

PROXYWARE IMPACT REPORT

Q1 2026 | Protecting People





Executive Summary

In Q1 2026, Proxyware expanded its Digital Safety Program across senior living communities and school systems, delivering measurable impact in preventing financial fraud, reducing exposure to harmful digital content, and disrupting malicious activity at its source.

Through active deployments, Proxyware continues to demonstrate that digital crime is preventable when addressed upstream, before it reaches vulnerable populations.

THIS QUARTER HIGHLIGHTS

- Expansion into 8 new senior living communities and school systems
- Significant financial loss prevention for seniors; \$294,609 at one senior living location during a 30-day period
- Real-world examples of disrupted scams and harmful content from ads and websites targeting children
- Continued validation of a proactive, victim-first approach to digital safety



Q1 2026 Growth Highlights

TOTAL REACH

Proxyware is now actively protecting residents and students across multiple states, including *Arkansas, Colorado, District of Columbia, North Carolina, Maryland, Michigan, Missouri, New York, Pennsylvania, South Carolina, Texas, Virginia, and West Virginia*, with impact extending beyond installation sites through upstream threat disruption.

GROWTH IN LOCATIONS

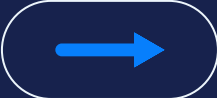
Senior Living Communities Added:

- Sunrise Senior Center, McLean, VA
- Lutheran Homes, Chapin, SC

K-12 School Systems Added:

- Damascus Middle School, Washington County VA
- Bland County Elementary School, Bland County, VA
- Rocky Gap High School, Bland County, VA
- Dillon School District, Dillon, SC
- Harding School, Searcy, AR
- Brentwood Christian School, Brentwood, TX

New senior communities added	2
New school systems added	6
Cumulative people protected	71,142
Cumulative attacks disrupted	451,621
Cumulative dollars protected	\$99.4M



IMPACT IN ACTION

Senior Protection: Lutheran Homes

Proxyware identified and disrupted malicious activity originating from trusted, everyday websites seniors visit daily, such as:

- WikiHow
- AllRecipes
- MegaMillions
- Vanity Fair
- The Washington Post
- The Charlotte Post

These attacks were not coming from suspicious or unknown sources, but from environments residents already trust and use regularly. Backdoor attacks were the primary vector, enabling deeper exploitation, while investment scams showed the fastest growth and became the leading financial risk. Without intervention, these attacks would have reached residents through normal browsing. Within a single community, Proxyware prevented \$294,609 in financial losses in just 30 days, with an annualized impact estimated at \$3.5 million.

KEY INSIGHT

Scams and malware are now being delivered through what people "know" are "trusted websites" that people use every day, breaking the assumption that "safe browsing" is enough to stay protected.



IMPACT IN ACTION

Protecting Students: Dillon School District

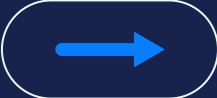
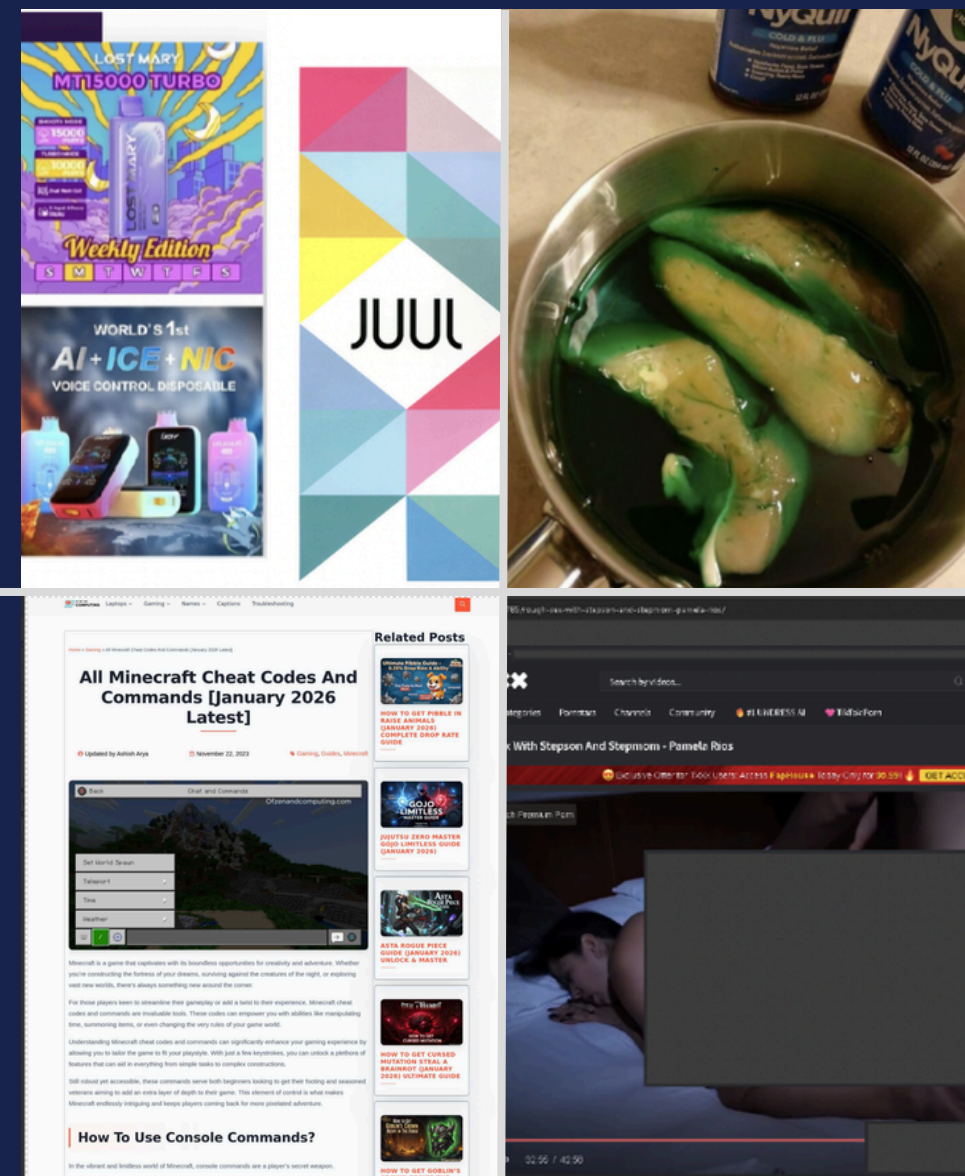
Dillon School District, representing four elementary schools and one combined 6–12 school, Proxyware identified and removed more than 1,000 harmful and non-compliant domains in one month.

These detections prevented children exposure to:

- Adult content without age verification
- Grooming-related behaviors
- Sextortion attempts
- Cloaked and deceptive advertising
- Malicious redirects and scam pathways

Key Insight

Proxyware identified widespread exposure to content and infrastructure that is inappropriate or dangerous for children. These risks did not require intentional misconduct by students; most were delivered through normal browsing, ads, search results, or seemingly benign tools. Without intervention, these attacks would have reached students without any deliberate action.





Attack Trends & Insights

Attack Patterns Across Environments

Data from Q1 2026 Digital Crime Database reveals several important shifts:

- Backdoor attacks remain the dominant vector, enabling persistent access and control
- Scam-based attacks are rapidly increasing, with over 50% growth month-over-month
- Trusted websites are a primary delivery mechanism for malicious activity
- Attack volume increased mid-quarter, indicating accelerating threat cycles

What this tells us:

Digital crime is becoming more sophisticated, more targeted, and more embedded in everyday online behavior.



Priorities & Recommendations



SCALE SENIOR PROTECTION PROGRAMS

Financial fraud targeting seniors is accelerating. Expanding deployments across senior living communities can prevent billions in losses annually.

EXPAND K-12 COVERAGE

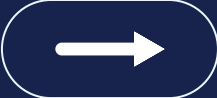
Schools are a critical environment where harmful content and exploitation risks can be significantly reduced through upstream intervention.

STRENGTHEN PUBLIC-PRIVATE PARTNERSHIPS

Collaboration with state leadership, including Attorneys General and local agencies, is essential to scaling impact and aligning with enforcement priorities.

FOCUS ON SOURCE-LEVEL DISRUPTION

Efforts should continue to prioritize identifying and removing malicious infrastructure, not just blocking it.





DIGITAL THREAT ANALYSIS

Powered by

PROXYWARE

www.Proxyware.com