How can I tell if I have a Spam/ Scam Email?

A Spam/ Scam Email are unwanted messages sent to you in order to advertise, scam you, steal your information and even try to steal your malware. Here are some clues in order to know if an Email is a spam/ scam email as well as what you should do if you encounter one of these messages.

Clue 1: Suspicious Email Address

If you receive an Email that you might find suspicious, be sure to check the Email address. This is because while it might seem professional, the Email address might have a misspelled name and might not even use a professional company email (E.G It might use a public domain email address such as @gmail.com).

Clue 2: Misspelled and suspicious choice of words

When viewing what you might think may be a spam/ scam email, one of the most obvious clues would be any choice of words that feel unnatural and/ suspicious (for example words such as "Greetings valued costumer" or something more

generic). In addition, if there are obvious grammatical error and spelling mistakes, it is an obvious indicator that this Email is a Scam and should not be trusted.

Clue 3: Suspicious Links

A large majority of Spam/ Scam Email will urge you to click on any links within the Email. Do not click any of these if you are unsure that the Email is authentic or not as clicking on it might cause your personal Information to be stolen or even install unwanted Malware.

If you find any of these Clues and Hints within an Email, make sure you mark the email as Spam, block the sender and even report them. Be sure to trust your instinct and not blindly trust any Emails you do not 100% recognize. Stay Safe.

Made with the help and support of Inclusive Bytes CIC