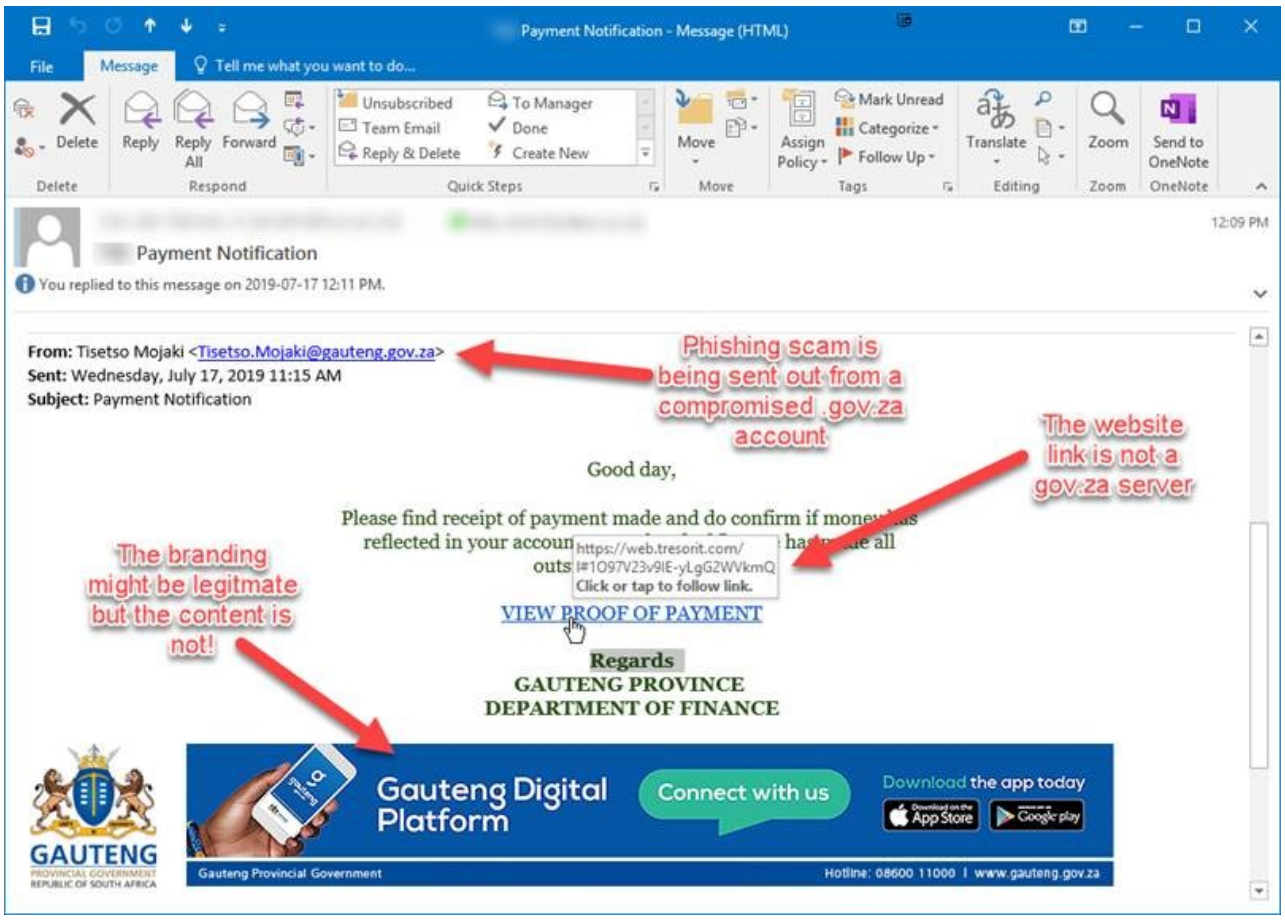
PHISHING SCAM SENT FROM COMPROMISED GOV.ZA ACCOUNT

*Posted on **January 01,1970** by **David Wiles***

Please be aware of the following phishing e-mail which is now starting to be sent to university accounts and might be thought to be legitimate especially if the department has dealings with the Gauteng Government.

The Subject of the mail is “Payment Notification” and asks its victims to click on a link to “VIEW PROOF OF PAYMENT”.

Firstly the link is not a gov.za website and government departments do not usually send out e-mails asking you to click on unverified links.



The suspicious mail takes you to a site that asks you to download a file. This file has a encoded script (malware) that looks like an ordinary web page that asks you to enter your username,password and your cell number to “confirm” your details and “allow” you to view the encrypted PDF file. Of course this malware, now sitting on your PC sends your login details and password to another server overseas controlled by the scammers, which they will
then use to break into your account at the university in order to do all sorts of nasty things.

So please be very careful, especially in the light of the compromised university accounts that were used earlier this week to launch a phishing attack from within the university.

The university is now a very popular target for phishers because they can easily gain access to personnel and student

accounts as the users are not often aware of the dangers of phishing and are not informed about how to spot them.

You can report phishing scams and spam in two ways:?

1. **By reporting it on the ICT Partner Portal.??**

- Go to https://servicedesk.sun.ac.za/jira/servicedesk/customer/portal/6/create/115.??
- Fill in your information and add the email as an attachment. Your request will automatically be logged on the system.?? ??

2. By sending an email.??

- Start up a new mail addressed to csirt@sun.ac.za.??
- Use the Title “SPAM” (without quotes) in the Subject.??
- With this New Mail window open, drag the suspicious spam/phishing mail from your Inbox into the New Mail Window. It will attach the mail as an enclosure and a small icon with a light yellow envelope will appear in the attachments section of the – New Mail.??
- Send the mail.?? ??

If you have accidentally clicked on the link and already given any personal details to the phishers it is vitally important that you immediately go to the USERADM page (either http://www.sun.ac.za/password orwww.sun.ac.za/useradm and change your password immediately.) Make sure the new password is completely different, and is a strong password that will not be easily guessed, as well as changing the passwords on your social media and private e-mail accounts, especially if you use the same passwords on these accounts. Contact the IT Service Desk if you are still unsure.

Posted in:Phishing,Security | Tagged:Phishing | With 0 comments