

Don't Fall for Phishing

What is Phishing?

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers

You probably have heard of Raymond Abbas aka Hushpuppi who was arrested along with 11 others by the Dubai police. The scale of fraud he was involved with targeted more than 1,926,400 victims.

Do not become one of the statistics, it may cost you untold hardship from which you may not recover from



What to do, if you suspect Phishing



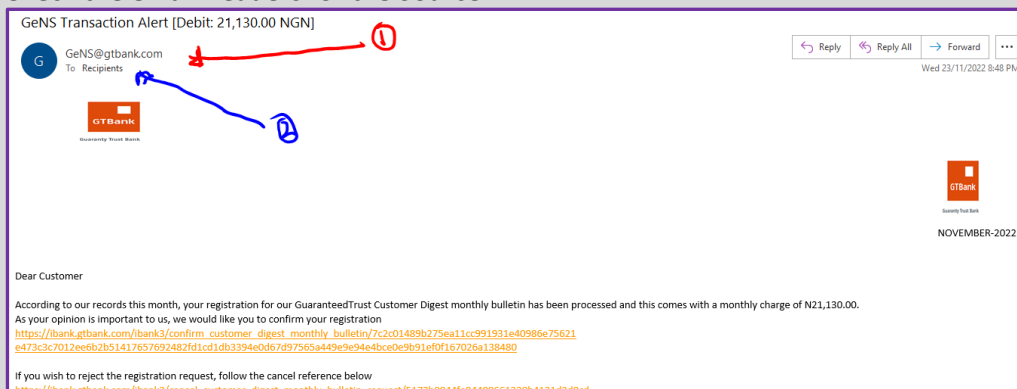
You are not alone; millions of people get unsolicited emails in their inboxes from cyber criminals daily.

Maintaining a healthy level of suspicion is the best advice with regards to all emails, especially those relating to financial and asset transactions.

The following are some steps that you can take to validate the authenticity or otherwise of an email

Step 1:

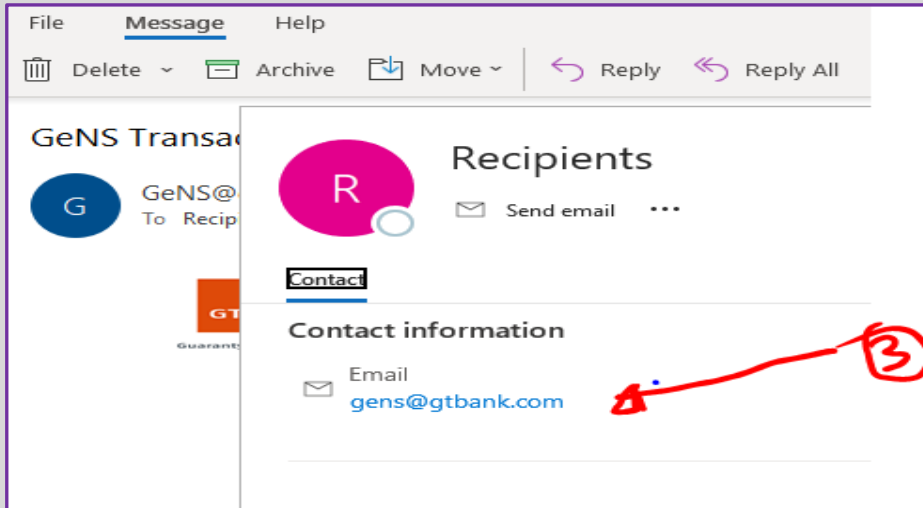
Check the email headers for the Source.



From the above, we note the following:

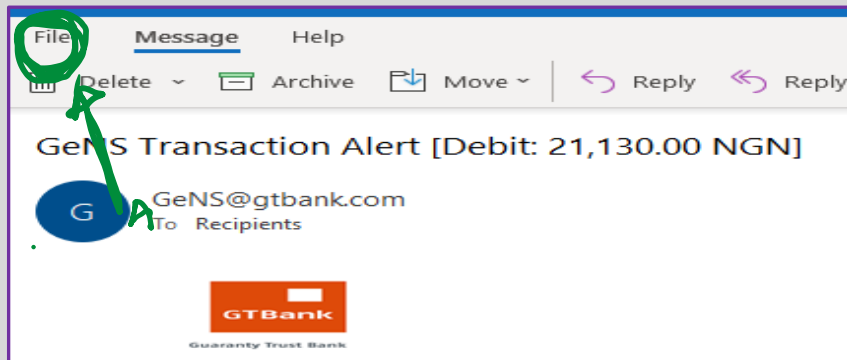
1. The source email address looks very genuine – see (1). It uses the GeNS@gtbank.com address usually used by GT Bank
2. However, the address in the To: line is suspect. It should normally be your own email address that you had registered with the bank. In this case, it is addressed to Recipients, see (2) above.

Further examining the recipient address in (2) above by clicking on it, shows that the email is NOT addressed to you but to gens@gtbank.com, which is odd and very suspicious.

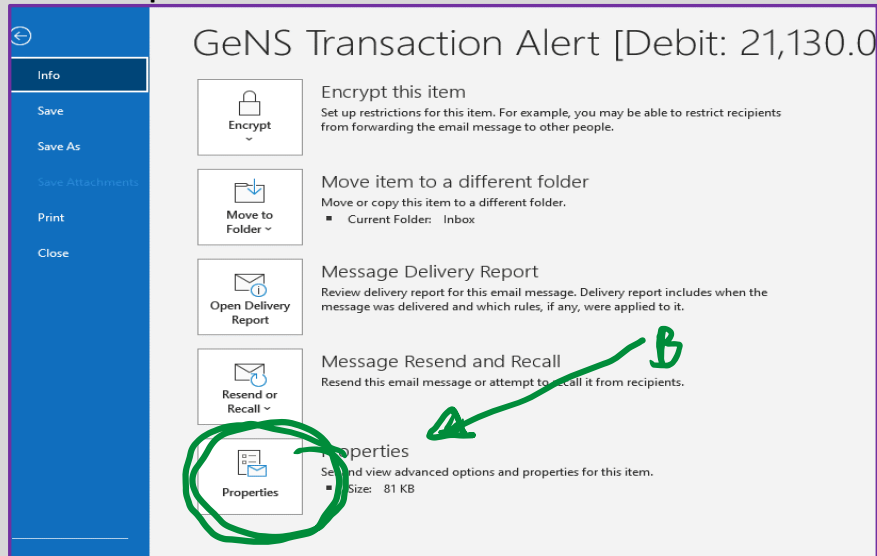


Step 2: Check the email properties

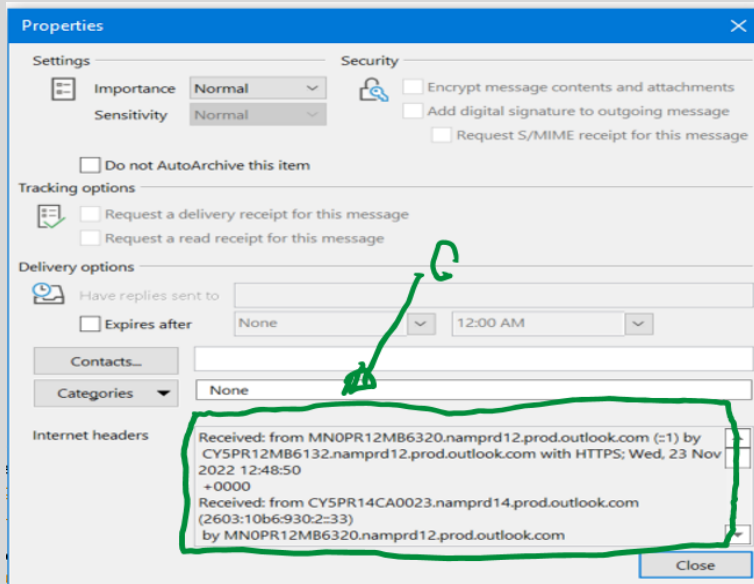
A. Click on File



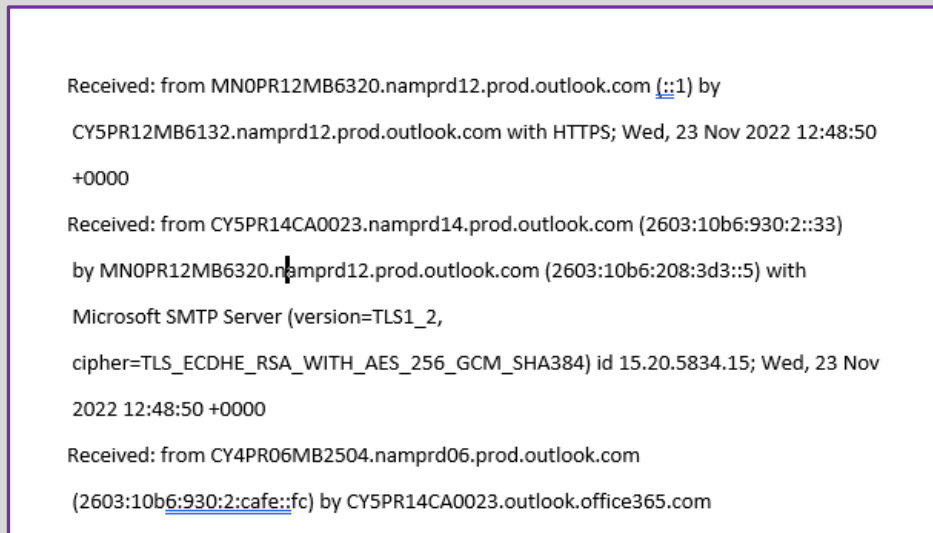
B. Click on Properties



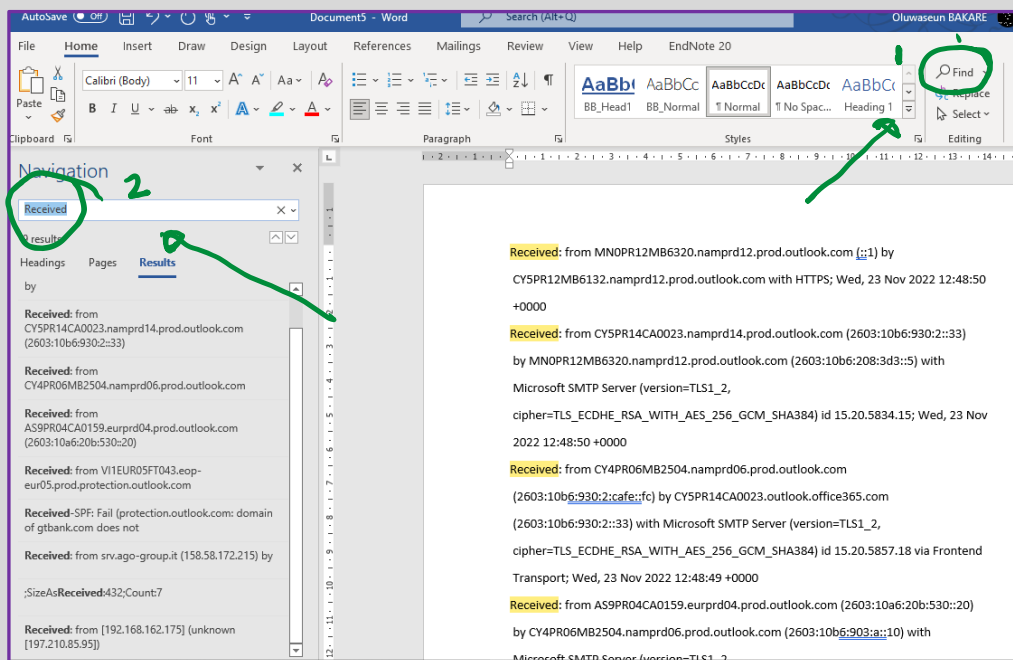
C. Copy all the items in the “Internet Headers” box and paste in a word document



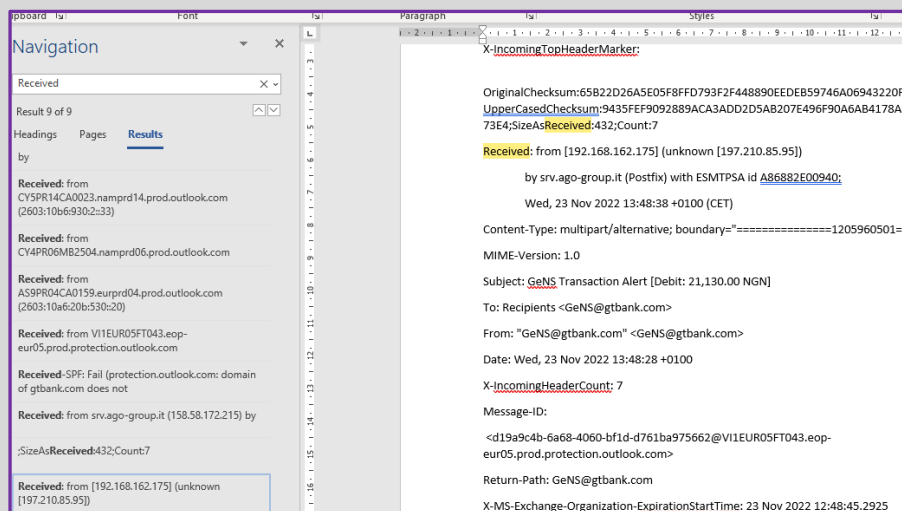
D. You will have something similar to the following:



E. Do a search for all the words ‘Received’ in the new word file that you have by clicking on Find and typing “Received” in the dialog box that comes up

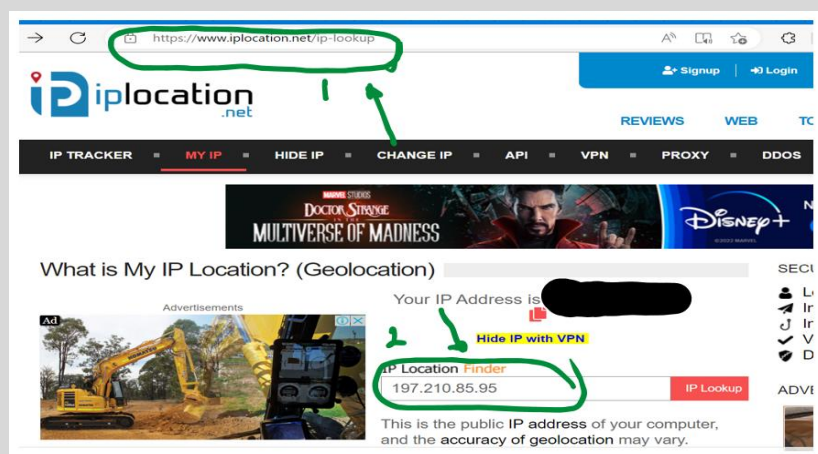


- F. Click on the last “received” shown in the Navigation box and see the result in the word document. In this case, it gives the information about the originator of the email as *Received: from [192.168.162.175] (unknown [197.210.85.95])*

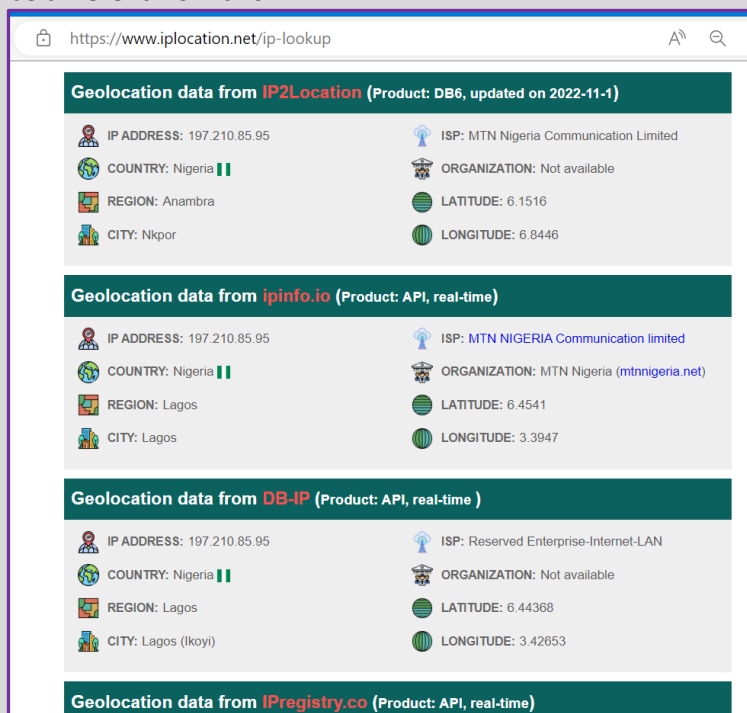


Step 3: Determine who the culprit is

- A. Open your Internet Browser and type <https://www.iplocation.net/ip-lookup> in the address field. Then type the 197.210.85.95 we got from Step 2F above and click on the IP Lookup button



- B. You will get a result similar to the one below. Note that your result will definitely be different from this.



This tells us the following about the culprit:

- A. Is based in Nigeria
- B. Is using Internet Facility provided by MTN
- C. Might be in any of the following cities – Nkpor, Lagos, Ikoy, Port Harcourt or Abuja.



How to Report Phishing

MorinGa Cyber and Allied Research (MorinGa CARE) is currently developing a state-of-the-art database for use by the general public to report phishing and other cybercrimes.

This repository will help Cyber Researchers in identifying current and emerging threats in the landscape, the prevalent types and cyber actors. In addition, MorinGa Care will use this to provide early warnings to all and recommend actions to be taken to keep everyone safe.



At MorinGa CARE, we are driven by a passion to keep people, critical infrastructure, and the environment safe from Cyber criminals.

Why not join us today?

Each Phishing case is different. As such, the approach to report this will be obviously different.

In the case of the Example that we are using, the following can be done:

A. Call the Internet Service Provider (ISP):

Here, the ISP is MTN Nigeria Communications PLC. The company has not provided known dedicated contact details for reporting of cyber crimes. However, one can call their

- dedicated ethics line +234 800 862 862 862;
- Customer care line +234 803 100 0180
- Email: customercare.ng@mtn.com

B. Call your Bank:

Your Account Officer is your best contact. Here, the bank is GT Bank PLC. The company has a dedicated web page to security related issues available at – <https://www.gtbank.com/security-centre/security-information>

Call the 24 hour GT Contact Centre on any of the following:

- +234 700 4826 6632 Or +234 1 448 0000
- +234 802 900 2900 or +234 803 900 3900

Cyber Education & Training
Issue 221101
Lagos. 25th Nov 2022



