PHISHING SCAM DISGUISED AS A STANDARD BANK ACCOUNT STATEMENT

*Posted on **January 01,1970** by **IT Communications***

We all regularly get phishing scams on our mail boxes, and normally they do not pose a threat if we are not Standard Bank customers. However, if any of you are Standard Bank customers, then there might be a risk.

Today's phishing mail comes from a forged e-mail address like info@standardbank.co.za.

The Subject line is usually: **"Standard Bank: Account Statement June-201**7" (or iterations of the month and year)

The body of the e-mail contains variations of the following:

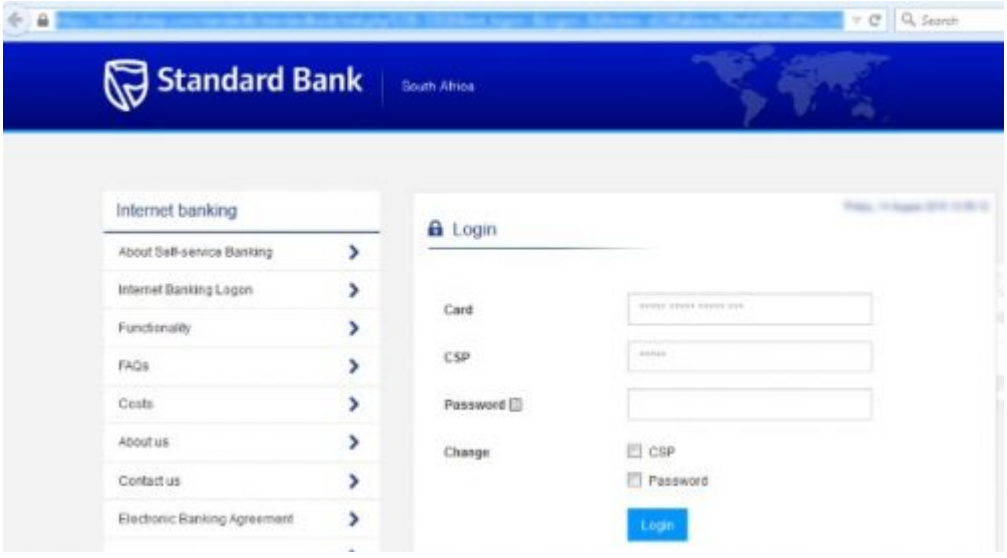
Dear Customer

Attached to this e-mail is your Standard Bank account statement.

Click the download button and follow the easy instruction.

Regards
Standard Bank

There will be an **HTML** file attached which if you do double-click to open up, will give you a forged login page similar to the following, where you will be asked to fill in your bank card details, your PIN and your password – and if you are fooled, the scammers will gain access to your bank account.



The **dangerous** thing about this particular version is that there is a small JavaScript code embedded in the HTML file, which will run as soon as you visit the forged site, and will trigger and attempt to download malware onto your computer to steal data like passwords, bank account details, or to turn your computer into a "zombie" under their control to send out further email or to attack the university from within the network.

This week it might be Standard Bank, next week it might be ABSA or FNB or Nedbank. Phishing scammers are constantly changing their tactics.

Here are 5 easy tips to spot most phishing scams:

1. **The sender's e-mail may appear to be legitimate. It is easy for the criminals to forge an address to make it look like it is coming from the bank.**
2. **The e-mail is addressed to "Dear Customer", with no specific name being mentioned. (Banks have enough information of their customers to be able to address you personally!)**
3. **Hovering your mouse cursor over any links will show a fraudulent URL – not the bank's trusted web address.**
4. **The e-mail contains a link to 'Logon" or "Update Details". Banks will not ask you to access Internet banking directly through an e-mail.**
5. **The contents of the e-mail will be vague or reference a specific transaction which you would not normally conduct or receive.**

The university's spam and phishing filters are quite effective in blocking these forms of phishing emails, but common sense and becoming informed should always be your first line of defence!

[ARTICLE BY DAVID WILES]

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