The Guide to Protecting Your Campaign Website

WHAT IS CLOUDFLARE?

Cloudflare is on a mission to help build a better Internet.

We are a leading security, performance, and reliability company whose platform protects and accelerates any Internet application online without adding hardware, installing software, or changing a line of code. Internet properties powered by Cloudflare have all web traffic routed through its intelligent global network, which gets smarter with every request. As a result, they see significant improvement in performance and a decrease in spam and other attacks.

TABLE OF CONTENTS

WHY CAMPAIGN WEBSITES CAN BE TARGETS

Campaign websites serve a powerful role in democratic elections.

They provide crucial information to people before, during, and after elections. Campaign websites can also be targets of attack and can face vulnerabilities due to peaks in traffic.

Here are just some of the ways that vulnerabilities can interfere with an effective, efficient campaign:

Before elections

Security and performance vulnerabilities can cause these sites to become unavailable, to spread false information about their candidate, or to expose supporter data.

During elections

Security and performance vulnerabilities can prevent undecided voters who visit campaign websites from accessing important information that might convince them to vote for your candidate.

After elections

Security and performance vulnerabilities can interfere with people who visit campaign websites after an election to see the results and get real-time updates.

VULNERABILITIES AND SAFEGUARDS - HOW TO PROTECT YOUR CAMPAIGN WEBSITE

The Internet's open, distributed nature creates security and performance vulnerabilities for campaign websites.

Here's what you need to know to protect your Internet presence before any damage is done.

THREAT #1	Distributed Denial-of-Service (DDoS) attacks
THREAT #2	Data Theft
THREAT #3	Malicious Bots
THREAT #4	Website Availability

THREAT #1

Distributed Denial-of-Service (DDoS) attacks

What is it?

Bad actors can target campaign websites with denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks that target websites and network infrastructure. These attacks overwhelm available resources, often utilizing application layer (layer 7) attacks.

How Cloudflare protects your campaign website:

Protect your network

The first step in protecting against a DDoS attack is to ensure that multiple layers of security controls are able to protect your network. Example controls include utilizing a web application firewall or IP reputation database.

Block malicious traffic at the edge

A CDN provider will have insights into global traffic that would be impossible for individual websites to maintain. This knowledge is often fed into security actions. For example, Cloudflare employs a program called Gatebot, which automatically blocks bad traffic at the edge, preventing this traffic from reaching your origin.

THREAT #1

Distributed Denial-of-Service (DDoS) attacks

How Cloudflare protects your campaign website:

Protect your DNS

DNS, short for Domain Name System, is the phone book for the Internet. It associates an IP address with a corresponding URL address. Nearly every action you take on the Internet starts with a DNS request. For example, when you type 'google.com' into a web browser, DNS is the system that finds the numerical IP address behind the letters. Cloudflare can help protect DNS because our authoritative DNS servers run on the same 30 Tbps network which protects more than 20 million Internet properties from DDoS attacks.

Did you know?

To date, the largest attack on record is 1.7 Tbps

THREAT #2

Data Theft

What is it?

Campaign websites can be vulnerable to security breaches like SQL injection attacks, cross-site scripting, and cross-site forgery requests, which can lead to the theft of data, including data from donors and other supporters.

What’s SQL injection?

Structured Query Language (SQL) injection is a code injection technique used to modify or retrieve data from SQL databases. By inserting specialized SQL statements into an entry field, an attacker is able to execute commands that allow for the retrieval of data from the database.

How Cloudflare protects your campaign website:

Use HTTPS encryption

Protecting your website starts with strong encryption practices. Secure Sockets Layer, or SSL, is the first widely-adopted web encryption protocol. The latest protocol is called TLS, short for Transport Security Layer. Because data on the Internet is transferred across many locations, it is possible for bad actors to intercept packets of information as they move across the globe.

By using a cryptographic protocol, like TLS, websites ensure that only the intended recipient is able to decode and read the information, and intermediaries are prevented from decoding the contents of the transferred data.

THREAT #2

Data Theft

How Cloudflare protects your campaign website:

Use a Web Application Firewall

A Web Application Firewall (WAF) monitors, filters, and blocks HTTP traffic to a web application. Using a WAF protects your Internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests.

Did you know?

Cloudflare develops automatic rules for our WAF based on intelligence we gather from our global network.

USE DNSSEC

If DNS is the phone book of the Internet, DNSSEC is the Internet's unspoofable caller ID. It guarantees a web application's traffic is safely routed to the correct servers so that a site's visitors are not intercepted by a hidden 'man-in-the-middle' attacker which can go unnoticed by site visitors, increasing the risk of phishing, malware infections, and personal data usage.

THREAT #3

Malicious Bots

What is it?

Bad actors can create bots that interfere with campaign websites. Common types of abuse include content scraping and account takeover, which can lead to increases in operational costs and data loss.

How Cloudflare protects your campaign website:

Use a Web Application Firewall

A Web Application Firewall (WAF) filters, monitors, and blocks HTTP traffic to and from a web application. Using a WAF protects your internet property from common vulnerabilities like SQL injection attacks, cross-site scripting, and cross-site forgery requests.

Use an IP reputation database

IPs that perform malicious actions can be tracked with a global reputation system. An IP reputation database enables shared network intelligence and predictive security to identify and block abusive bots.

THREAT #4

Website Availability

What is it?

Oftentimes, campaign websites experience periods of high traffic, often referred to as network spikes. These spikes in traffic can overwhelm websites creating a poor user experience — at times, content on the website will slowly load; at other times, the content will not load at all.

Spikes in traffic can also lead to increased network infrastructure bills, due to higher network and server utilization. Using a CDN and caching will help offload resources from your server at all times, optimizing your website's resources and reducing the burden of spikes in traffic.

How Cloudflare protects your campaign website:

Reliable DNS

Reliable DNS providers like Cloudflare use vast networks of servers to ensure that your content is always reachable and decreases delays in resolving your DNS.

Anycast Content Delivery Network

Cloudflare is an Anycast CDN which quickly routes incoming traffic to the nearest data center with the capacity to process the request efficiently, handling surges in web traffic due to recent press features, public appearances, and other high-profile events.

THREAT #4

Website Availability

How Cloudflare protects your campaign website:

Perform country blocks at the edge

Oftentimes, campaign websites are looking to serve web traffic to countries in which the visitor is not a potential voter. Being able to block specific countries frees up resources and prevents malicious attacks.

CDN/Caching

Serving static assets from a CDN provider will significantly offload resource load from your origin. This will allow for more processing power from your servers, especially during high-traffic periods.

Knowing is half the battle

It’s important to monitor how your campaign website is performing. With Cloudflare, you have access to an analytics platform that gives you full insight into your site's performance, availability, and security.

Ok, you’re well on your way!

You now have the fundamentals of campaign website vulnerabilities and the steps you can take to make them secure and reliable.

HOW CAN I SIGN UP FOR CLOUDFLARE?

We have launched Cloudflare for Campaigns to help protect campaign websites.

Cloudflare for Campaigns is a suite of products designed to safeguard and optimize the performance of your candidate's web presence, and to protect your campaign's internal data.

It allows you to leverage the collective intelligence of Cloudflare's global network, which automatically deploys countermeasures to thwart the latest Internet threats as they emerge.

LEARN MORE AT:

https://www.cloudflare.com/campaigns