How to identify a SPAM / potential Malware email.

When you receive an unsolicited email, with or without a file attachment, there are a number of clues that can show you whether the email has come from the person you might at first think it came from, including the person (or organisation) shown in the 'From or Sender' field in your email processing program.

Example:

Subject	**From**
important message	D GRIFFIN

The above email was received and flagged as 'Junk' by my email program and contained a web page link that if visited could contain malware (virus, trojan, ransomware) or plain spam wanting to advertise a wide range of unwanted products or services (pharmaceuticals, sex aids or pills etc).

Looking at the source of this email message using the option provided in Mozilla Thunderbird (my email program) – View >> Message Source – Ctrl+U.
This showed the following indicators that this was not a genuine message!

```
Return-Path: <peteh******213@virginmedia.com>
Received: from redirecciones.axarnet.es ([91.142.212.252]) by
 mx.kundenserver.de (mxeue003) with ESMTPS (Nemesis) id
 0LvBgM-1ZzIKF30b4-010LsD for <steve@*************.net>; Mon, 01 Feb 2016
 17:15:50 +0100
Received: (qmail 27081 invoked from network); 1 Feb 2016 17:15:44 +0100
Received: from r167-62-186-23.dialup.adsl.anteldata.net.uy (HELO nshz.com)
(167.62.186.23)
  by redirecciones.axarnet.es with (DHE-RSA-AES256-SHA encrypted) SMTP; 1 Feb
2016 17:15:43 +0100
From: D GRIFFIN <peteh******213@virginmedia.com>
```

From the above message source details, the first thing that stands out is that this message was Received: from **redirecciones.axarnet.es** ([91.142.212.252]) – a server located in **Spain**, but this was not the place where the message originated from!

Looking at the further message details, there is another Received line shown:
Received: from **r167-62-186-23.dialup.adsl.anteldata.net.uy** (HELO nshz.com) (167.62.186.23) by redirecciones.axarnet.es – which shows that the message originated from a server in **Uruguay** before being sent via the server in Spain.

Finally, one last clue in the source details:
The sender who is supposed to be D GRIFFIN is shown to be coming from a completely different sending email address, which strongly suggests that the sender information has been spoofed or falsified.

To determine the countries which the email came from, you can use the GeekTools Who Is service at: http://www.geektools.com/whois.php where you enter to numeric (IP) address shown in the source detailed information. i.e. 167.62.186.23 and 91.142.212.252.

This shows for 91.142.212.252:
org-name: Axarnet Comunicaciones SL
address: Avda. Andalucia 81, 2C
address: Torre del Mar (Malaga)
address: SPAIN

And shows for 167.62.186.23:
person: ANTELDATA ANTEL URUGUAY
address: Mercedes, 876, P. 2
address: 11100 - Montevideo -
country: UY

If the message does have a file attachment, then DO NOT open this unless you are 100% certain that you know that the file is genuine and from a person you trust, and was expected!

If you have any doubt at all, then follow the steps below:

1. Save the file attachment to your desktop (or other place on your computer that you choose).

2. Go to the VirusTotal website - https://www.virustotal.com/

3. Click on the option to **Choose File** shown on the VirusTotal page, then select the file you saved in step 1 above.

4. Finally, click on the option to **Scan it!** To start the process of validating the suspect file by scanning it with a comprehensive range of over 50 Antivirus software tools.

VirusTotal will scan the file and produce a report showing how safe the file is considered to be – if it is safe to open, then you should see a report similar to that below:

SHA256: 8416c06c509e8a130324fb5d88d43e7651cbcd634a9c4a678562b26b66feac71
File name: 29.jpg
Detection ratio: **0 / 53**
Analysis date: 2016-02-01 19:24:16 UTC (1 minute ago)

The key line is the Detection ratio of 0 / 53 (zero out of 53 Antivirus programs found evidence of a virus or other malware content in the file).