Secure Website

Nine Steps to Protect Your Website

About The Author

Marwyn Allen is an Information Security enthusiast and business man. Marwyn Allen, originally born and raised in Jamaica came to America in 2011 to pursue his business and education goals. Marwyn has worked in corporate America for over 10 years with brands such as Amazon and Truist in various roles such as Shipping Manager, IT Business Analyst, IT Support Engineer, Cyber Incident Management and Senior SOC Analyst.

Marwyn is also a serial entrepreneur that owns a consulting agency, Information Security firm and an events business. Marwyn along with his team has helped to build over a dozen brands using the skills of business management and expert business automation. Marwyn is a lover of nature, wildlife and true crime junkie. Marwyn spends most of days during the week building his various brands, spending time with his family, working out in the gym and binge-watching documentaries. **You can find a list of Marwyn's credentials and portfolio below:**

About The E-Book

This book was created with the intention of providing every day adults, small to medium size business owners and beginner Information Security students with general knowledge of threats, threat actors, scam techniques and ways to secure themselves and their businesses online.

The information given in this book is ever changing due to the nature of the information security industry. Readers are advised to do their own research and validation when implementing any information security protection and or policies.

Allen's InFoSec agency is not responsible for any damage, harm or loss of finances, resources and or life caused due to any information displayed in this book.

This book should not be copied, resold or used a paid teaching guide by anyone but Allen's InFoSec Agency. This book is for personal use only.

Nine Steps to Keep Your Website Safe

There is nothing worse than having your website compromised by a hacker. It can cause so much customer distrust if you compromise your customer's security and just in general leaves you with a huge mess to clean up. So you want to make sure that you have a safe website. Here are nine ways you can keep your website free from the dangers of hackers.

1. Know what threats are out there. Hackers are always coming up with new ways to get into your website. You need to stay one step ahead of them by knowing the latest in tricks to compromise your site. There are tech sites that can help you know what the latest and greatest hacks are out there so you can protect your site from that danger.

2. Lock it up. Make it harder for them to get in by having stronger passwords and more security like limiting the number of password guesses on your site. Make sure passwords are strong and changed frequently. Frequent automatic logouts and re-logins will help keep you ahead of those hackers. Refrain from sending passwords through email just in case your email has been compromised and you're unaware.

3. Stay up to date. If you always update your computer software and security software when updates are available instead of waiting, then you will keep your website safer. Software companies are always looking to protect their clients. Following step number 1 above, they are aware of the latest hacker tricks and work to find ways to prevent that from happening with their software. So as soon as an update is available, don't drag your feet on accepting it.

3 - 4

4. Use firewalls. Put up a firewall that will help keep people out. This might require a monthly fee, but it's well worth it if it stops any unauthorized people from getting into your website. In the long run it could save you so much time, money, and heartache.

5. Admin pages should be hidden. You never want an admin page to be found through a search engine. There's a way to prevent these from showing up in search engines, preventing access to the entry portal of your website. There are robots you can use to prevent your admin page from showing up in search engines.

6. Stop file uploads. Well, not entirely, but you should limit them. Bugs can get into your system through file uploads, even if they are scanned. Speak with your website host about setting up an outside root directory and using a script to access them instead.

7. Use encryption software. Do you know what's so reaffirming to customers? When they go on your site and see "https". The "s" means secure. Adding this to your website's database will prevent information from being read during transit.

8. Don't allow auto-fill. While it's great for customers and they may love it, it has its risks. If a user loses their phone or computer, then anyone who gains access to the person's phone/computer can then fill out the information, giving them access to the user's private information. They might not know that your site caused that, but you don't want to be the reason someone's information is compromised.

9. Always back up. In case the worst happens it's always best to have information backed up in more than one location. Back up in multiple locations. Back up often. Back up off-site.

Following these nine tips will help keep your website and your clients safe. What other tips do you have for keeping your website safe?

4 - 4

Thank You!

You have reached the end of this e-book, we hope you enjoyed the summary of contents that we've put together for you. We are always looking to improve our content so please feel free to reach out to us with feedback on your experience. We also have several other eBooks in our catalog that may interest you. Please review our website at allensinfosecagency.com for additional details.

https://allensinfosecagency.com/home/services/

support@allensinfosecagency.com

ALLEN'S INFOSEC AGENCY