WEBSITE SECURITY

Online criminals, including both 'professional' criminals and 'enthusiast' hackers, are becoming ever more sophisticated and creative. Unprotected websites - particularly complex ecommerce sites that capture client data and process payment details - and other online systems are potentially highly vulnerable to so-called 'cyber attacks'. However, there are steps you can take to protect your website, your customers, and any data you have online.

What are the security risks?

- Hackers can steal information or even funds by penetrating your website security systems. Sometimes an insecure website provides an unauthorised way in to other business IT systems.
- Malicious users could modify the information on your website without your knowledge or consent.
- Hackers and 'crackers' can attack your website systems such as databases and stop them from working properly by executing commands and modifying them.
- Computer viruses and other malicious software can infect your website and compromise the security of anybody who visits it.
- 'Denial-of-service attacks' can pull your website off the web, making it unavailable to customers.
- Fraudsters can carry out ecommerce transactions using stolen credit cards, which could leave your business liable for the cost.
- Copycat or ambiguous domain names and websites can dupe online customers into disclosing personal or financial information in the belief that they are using your legitimate website - a practice known as ‘phishing’.
- Insecure tools and applications on your website could compromise users' privacy or security.

What are the potential impacts of security breaches?

- Website down-time.
- Significantly increased IT support requirements.
- Potentially huge financial losses.
- Loss of valuable data.
- Damage to systems.
- Loss of customer and supplier confidence.
- Serious damage to your company’s reputation.

What are the benefits of having a secure website?

- Improved functionality - a proven secure online system can offer a number of useful functions, such as secure extranet functionality.
- Greater customer confidence, often resulting in higher sales on an ecommerce website.
- Better risk management, cutting down on losses and potential legal liabilities.
- Reduced need for IT support and 'fire-fighting' measures to counter attacks as and when they happen.

Who is responsible for website security?

The security of your website, and all the systems associated with it, is your responsibility, not that of your ISP (internet service provider). A good ISP will take certain basic measures to ensure a level of security - for example restricting physical access to web servers in their data centre. But it's up to you to ensure that any specific security requirements are in place to protect your website and to avoid doing anything that compromises existing security measures.

Be aware that different types of web hosting solution pose different security issues. A basis 'shared hosting' solution, for example, where many basic websites are hosted on the same server, may provide quite advanced security put in place by the ISP to protect their systems. However, a 'dedicated server hosting' solution generally comes with little security in place as standard and it's up to you to put in place any necessary security measures.

Basic steps to secure a website

- **Assess your website security needs and potential security holes**. Get expert help if you need it. Also assess the level of risk. While a large ecommerce site has significant security risks and requirements, a basic non-transaction website used only to provide information to users may be less of a risk.

- **Remember the value of the data your business holds and store it safely**. If you store customer details you will need to secure your database and monitor access. Data protection legislation requires you to prevent unauthorised or unlawful processing of information you hold, and obliges you to prevent accidental loss or damage to the information.

- **Choose a quality hosting solution from a reputable provider**. Service levels and quality vary enormously, and the cheapest web hosting solution is seldom the best value unless your needs are very basic. Search online to find reviews of different providers.

- **Ensure that high-risk transactional areas of the website are placed on a secure server**. This means all information and transactions - particularly financial transactions - sent via your website will be securely encrypted using technology known as SSL (Secure Socket Layer). Most quality ISPs offer this as an option.

- **Choose reputable partners to process card payment transactions**. Transaction security is vital for customer confidence. Reputable payment clearance providers use encryption technology to process online payments safely.

- **Use a robust and properly configured firewall if necessary**. This can come either as a hardware device or as software. A firewall may come as standard with a quality hosting package or ecommerce solution.

- **Ensure that server operating systems are kept patched and up to date**. If you are using a dedicated server solution this may be your responsibility.

- **Use anti-virus or intrusion detection software where necessary**. Make sure it is updated regularly to ensure it can detect even the newest threats.

- **Configure the server to be as secure as possible**. If you have access to server configuration that ensure settings are as secure as possible while still allowing your website to operate properly.

- **Restrict access to the web server**. Administrative and access passwords should only be given to those who need them.

- **Ensure that all web applications are securely designed and bug-free**. Bugs in 'active content' like transactional web applications can be a major security risk.

- **Consider using digital signatures**. This gives added confidence and security for agreeing contracts online, sending sensitive documents and handling high-value transactions. Most popular email packages come with optional signatures or certificates which sit on your computer’s hard-drive as a small piece of software.

- **Be vigilant, and encourage others to do the same.** Be on the look-out for domain name registrations set up to impersonate your business and cultivate awareness through employee training.

- **Help to protect your customers**. Make your customers aware of any scams or security by placing notices in the login section of their websites and encourage the use of imaginative passwords. Adopt policies which do not require your customers to provide security information in response to email communication.

- **Be alert to customer fraud**. Fraudulent transactions will cost your business money. Always ask for customers' email addresses. For high-value goods, you should also require that products be shipped only to the billing address.

Finally, ensure that all data and systems are backed up regularly and securely. If the worst happens, you will at least be able to restore your systems from your backups.