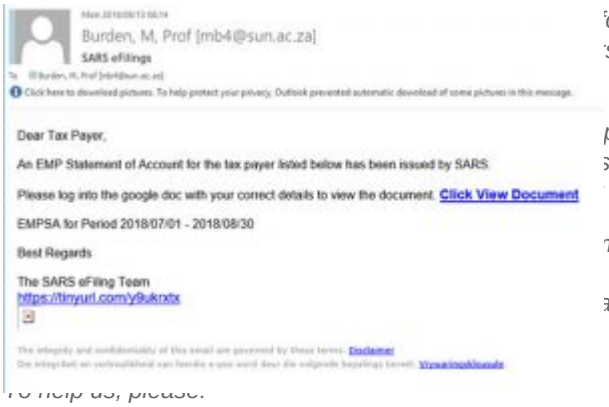
INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

SARS PHISHING SCAM FROM SUN EMAIL

If you receive an email with the subject “SARS eFilings” from any university email account, do not respond or click on the link. This is not a legitimate email from SARS.

The suspicious email is being sent from compromised staff email accounts informing users that "An EMP Statement of Account for the tax payer listed below has been issued by SARS" and you "need to log into the google doc with your correct details to view the document". (as shown in example below):



orming us about suspicious mails and letting your colleagues and s, and your input, information and questions are extremely

phishing emails, criminals will be able to gain access to your shing email, immediately go to the www.sun.ac.za/useradm accounts.

mpromised account they might simply move over to another using once it is blocked by us and would use another one that are servers in Europe to launch their attacks. This is a common

To help us, please:

- *continue to watch out for mail like or similar to this and do NOT respond to it, click on links or provide your email address username or password*
- *report the new phishing mail to the correct e-mail addresses of Information Technology Cyber Security using the method added to the bottom of this post*
- *remember, just because a mail comes from a “student” or a “personnel” e-mail address and has university branding does not mean in any way that it is legitimate*

If you have received mail that looks like this please immediately report it to the Information Technology Security Team using the following method: (especially if it comes from a university address)

1. *Start up a new mail addressed to sysadm@sun.ac.za (CC: help@sun.ac.za)*
2. *Use the Title “SPAM” (without quotes) in the Subject.*
3. *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.*
4. *Send the mail.*

IF YOU HAVE FALLEN FOR THE SCAM:

If you did click on the link of this phishing spam and unwittingly give the scammers your username, e-mail address and password you should immediately go to http://www.sun.ac.za/useradm and change the passwords on ALL your university accounts (making 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.)

For more information on reporting and combating phishing and spam: http://blogs.sun.ac.za/it/en/2017/11/reporting-spam-malware-and-phishing/

[Information supplied by David Wiles]

Posted in:E-mail,Phishing,Security | | With 0 comments