

# U.S. PRESIDENTIAL CAMPAIGN LACKS SECURITY



THE MEDIA TRUST  
We know digital security.

## Candidate Websites Filled with Unmanaged Third-Party Code

Unmanaged third-party code on candidate websites creates risk for consumers. When browsing these sites or making a donation, consumers are exposed to suspicious activity and unnecessary collection of their personal and financial information.

### Campaign websites do not meet industry best practices for security and data privacy

## RISKS

**81%** Executing code from digital third-party vendors

**6%** Domains present malicious or suspect activity

**3X** Klobuchar's cookie use is significantly larger than the other candidate websites

**2** Security incidents exposed consumers to adware or typically unwanted programs

## TRACKING

**71%** Code on the payment pages had **zero** relevance to the purchase transaction

**95%** Code on Booker donation page is **NOT** relevant to payment processing



All candidate websites allow tracking of consumers, **6 candidates track for 20 years or more**



Warren's donation page had **56 data tracking entities** that could gain access to consumer payment information

## Controlling Your Digital Ecosystem

To defend against attacks and the misuse of consumer information, every enterprise needs to safeguard their websites or mobile apps. Specifically, they should:

- Continuously monitor the website from the consumer's point of view to capture the entire code base involved in rendering each page
- Understand the provenance of all executing code; digital vendors may have multiple domains performing different functions
- Analyze the necessity for all code accessing consumer devices to minimize unnecessary data collection, and, as a bonus, realize improved page speed
- Document, communicate and enforce operational policies with digital vendors to evaluate their compatibility and compliance with your requirements

## BOTTOM LINE: Protecting Consumers is Your Responsibility

Candidates—like enterprises—are responsible for the code their websites and mobile apps put on consumer devices. To protect consumers, partners and clients from harm, enterprises need to control the code that executes via their owned digital assets. What's your website's attack surface? Request your Digital Assessment at [www.MediaTrust.com/US-Election-Security](http://www.MediaTrust.com/US-Election-Security).