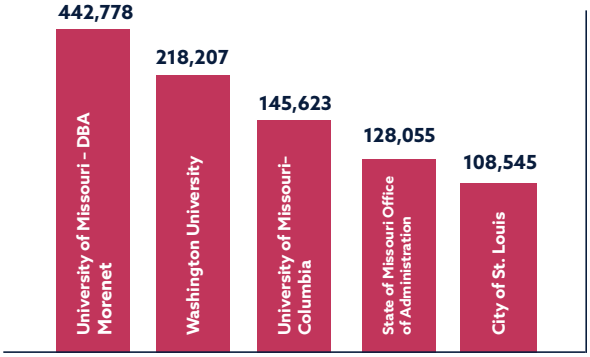


Source:
Digital Crime Index,
The Media Trust

ATTACK PATTERNS ACROSS SECTORS

Missouri's top five most-attacked organizations represent the heart of its digital ecosystem—research, governance, and urban infrastructure. The state's combination of academic innovation, centralized IT systems, and growing digital dependence creates a broad and attractive attack surface for cybercriminals.

Top 5 Most-Targeted Missouri Organizations (all sectors)



Source: Digital Crime Index, The Media Trust

Attack Patterns Across Sectors

Phishing and backdoor attacks dominate Missouri's digital threat landscape:

Phishing is the leading attack type, used to harvest credentials or deliver malware-laced links.

Backdoor attacks are prevalent in schools and local governments, where persistent access allows criminals to move laterally through systems.

The combination of ransomware, credential theft, and infrastructure exploitation continues to threaten every level of Missouri's digital ecosystem.

EXPERT PERSPECTIVE

Located near Sedalia, Whiteman Air Force Base, home to the B-2 Spirit stealth bomber fleet, represents one of Missouri's most strategically significant assets. The base's dual capability for conventional and nuclear operations makes it a high-value target for state-sponsored cyber activity. Threat actors have long sought to infiltrate military supply chains, defense contractors, and research partners connected to installations like Whiteman, often using phishing, credential theft, and social engineering to gain access to sensitive systems.

While there is no confirmed breach, the base's prominence underscores Missouri's heightened exposure to espionage-driven cyber operations, particularly from adversaries seeking defense intelligence or operational disruption. Increasingly, these same threat actors exploit the families and communities surrounding military bases, including children and teens, as indirect targets.

Cybercriminals often use social platforms, gaming networks, and messaging apps to recruit, manipulate, or surveil youth living in military families, capitalizing on their proximity to defense personnel and potential access to shared or household devices. What begins as online grooming or phishing can evolve into reconnaissance activities that expose personal information, network details, or behavioral data.

This growing pattern highlights a dangerous evolution in cyber warfare where the digital battlefield extends beyond classified systems to include the human networks that support them. Protecting military families, especially children, from online exploitation is critical.

CHRIS OLSON
CEO

THREAT LENS SUMMARY

Missouri's growing dependence on digital infrastructure has made it an inviting target for cybercriminals and nation-state actors alike. From the University of Missouri system and Whiteman Air Force Base to local schools and utilities, the state's institutions hold data and capabilities of immense strategic value.

As phishing campaigns grow more deceptive and backdoor intrusions more persistent, Digital Threat Report: Missouri 2025 underscores the urgent need for proactive defense. Cybercrime in Missouri is no longer just a technical issue, it's a human one, impacting education, defense, and the livelihoods of millions across the state.

Proxyware continues to lead the charge in protecting the people behind the data, stopping digital harm before it starts.

DIGITAL THREAT REPORT

Powered by

PROXYWARE

WWW.PROXYWARE.COM