



DIGITAL THREAT REPORT

DIGITAL THREAT REPORT: FLORIDA 2025

New Report from Proxyware's Digital Crime Database Reveals
Florida as One of the Most Targeted States for AI-Driven
Scams and Cyberattacks

PROXYWARE

WWW.PROXYWARE.COM

EXECUTIVE SUMMARY

Proxyware's Digital Threat Report: Florida 2025 exposes the Sunshine State as a major battleground in the fight against cybercrime. With nearly 3.4 million digital attacks recorded this year, Florida ranks as the second most targeted state in the U.S., trailing only California.

The state's large population, diverse industries, and vast digital infrastructure make it a prime target for cybercriminals; especially in education, local government, and research institutions.

Florida's K-12 schools alone have faced nearly one million attacks in 2025, while local governments absorbed 850,000 incidents, and the state's universities experienced 1.5 million targeted attacks - the third-highest total among higher-education institutions nationwide.

The scale of these intrusions underscores the evolving threat of AI-driven phishing and backdoor campaigns designed to exploit human behavior as much as system vulnerabilities.

KEY FINDINGS

- Florida is the second most targeted state in the nation for cyberattacks.
- Phishing and backdoor attacks dominate across all categories, with phishing representing the majority of incidents statewide.
- K-12 schools are among the hardest hit, ranking second nationally for total education-related attacks.
- University research centers are being increasingly targeted for intellectual property theft and data compromise.
- The Florida Department of Corrections (FDC) has emerged as a high-risk target due to its sensitive data holdings and recent publicity.

Sector-by-Sector Analysis

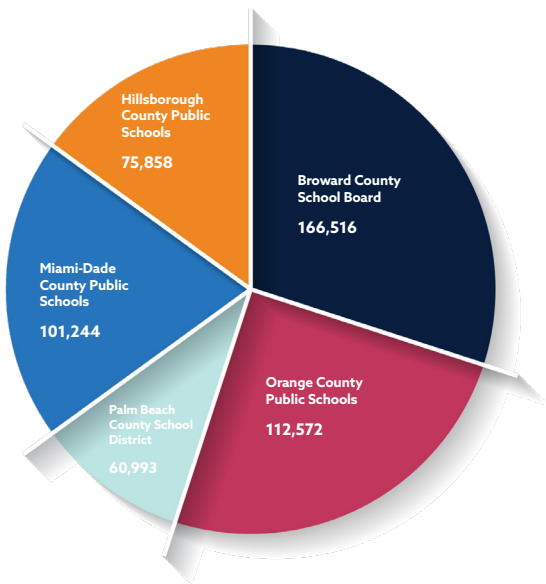
K-12 SCHOOLS

The Florida education system’s broad digital footprint, spanning online learning portals, student records, and public Wi-Fi networks, creates an environment where young users and educators are continually exposed to digital harm.

Florida’s K-12 schools have been targeted by nearly one million digital attacks in 2025, placing the state second in the nation for school-related cyber incidents. The state’s seven largest school districts have each experienced over 50,000 attacks, revealing how deeply cybercrime has infiltrated the education system.

Children in these districts are frequently targeted not only for data theft, but also for extortion, bribery, and harassment. Attackers exploit weak controls in educational systems to access personal details, school email accounts, and family information. Backdoor attacks are especially common in this sector, allowing bad actors to install malware that provides long-term system access.

Top 5 K-12 Schools Attacked in 2025



Source: Digital Crime Index, The Media Trust

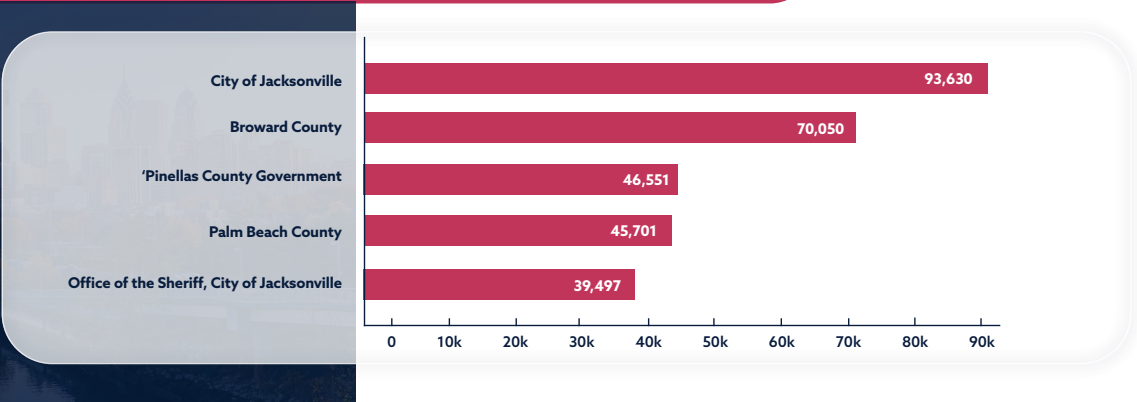
LOCAL GOVERNMENT

Florida’s local governments have endured more than 850,000 attacks in 2025, ranking fourth in the nation for public-sector targeting. Major municipalities such as Jacksonville and Broward County experienced concentrated surges of phishing and backdoor attempts aimed at disrupting essential services.

The City of Jacksonville’s nearly 100,000 attacks highlight how metropolitan governments have become high-value digital targets. Cybercriminals view these entities as gateways to critical infrastructure and citizen data.

With many municipalities still relying on outdated systems and limited security resources, Florida’s local governments face mounting pressure to modernize defenses.

Top 5 Government Organizations Attacked in 2025



Source:
Digital Crime Index,
The Media Trust

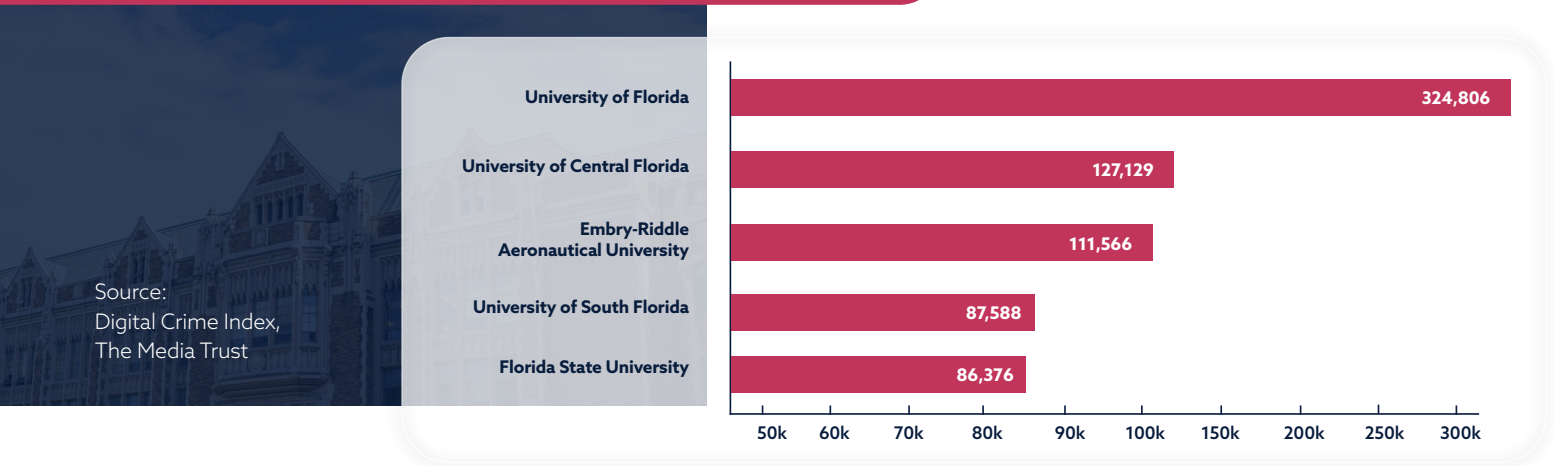
HIGHER EDUCATION

Universities represent the intersection of innovation, personal data, and underfunded cybersecurity. Students and faculty are being targeted for credentials, research access, and intellectual property, underscoring the human cost of digital harm.

Florida’s universities have seen nearly 1.5 million attacks in 2025, the third-highest total of any U.S. state, demonstrating how education and research institutions remain prime targets for sophisticated cybercriminal networks.

The University of Florida (UF), the state’s largest research institution, has been hit hardest with nearly 325,000 attacks. UF Health alone accounts for more than half of the university’s total research funding, making it a prime target for IP theft and ransomware.

Top 5 Universities Attacked in 2025



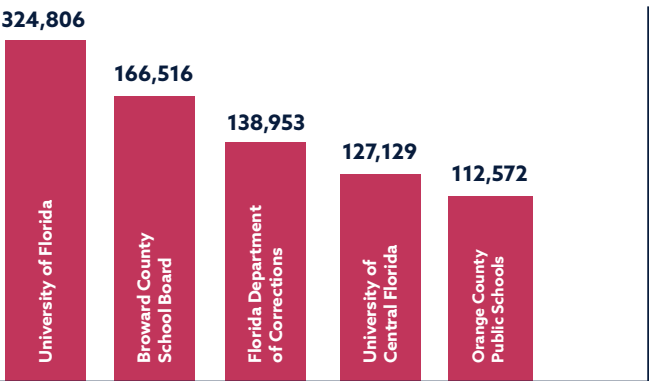
ATTACK PATTERNS ACROSS SECTORS

Phishing and backdoor attacks dominate Florida’s digital threat landscape, with phishing accounting for the majority of incidents statewide. Universities, hospitals, and government agencies are primarily targeted by phishing attacks, which use increasingly realistic lures to capture credentials or deploy malicious links.

In contrast, K-12 schools experience more backdoor attacks, where hackers embed code within systems to establish persistent, covert access. The dual nature of these attack types demonstrates the scale of Florida’s cybersecurity challenge; protecting both people and infrastructure in a digital environment where deception, automation, and persistence are key.

Source: Digital Crime Index, The Media Trust

Top 5 Most-Targeted Florida Organizations (all sectors)





CHRIS OLSON
CEO

EXPERT PERSPECTIVE

Florida's scale and digital complexity make it an attractive target for organized cybercrime. Phishing and backdoor campaigns are eroding trust in the systems that educate our children, serve our communities, and fuel innovation.

We are also witnessing an emerging risk vector in Florida. The Florida Department of Corrections (FDC), with more than 138,000 attacks in 2025, is drawing increased attention from cybercriminals. The FDC's databases contain sensitive data on inmates, juveniles, and victims, making it a lucrative target for ransomware. A successful breach could disrupt operations or extort the state for ransom payments.

Compounding this risk, inmates have been known to use contraband cell phones to perpetrate scams, often against elderly Floridians, by exploiting compromised systems or stolen personal data. The combination of insider manipulation and external intrusion makes FDC another one of the state's most concerning digital vulnerabilities.



THREAT LENS SUMMARY

Florida's leadership in education, research, and innovation comes with a growing cost: relentless targeting by cybercriminals using AI-powered deception and persistent infiltration tactics. From K-12 schools and universities to correctional facilities and city governments, the state's institutions are facing digital attacks that exploit both technology and human behavior.

Proxyware's Digital Threat Report: Florida 2025 underscores the urgency of strengthening defenses across all sectors to protect not just networks, but the people who depend on them.



DIGITAL THREAT REPORT

Powered by

PROXYWARE

WWW.PROXYWARE.COM