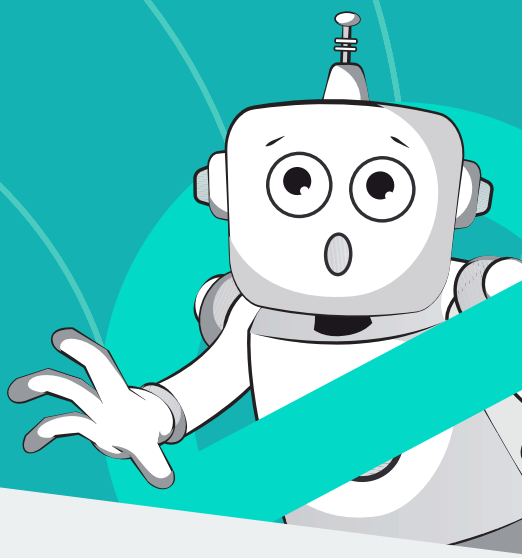
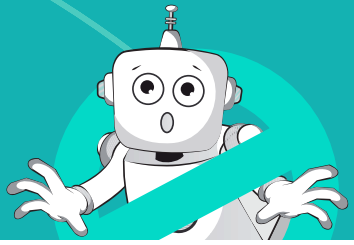


DONATION SITES SECURITY ALERT

SECURITY ALERT: U.S. POLITICAL DONATION SITES AT RISK



With the upcoming U.S. presidential election, there has been a recent surge in campaign donations, resulting in large volumes of transactions being processed by donation platforms, making them attractive targets for cybercriminals.

Donors often provide personal and financial information, such as names, addresses, and credit card details. Securing this information is crucial to prevent identity theft and financial fraud, which can have severe consequences for individuals and damage public trust in the platforms.

Trust in the integrity and security of donation platforms is vital for encouraging continued election participation and contributions. A breach or data leak could undermine confidence, leading to reduced donor engagement and potential financial losses for political campaigns.

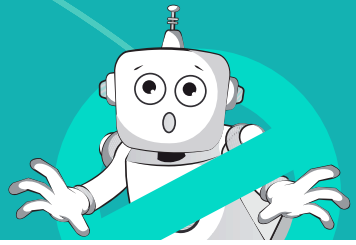
SECURITY ASSESSMENT OF DONATION SITES

DataDome tested three major US political donation platforms in order to assess their security measures against automated and fraudulent activities.

Key findings:

1. 2/3 of the Donation Sites Lack Critical Security Measures

- When evaluating the three donation sites, DataDome found that all lacked critical login security measures to protect against bot traffic and credential stuffing attacks.
- Only one platform implemented two-factor authentication (2FA), offering a layer of security for user accounts.
- The other two platforms had no effective security measures, relying solely on basic defenses that are no match for today's sophisticated bots and fraudsters.



2. Ineffective Use of reCAPTCHA v2

- All three platforms employed reCAPTCHA v2 on their **registration** pages. However, this free version is widely recognized as insecure and easily bypassed by sophisticated bots.
- Importantly, **login endpoints on these platforms were left completely unprotected**, presenting a significant opportunity for account takeover. Using a popular open source bot framework, we were able to create a bot capable of successfully logging into our own account **without** being challenged by any security countermeasures.

3. Potential for Credential Stuffing Attacks

- The lack of robust protection on login endpoints exposes user accounts to credential stuffing attacks. These attacks can lead to unauthorized access, allowing attackers to harvest personal information and stored credit card data.
- Many users save their credit card information for recurring donations, further increasing the risk of financial theft and data breaches.

IMPLICATIONS AND RISKS

- **Credential Theft and Account Takeover:**

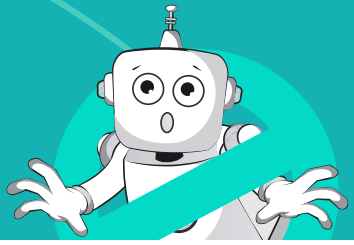
Attackers gaining access to user accounts can scrape sensitive information, including credit card details. This poses a high risk for both financial fraud and identity theft.

- **Reputation Damage and Loss of Donor Trust:**

Security breaches can lead to significant reputational damage, potentially eroding donor trust and impacting future fundraising efforts.

- **Financial Implications:**

The financial losses from fraudulent activities, chargebacks, and potential legal penalties could be substantial for these platforms.



RECOMMENDATIONS

To mitigate these risks, donation sites and donors alike can take steps to enhance their security posture.

Donation sites:

- **Enhanced Authentication:**

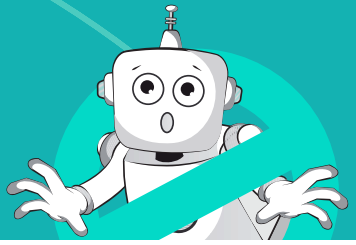
Deploy two-factor authentication across all critical user interactions, including logins and transactions, to add a layer of protection against unauthorized access.

- **Advanced Bot Protection:**

Transition from basic CAPTCHA systems to more sophisticated bot management solutions that provide real-time detection and mitigation of automated threats. In particular, the bot protection must be resilient against sophisticated attackers capable of passing CAPTCHAs using CAPTCHA farms, be able to detect attacks started from thousands of IP addresses using proxies, and be able to detect bots that mimic human-like behavior.

Donors:

Donors can shore up their account protection by using a unique and strong password generated using a password manager, either a dedicated one like Bitwarden or Dashlane, or the one from their browser. Credential stuffing attacks work because people reuse the same email/password across different websites/applications. Thus, if one of these services gets breached, attackers can try to reuse passwords from this leak on (an)other website(s).



The current surge in campaign donations underscores the urgent need for robust cybersecurity measures on donation platforms. Protecting donor information not only safeguards individuals but also upholds the integrity and trust essential for democratic participation. By prioritizing security, campaigns can foster confidence among supporters, ensuring their continued engagement and financial backing in the electoral process.