

Web Security

Joe Varner

Firehawk  *Digital*



Web Security

What we are going to cover:



Why



How

Web Security

What are the risks of not having your website secure?

- Between 30,000 and 50,000 websites are hacked daily.
- Cyber attacks happen every 39 seconds
- Costs the US Economy 3.5 billion a year
- 43% of cyber attacks target small business
- Over 500,000 malware programs are detected daily (1 billion programs to date)
- Website Blacklisting
- Website Defacement
- Accessing Personal data

Web Security

Malware

- Short for “malicious software”.
- Malware is a file or code, typically designed to infect a system which then is used to explore and then steal any information the attacker wants.

Web Security

Types of Malware

- Viruses
- Keyloggers (Logs key strokes)
- Worms
- Trojans
- Ransomware / Crypto-Malware
- Bots / Botnets
- Adware & Spyware
- Rootkits

Web Security

Website Blacklisting

- When a website is attacked by a malware or other suspected malicious code search engines stop indexing the site. This produces a loss in sales, potential clients and other loss of business current and potential business.

Web Security

Website Defacing

- Malware and hackers will change the information on a site with their own messages. These can be political, vulgar language, or any other change that could embarrass web owners.

Web Security

Recent data compromises in 2022:

- September 2022: U-Haul discloses data breach which included the breach of driver's license data.
- July 2022: Hacker posts data on 5.4 million Twitter users for sale.
- January 2022: Over \$30 million looted in Crypto.com breach.

Don't assume that this wont' happen to you!

Web Security

How to protect your websites.

- Keep your website updated.
- Use Web Scanners.
- Use SSL Certificates.
- Use HTTPS instead of HTTP
- Use trusted 3rd party plugins and addons
- Change passwords frequently

Web Security

Things to update with your website:

- If using Wordpress, update plugins, code, etc.
- Change passwords frequently
- Encrypt your Login pages
- Always back up data (web files, databases information, etc).
- Hiring a web security expert to help keep your site secure.

Web Security

Website Scanners

- Programs that run through your websites code, database and files and checks for areas where areas of compromise are found.
- Examples of websites scanners are:
 - Invicti
 - Acunetix
 - Indusface WAS

Web Security

SSL Certificates

- This provides one of the most important components of any online business because it creates a secure connection for purchases and transfer of personal information.

Web Security

Use HTTPS

- Using HTTPS for your website is not just for websites that pass data from the user to the database.
- HTTPS is used to keep from an unwanted listener (hacker, malware, etc) from passively listening to the 'website' conversation.

Web Security

Let Us Help

(937) - 805 - 9270

firehawkdigitalohio@gmail.com

Firehawk  *Digital*