Eight digital banking scams to lookout for

20 February 2017: As access to banking services through digital channels continues to grow, so does the need to protect consumers against the prevalence of online banking fraud.

Yolande Steyn, Head of Innovation at FNB says "We view security as an integral part of a seamless online banking experience. Therefore, due to the prevalence of banking scams, we urge consumers to be more vigilant and familiarise themselves with the different types of online banking fraud."

"FNB proactively closes down fraudulent phishing websites used by criminals to try and access customers' confidential banking details," adds Steyn, as she unpacks the latest online banking scams that consumers should be wary of.

Flight purchase debit scams - you will receive an SMS informing you of a flight purchase debited to your account. Fraudsters will request you to select a link in the SMS to revise the transaction.

When you select the link, you will be redirected to a fake FNB website. You are then redirected to an 'Update and Confirm Details' screen requesting more information to be verified. The fraudsters will now be in a position to access your banking profile.

Social media scams - beware of fraudsters pretending to represent FNB or RB Jacobs on social media channels such as Facebook, Twitter, LinkedIn, WhatsApp or any other social media platform. We will never ask for your credit or cheque card, account number, online banking login details or password or One Time PIN (OTP) on social media platforms. FNB's official social media accounts are @FNBSA and @RBJacobs on Twitter and FNBSA on Facebook. The official accounts also display a blue tick indicating that they are verified.

Change of banking details scam - you will receive an email that pretends to come from one of your suppliers asking you to update your banking details. Beware of this even if it is on the supplier's letterhead.

Contact your supplier on the number that you already have for them and not the one on the fraudulent letter. Speak to someone you know at the supplier to confirm the change in banking details.

Copy of payment notification scam - you will receive an email requesting you to open a copy of your payment notification. Fraudsters will prompt you to login via the email attachment.

When you open the attachment in the email, you will be redirected to a fake FNB website. In an attempt to steal your banking details you will be requested to login. As soon as you enter your login details on the screen, you are redirected to a successfully logged out screen. The fraudsters will now be in a position to access your banking profile.

419 scams - this is communication by e-mail to a recipient making an offer that would result in a large pay off for the recipient. The details vary and large amounts of money are usually involved. Invariably, the victims' banking details as well as sums of money are said to be required in advance in order to facilitate the payment of the funds. Essentially, the promised money transfer never happens and in addition the fraudsters may use the victims' banking details to withdraw money for themselves.

Vishing and smishing scams – this is phishing, but instead of being lured to a fake website via email,

you receive a call or SMS, where the individual pretends to be from the bank or other companies and gets you to disclose personal information such as your ID number, address, account number, username, login details, password and PIN. This information can also be used to gain unauthorised access to your banking account online.

OTP Email Fraud – using various methods of phishing, criminals also try to get access to your email accounts, commonly Gmail, Yahoo, etc. They produce fake login sites that look like Gmail or Yahoo. Once they have your email username and password, they have access to your emails (statements, personal communications) and this helps a criminal to build a social profile of you. Criminals can also intercept One Time Pins (OTPs) that are sent to emails once they have access to your email account.

OTP SIM Swop Fraud – once criminals are in possession of your username and password, they can easily access your accounts on Online Banking. They can also contact your service provider to do a Sim Swop which basically means that they hijack your sim and have access to your SMS. This also gives them access to your One Time Pin (OTP).

"Remember, the bank will never ask for your username, password or PIN in an email, SMS, social media or phone call. Never select a link to our website that was sent via email. Always type in FNB's web address," concludes Steyn.