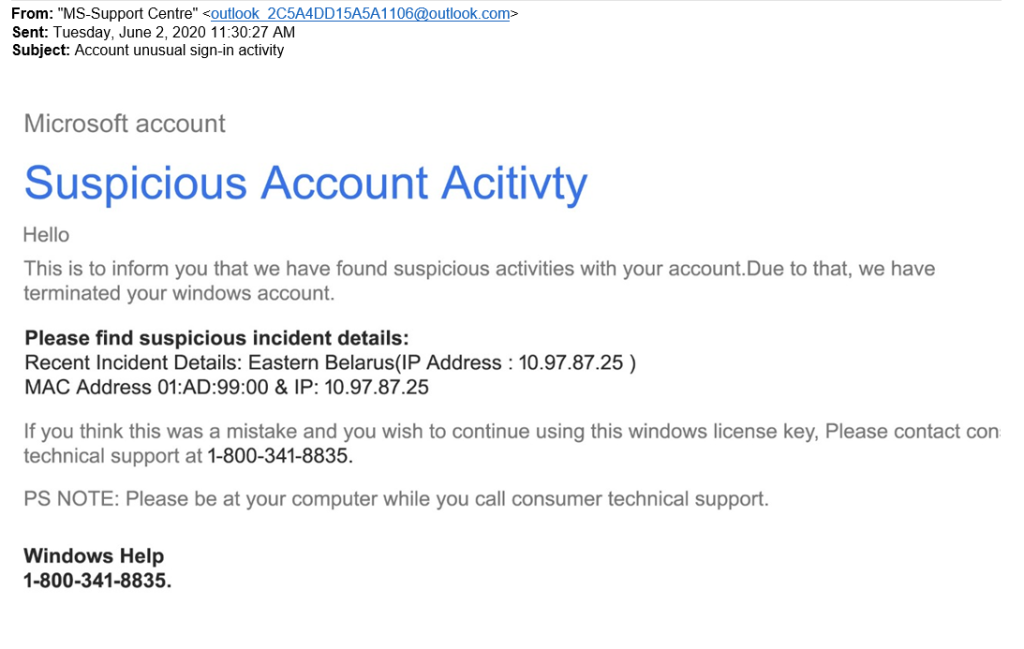
Task 2: Analyzing a sample phishing email



* The above image is a sample phishing email taken from the internet.
* In the above image, we can analyze the email beginning with email header.
* Email header contains From, To address and the subject
* In the above image From address of the mail looks suspicious, proves the email is not from the legitimate domain of Microsoft team.
* And there is no To address in the email header which looks suspicious
* Coming to the email body, it contains a message of urgency stating “we have found suspicious activities with your account, we have terminated your windows account”
* Mac address format in the email is not valid, valid format example: 00:1A:2B:3C:4D:5E
* Mac address only contains 4 pairs of hexa-decimal digit which is not valid and looks suspicious
* And there are several grammatical errors in the email body.
* There is no proper email structure which the reputable companies wouldn’t compromise on.
* And the IP address mentioned in the mail is a bogon address which means reserved for special use such as local or private networks.  These reserved ranges, along with other IP ranges that haven’t yet been allocated and therefore also shouldn’t appear on the public internet are sometimes known as bogons.
* So we can consider this as a spam email or a phishing email.
* Tool used to analyze this IP address: IpInfo.io
* The above are some of the phishing indicators found in the sample email.