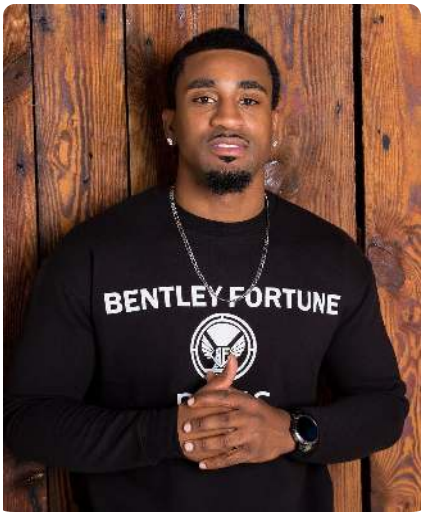
Signs That a Website Is Fraudulent

ALLEN'S INFOSEC AGENCY

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, an events business among others. 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.

Signs That a Website Is Fraudulent

Cybercrime is on the rise, so it is more important than ever to protect yourself from fraudulent websites. There are a number of things to look out for in order to keep you and your family safe from the many online scams being run.

What Is a Fraudulent Website?

A fraudulent website can be defined as one that is fake, set up in order to run some sort of scam or phish for sensitive private information, with a view to defrauding site visitors or even stealing their identities. Fortunately, there are a number of telltale signs to watch out for.

Signs That a Website Is Suspicious

1. The domain name

Fraudulent sites will usually use a domain name similar to a reputable company or brand name. There have been many scam sites based around Amazon.com, for example. They might include a brand name in the URL, such as AdidasBargains.com, but not be affiliated with the company in any way.

2. No contact information posted prominently

Honest websites have nothing to hide, so you will usually see some form of contact information posted at the site prominently, such as name, address, phone and email. Google requires this data to be obvious in order to include a site in their search engine results pages. If you don’t see a physical location as well as virtual contact data, steer clear.

3. Spelling and grammatical errors

Sometimes the URL looks legitimate apart from a spelling error. In other cases, the content at the site will be badly written. A lot of scam sites try to pose as American or Canadian companies in order to make consumers feel a false sense of security. Poor mechanics is a sign of overseas cybercriminals trying to con you.

4. Check the WHOIS registration for the domain

Not all of the data is completely visible; some pay more for secure accounts. In general, however, Network Solutions is the best place to see who owns the domain and where it is being administered from. Go to https://www.networksolutions.com/whois/index.jsp and put in the URL of the site you suspect. Check to see the location where it has been registered and the creation date to see how long it has been registered for. Scam sites are usually made on the fly and disappear just as quickly.

5. Try the phone number listed

WHOIS should list a phone number. Call it to see if it works. If it is an answer machine, the number is not in service, or no one ever answers during business hours, it is more than likely a scam. It might also be a website hosting service where the domain is parked, in which case there will be no way to contact actual staff for the site. Again, steer clear.

6. Look for the "s" in https://

This shows it is a secure site. If there is no "s", then the site is not secure and others can access your sensitive information. Google will not list sites that do not have https:// certification.

7. Run a Google search

See if the site has any reviews or if people are complaining it is a scam. Also, see if it shows up in search engine results.

8. Check the links on Google

If it is a legitimate site, it will usually have links pointing to it from other websites. If the only thing that shows up is the domain name, steer clear.

9. Beware phishing emails

These will often look like they come from PayPal or your bank, but there will be something off about the URL and it won't always look identical to the usual log-in page.

Go to https://www.usa.gov/online-safety to learn more about safety and report any scam site you come across.

Thank You

You have reached the end of this eBook, 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