

**Blue Team Level 1 Certification
(Standard)****Introduction to BTL1** Welcome to Blue Team Level 1!

4 Topics

 Lab and Forum Access**SECURITY FUNDAMENTALS DOMAIN** Introduction to Security Fundamentals

1 Topic

 Soft Skills

7 Topics

 Security Controls

5 Topics | 1 Quiz

 Networking 101

6 Topics | 1 Quiz

 Management Principles

4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN PA1) Introduction to Emails and Phishing

7 Topics | 1 Quiz

 PA2) Types of Phishing Emails

10 Topics | 2 Quizzes

 Section Introduction: Phishing Emails Reconnaissance Spam False Positives Credential Harvester Social Engineering Vishing, Smishing Whaling Malicious Files [Video] Types of Phishing Attacks & Examples Lab) Categorizing Phishing Emails Activity) End of Section Review: Phishing Emails PA3) Tactics and Techniques Used

12 Topics | 2 Quizzes

 PA4) Investigating a Phishing Email

8 Topics | 2 Quizzes

 PA5) Analysing URLs, Attachments, and Artifacts

8 Topics | 1 Quiz

 PA6) Taking Defensive Actions

12 Topics | 1 Quiz

 PA7) Report Writing

7 Topics | 1 Quiz

 PA8) Phishing Response Challenge

3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

Spam

Blue Team Level 1 Certification (Standard) > PA2) Types of Phishing Emails > Spam

COMPLETE



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).

Sum Bitcoin	Your chance has arrived! Brits are making thousands a day trading Bitcoin. Earn more than 40...	Fri 18:53
Oxybreathpro Deal	Viruses Are Scary! See How You Can Fight Them No preview is available.	Fri 16:55
Immediate Edge	Make \$950 to \$2200 Daily With Immediate Edge Make \$950 to \$2200 Daily With Immediate ...	Fri 02:48
Bitcoin Millionaire	FW: [REDACTED] The simple formula for becoming a Bitcoin millionaire. Missed out on Bitcoin...	Fri 01:42
Major Bitcoin	Your chance has arrived! Jim Davidson Reveals How He Bounced Back After The Bankruptcy -...	Fri 00:47
Immediate Earnings	Start Getting Rich with Immediate Earnings The World's Most Intelligent Crypto Software Yo...	Thu 20:42
Breaking News	don't miss out this chance ! \$10,000 Bitcoin Looks Imminent Based on This One Crucial Chart...	Thu 18:47
Charles A. Patel	[FREE SHIPPING]Fashion Protective Face Masks FACE MASKS FOR YOU AND YOUR FAMILY F...	Thu 17:54
Facebook Libra	Have you heard about Facebook's new crypto currency HERE'S WHY YOU SHOULD BE IN...	Thu 10:27
Hege Sastrand Bu	SV: FYI	Thu 07:33

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

TI1) Introduction to Threat Intelligence

7 Topics

TI2) Threat Actors & APTs

6 Topics | 2 Quizzes

TI3) Operational Threat Intelligence

7 Topics | 1 Quiz

TI4) Tactical Threat Intelligence

7 Topics | 2 Quizzes

TI5) Strategic Threat Intelligence

5 Topics | 1 Quiz

TI6) Malware and Global Campaigns

6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

DF1) Introduction to Digital Forensics

5 Topics

DF2) Forensics Fundamentals

10 Topics | 5 Quizzes

DF3) Digital Evidence Collection

8 Topics | 1 Quiz

DF4) Windows Investigations

3 Topics | 3 Quizzes

DF5) Linux Investigations

4 Topics | 2 Quizzes

DF6) Volatility

3 Topics | 1 Quiz

DF7) Autopsy

4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM

7 Topics | 1 Quiz

SI2) Logging

6 Topics | 2 Quizzes

SI3) Aggregation

2 Topics | 1 Quiz

SI4) Correlation

6 Topics | 1 Quiz

SI5) Using Splunk

5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response

8 Topics | 1 Quiz

IR2) Preparation Phase

10 Topics | 3 Quizzes

IR3) Detection and Analysis Phase

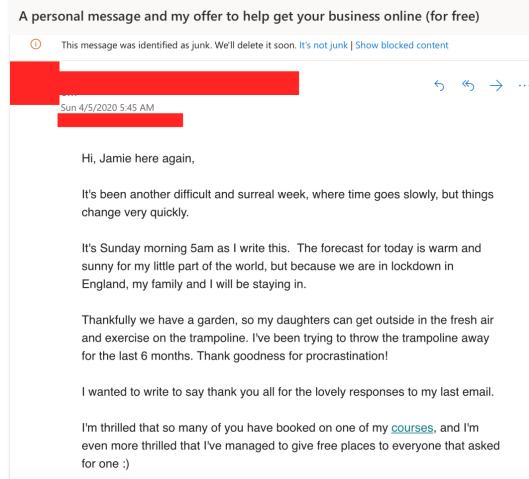
7 Topics | 5 Quizzes

IR4) Containment, Eradication, and Recovery Phase

5 Topics | 1 Quiz

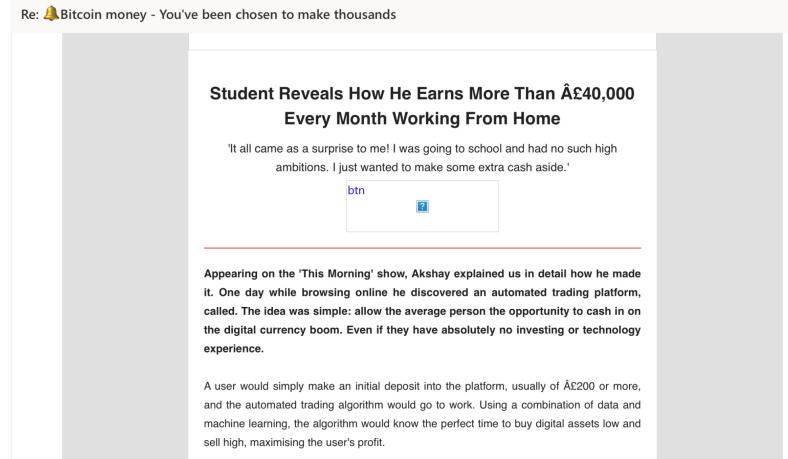
IR5) Lessons Learned and Reporting

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

7 Topics

IR6) MITRE ATT&CK

13 Topics | 2 Quizzes

BTL1 EXAM

Exam Preparation

Using RDP and SSH

How to Start Your Exam

the mailbox is in use.

[Previous Topic <](#)

[Back to Lesson](#)

[Next Topic >](#)

[Privacy & Cookies Policy](#)



Privacy - Terms