Internet Banking
Targeted Phishing Attack

1. Introduction

The phishing attack, targeted at Standard Banks' customers, initiated from unsolicited emails, requesting a verification of email address by clicking the URL contained in the email. The link was ultimately the means to dupe customers into divulging their sensitive credentials, such as card number, password and customer selected pin.

This phishing attack differs from traditional phishing attacks, as it displayed the legitimate Standard Bank web page (www.standardbank.co.za/site/about/index.jsp), and produced a pop-up screen after 5 to 10 seconds requesting customers to enter sensitive credentials. The pop-up screen overlaid Standard Bank's legitimate web page thereby making the request seem authentic. The pop up logon screen was embedded in the URL reference.

Once credentials were submitted to the pop up screen, it was transmitted to the perpetrators site.

This attack was similar to the one FNB endured on the 17th of May 2005 differing in that the FNB attack was through a spoof site emulating FNB's web page.

2. Objectives of Perpetrators

The objectives of the perpetrators was to obtain card numbers, customer selected pins and passwords. The request of ATM PIN, which seemed to be more noticeable, can be interpreted as a means to obtain card pin data, as seen in the sample screen of an attack. The latter widens the potential avenues of risk to white carding.

The attackers deliberately used non-traditional spoofing methods as a means to prevent early detection of their fraudulent activities, by detection specialist Cyota. Hence there was no means of closure of the operation prior to the attack becoming known. Furthermore, the perpetrators used multiple hosting sites to increase their window of opportunity.

3. Compromised Credentials

The method of obtaining the credentials was to send targeted unsolicited email to potential Standard Bank customers. The email, as shown below, contained a URL that directed the client to legitimate Standard Bank web page when clicked. Furthermore, embedded code produced an overlay pop-up onto the web page after 5 to 10 seconds, creating an effect of a legitimate flow. Unaware to the customer this pop-up was a phishing method to obtain credentials such as card number, customer selected pin (or ATM pin) and password, as shown in the sample screens below.
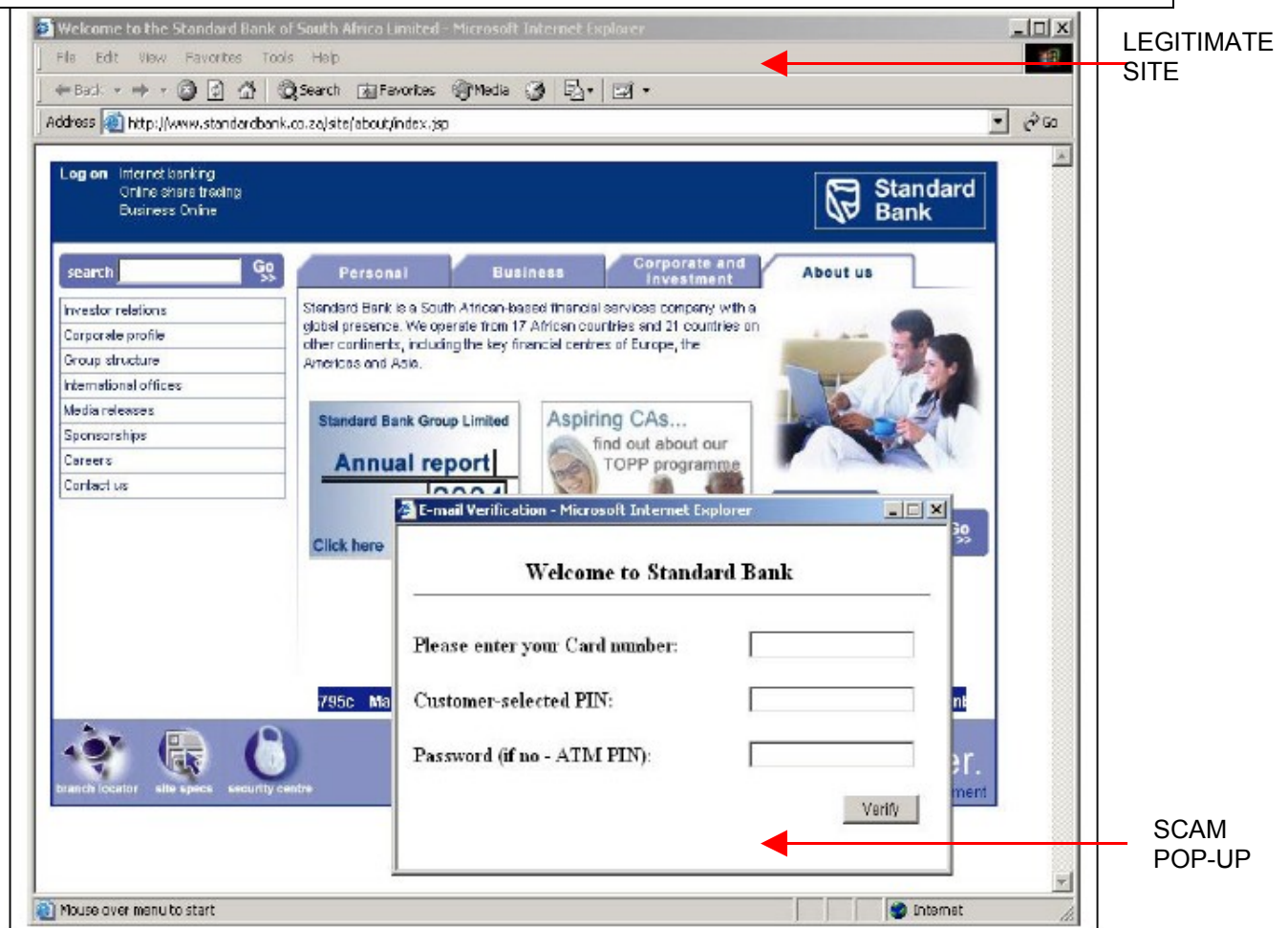
----- Original Message -----

Dear Standard Bank Member,

This email was sent by the Standard Bank server to verify your e-mail address. You must complete this process by clicking on the link below and entering in the small window your Standard Bank online access details. This is done for your protection - because some of our members no longer have access to their email addresses and we must verify it.

To verify your e-mail address and access your account, click on the link below:

http://www.standardbank.co.za/7mcSUK2Q5VjwhuD3MnH3kxdYLi8GE3Pd4U7sw3ydmxs9sFsZ4q8b29i7g6g95n

---- End Message ----

LEGITIMATE SITE

SCAM POP-UP

4. Compromised Customers

All customers who entered their details on the fraudulent pop-up were compromised. One must note that the targeted unsolicited email was directed to random email users who may not be Internet registered users. Hence there is a potential risk to non Internet Banking users, who inevitably entered their ATM card and pin number, as instructed by the attack.