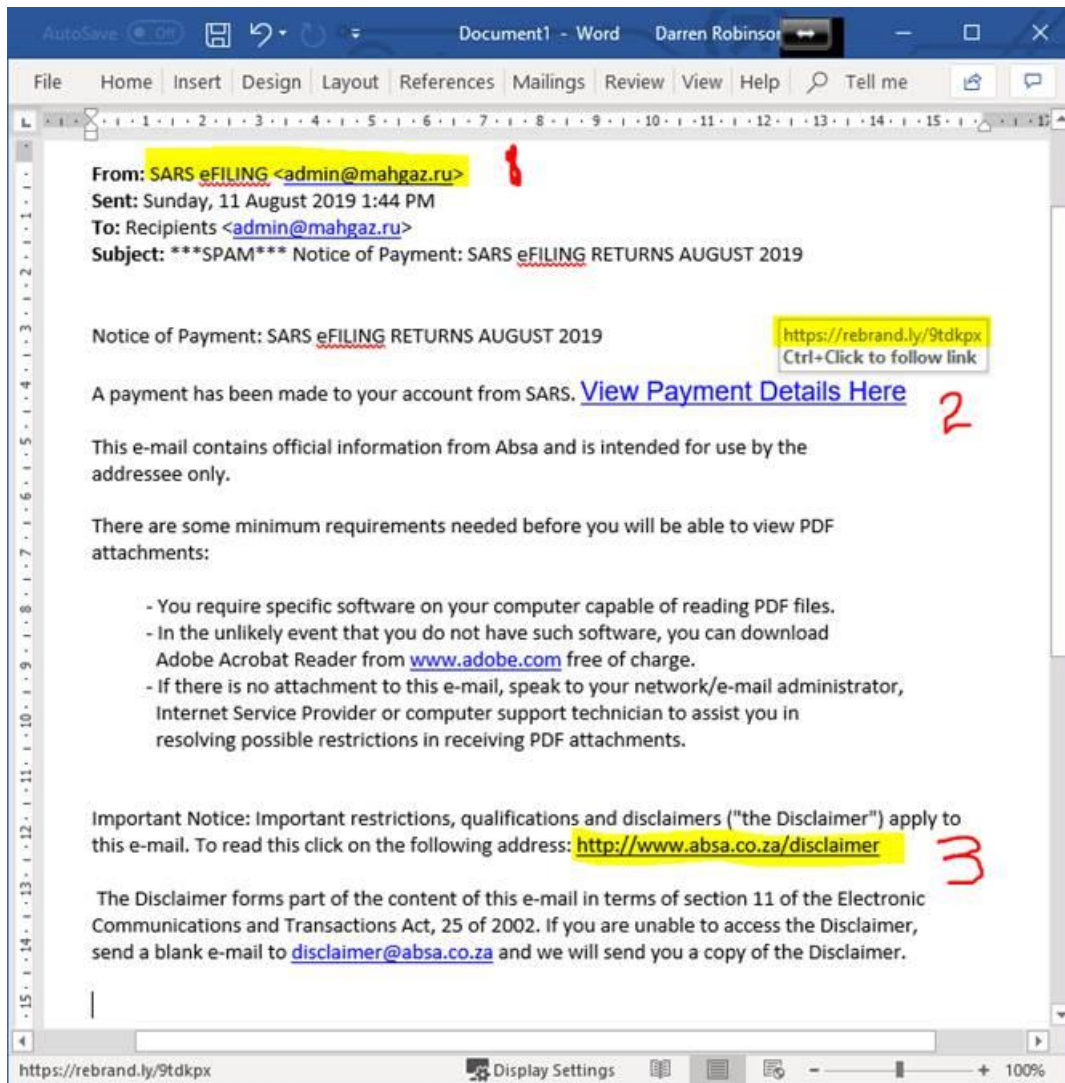


We have seen an increase in the number of fraudulent mails and other phishing activities that criminals are using to try and access systems, so thought I would put together two examples of mails that were recently sent to one of my mail accounts.

The first example supposedly comes from SARS advising that they have made a payment to me and the second example is from PayPal advising that my account has been limited. Both examples work on human nature effects that are set to drop our guard and try to get us to click on the links.

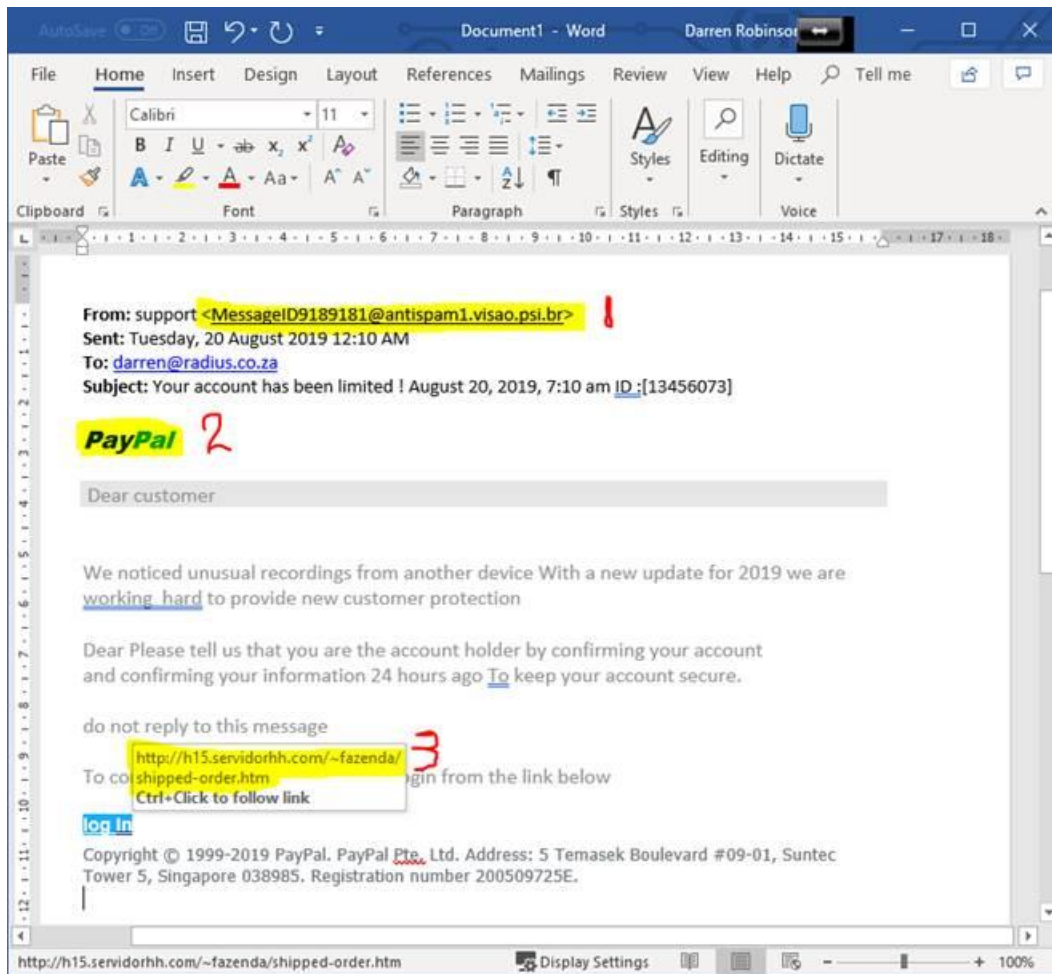
BE AWARE- BE VERY AWARE!!



Point 1- if mailed out by SARS, why would the senders address say admin@mahgaz.ru??

Point 2 – The link they want you to click on to vie your “refund” would take out to a website that is not SARS, or your bank!!. It will take you to a site that in all likelihood will download a virus, trojan, or piece of ransomware software that will infect your computer and have other potentially crippling effects. DO NOT click on links like this!!

Point 3 – If the mail as sent by SARS (point 1) why would the ABSA disclaimer be on the mail? Be aware of issues like this that show mails have been cut and pasted. Taking an extra minute to read mails will save you lots of heartache.



Point 1- If from PayPal you would expect the domain to end with @paypal.com or something similar and not with a strange address like this!!

Point 2- This is placed to make it look like a genuine PayPal mail that has been sent to you. Be careful of people spoofing pictures or images as this is really easy.

Point 3 – If you had clicked on the “Log in” button at this point, you would have been taken to a website that is definitely not a PayPal site and in all likelihood had a piece of ransomware or malware downloaded and installed on your PC to try and steal your data, or hold you to ransom. Please be careful!! If unsure hover your mouse over the link and the hyperlink or website connected to the “hotkey” will show up like this. Check the address of the site. If unsure DO NOT Click!!

In closing, the easiest way for criminals to access a company is through the mail system as they believe staff to be a weak link. PLEASE DO NOT be the weak link – Even if you expecting a mail form a user, please check it carefully to ensure that it is legitimate.

Keep your eyes peeled and have a great day.

Regards

Darren

Darren Robinson

Director



Unit 5, Verona Office Park, Cnr Malibongwe Drive & MacArthur Avenue, Robindale, Randburg
P.O.Box 886, Fontainebleau, 2032

Cell: +27 (0)82 337 2198 **Tel:** +27 (0) 87 822 1972

Email: darren@omsa-connect.co.za **Website:** www.omsa-connect.co.za

Please feel free to pass this mail onto any friends, colleagues or family members that you believe may find it useful. If you wish not to receive any further mails of this nature, please let me know and I will remove you off the mailing list.