Online Scams

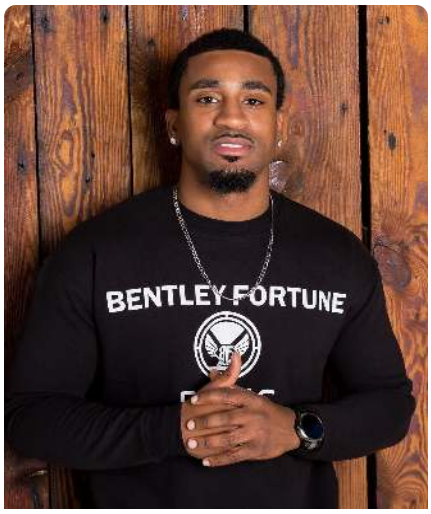
The Most Common Types of Online Scams

By: Marwyn Allen

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 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.

The Most Common Types of Online Scams

The internet can be a blessing for most of us, but there are some cybercriminals who threaten to ruin its usefulness for shopping and information gathering by trying to scam unsuspecting online victims. There are a number of common scams to watch out for. Here are seven of the main ones.

1. Phishing

Phishing is when a cybercriminal contacts you to try to get you to hand over your personal information or money. It might also try to get you to download a virus that infects your computer with malware or opens up a back door so they can steal sensitive data such as your usernames, passwords, account numbers and so on. Phishing happens most often via email, but it can also happen over the phone, via text, and on social media.

In particular, beware of online quizzes on social media. They will often try to get your passwords by asking you common questions so they can then guess your passwords in order to access your accounts and so on. Many people base their passwords on birthdays, children and pet names, and so on, so beware.

Phishing emails usually look legitimate, but pay attention to any landing page you might be sent to. They will usually try to make the site appear the same as the original, such as PayPal, but comparing the two side by side will usually demonstrate which is the scam.

2. Keystroke Software

One form of malware captures all your keystrokes, so it can pretty much log every site you go to, your username, and password. This could be a real disaster in terms of identity theft and money being stolen.

3. International Scammers

Believe it or not, this scam still works on some people. It usually involves an email from a desperate person asking for help in getting a large amount of money from the bank. Those who get hooked in pay small amounts to get paperwork for the transaction and then finally get the money, but all they are doing is putting money in someone else's bank account, and possibly even revealing their sensitive financial information.

The scam relies on greed and getting lots of money for very little effort, so remember - if it sounds too good to be true, it usually is.

4. Greeting Card Scams

There are lots of free greeting card sites online, but they can be very dangerous. The images can carry malware that will attack the recipient's computer and it will often open up a Trojan horse for them to get more information. If you do have to send an eCard, use a reputable site and watch out for spoof sites, such as clones of Hallmark.com.

5. Great Loan, Credit Card and Re-Fi Offers

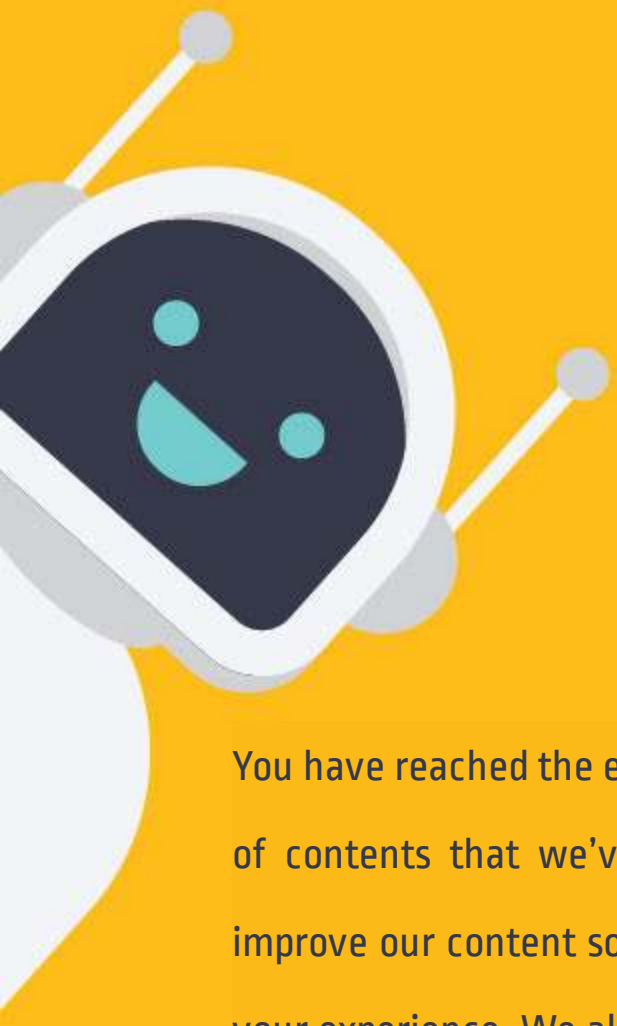
These also play upon greed and/or desperation, especially when people are struggling financially. But no reputable bank is going to send you these offers via email. And if you have a bad credit score, there is also no way you would be offered the best deals, which are reserved for the best customers.

6. Lottery and Contest Scams

These have also been around for some time and still fool people. The email tells you that you are a winner and need to pay a small fee to get your cash or prize.

7. Ransomware

This is a very dangerous scam that is hard to overcome. The ransomware locks your computer until you pay them in bitcoin. The longer you wait to pay, the more money they ask for. So far, even top computer security pros have not been able to restore data or track down the criminals. Note that if you have a backup hard drive connected to your computer, the ransomware can lock that up as well. Back up all your data in a reliable cloud storage system and avoid clicking on anything that does not look legitimate.



Thank You For Reading!

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