Cyber Security: Three Steps To Keep Every Site More Secure

Almost every week, there’s another report of a website security breach and the theft of data, financial information, and thousands of personal records. In the past year alone some of the biggest companies in the world have been hacked. The list includes Home Depot, Ebay, JP Morgan Chase, the IRS, Uber, Staples, Target, British Airways, AOL, Adobe, Living Social, Zappos, Facebook, Sony, TJ Maxx and many more. This is in addition to Internet-wide bugs such as Heartbleed, Bash, and POODLE that weakened systems around the world.

It doesn’t look like cyber attacks are going to slow down anytime soon.

- Verizon’s recent Data Breach Investigations Report estimated that there were 2,122 confirmed data breaches in 2014, generating $400 million in losses.
- Akamai Technologies’ State of the Internet Report showed that hacker attacks on websites went up 75% in the final quarter of 2013, with hackers in China responsible for 43% of all attacks.
- Earlier this year, Juniper Research estimated that the annual cost incurred from malicious data breaches worldwide will exceed $2 trillion in 2019.
- See the World’s Biggest Data Breaches Infographic here.

Why are there so many security breaches these days? And how can you protect your site?

One reason there are so many large hacks is that companies are moving their businesses and their data online. As the world gets more mobile and smartphones proliferate, companies want to give customers and employees 24/7 access to their sites. It's an always-on, global world. Customers want to shop and employees need to work from anywhere, anytime.

This creates many more opportunities for folks with bad intentions who want to get access to your data. Web-based attackers can more easily access high-value assets, and they have shifted their methods to new attacks accordingly. Experts predict that going forward, hackers will continue to target credit card numbers and point-of-sale systems, but will increasingly aim for health care data. The bad guys' motives can range from using your website resources, redirecting your website traffic, and displaying pop-up ads or hyperlinks to stealing and selling sensitive information on the black market.

Security is an ever-growing issue. A website that is not secure is open to hackers and viruses. If a hack happens on your website and personal information is released, it could ruin your brand and customer trust in your company. Protecting the information of your site's visitors is imperative, just as protecting any proprietary company information and ensuring the inherent ability of your site to fend off unwanted visitors.

What would happen to your business if your internal network, website, or emails got hacked? Having a secure website is essential to reduce the risk of data theft, downtime, loss of business and customer trust. As hackers get more sophisticated, so too must your Internet security. If you haven't already, now is the time to review your site and your security practices.

What You Can Do to Increase Cyber Security

Hackers are on the lookout for security vulnerabilities in your web applications. Shopping carts, forms, login pages and dynamic content are easy targets. Here are three steps you can take.

Step 1: PCI compliance, a standard set by credit card companies, is a great benchmark for the security of your site even if you're not an e-retailer. If you have a shopping cart on your site or another payment gateway where customers are entering credit card information you need to make sure your site is PCI compliant.

Step 2: Make sure customer data is encrypted and that your site's CMS is updated at all times to avoid cross-site scripting attacks that allow a hacker to control the look and feel of your site or, worse, get access to login information and customer passwords. This is a very common site vulnerability.

Step 3: Make sure that all code is updated regularly and protected by strong passwords and run regular audits to check for known vulnerabilities in your web applications. Reach out to an agency partner with a firm understanding of website security and how to ensure the safest experience for your customers.

Key Questions to Ask

Start by reviewing your current site and security practices. Some key questions that may apply to your site include:

- Does your site have any obvious security flaws?
- How resilient are any forms on the site to special characters?
- Are private directories password protected via .htaccess?
- Are public non-document directories indexable or are appropriate permission settings in place to block access?
- Is customer data stored online?
- If so, is this database appropriately safeguarded against external access?

The Bonus

In August of last year, Google announced that it would be giving preference to secure sites, and that adding encryption would provide a "lightweight" rankings boost. It stressed that this boost would start out small, but implied it might increase if the changed proved to be positive. This means that not only does improving security protect your business and its reputation, it may also give your site a boost in the rankings.

For more information about designing a safe and secure website that can help turn your **Digital Ambitions Into Business Results** call Geary LSF at 877.616.8226 or email sales@gearylsf.com.