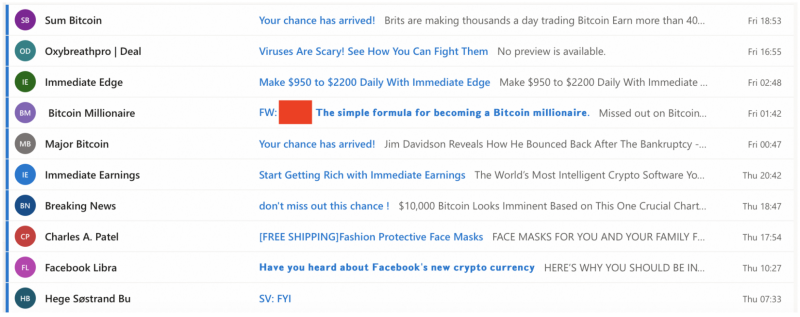
# Spam




Spam emails (also known as "junk mail") are messages that are unsolicited, unwanted, or unexpected but are not necessarily malicious in nature. Examples of spam emails are:

- Newsletters that the user has unknowingly signed up for
- Marketing emails trying to promote products and services
- Update announcements from companies and services the user has registered with

Spam emails should not be confused with malicious spam emails (malspam for short). Malicious spam emails are malicious messages that are sent on a mass scale (as opposed to being targeted at an individual or organization).




Above is a screenshot from a honeypot mailbox we use to collect spam and malicious emails. You can see the scale of the unsolicited spam emails we have received, with the majority being bitcoin-based, trying to get recipients to sign up to different cryptocurrency exchanges or buy into schemes to make them millions! Without further investigation, these emails would be classified as spam, but some could potentially be malspam.

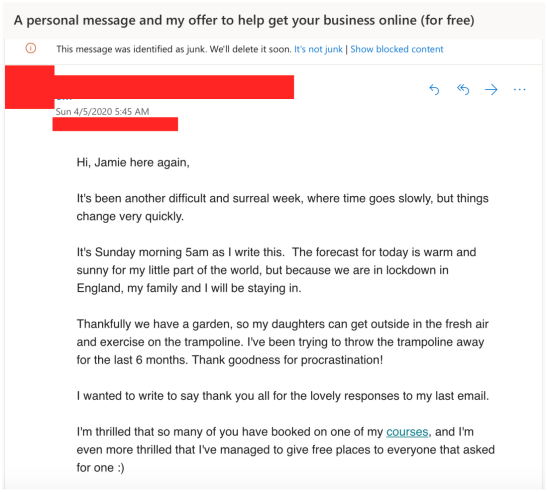
Our junk inbox included emails covering the following topics:

- Bitcoin/cryptocurrency
- Personal Protective Equipment (PPE – expected to see emails of this nature due to COVID-19 pandemic at time of writing)
- Sexual performance-enhancing products
- Non-cryptocurrency financial schemes
- Adult dating
- Marketing emails from restaurants
- Diet/weight-altering products

It's worth mentioning that we haven't signed up to receive these emails. It appears that this email address has been shared or sold between organizations, and we have been added to email marketing lists without our expressed permission.

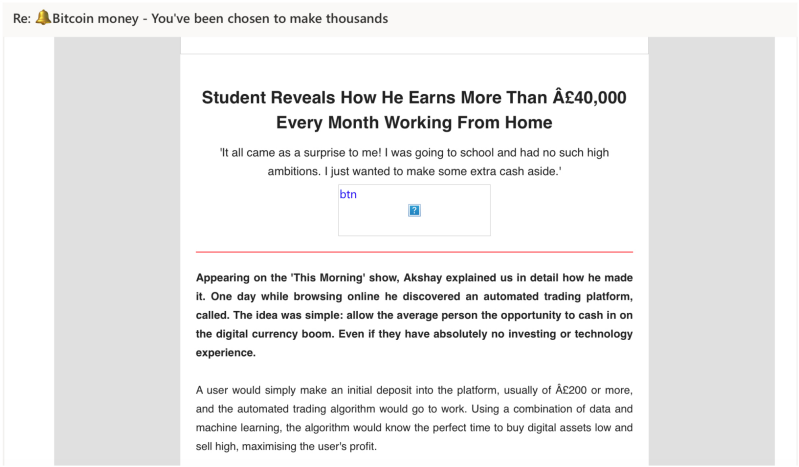
## EXAMPLE ONE

In this example, a WordPress plugin vendor is sending a marketing email to anyone that has registered on their site. Whilst the user likely gave consent to receive emails like this by agreeing to a Terms of Service and Privacy Policy whilst registering their account, most of these emails are unwanted. Emails like this should always feature an "unsubscribe" hyperlink at the bottom of the email, allowing the recipient to delete their address from the mailing list. This email is not malicious, but adds clutter to a mailbox.




## EXAMPLE TWO

In this spam email the sender is promoting a cryptocurrency platform, and enticing the user to sign up and deposit money.




## CONCLUSION

While spam emails are often not malicious, users should always be very cautious when opening these emails, and should not interact with attachments or hyperlinks. Depending on how the organization handles phishing emails, these should either be deleted by the receiving user or forwarded to the security team. Unsolicited spam emails should not be confused with malicious spam campaigns, phishing attacks that distribute malware via email on a huge scale (such as the Emotet trojan). Spam emails can also be utilized as a form of reconnaissance, and if users click on an unsubscribe link taking them to a website, this can lead to system fingerprinting and confirms that

the mailbox is in use.

Previous Topic
Back to Lesson
Next Topic