

SARS WANTS TO GIVE YOU MONEY?

Posted on *February 08,2013* by *IT Communications*

It's that time of the year when our mailboxes are infiltrated by messages from SARS and we start making sums and filling out forms. Unfortunately elusive cyber criminals also know that this is the perfect time to prey on our gullibility.

So it's most likely that you will be receiving (if you haven't already) a so-called e-mail from SARS asking you either to verify your information or to let you know that a much-welcomed amount has been paid into your account. (see example below) Don't get excited - it's not really SARS.

Clicking on the hyperlink in the email takes you to a fake "e-filing" site that has hyperlinks for the four big South African banks and instructions to log on to your Internet banking site for "confirmation of your details". When you follow the Nedbank link (as an example), you are taken to a copy of the Nedbank internet banking site that asks for profile, pin and password. Supplying these takes you to a second page that asks you for your mobile number. Submitting information on this page takes you to a page that requests the reference number sent to your cellphone.

Do not authorise any cellphone message that comes through if you end up in the above situation. Furthermore, do not click on any hyperlinks in emails or divulge your account or mobile number details to anyone over the phone or via email. Banks will never ask you to access internet banking through a link in an email, neither will banks ever ask for your mobile number when you access internet banking.

Look out for the following tell-tale signs:

- when you move with your pc's mouse over the link, it won't be the official, correct web address
- the e-mail isn't addressed to you personally - your name isn't mentioned anywhere
- the address it was sent from is a generic one that doesn't exist
- there is no reference or account number
- no contact person is mentioned

If you're unsure, rather go directly to the SARS e-filing web site (type in <http://www.sarsefiling.co.za/>) and see if there were any payments made to your account.

From: Sars Efiling <message@sars.co.za>
Date: 30 July 2013 19:37:38 EDT
To: <fakeaddress@sun.ac.za>
Subject: **You have a new transaction message**

We have filed your return and made a deposit of R3,650.80 into your account.

Confirm your filing

This is an automated email, replies sent to this address will not be received.

Sars eFiling

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