INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

PHISHING: ABSA SURECHECK PROFILE APP

Over the weekend and as already reported by a number of Tygerberg colleagues & students, a variant of last week's ABSA phishing scam has started flooding our email.

The tactics have changed slightly and the criminals are now using a South African domain name to launch their attack. Below is the example of the phishing email, with the forged "ABSA Bank" login page to attempt to convince you to give your bank details willingly to the scammers.

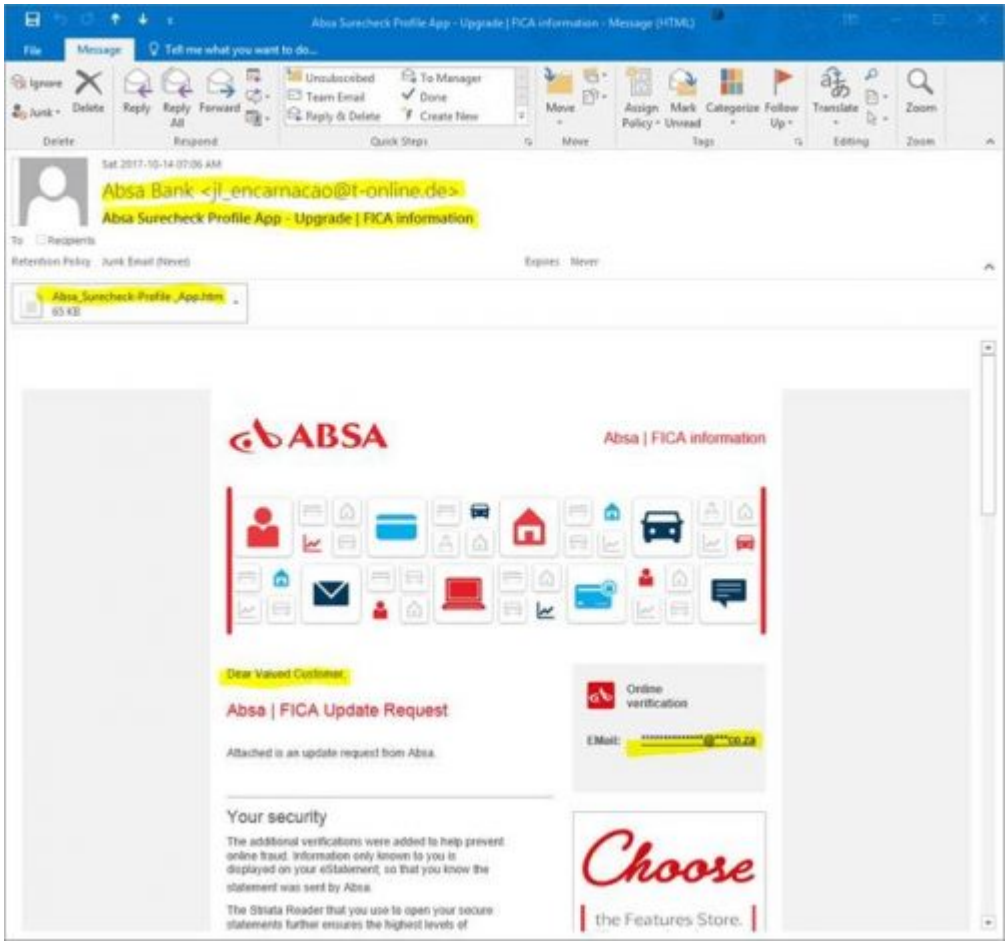
The subject of the email is "Absa Surecheck Profile App – Upgrade | FICA information" which is designed to say absolutely nothing. It is what is known in information technology circles as "techno-babble"

While the methods used to steal a your banking details may differ, the process followed by fraudsters to steal money from their victims in South Africa are nearly always the same:

1. *Get the person's Internet banking details, typically through a phishing attack. (as shown below)*
2. *Get a banking account/s to which money can be transferred to and withdrawn.*
3. *Clone the SIM card used by the victim.*
4. *Create beneficiaries (using the list of banking accounts) and transfer money to these beneficiaries.*
5. *Withdraw the money from these accounts.*

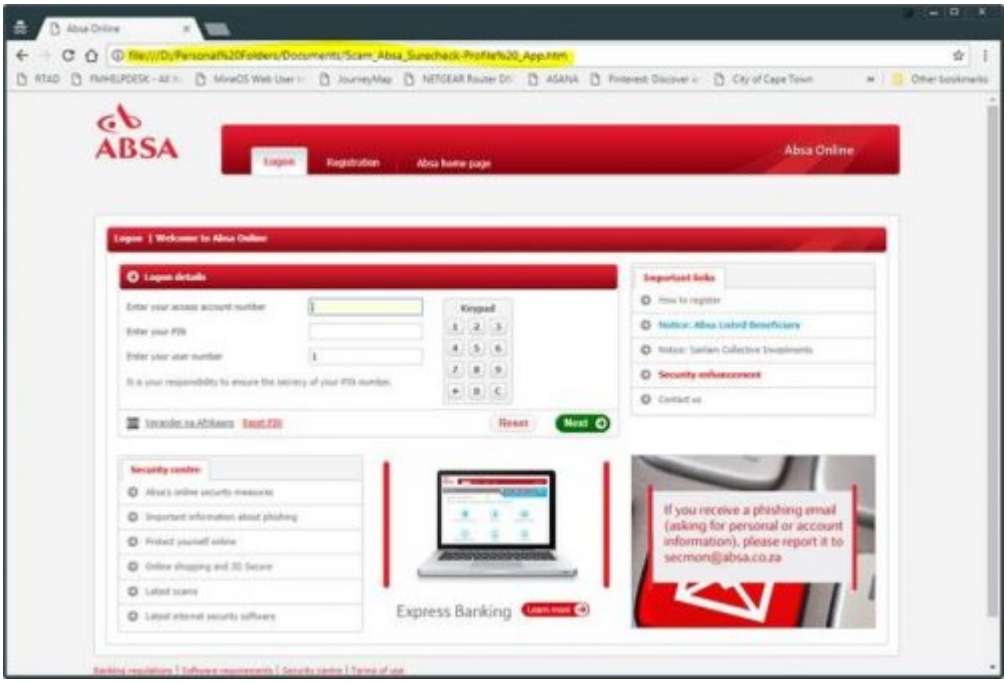
Here are the obvious warning signs:

1. *The sender is not an ABSA email account (in this case a "throwaway" German email account used to send millions of phishing e-mails)*
2. *Vague and deceptive subject lines (Techno-babble)*
3. *An attached file (.htm) that contains a web page that opens up in your browser and links in the background to the server in South Africa.*
4. *Impersonal salutation. "Dear Valued Customer". Banks will never address you like this. They have your money – so it stands to reason that they will know your name as well.*
5. *"Online verification" has **** to convince you that the email is genuine, but university addresses end with ac.za, not co.za.*



The web page that you are directed to is actually the .htm file based on your computer (as an attachment, but links directly to the phishing server in the background.)

In this case is iteron.co.za which is listed as "undergoing maintenance" but is fully functional in the background.



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

Send the spam/phishing email to the following addresses

help@sun.ac.za

...and sysadm@sun.ac.za as well.

Attach the phishing or suspicious email 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 email 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 email from your Inbox into the New Mail Window. It will attach the email 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 email.*

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.)

[ARTICLE BY DAVID WILES]

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