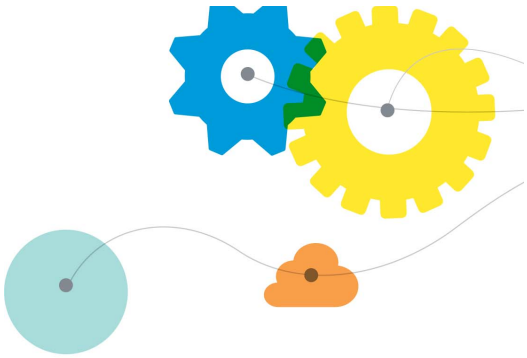
Tel 27 11 262 3632 Fax 27 86 637 8868
Block D, Sandhaven Office Park, Sandton, 2090
PO Box 342, Strathavon, Sandton, 2031
@synaq www.synaq.com



PHISHING ACTIVITY TRENDS REPORT JANUARY – JUNE 2013

PUBLISHED AUGUST 2013

Block D, Sandhaven Office Park cnr Katherine & Pongola Crescent, Sandton 2090
PO Box 342, Strathavon, Sandton 2031 Tel +27112623632 Fax +27866378868

Phishing Report Scope

The SYNAQ Phishing Trend Report is a quarterly account and analyses of phishing activity directed at SYNAQ clients against South African financial organizations.

Data is obtained from monthly stats obtained on the SYNAQ Securemail Inbound services.

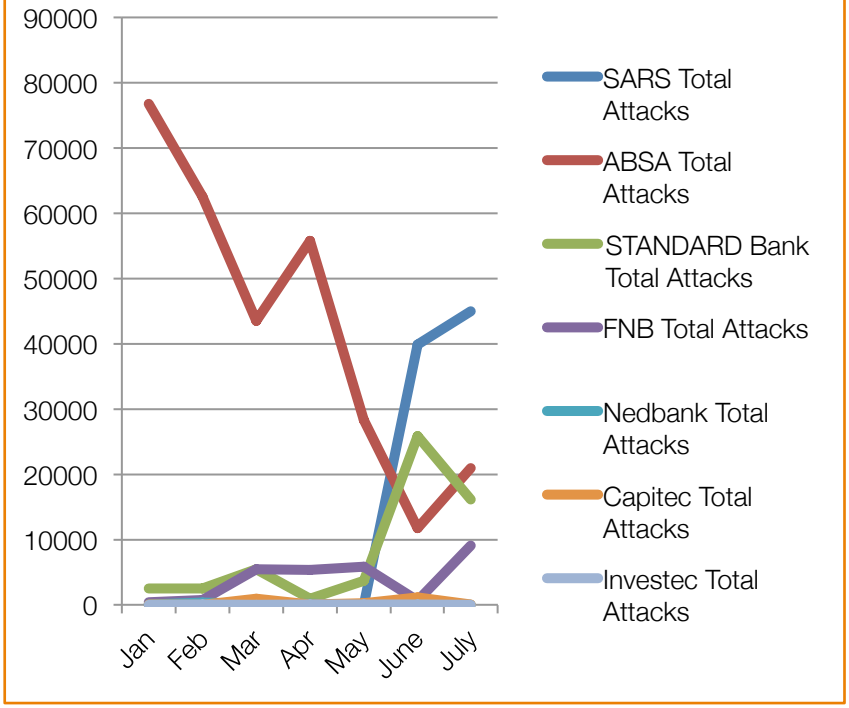
Phishing Defined

Email phishing occurs when fraudsters use official-looking emails to lure individuals to a spoof website in order to obtain their banking or credit card information for use in identity theft.
Phishing can take one of three avenues:

- URL - this is consistently the most frequent form of attack. The user is prompted to click on a url link which emulates a banking logon used for gathering login credentials.
- Forms - this is second most popular method of attack. The user is provided with an email embedded form to fill in, and the details are then mailed to the scammer.
- Malware - this is usually a trojan download attached to the email message which the user is asked to install for better security.

Table of Contents

Tax season boosts phishing activity in June



Phishing attacks are down from 2012 year-on-year comparisons but the opening of tax season in June has seen an upsurge in the trend

1st and 2nd Quarter 2013 Phishing Trends Summary

- Phishing attacks against South African banks have dropped
- The start of the tax-fiing season in May has seen a significant reversal in the downward trend
- ABSA Bank remains the most targeted bank
- In two months (May and June) SARS has become the second most targeted institution for phishing activities
- Phishing attacks against FNB have risen in 2013
- Nedbank has continued to enjoy a declining interest from scammers

Statistical Highlights for 1st Half 2013

	Jan	Feb	Mar	Apr	May	June
Number of unique URL attacks	593	909	666	483	97	185
Number of unique Malware attacks	343	13	13	34	16	0
Number of unique Webforms	6	4	8	17	28	22
Total URL attacks	71455	53967	45766	48678	31375	53561
Total Malware attacks	3824	295	13	747	16	0
Total Webform attacks	4504	15048	9736	12717	6779	25697

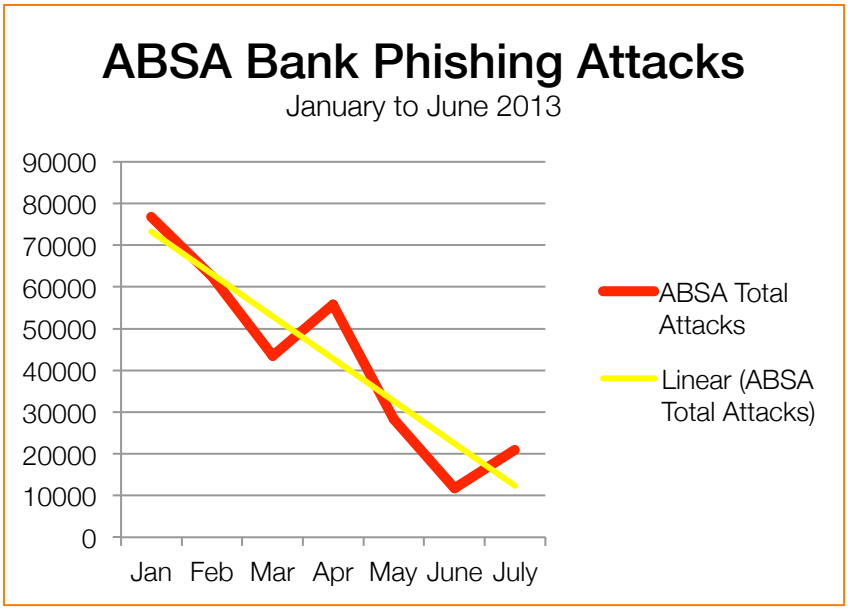
Phishing Trends for 1st Half 2013

- Phishing attacks against South African banks have dropped by almost 47% in the first six months of 2013, compared to the same period last year.
- The start of the tax-filing season in June, has seen a significant reversal in this downward trend.
- SARS received 39 905 Phishing attempts in June, well over 3 times the amount leading phishing target ABSA Bank received in the same month, and just under the total amount of attempts on Standard Bank for the period of January through to June.
- ABSA Bank remains the most targeted bank in South Africa, despite a 15% drop in total attempts year-on-year and has continued to enjoy a 22% decline in attacks from January to June 2013.
- Standard Bank, the second most targeted bank in South Africa, has seen a massive increase in total attempts year-on-year from 4 833 in 2012 to 40 884 in 2013. A 63,2% upswing of 25 867 attempts against Standard Bank was recorded in June.
- The reverse is true for FNB, while the overall trend from January to June has been a stready increase in attempts month-on-month, the yearly comparison indicates that attempts against FNB in 2013 total 12,45% of last years 147 525 attempts during the same period.
- Nedbank has recorded the most significant positive change in phishing attempts year-on-year receiving only 6,8% attempts on last years total. Further, Nedbank has only recorded 0,17% of all attempts against South African banks. February was the only abnormal month, recording in excess of 300 attempts.
- Capitec, while a relatively small bank in terms of marketshare has mirrored its performance of 2012, but recorded a 46,3% increase in June

Targeted Financial Institutions Activity for 1st Half 2013

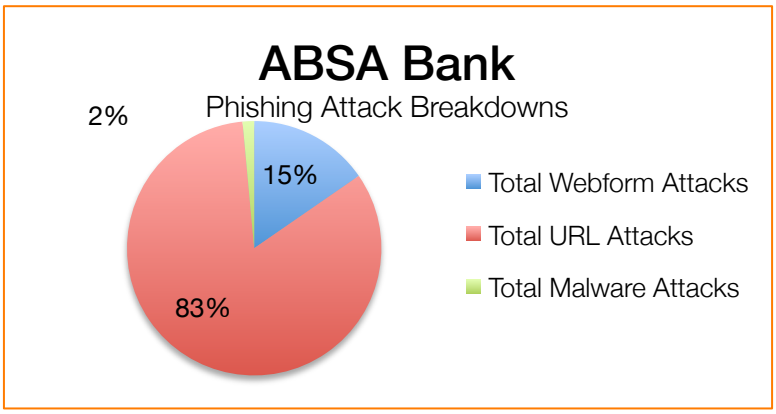
ABSA BANK

ABSA Bank is the most-targeted financial institution in South Africa but has recorded a downward trend in attempts levered against the bank this year.



To get best results, scammers pay attention to areas where they have the highest chance of success. "For the most part, client demographics play a stronger role than the actual bank as a target for scammers" explains Darryl Sutherland Phishmonger Lead Technical Architect at SYNAQ. Studies have shown that of the 5 dominant South African banks, ABSA is by far the largest retail bank - possibly twice as large as it's competitors.

83% of phishing attempts are in the form of URL



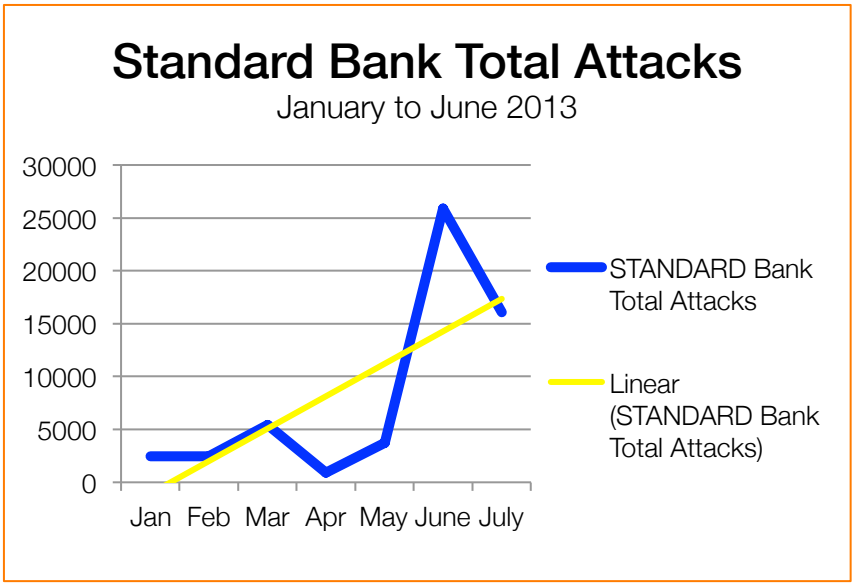
"As such, working on a 1% average success rate, ABSA offers the highest potential for successful phishing verses alternative banks," says Darryl "so scammers focus primarily on waters with the richest pickings, which is why ABSA is routinely the highest target".

Phishing attempts against ABSA have declined by 22%, from January until June. With a record 18 month low reported in June of only 11,746 phishing attempts reported on SYNAQ servers.

	Jan	Feb	Mar	Apr	May	June
Total Attacks	76813	62577	43503	55746	28332	11746
Total Webform Attacks	3557	14820	9735	12456	4267	4723
Total URL Attacks	69767	47463	33768	42569	24064	7023
Total Malware Attacks	3489	294	0	721	1	0
Unique Webforms	5	3	8	12	18	4
Unique URLs	557	358	261	384	84	24
Unique Malware	14	2	0	8	1	0

STANDARD BANK

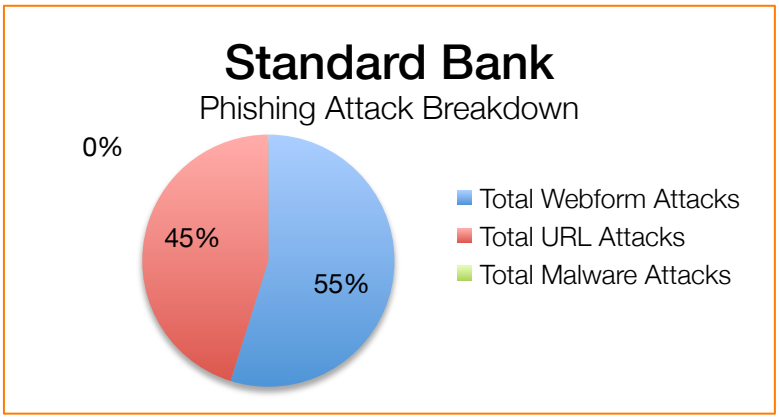
As the second most-targeted financial institution, Standard Bank has recorded an increase in volumes and an upward trend in phishing attempts between January and June 2013.



"Scammers often test the waters and will switch targets and methods periodically to get the best results," suggested Darryl as the reason for the Standard Bank upward trend.

While attempts peaked in June at 25867, the highest recorded activities against the bank, the monthly average has remained consistantly around the 3000 mark.

63,2% increase in phishing attempts in June



55% of phishing attempts against Standard Bank are Webform attacks. A webform attack is defined as an email embedded form which requires completion from a user, once completed the details are then mailed to the scammer.

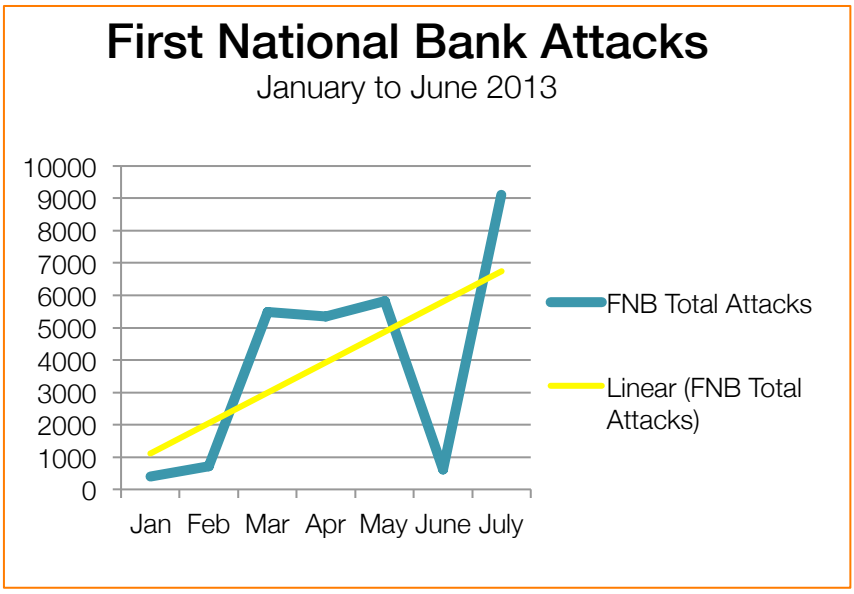
Phishing attempts against Standard Bank take the form of either a Malware or URL attack.

Malware, short for malicious software, is software used or programmed by attackers to disrupt computer operation and gather sensitive information.

	Jan	Feb	Mar	Apr	May	June
Total Attacks	2488	2486	5417	912	3714	25867
Total Webform Attacks	947	227	0	154	2460	18635
Total URL Attacks	1537	2258	5417	758	1253	7232
Total Malware Attacks	4	1	0	0	1	0
Unique Webforms	1	1	0	2	9	16
Unique URLs	31	55	96	76	5	22
Unique Malware	2	1	0	0	1	0

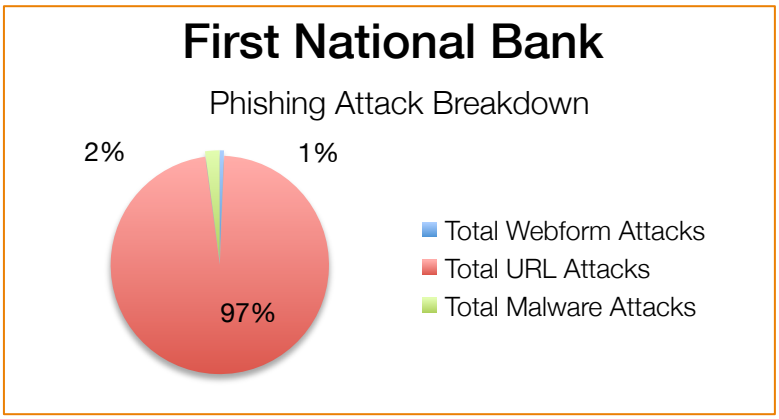
FIRST NATIONAL BANK (FNB)

Recognised as the World's Most Innovative Bank in the 2012 BAI-Finacle Global Banking Innovation Awards, FNB has been on an aggressive branding campaign for a couple of years and this has elevated the bank on the phishing radar.



"Targeted phishing activities keep pace with banks email campaigns. As banks make adjustments to their online presence, and advertise these changes to their clientele, scammers take advantage of these campaigns by directing attacks at banking clients during or shortly after campaigns. The probability of success increases during this uncertain time", explains Darryl.

Banks are most vulnerable during new marketing campaigns

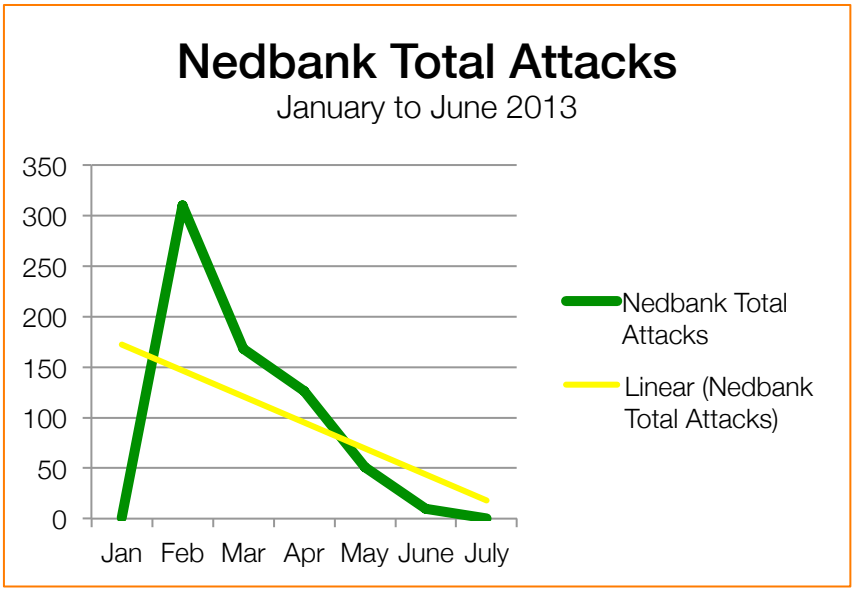


Phishing trends against FNB have been on a steady increase from January to June. However, the year-on-year data comparison reveals that phishing attempts against FNB in 2013 have dropped to 12% of last years 147 525 attempts over the same period. This could be because FNB has slowed down their branding campaigns.

	Jan	Feb	Mar	Apr	May	June
Total Attacks	392	718	5490	5338	5813	623
Total Webform Attacks	0	0	1	106	11	1
Total URL Attacks	61	708	5476	5206	5789	622
Total Malware Attacks	331	10	13	26	13	0
Unique Webforms	0	0	0	3	0	0
Unique URLs	1	3	51	22	6	10
Unique Malware	327	10	13	26	13	0

NEDBANK

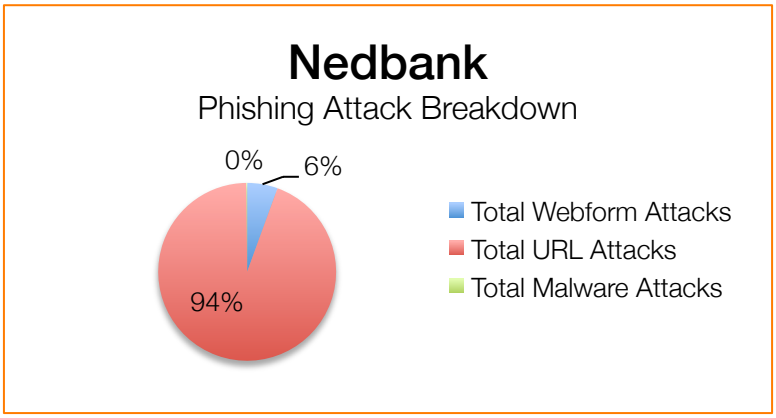
Nedbank is known for being serious about mail and Internet banking security. Last year, the bank launched their advanced Internet banking security feature Approve-it and this focus on security has resulted in a reported 99% decrease in phishing losses for the bank in 2013.



"The phishing statistics for Nedbank confirms the effectiveness of their campaign," confirms Darryl "we don't see a lot of Nedbank phish passing through our Securemail servers, because Nedbank targeted phish are mostly unsuccessful"

Security focus results in a 99% reduction in phishing losses

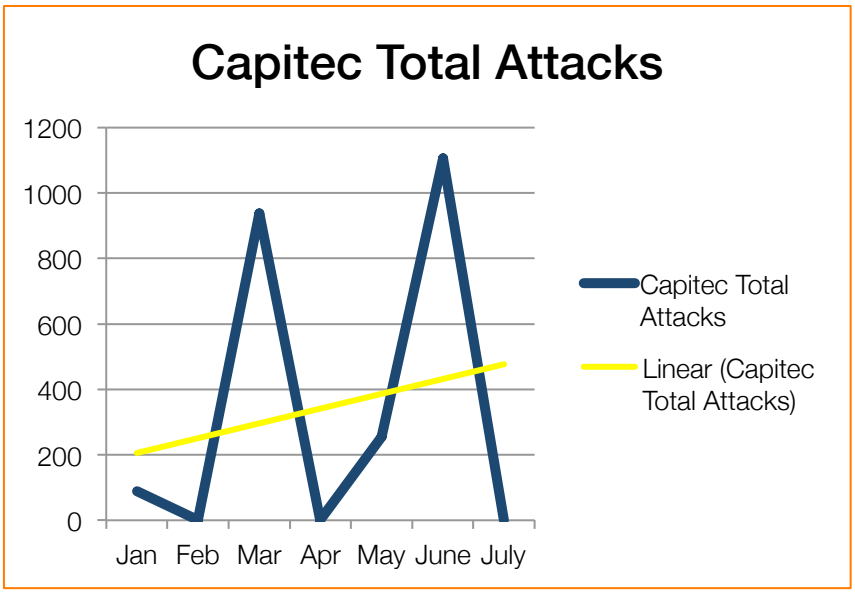
Nedbank has recorded the most significant change in phishing attempts, being exposed to less than 6,8% phishing on last years efforts. While, February was an abnormal month for the bank, with 300 phishing attempts passing through the SYNAQ servers, Nedbank continues to experience a downward trend in phishing activities and represents only 0,17% of recorded phishing activities.



	Jan	Feb	Mar	Apr	May	June
Total Attacks	1	310	168	126	51	10
Total Webform Attacks	0	1	0	0	36	0
Total URL Attacks	1	309	168	126	14	10
Total Malware Attacks	0	0	0	0	1	0
Unique Webforms	0	0	0	0	1	0
Unique URLs	1	1	166	1	1	3
Unique Malware	0	0	0	0	1	0

CAPITEC BANK

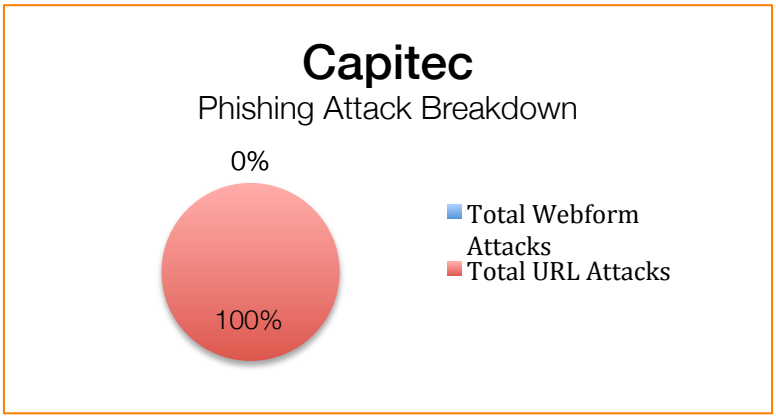
Capitec Bank is the new kid on the banking block and has a relatively small customer market share - compared to the established big four - but this has not protected the bank from being exposed to phishing scammers.



Phishing attempts against Capitec Bank are sporadic and vary month-on-month from zero attempts, to a 46,3% increase in June of 1106 attempts. The overall upward phishing trend mirrors the bank's increasing capture of the banking customer market share.

All phishing attempts against Capitec Bank are in the form of URL attacks

June sees a 46,3% jump in phishing attempts against Capitec

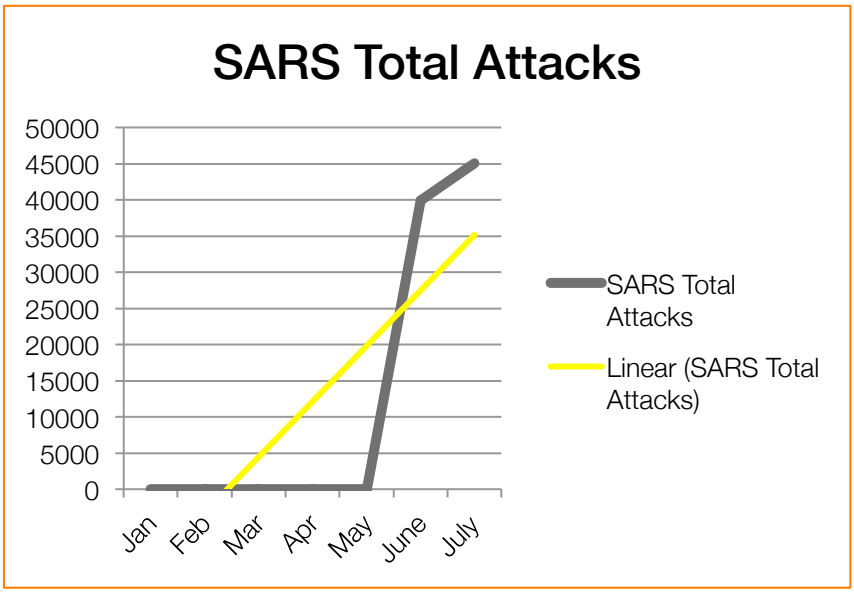


A URL phishing attack, is a form of phishing that requires a user to click on a URL link that directs the user to a false site that appears real but on closer inspection the URL in the browser address bar is not the banks address. The purpose is to capture the users login credentials and use them on the real bank site.

	Jan	Feb	Mar	Apr	May	June
Total Attacks	89	3228	937	0	255	1106
Total Webform Attacks	0	0	0	0	0	0
Total URL Attacks	89	3228	937	0	255	1106
Total Malware Attacks	0	0	0	0	0	0
Unique Webforms	0	0	0	0	0	0
Unique URLs	3	492	92	0	1	3
Unique Malware	0	0	0	0	0	0

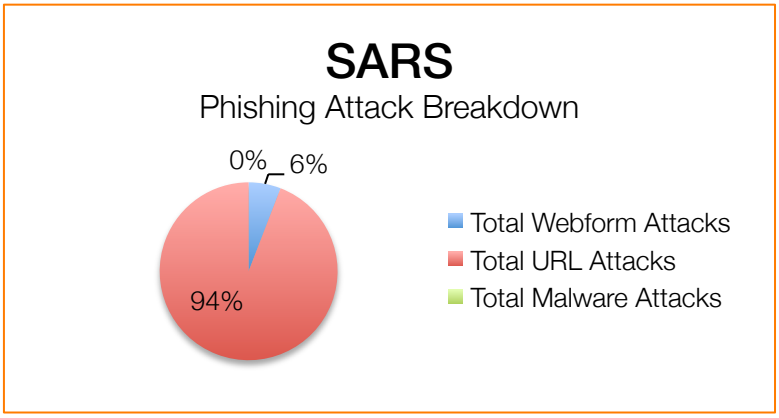
SOUTH AFRICAN REVENUE SERVICES (SARS)

Phishing attacks aimed at The South African Revenue Services have dominated the phishing landscape since the start of the annual tax return season, in May.



While these attacks are recorded against SARS, they are in fact another form of bank phishing, intended to direct the taxpayer to provide their bank and personal account details to the scammer. Unsuspecting taxpayers are sent official looking false "spoofed" emails, claiming they are entitled to a tax refund from SARS.

39,905 phishing attempts in one month



Phishing attacks against SARS are normally attempted through Webform or URL attacks. A Webform attack requires taxpayers to supply their banking details on an embedded email form, the details are then mailed back to the scammer. Alternatively the scammer will attempt to obtain personal bank details via a URL attack, directing the user to a false official looking website and obtaining the users banking details on the fake SARS website.

	Jan	Feb	Mar	Apr	May	June
Total Attacks	0	0	0	0	0	39905
Total Webform Attacks	0	0	0	0	0	2338
Total URL Attacks	0	0	0	0	0	37567
Total Malware Attacks	0	0	0	0	0	0
Unique Webforms	0	0	0	0	0	2
Unique URLs	0	0	0	0	0	123
Unique Malware	0	0	0	0	0	0

39,905 attacks were recorded against SARS in June, 94% of which were in the form of URL attacks.

INTELLECTUAL PROPERTY DISCLAIMER

Information published in this report is based on data vetted and testified by SYNAQ Phishmonger ™, the anti-phishing module of SYNAQ Securemail, and represents phishing activity against South African banks as monitored on the SYNAQ platform.

This report is for informational purposes only and is provided “as is” with no warranties whatsoever including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample.

No license, express or implied, to any intellectual property rights is granted or intended hereby.

SYNAQ (PTY) LTD disclaim all liability, including liability for infringement of proprietary rights, relating to implementation of information in this specification. SYNAQ (PTY) LTD do not warrant or represent that such implementation(s) will not infringe such rights.
Product or company names mentioned herein may be the trademarks of their respective owners.

FOR MORE INFORMATION

For information on SYNAQ Securemail or Phishmonger ™ please visit www.synaq.com or contact SYNAQ on 011 262 3632