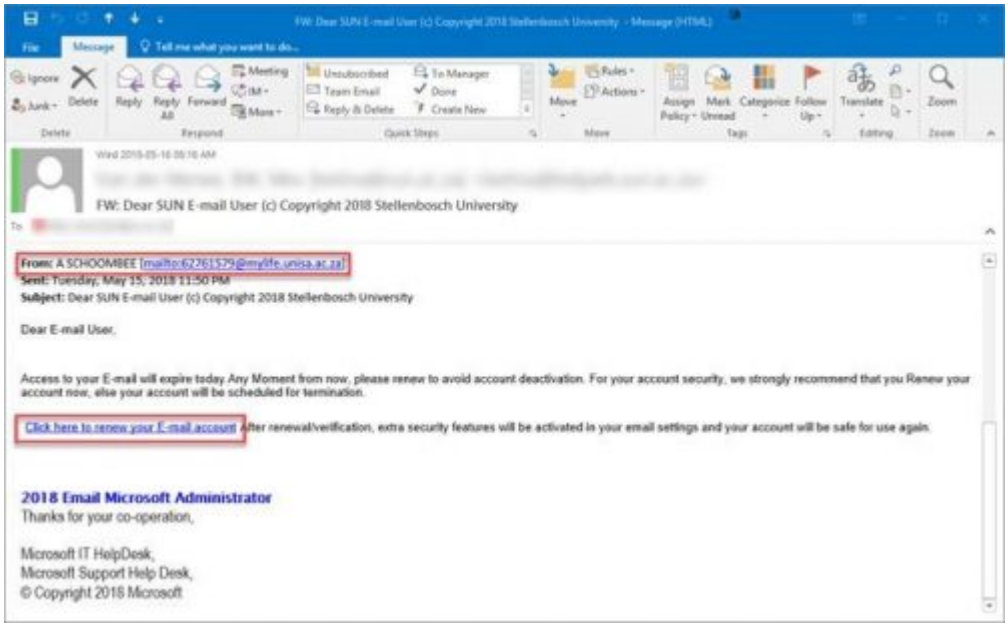
PHISHING SCAM DISGUISED AS THE UNIVERSITY'S SINGLE-SIGN ON PAGE

*Posted on **January 01,1970** by **IT Communications***

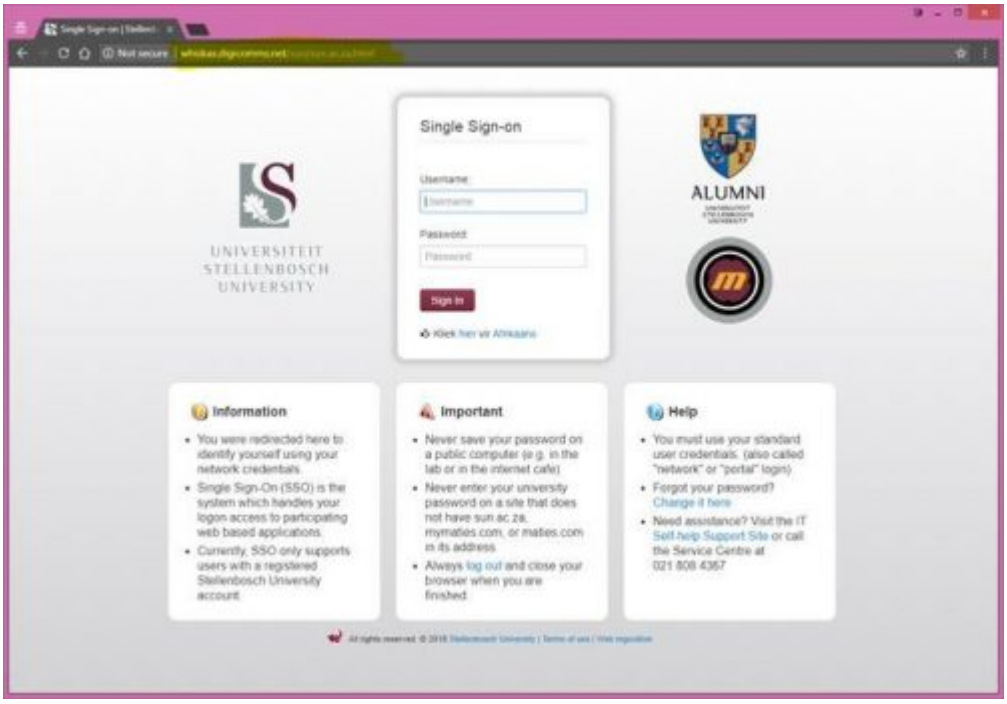
Due to the vigilance of an observant personnel member from the US Business School, we have encountered a dangerous phishing scam being sent from a **compromised UNISA account**.

The Subject is **"Dear SUN E-mail User © Copyright 2018 Stellenbosch University"** which should immediately raise eyebrows. The phishing email "warns" you about the pending expiration of your e-mail account and prompts you to click on a link to reactivate it.

See below what the mail looks like:



The danger is that the phishing scammers have perfectly forged the university's **SINGLE SIGN-ON** page, that is used by students an personnel to access the portal pages, the my.sun.ac.za page, SUNLearn etc., as you can see below. Not many people will notice that the address is not a university address, neither is it secure.



It is imperative that you **do not click on the link** in the mail, and do not provide the scammers with your username and password as they might be able to access the university's systems that are accessible through the Single Sign-On page.

Last year scammers were able to forge the e-HR login page through a phishing scam and several staff members had their bank accounts details and other personal details exposed to the scammers. In the light of the issues that Tygerberg staff have been having with general network access earlier this month, and this week's issue with e-mail, the arrival of this sort of mail at this time can fool some people into thinking that it is legitimate and lead to compromised network and e-mail accounts.

Here's how to report any phishing or spam mail:

Send the spam/phishing mail to help@sun.ac.za and sysadm@sun.ac.za.

Attach the phishing or suspicious mail on to the message if possible.
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.

[Information supplied by David Wiles]

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