MABUS

—

Website Security

71 South Green Street I Tupelo, MS 38804 I 662 823 2100 I mabusagency.com

Website Security

Mabus Agency specializes in creating cutting edge, dynamic, data-driven websites. To accomplish this, we use a Content Management System (CMS). Whether built using Wordpress, Drupal, or another system, our security stance doesn't change. There are many security concerns that arise when discussing a platform that allows user logins. Mabus Agency knows that the best site is useless if it's not secure.

Below, you will see our rigorous methodology for protecting your site from hacks, takeovers, malware uploads and almost all other attacks. No system is foolproof, but you will find that while we put an incredible amount of importance on creativity, design and copy; we also put an equal-or-greater effort into securing our websites.

Secure Host

Our hosting provider uses multiple layers of information security protection to keep your data safe. Physical and network security protocols have been put in place, and our provider will contact us immediately in the unlikely event of inappropriate or unauthorized access to sensitive information.

Physical security ::

- Facilities staffed 24/7/365
- CCTV security cameras covering the inside, outside, and entrances to all data centers
- Electronic perimeter access card systems installed at site entrances
- Third-party remote monitoring of all sites
- Mantraps with interlocking doors at all entrances

Transport ::

- SSAE-16 & HIPAA compliant
- Safe Harbor certified
- Hardware firewalls that limit inbound and outbound data access
- Automatic IP blocking of suspicious network activity
- Daily server backups

Our host has also completed and passed its EU-US and Swiss-US, Privacy Shield audit, SOC 1, 2, 3 attestations, and PCI Service Provider recertification.

Website Security

SSL (Secure Sockets Layer)

SSLs establish an encrypted connection between a server and a user's browser. This connection keeps incoming and outgoing data private. We implement SSL protocol on every bank website to ensure protection.

Server-Side Authentication

We require an initial HTTP authentication before any attempt to access a website's backend. This means the login page for the backend will not be accessible until a user is authenticated. After three failed attempts, a user's IP address is blacklisted and that user will be unable to access any websites or information stored on the server.

CMS Login

Users will only be presented with the CMS login if they pass server-side authentication. CMS accounts require a strong password containing a mixture of special characters, capital letters, and numbers. This protocol is combined with a strong username requirement. Usernames like "admin" and "user" cannot be used. All passwords must pass rigorous strength requirements before they are accepted. This alone significantly reduces the risk of successful CMS attacks.

User Management

When it comes to user accounts, less is more. We make sure only the minimum number of user accounts are added to a site. We handle all user account activations and give you all the access you need to manage these accounts. User activation only occurs after a two-step authentication process that requires account verification through email.

Coding Practices

Our developers are highly experienced in detecting security issues in code. This awareness allows them to avoid creating open doors or vulnerabilities that can be exploited. They also work with the most up-to-date and stable versions of coding languages and database tools. While communication between a website and its database is crucial to the utilization of data, we also make sure there are no unnecessary calls to and from the database.

Website Security

Constant Monitoring

Website traffic is constantly monitored and analyzed. Any suspicious activity or behavior is flagged and blocked. The IPs associated with those activities will be blacklisted as well. Finally, the growing repository of known vulnerabilities and malicious behaviors is updated in real time to ensure our library is as up-to-date as possible.

Security Auditing and Monitoring

We use Defiant, which is a best-in-class security audit and monitoring tool that boasts an impressive number of security features that keep our websites safe from malicious activity. Through Defiant, we utilize the following techniques and tools:

- Web application firewalls
- Real-time threat defense feeds
- Brute-force attack blocking
- Country blocking
- Advanced manual blocking
- Malware scans
- IP and website spam checks
- Reviews of crawlers, bots, login/logout, and visitor activity
- Cell phone sign-in authentication
- File repair
- Password audits
- Spam filters

Continuing Education/Support

Continued learning and support for website security is just as important as implementing security protocols in the first place. We are constantly researching the newest security procedures, then immediately implement them into our sites. And, once a site goes live, we do not disappear. Your site will continue to be updated and monitored to make sure it remains stable and secure.