Report : Phishing or not ?

Email 1 :

* What is the email's timestamp?
  + 04:57 pm, Mar 20th 2023
* Who is the email from?
  + PayPal
* What is his email address?
  + service@paypal.be
* What email address will receive a reply to this email?
  + service@paypal.be
* What brand was this email tailored to impersonate?
  + Spotify
* What is the originating IP? Defang the IP address.
  + 66.211.170[.]87
* What do you think will be a domain of interest? Defang the domain.
  + www.paypal[.]com
* What is the shortened URL? Defang the URL.
  + hXXps://www.paypal.com/cgp/app-redirect?intent=xo\_email\_txn\_details
* Do you think this is a phishing email?
  + It’s not one to me as the IP address belongs to PayPal and none of the included URL’s seem phishy as they all are from legit websites.

Email 2 :

* What is the email's timestamp?
  + 09:56 am, Dec 12th 2022
* Who is the email from?
  + noreply
* What is his email address?
  + stainless@midnightmagicevents.com
* What email address will receive a reply to this email?
  + stainless@midnightmagicevents.com
* What brand was this email tailored to impersonate?
  + Trust Wallet
* What is the originating IP? Defang the IP address.
  + 85.209.134[.]107
* What do you think will be a domain of interest? Defang the domain.
  + hXXps://trustwallet.com/
* What is the shortened URL? Defang the URL.
  + hXXps://climovil.com/
* Do you think this is a phishing email?
  + Yes: the IP redirects to multiple companies based in the Netherlands or Egypt. Also, the mail is weird if coming from a company as it looks more like a private person’s mail.

Email 3 :

* What is the email's timestamp?
  + 03:31 pm, Mar 26th 2023
* Who is the email from?
  + Tinder
* What is his email address?
  + gq@80-78-255-128.cloudvps.regruhosting.ru
* What email address will receive a reply to this email?
  + gq@80-78-255-128.cloudvps.regruhosting.ru
* What brand was this email tailored to impersonate?
  + Tinder
* What is the originating IP? Defang the IP address.
  + 80.78.255[.]128
* What do you think will be a domain of interest? Defang the domain.
  + hXXps://tinder.com
* What is the shortened URL? Defang the URL.
  + hXXp://blog.tulingxueyuan.cn/contradictedqm.php?utm\_campaign=tpdjuresn
* Do you think this is a phishing email?
  + Yes : it redirects to a weird Chinese website with a 404 error while being hosted in Russia.

Email 4 :

* What is the email's timestamp?
  + 12:44 pm, Mar 3rd 2023
* Who is the email from?
  + Dr. Dan Miller
* What is his email address?
  + babakingsouthmichael@gmail.com
* What email address will receive a reply to this email?
  + imorourafiatou0@gmail.com
* What brand was this email tailored to impersonate?
  + The United Nations
* What is the originating IP? Defang the IP address.
  + 209.85.220[.]41
* What do you think will be a domain of interest? Defang the domain.
  + /
* What is the shortened URL? Defang the URL.
  + /
* Do you think this is a phishing email?
  + Yes : it’s aimed at getting personal information about the recipient in the hope, I’m guessing, that these info can be used to penetrate other accounts of this person.

Email 5 :

* What is the email's timestamp?
  + 11:42 am, Aug 27th 2022
* Who is the email from?
  + Ariana
* What is his email address?
  + newsmail@app9l.serenitepure.fr
* What email address will receive a reply to this email?
  + news@aichakandisha.com
* What brand was this email tailored to impersonate?
  + Whatsapp
* What is the originating IP? Defang the IP address.
  + 51.83.34[.]109
* What do you think will be a domain of interest? Defang the domain.
  + hXXps://www.whatsapp.com
* What is the shortened URL? Defang the URL.
  + hXXp://secure-netcloud.com/?a=71&amp;c=76&amp;s1=dadaa&amp
* Do you think this is a phishing email?
  + Yes : weird message that talks about meeting people on Whatsapp while the mail isn’t an official one. Also, the IP redirect to a cloud server in France and the URL links to a 403 Forbidden webpage (while having “phishing” in its url)