INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

WARNING: PHISHING SCAM EXPLOITING ABSA NEW LOGO

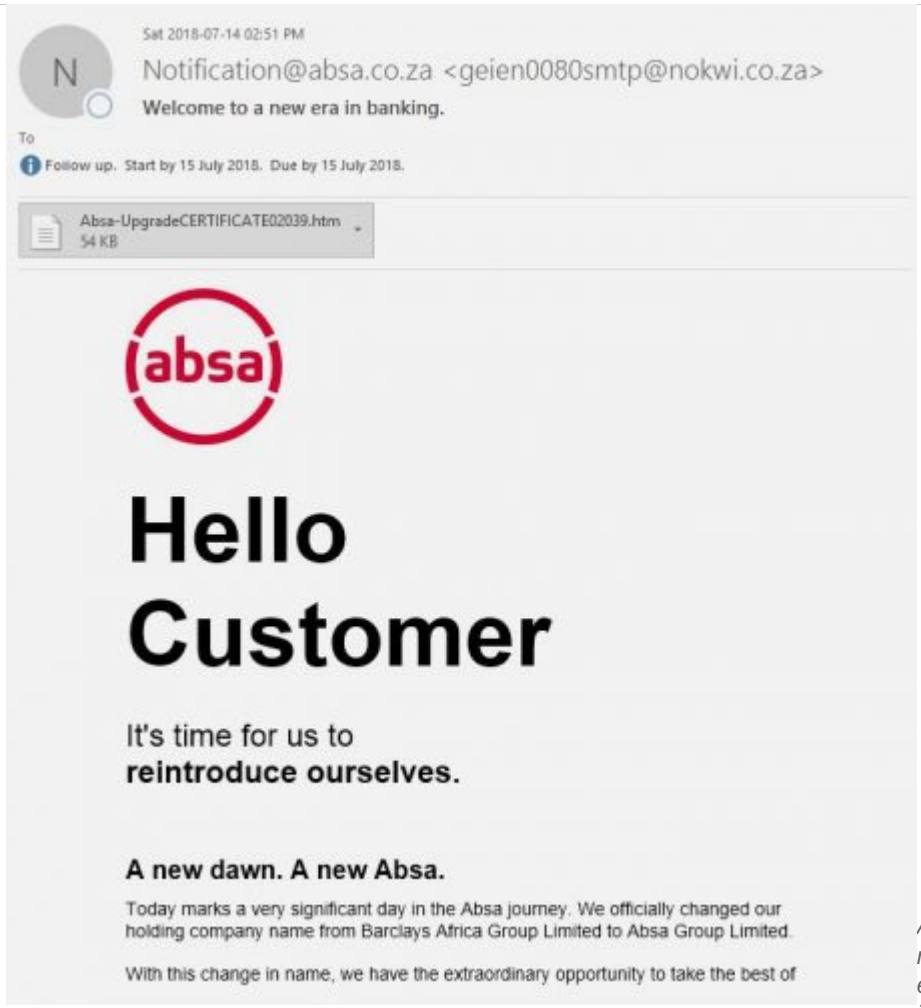
Many of you use ABSA as your bank of choice, as well as making use of ABSA Bank's Internet Banking facilities, so this warning might be of particular significance.

Earlier this month ABSA announced a new logo - part of its rebranding campaign - and almost immediately phishing scammers exploited this opportunity to continue their nefarious campaign of identity theft through phishing email attacks.

Several users have reported getting the following email - allegedly from ABSA - taking advantage of the new logo to target the bank's customers in a phishing email scam by attempting to trick users to click on a link to take them to a fake website.

The scam email states that it comes from Absa CEO Maria Ramos, but it's actually from an outside source and informs victims that "today marks a very significant day in the Absa journey". The email uses Absa's slogan, saying "We are also launching a new, fresh and vibrant Absa logo and identity that reflects our commitment to you, our customers". Potential victims are then encouraged to click on their "New Absa eStatements" in PDF format. This is not a statement, but an HTML file which takes users to a phishing website.

Here is one example of the phishing e-mail which has already appeared in several University email accounts, as well as personal home email accounts:



As always, you should never respond to a suspicious looking email or message or click on a link in any suspicious looking email. Rather delete the email. No South African bank will ever contact customers and request sensitive information (card PIN, card CVV or online banking password) via email, telephone or SMS.

If you have received a phishing email, immediately report it to the Information Technology CyberSecurity Team using the following method:

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 a phishing spam and unwittingly gave the scammers your username, email address and password 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 email accounts (especially if you use the same passwords on these accounts.)

Useful information on how to report and combat phishing and spam can also be found on our blog

[ARTICLE BY DAVID WILES]

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