INFORMASIETEGNOLOGIE

INFORMATION TECHNOLOGY

CYBERSECURITY AWARENESS MONTH: SPEAR PHISHING

shing". Spear phishing attacks deliberately target the university instead of will respond. This approach is successful because scammers focus on ir phishing emails accordingly.

geted with a few large-scale spear phishing attacks resulting in student and al instances, some of the victims suffered financial loss.

nbosch Payroll" with the subject of "NOTIFICATION: Your 13.69% Salary e certainly attracted attention and was sent at a time when salary increases

---------- Forwarded message ----------
From: Stellenbosch Payroll <jonathan.higgins@newcastle.ac.uk>
Date: 4 Apr 2017 10:13
Subject: NOTIFICATION: Your 13.69% Salary Increase
To:
Cc:

and spelling mistakes. The lure of a 13.69% n to the wind. The university branding also

UNIVERSITEIT STELLENBOSCH UNIVERSITY

Hello,

Attached herewith are two (2) documents summarizing your April salary as reviewed for a 13.69% merit increase in Financial Year 2017.

This review is with immediate effect starting Friday April 28th Paycheque. Deductions and bonuses are advised therein

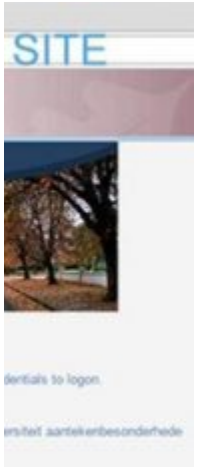
The documents are attached below:

Download Here

Human Resources & Employee Benefits

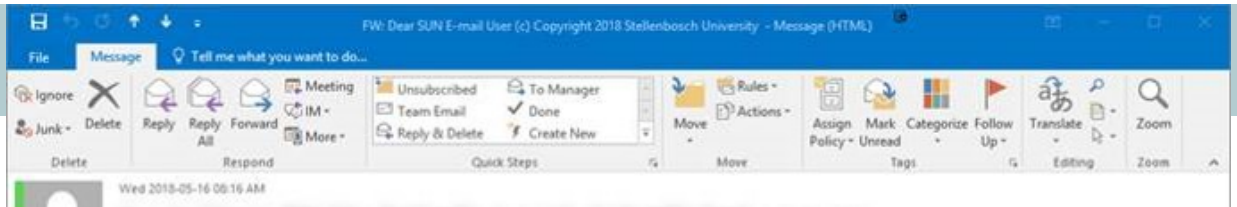
Stellenbosch University

ents with information on the salary increase. entical to the real login page of the University versity domain but very few people would spot



e documents explaining their so-called salary nes and passwords and gained access to the account details so that their salary would be paid into the scammer's own account. The person's bank account details were also captured and could be for further exploitation.

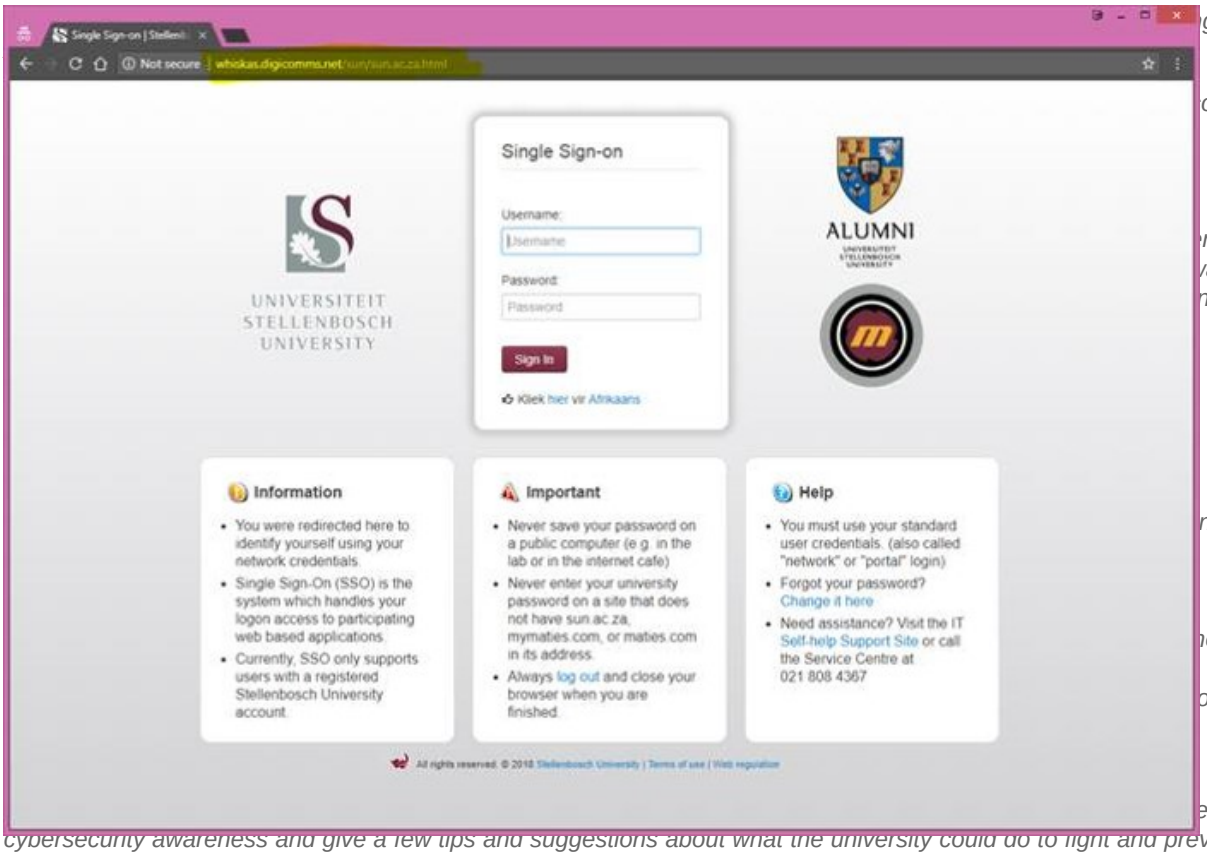
A second spear phishing attack occurred a year later in May 2018.



An email was sent from an already compromised UNISA account. The mail warned that the receiver's email account was due to be deactivated and that they should click on a link to renew it. The Subject said ***"Dear SUN E-mail User (c) Copyright 2018 Stellenbosch University"*** *and the signature was from the* ***"2018 Email Microsoft Administrator",*** *which many saw as legitimate.*

> *Clearly, the spear-phishing scammers researched their intended target and used words and other details like* ***SUN****,* ***Stellenbosch University*** *&* ***IT HelpDesk*** *that would increase its legitimacy.*

The link took the victims to another forged website. This time it was a perfect copy of the University's own ***"Single Sign-On"*** *page students and staff use to access important University services, for example SUNLearn and the staff portal. (see below)*



cybersecurity awareness and give a few tips and suggestions about what the university could do to fight and prevent these attacks.

Keep safe out there.

Posted in:Phishing,Security,Tips | Tagged:Phishing | With 0 comments