INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PHISHING SCAM ABOUT REACHING YOUR MAILBOX STORAGE LIMIT

Monday started with a phishing scam threatening to close your mailbox, and Monday is ending with another attack, using a similar intimidation tactic about your mailbox size.

The grammar and spelling is very poor on this one so it should be rather easy to spot. However the use of University branding and "STELLENBOSCH HELP DESK" might fool some people.

The Subject will be "We apologies" (sic)

Dear User,

You have reached the storage limit for your mailbox. Please visit the following link to complete your e-mail access restore.

Follow this link to complete the process: Click Restore

STELLENBOSCH HELP DESK

If you do click on the link (which does not go to a university website) …this webpage will appear.

Many thanks to all of you who reported this.

Remember these 5 guidelines:

1. *Information Technology will never request sensitive information such as passwords.*
2. *Phishing e-mails often appear as an important notice or urgent matter such as threats that your mailbox is over quota.*
3. *Use of aggressive or intimidating language such as 'immediately' and threats of consequences of not verifying your account.*
4. *Misspelled words and poor grammar that take away from the professional context of the e-mail. (this one is quite obvious)*
5. *Use of an impersonal greeting. (Dear User)*

If you have received mail that looks like this please immediately report it to the Information Technology Security Team using the following method:

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. There is a good tutorial on how to do this at the following link (Which is safe) : http://stbsp01.stb.sun.ac.za/innov/it/it-help/Wiki%20Pages/Spam%20sysadmin%20Eng.aspx

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.)

IT have set up a website page with useful information on how to report and combat phishing and spam. The address is: http://blogs.sun.ac.za/it/en/2017/11/reporting-spam-malware-and-phishing/

[Article by David Wiles]

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