Email Scams

Signs That an Email 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 also is 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.

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.

Signs That an Email Is Fraudulent

In the modern world, we can't live without email. But sadly, it has become a tool for cybercriminals that we need to be ever on our guard against.

There are a number of ways to spot a fraudulent email. Train yourself to not take emails for granted by looking at the points listed below.

1. The "From" Address

This should be from a site you recognize, and not a free site like Yahoo or Gmail. Hit reply to email the sender back and see what happens. If it bounces, it is in violation of CAN-SPAM email regulations that require each emailer to have a viable return email address.

2. Is the Greeting Strange?

Does it read as though it was written by a native speaker of English? Is it personalized, or just a hi? Most legitimate online marketers will use personalization.

3. Are There Obvious Misspellings?

Check the From field, subject line, greeting, and opening paragraph. If there are errors, chances are the email is from overseas and could be a scam.

4. Is There Contact Information at the Bottom of the Email?

A full, legitimate mailing address is also required under the CAN-SPAM laws.

5. Are Dates in the Email Recent?

Some scams will get run over and over again and may have an old back date.

6. Is the Brand or Company Name Spelled Correctly?

Misspellings of either of these are a strong sign that the email is a scam.

7. Does the Link URL Included in the Email Look Right?

Scam emails will want to send you over to a URL to get phished or infected with malware and so on. If it is not a URL you are familiar with or it is misspelled, don't click.

8. Does the Link Take You to a Legitimate-Looking Page?

Spoof emails regarding banking and PayPal are all too common, as cyberthieves try to steal your security information and access your hard-earned cash. If the site looks odd in any way, click out. Also make sure the URL has https:// in front, which shows a higher level of security that most phishing sites won't have.

9. Beware of Images

A lot of malicious code is snuck onto computers through images in emails. Set your email client such as Outlook to suppress the images in an email. Only view images from a trusted source.

10. Never Open an Attachment

This is another way cybercriminals try to sneak malicious items onto your computer.

11. Keep Your Antivirus Software Up to Date

Get a reliable program like Norton 360 or McAfee. If you have Kaspersky on your computer, delete it and get Norton or McAfee. Kaspersky is known for having multiple security issues. Once you have Norton or McAfee installed, take the time to upload all the updates and schedule the program to update itself automatically so you are always covered against the latest threats.

12. Asking for Too Much Information

No bank or financial institution like PayPal will ever ask for personal details such as your password, social security number, and so on.

13. Bad Presentation

If the email looks ragged and unprofessional, it is probably spam or a phishing email.

14. Phony "Official" Language

Some emails will try to make it seem as if they are important and come from some sort of official body in order to try to intimidate you into taking the action they are insisting upon in the email. Most legitimate government entities will not be sending you email.

15. Time-Sensitive Emails

Emails that try to push you into taking action quickly for fear of some consequences when the time runs out will also usually be scams to try to bully you into doing something foolish.

If you suspect you have a scam email, report it here:
https://www.consumer.ftc.gov/articles/0003-phishing

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