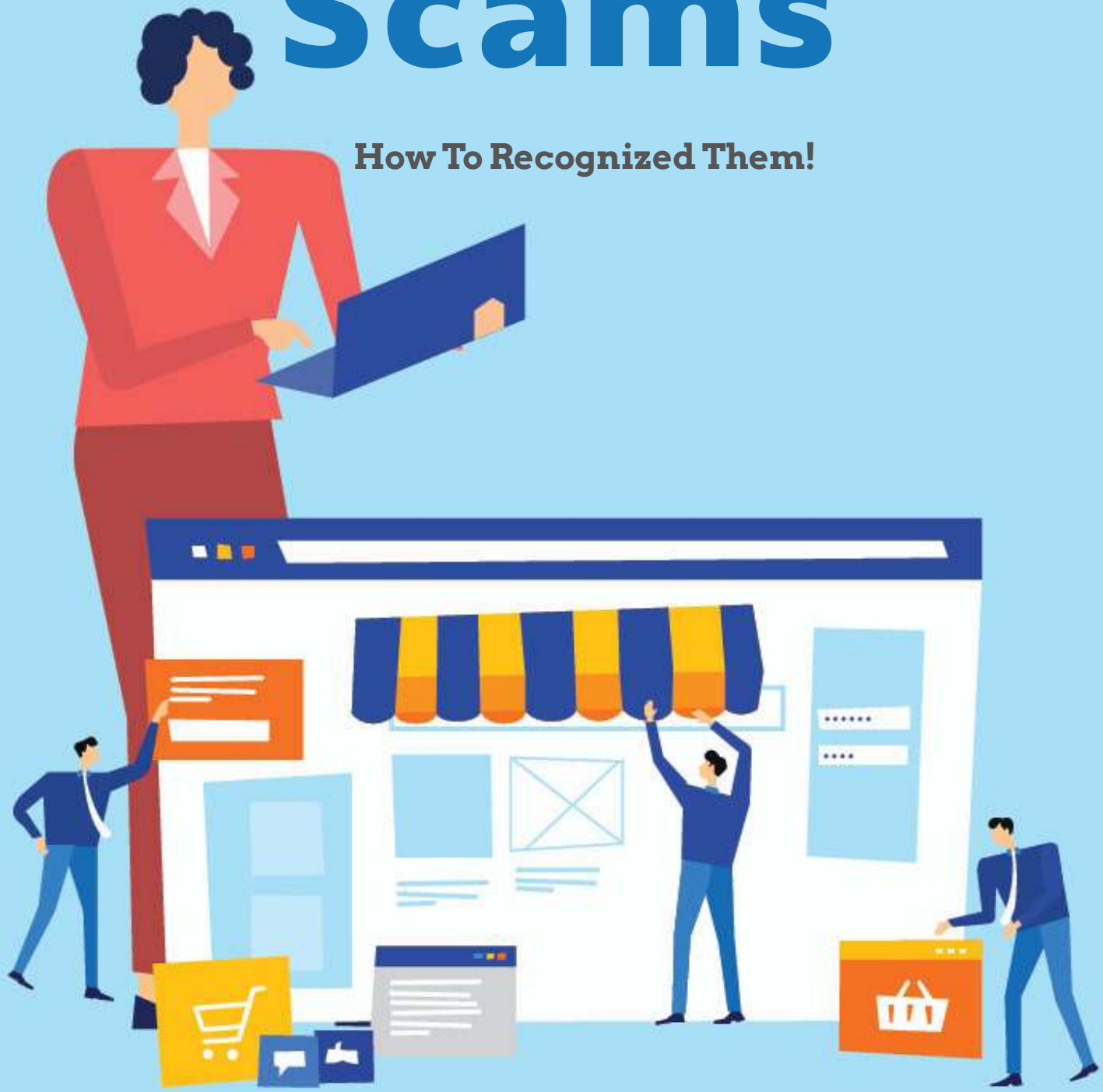
Online Shopping Scams

How To Recognized Them!



ALLEN'S INFOSEC AGENCY

About The Author

Marwyn Allen is an Information Security enthusiast and businessman. 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, financial 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.

Online Shopping Scams

Everyone loves to get bargains and enjoys life being as convenient as possible. Online shopping can offer both. However, it can also be a double-edged sword due to the number of online shopping scams that have sprung up. Here are several to keep an eye on.

1. Copied Sites

Many name brands' sites are being copied in order to trick shoppers into buying from them instead of getting the real deal from the genuine site. At best, you might end up with knockoffs from China. At worst, you might have your identity stolen. Knockoffs cost companies almost one trillion dollars a year, so check out the sites you shop at carefully to make sure they are real.

2. Huge Discounts

Sites that offer huge discounts all the time are suspect because brand-name goods should sell for more and these supposed bargains are more than likely either knockoffs, or lures to spend money but no goods will ever be delivered. Go to Google Shopping to compare prices and then shop around until you find the right item. Avoid the bargain basement — you get what you pay for.

3. A Bad Website

If you see spelling and grammar errors and the whole site looks like it has been thrown together, this is not a site you should be shopping at.

4. Not a Secure Socket Layer (SSL)

Sites with https:// in front of them have an SSL certificate, which is a higher level of security than a regular website. Most scam sites will not bother to get certified.

5. Suspicious Domain Names

In terms of URLs, the brand name and .com extension are preferred and usually a sign of a legitimate site. However, many new extensions have become available, meaning scammers can use the brand names for a time until they are eventually caught. Extensions such as .net, .us, .info and more are all used to create sites that look like the real ones, but aren't.

6. The Site Was Just Created

Search for the URL at https://www.networksolutions.com/whois/index.jsp and check the creation date. If it is recent, chances are the site has been started for the express purpose of scamming unsuspecting shoppers.

7. They Don't Accept Credit or Debit Card Payments

Beware of any site that requires you to pay by wire transfer, pre-paid gift cards, bitcoin or other cryptocurrency. These are not secure methods and in most cases, you will not be able to get your money back.

8. They Ask For Too Much Personal Information

No site should ask you for your social security number or other details that could be used to steal your identity.

9. Their Physical Mailing Address Is Not Legitimate

Thanks to Google and MapQuest.com, you can pretty much find any address in the world, see a map of it, and get a Google satellite image of it. If the address does not exist, or the building looks suspicious, don't shop at that site.

10. No Clear Terms for Doing Business with Them

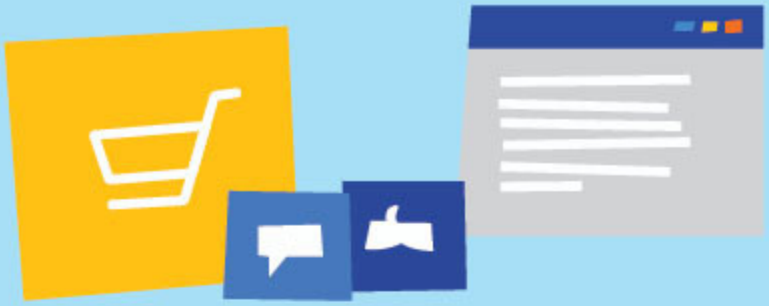
The site should have terms of service and a refund policy. The refund policy should usually be to refund in full within 30 days. Some states, like Florida, give only 20 days. Full details should be provided on how to return the item and get the refund. Beware of charges like credit card transaction fees and restocking fees, which can take a big bite out of your refund.

11. Bad Reviews

Type in the name of the site or the product you are thinking of buying, and then add the word "scam". Take seriously all the feedback you find before doing business with that site.

12. Delivery Problems on Ebay and Amazon Marketplace

Beware of individual sellers who don't send your goods. They have either mixed up their inventory levels, or they are running a scam.



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

By: Marwyn Allen