



Best Practices Top 10: Keep your e-marketing safe from threats

Months of work on a marketing campaign can go down the drain in a matter of minutes thanks to an unforeseen vulnerability on your campaign's microsite. Don't let your company's brand (or your own) get tarnished by a preventable hack. Here are 10 quick tips to make sure your e-marketing is safe from outside—and inside!—threats.

1 Choose a dedicated server over a shared server

To save money, many companies opt to use a shared server to host their site's files. This means many different sites are running on the same machine, sharing the same programs and scripts to run applications that are common to all of the sites—things like email services or control panels, for example. This means that it's not just you or your company's staff that has access to your server. Hundreds (if not thousands) of other people in other companies do as well. If your provider or a fellow customer is lax in its security and a site on your shared server gets compromised, your site and its data are at risk as well. Worse, using a shared server means it's a lot easier for someone with malicious intent to gain access to your files, simply because that hacker has many more gateways to exploit on a shared server with multiple sites.

While a dedicated server is by no means a silver bullet in website security, it is a good first step. When you use a dedicated server, your site will have its own machines with scripts and programs exclusive to your site. This means you can exert full control over what's running on your server as well as the level of security behind your website. A dedicated server allows your company to significantly reduce the opportunities for your site to be hacked by an outside force and or made vulnerable by another site's weak security.

2 Check the frequency of security updates and speed of patching

Server and data security is often a low priority for hosting companies (if it's even a priority at all). A hosting company can promise that they run the latest and greatest in security programs to protect your site's data, but if they don't bother to keep all the programs running on a server up-to-date and patched—and patched quickly—your site is vulnerable to threats.

When a software companies sends out a software patch to fix security vulnerabilities, it is important that these fixes are deployed quickly. A slow reaction to changing threats gives a hacker time to exploit a vulnerability, putting your site and its data at risk. So when you're investigating web hosting companies, it's important to know how often they check for updates on programs your server runs and how quickly and regularly they patch security holes. If your hosting company doesn't patch quickly, your security policy is effectively negated.

3 Don't run what you don't need (or shouldn't have)

Many web hosting companies offer a number of services to their customers out of the box; however, every application hosted on your server represents another opportunity that a hacker can use to break into your site. A number of these common programs represent large vulnerabilities, including web mail. If your web host offers a service that you simply don't need, make sure they are not installed on your server. In addition, some programs that hosting services common provider are just a bad idea when it comes to security—for example, FTP (file transfer protocol) is very common but extremely vulnerable to exploitation, as it does not use a secure connection. Any company serious about site security should use disable use of FTP and instead use SCP, a secure alternative.

4 Stay up to date on server-side changes

When site security is a priority, you can't have just anyone accessing your site's files ad-hoc, because this can compromise your site as well as your customers' confidential data. You need to have a process in place that dictates and restricts specifically who can access and modify your site's files. In addition to a contact list, there needs to be a policy in place between your company and your hosting provider that someone on your staff—be it marketing or IT—is notified if and when there are changes to anything that lives on your server, from website files to programs and scripts that run in the background. Any kind of change to a program or file can present a security vulnerability (either alone or in tandem with other files), and it's important that staff in charge of security in your firm know if and when this happens. If there are no clear communications contacts or processes, important information about changed files can go uncommunicated, leaving your site at risk.

5 Know who's modifying your data and when

As important as knowing what's been changed on your site is knowing who made that change and when. A change control system allows for versioning and tracking of activity—which lets you fix innocuous errors more easily, and also enables you to track any malicious activity being inflicted on your site. Remember, it's not just outside threats that can present a problem to your site—unauthorized data access or internal changes from employees with less-than-honest intentions can be an even bigger problem than a hacker from the outside.

6 Ensure your data and server's physical security

Just as you'd restrict access to your company's confidential files, it's important to know how someone could get physical access to your site's server. Perhaps your server is frequently patched and has high-level encryption, but are the doors to the server room locked? Consider hardware end of life, too. What does your hosting company do with a failed hard drive? If they don't completely wipe that hard drive of its data, stealing your customer's confidential data could be as easy as going through the trash. Worse, you could be legally vulnerable for the data theft. A good way to know if your web host takes security seriously is if they comply with ISO/IEC 27001 and 27002, standards of virtual and physical information security. While such standards are not an absolute measure of security, they are a good starting point.

7 Establish a legal policy on Personally Identifiable Information (PII)

Data leakages—whether your fault or not—can leave you legally liable. Complicating the matter is that data protection guidelines vary widely between jurisdictions and frequently change. In order to protect yourself from a lengthy legal mess, your company needs to have a Personally Identifiable Information (PII) protection and responsibility policy stipulated in the legal agreement. Many hosting companies neglect to mention PII policy in the contract, leaving you (the customer) legally responsible for stolen customer data, even if it is the hosting company's fault. Best case scenario: put it in writing in your contract with the hosting company that they are responsible for maintaining the integrity of customer's data and legally responsible should it be compromised. Keep in mind, however, that even if the host agrees to take on responsibility, should there be a data leak, your company can still take a big PR hit.

8 Implement code sanitizing on any input fields

Anywhere a user can input information, there's potential for abuse through common attack vectors like a SQL injection, for example. Assume that all input to a webpage can be malicious in intent—meaning email address fields, drop-down menus, even text on bulletin boards all present abuse potential. One option is to use an allow listing, which is a list of IP addresses known to be safe, in other words, not sources of spam or malware. Another option is to make sure the input fields on your site sanitize anything coming in, rendering malicious code useless; however, this isn't the easiest thing to do. Working with an experienced and trusted penetration testing company is a great way to spot potential problems in this area.

9 Get your site added to list of monitored websites

Should the worst happen, you want to know as soon as possible. If you add your site to a malware checking service (such as Sophos WebAlert), you can be quickly notified should your site become compromised, allowing for quick action and mitigated impact.

10 Scan all outgoing campaign emails

While this won't help your campaign from being vulnerable from hackers, it will prevent your campaign from being blacklisted as malicious by others. You don't want your campaign's emails to be deleted by user's anti-spam devices! To avoid embarrassment, make sure to thoroughly scan any outgoing emails for embedded malware before you send them—and run your email through spam checkers to make sure its content doesn't set off any red flags in email filtering systems.

For more detailed information on how to keep your website safe from threats, see “Securing websites,” a Sophos technical paper:
<http://www.sophos.com/security/technical-papers/sophos-securing-websites.html>