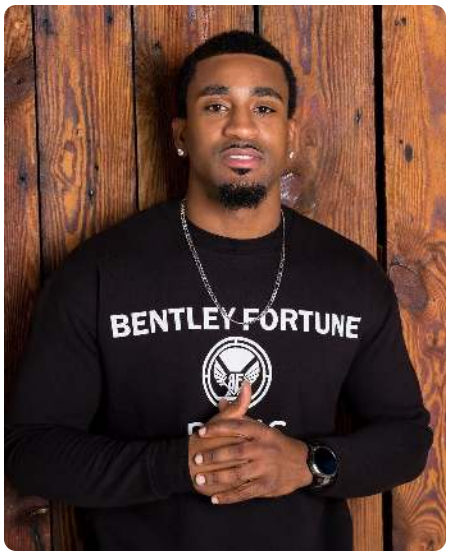
MINIMIZING FRAUD

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.



About The Author

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 eBook

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.

Let's Begin!

There are a number of things you can do to minimize the risk of being defrauded online. A little bit of vigilance and common sense can go a long way toward keeping you safe. Here are some do's and don'ts.

1. Do Protect Your Identity at All Costs

Shop only at reputable sites. Keep passwords secure. Change them regularly.

2. Don't Click on Links in Emails

Be especially vigilant if the email claims to come from your bank or a sender you don't know. Many of these links will take you to a fraudulent site where they will try to get money from you. Or they might be phishing sites trying to steal your identity. They might also be spoof banking sites and PayPal to try to steal your username and password and thus gain access to the account.

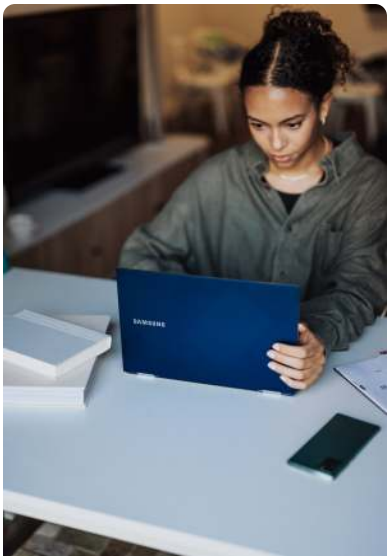
3. Do Use Antivirus Software and Keep It Up to Date

These programs aren't perfect, but they do offer a lot more protection than not having any installed at all.

4. Don't Store Credit Card Information at ECommerce Sites

One-click shopping can be very convenient, but with so many data breaches these days, the last thing you want to do is make it easy for cybercriminals to steal your financial data.

5. Do Be Vigilant about the Identities of Email Senders and Website Owners



It only takes a few minutes to check on whether or not the website or email contact information is legitimate. You can also go to Network Solutions' WHOIS database to see who owns the site, how long it has been in business, and so on.

https://www.networksolutions.com/whois/index.jsp

6. Don't Shop at Overseas Sites

US residents will get consumer protection shopping at a US-based site, but will have little to no recourse if you are scammed by an overseas site. Check the contact information, try testing out their customer support first before shopping and do a company reputation search on Google as well.

7. Do Use a Credit Card to Pay, Not Debit Card or Check

A credit card will give you the greatest amount of protection from fraud. You have up to 30 days to report fraudulent activity, as compared with only 48 hours for debit cards. Issues with checks can take weeks to track down.

8. Don't Fall Prey to Fake Contest Scams

These scammers tell you that you've won a prize and will often ask for shipping and handling to get it. Then they have your financial information, address, and so on to do with as they wish.

9. Do Sign Up for Free Scam Alerts from the FTC

The Federal Trade Commission in the US keeps a watchful eye out for the latest scams, and posts them here: https://www.consumer.ftc.gov/features/scam-alerts You can subscribe to these email alerts as well and check the page regularly to help keep you and your family safe.

10. Don't Get Scammed by Free Trial Offers

These can be used to steal your important information. They can also end up hitting your account with renewals each month if you are not careful. Check your PayPal account regarding auto-payment settings and delete repeat payments as needed.

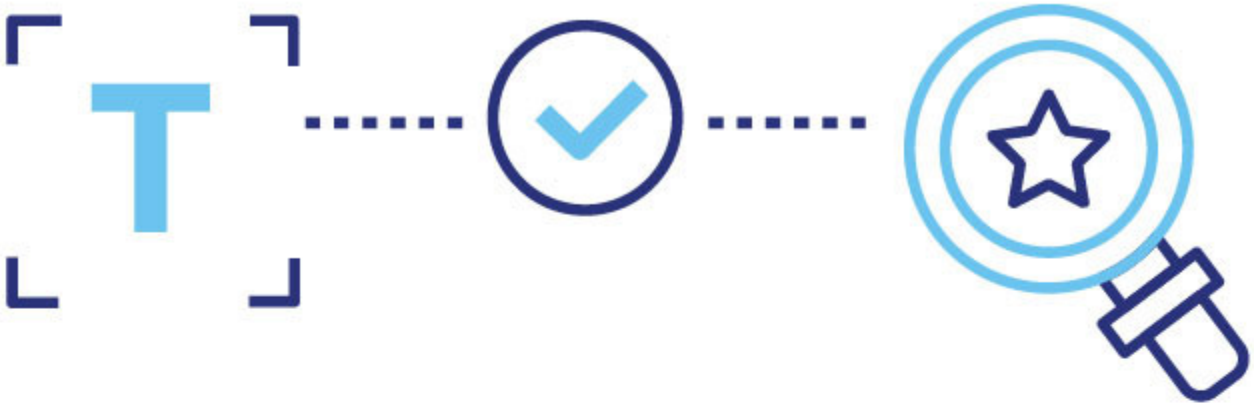
11. Do File a Police Report

Look up your precinct and file a non-urgent incident report. Having a record of going to see the police could help give you more protection if the fraud is extreme.

12. Do Report It to the FTC If You Are the Victim of a Scam

Go to https://www.ftccomplaintassistant.gov/#crnt&panel1-1 and give full details of what happened. They rely on the public to help spot scams and stop them.

You can never be 100% safe online, but these guidelines will help minimize the risk of fraud.



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