HUMAN

Securing Citizen's Online Experience for State and Local Governments

Cyber threats to citizen accounts are evolving, posing significant risks to public trust, financial stability, and data security. Governments must invest in targeted cybersecurity to protect citizens and infrastructure effectively despite tight budgets and resources.

Protect Citizen's Information

State and local agencies collect extensive data on citizens and maintain databases for their services. Cybercriminals frequently use bots to gain unauthorized access to these databases, create fake accounts to apply for services or grants, and fraudulently obtain public funds. These activities divert resources from citizens and strain the systems, undermining the agencies' ability to provide essential services.

By safeguarding citizens' online accounts, HUMAN ensures a safe, secure, and optimized experience. Our solution effectively manages bots to prevent account takeover and fake account creation.

Protect Critical Infrastructure

A 2022 report revealed that bots generated 47% of all internet traffic, and 30% of that traffic was from bad bots. While government agencies defend their systems with best practices such as DDoS protection and web application firewalls (WAFs), malicious bots continue to infiltrate systems, gaining access to sensitive information, disrupting critical activities, and scraping publicly available data like business registries, legal documents, and financial reports.

By implementing HUMAN, government security staff can effectively neutralize fake accounts and mitigate bot-driven attacks, empowering them to stay ahead of potential threats.

Protect Payments

Government websites that enable citizens to pay for services online must adhere to the PCI DSS 4.0.1 standard. This standard applies to agencies that manage their own websites and utilize scripts in their payment portals. This PCI DSS update introduces new script management and page monitoring requirements to prevent unauthorized changes and security breaches. Compliance with this standard is essential for maintaining trust, securing financial transactions, and protecting citizens' payment card information.

With a single line of Javascript, HUMAN simplifies compliance with the updated payment page script requirements by discovering all scripts on the page and allowing simple authorization, justification, monitoring, and reporting to ensure ongoing compliance.

Visit www.humansecurity.com/publicsector
Or reach out to HUMAN directly by contacting Jamie Ward, Government Cybersecurity Manager, at 305-877-7027 or jamie.ward@humansecurity.com.