Mailers' Technical Advisory Committee (MTAC)

Greg Crabb
Chief Information Security Officer

6/19/2019

USPS Third Party Risk Management

The Postal Service employs a defined third party cyber risk management process to ensure the appropriate controls are in place to reinforce the enterprise's cybersecurity posture and that of its business partners.

Third Party Risk Management Process

Identify and Prioritize Dependencies

1. Identify and prioritize dependencies, including those resulting from external suppliers and internal USPS stakeholders.

Manage Cyber Risks

2. Identify risk owners, develop risk mitigation plan(s), and track and monitor remediation strategies.

Establish Relationships

3. Formalize relationships with partnering entities and document agreements.

Manage Performance

4. Document risks based on security specifications and monitor performance of business partners.

USPS Digital Advertising Overview

The Postal Service has an opportunity to expand digital revenue through Informed Delivery® advertisements. Careful consideration of digital advertising risks will help prevent advertiser fraud and cyberattacks.

GOALS

USPS aims to provide its users with a trustworthy digital experience while embracing and extending online advertising opportunities for USPS mailers

CHALLENGES

USPS must develop systems and processes which are scalable and dynamic to meet the needs of advertisers, while addressing known cyber threats in the advertising space

REQUEST

USPS needs mailer input to develop a policy grounded in leading industry standards for ad security, privacy, and user experience

Scope of Potential Acceptable Ads Policy

- Enrollment and Identity Proofing
- Ad Submittal Process
- Scanning/monitoring of ad links/images
- Scanning/monitoring of ad landing pages
- Mailer web/server infrastructure

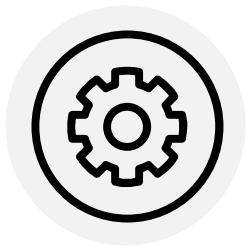
Informed Delivery® Campaign Security Lifecycle & Strategy

The Postal Service is committed to the continuous monitoring of all links and landing pages associated with Informed Delivery® in identification of security and privacy issues and to ensure adherence to program and mail-ability standards.

Informed Delivery® Campaign Security Lifecycle & Strategy

Monitored 35,000+ campaigns to-date

Actively investing in tools and monitoring services



Security-based system architecture

SUBMISSION

DURING CAMPAIGN

POST-CAMPAIGN

Digital Advertising Concerns

The Postal Service seeks to provide a trusted experience consistent with customers' expectations of both USPS and its mailer brands. Failure to abide by digital advertising standards on the USPS Informed Delivery® platform can result in a number of threats to the USPS user experience.

Advertising Performance & User Experience Issues

Ad pop-ups and pop-unders

Privacy issues related to end user tracking, data sharing, and data management policies

Auto-play videos on ad landing pages

Excessive ad landing page load times and ad latency due to multiple re-directs

Ad landing page and server issues (404 errors, time-outs, broken links)

Security warnings/blocks for non-https landing pages or expired SSL certificates, script warnings, and server IP reputation issues

Impact of Unacceptable Digital Advertising

Unacceptable digital advertising poses substantial risk to the Postal Service and its digital mailing partners. These risks include reputational damage as well as increased susceptibility to fraud and cybersecurity threats.

Impacts to USPS and Mailing Partners

LOSS OF BRAND VALUE

Customers begin to associate USPS products and services with an undesirable or insecure user experience

LOSS OF CUSTOMER BASE

Customers unsubscribe from USPS digital products (like Informed Delivery®) and stop interacting with mailer brands

MALVERTISING

Absent acceptable ads standards, cyber actors use USPS platforms to serve malicious ads, spreading cyber threats and stealing USPS user data

Preventing Malvertising: A Customer-Focused Approach

USPS CISO is actively exploring ways to prevent malvertising while minimizing resulting disruptions to the customer and consumer experience.

Preventing Malvertising

Implement **protections from malicious ads** that breach various phases of legitimate advertising campaigns.

Resolve offending campaigns without blocking entire advertisements or impacting upstream partners.

Detect and **monitor excessive website redirects** and unapproved updates to advertisement landing pages.

Enable a trusted network of digital campaigns and partners, reducing recurring violations through **early isolation of bad actors.**

Explore and focus on ways to proactively **enhance overall customer experience**.

Improving the Advertising Experience

In collaboration with partners, USPS CISO will devise solutions to combat malvertising and preserve the integrity of its digital mailing footprint.

Combatting Malvertising and Enhancing the Advertising Experience

Establish monthly working group to consistently plan and implement solutions and policies to prevent malvertising.

Create a reliable channel to report security and privacy concerns or forward-looking suggestions.

Develop and commit to a service level agreement (SLA) for responding to advertising-related supplier inquiries.

Will you help? Provide input into the development of an acceptable ads policy founded on industry standards and focused on the preservation of privacy and the promotion of quality advertising.

Thank You

Greg Crabb
Chief Information Security Officer
U.S. Postal Service