Responsible Disclosure Policy

Marketo is committed to keeping its marketing platform safe for everyone, and data security is a top priority. If you are a security researcher and have discovered a potential security vulnerability with Marketo SaaS, we encourage you to let us know right away and we appreciate your help in disclosing it to us in a responsible manner.

The Marketo security team acknowledges the valuable role that independent security researchers play in Internet security. As a result, we encourage responsible reporting of any vulnerabilities that may be found in our site or applications. Marketo is committed to working with security researchers to verify and address any potential vulnerabilities that are reported to us in a responsible manner.

Please review this policy before you test and/or report a vulnerability. We will investigate all legitimate reports and do our best to quickly fix the problems.

Testing for security vulnerabilities:

To ensure performance, availability, and security of Marketo SaaS instances, Marketo does not allow use of Production, Trial, Sandbox, or Demo instances for security testing. Automated security scanning tools may damage your subscription data.

To conduct a security assessment of Marketo SaaS, please contact security-support@marketo.com and request a security test subscription. The security test subscription will be identical to production subscription, but will be located on non-production cluster dedicated for security tests and QA activities.

If you accidently find a security vulnerability on a production Marketo SaaS instance, immediately cease testing and follow the reporting steps below.

Reporting a Potential Security Vulnerability

Privately share details of the suspected vulnerability with Marketo by sending an email to security-support@marketo.com with “Potential Security Vulnerability” in the Subject line.

Provide full details of the suspected vulnerability so the Marketo security team may validate and reproduce the issue.

Attributes of a Good Report

Please include detailed steps in your message explaining how to reproduce the vulnerability. Include any links you clicked on, pages you visited, URLs, user IDs, etc. Images or video can be helpful. Be sure to include clear descriptions of any accounts used in your report and the relationships between them.

Conduct

While we encourage you to discover and report to us any vulnerabilities you find in a responsible manner, the following conduct is expressly prohibited. If you comply with this policy

when reporting a potential security vulnerability to Marketo, we will not initiate a lawsuit or law enforcement investigation against you in response to your report. We ask that:

- You give us reasonable time to investigate and mitigate an issue you report before making public any information about the report or sharing such information with others.
- You do not interact with a Marketo customer or lead (which includes modifying or accessing data from the customer or lead) if the customer or lead has not consented to such actions.
- You make a good faith effort to avoid privacy violations and disruptions to others, including (but not limited to) destruction of data and interruption or degradation of our services.
- You do not exploit a security issue you discover for any reason. This includes demonstrating additional risk, such as attempted compromise of sensitive company data or probing for additional issues.
- You do not violate any applicable laws or regulations.

Prohibited Activities

Marketo does not permit the following types of security research:

- Performing actions that may negatively affect Marketo or its users (e.g. Spam, Brute Force, Denial of Service, etc.)
- Accessing, or attempting to access, data or information that does not belong to you
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you
- Conducting any kind of physical or electronic attack on Marketo personnel, property, or data centers
- Social engineering any Marketo support desk, employee or contractor
- Conducting vulnerability testing of participating services using anything other than dedicated security test SaaS instances
- Violating any laws or breaching any agreements in order to discover vulnerabilities

Commitment

The Marketo security team commitment:

We ask that you do not share or publicize an unresolved vulnerability with/to third parties. If you responsibly submit a vulnerability report, the Marketo security team and associated development organizations will use reasonable efforts to:

- Respond in a timely manner, acknowledging receipt of your vulnerability report
- Provide an estimated time frame for addressing the vulnerability report
- Notify you when the vulnerability has been fixed

Marketo greatly appreciates the efforts of those security researchers who identify vulnerabilities and work with us to ensure that we can develop a fix and thoroughly test before a fix is applied for all our customers. We thank you for going out of your way to help us minimize the risk to our customers as well as help us in our vision to improve the overall security of our products and the Internet as a whole.