Getting a Website Designed? How to Make It Secure from Cyber Crime

By Alan Brogan, The Digital Department

Getting a website designed is an exciting time in any company. Whether your firm is creating a site for the first time or is redesigning its current site, a website launch is always something to be celebrated. In getting a website designed, companies often focus on style, colour schemes and functionality, all of which are extremely important. What companies can forget to do however is to focus on making their websites secure. Though particularly important for eCommerce websites, securing all websites is important no matter what type. If your site is not secure there are a host of issues that could occur. For example, customers' details could be taken; money could be stolen from your company and customers; important, confidential information could be obtained. And these are just the tip of the iceberg. Below is a checklist on how you can make your site secure:

Securing Your Website – The Ultimate Checklist:

1. **Choice for a Secure Platform:** Always ensure to develop your website on a platform that uses a sophisticated object-orientated programming language. WordPress, Joomla and Magento are some of the popular platforms for secure web designing.

2. **Strong SSL Authentication:** It is always vital to opt for SSL(Secure Sockets Layer) certificates to enhance the trust of your website among the web browsers, search engines and customers. If your website is integrated with any sort of payment system, the use of the SSL certificate is a must.

3. **Never Ever Store Sensitive Data:** It is not wise to store thousands of customers' sensitive records. Storage of Credit card numbers, CVV2 codes and expiration dates are strictly forbidden as per the PCI Standards. Always insist on keeping a minimal amount of customer data for charge-backs and refunds.

4. **Employ AVS & CVV Verification System:** Always enable a card verification value and an address verification system to ensure that only the legitimate users are using their saved credit cards. It is vital from the perspective of reducing fraudulent charges.

5. **Use Strong Passwords (Combination/Alphanumerical)**: With the existence of an assorted number of password guessing and sniffing tools available, the website owners should ensure to use a combination of alphabets, numbers and special characters to ensure a basic protection at the front-end.

6. **Suspicious Activity Alert System:** Always set up alerts for any kind of suspicious activity like logging in same account from different countries frequently, multiple tries of logging using wrong passwords, suspicious transactions from same IP address and so on.

7. **Multiple Security Layers:** One of the foremost ways to protect a website from the vulnerabilities implementation of different security layers. Use firewalls, login boxes contact forms, search queries and other measurable steps to protect the website from application-level attacks such as XSS and SQL.

8. **Regular Monitoring of Website:** Keep an eye on the website as well as the visitors to ensure that your website is protected from any sort of behaviours related to hacking and fraudulent activity. Set up real-time alerts for such vulnerabilities. Further, penetration testing is also a better option to check whether the website lacks any significant security feature.

9. **Periodic PCI Scans:** Among hundreds of PCI scan software available online, ensure to periodically scan your website to know how vulnerable is your website against the potential hacking attempts. It helps in detecting the potential areas from where the hackers can gain access to your website or its sensitive data.

10. **Update & Fix Everything ASAP:** Make a habit of upgrading the software and extension right after the stable release to ensure protection against cyber crimes. Besides, always ask the developers to fix the potential vulnerabilities as soon as possible so that your website and associated visitors can always remain safe from the cyber criminals.

Why Using The Checklist Is Important

Using this checklist will be extremely beneficial to securing your site. There are many day-to-day hassles in business and having someone hack into your website is not a headache you want. It is important to state that no matter what you do and how often you do it there is no sure-fire way to 100% security. With the above checklist you are definitely making things safer. If you have any further questions about securing your site then feel free to call us at the http://www.thedigitaldepartment.ie

About the Author: Alan Brogan is the Managing Director of The Digital Department at http://www.thedigitaldepartment.ie
Alan is a leader in website design and online marketing management. Email—info@thedigitaldepartment.ie