Assessing the information quality of phishing-related content on financial institutions’ websites

Rika Butler

School of Accountancy, Stellenbosch University, Stellenbosch, South Africa, and

Martin Butler

Business School, Stellenbosch University, Stellenbosch, South Africa

Abstract

Purpose – Phishing attacks exploit social vulnerabilities and remain a global concern. Financial institutions often use their websites as part of their online awareness and education efforts. This paper aims to explore the effectiveness of phishing-related information made available by financial institutions to raise awareness and educate customers.

Design/methodology/approach – In this mixed methods research, a survey of online consumers was first performed and analysed. Second, the information available on the websites of major financial institutions was analysed. Using the construct of information quality (IQ), content analysis was performed to determine whether the phishing-related information meets the IQ criteria.

Findings – The survey confirmed that consumers are indeed targeted by phishers. It established that they turn to their financial institutions, more often than any other source, for anti-phishing information. When analysing the IQ of phishing-related information, significant deficiencies as well as different levels of performance between the financial institutions, emerged. In general, the worst performing IQ criteria was information being current and fit for purpose.

Research limitations/implications – As the research is conducted within South Africa, the results cannot be generalised. The ethical clearance did not allow for identification of the different financial institutions and thus comparing consumers’ perceptions with the observed IQ from the content analysis to determine correlation.

Practical implications – Protecting consumers against phishing attacks remains critical, and this paper confirms that users turn to their financial institutions for information. Yet, the phishing-related information made available on the websites of financial institutions has severe deficiencies. Practitioners should use IQ to determine the appropriateness of phishing-related information and focus on improving customer awareness and education.

Originality/value – Researchers often highlight the importance of awareness and education programmes in protecting consumers, but rarely investigate if consumers access publicly available information and express an opinion on the quality of this information. Although the results should not be generalised, the recommendations, if necessary through similar analysis, has an impact beyond the geographical constraints of the study.

Keywords South Africa, Phishing awareness, Phishing, Information quality, Online security, Financial security

Paper type Research paper

The extent of the phishing challenge

The prevalence of phishing, which poses a significant risk to Internet security, continues to grow at alarming rates (Gupta et al., 2016). Phishing represents a method of online identity theft, in which cybercriminals attempt to deceive computer users into divulging personal financial information such as passwords and account numbers (Butler, 2007, p. 518).
Symantec’s 2016 Internet Security Threat Report (Symantec, 2016, p. 31) indicates that one in every 1,846 emails sent globally are phishing emails (this excludes directed spear phishing attacks). Furthermore, this report indicates that in 2015, malicious emails grew in number and complexity and remain an effective medium that cybercriminals employ to launch phishing attacks (Symantec, 2016, p. 31).

As first large-scale phishing attacks were launched in 2004 (Gupta et al., 2016, p. 2) and South African online users were targeted for the first time in May 2005 (Butler, 2005, p. 2), phishing attacks have increased in both quantity and sophistication and by 2013 more than 37 million users around the world had been subjected to phishing attacks (Kaspersky Lab, 2013). The latest South African statistics indicate a digital onslaught on South Africa. In January 2016, South Africa jumped from 67th to 22nd position in global cyberattacks (Check Point, 2016). Following this dramatic increase, the South African Banking Risk Information Centre (SABRIC) announced that the South African banking industry is embarking on a national campaign to empower consumers to avoid compromised cybersecurity (SABRIC, 2016).

The 2016 reports of the Anti-Phishing Working Group (APWG), an association committed to reducing phishing, indicate a 65 per cent year on year growth in phishing (Figure 1). It is evident from Figure 1 that although cyclic in nature, there is a clear increasing global phishing activity trend.

Cybercriminals can use the information obtained through successful phishing to either transfer funds from a victim’s account or to commit fraud, including identity theft, when they open accounts or enter into transactions in the victim’s name (Khonji et al., 2013, p. 2092). Cybercriminals are also increasingly taking advantage of social networks, instant messaging and mobile applications to reach potential victims (Symantec, 2016, p. 31).

Phishers target industries “with a heavy volume of monetary transactions” (Bose and Leung, 2014) and as a result the banking and financial services industry is a popular target (Lagazio et al., 2014, p. 59). Phishing emails often claim to come from organisations that are in authorised possession of personal financial information about the victim, such as financial institutions (Butler, 2007, p. 522). About one-third of the brands targeted in

![Number of unique phishing websites](image)

**Note:** graph prepared by authors using figures published by the APWG in their phishing activities trends reports for these periods

Information quality

515
phishing attacks in 2015 and 2016 were from the Financial Services and Payment Services sectors (APWG, 2016).

It is estimated that South Africans loose more than R2 billion annually due to internet fraud and phishing (SABRIC, 2016). Successful phishing attacks can negatively affect both the victim of the attack and the organisation whose brand is targeted (Lagazio et al., 2014, p. 60; Kirlappos and Sasse, 2012, p. 24). Besides suffering financial losses, other negative consequences can include numerous hours that the victim has to spend to resolve the issue, with associated levels of frustration (Butler, 2007, p. 524). The cost of phishing for victim organisations includes direct costs (such as the time spent by employees dealing with the fraudulent transactions and customer support) as well as intangible cost (those associated with brand reputation, decline in customer satisfaction and a loss of customers) (Davinson and Sillence, 2010, p. 1739; Bose and Leung, 2014; LookingGlass, 2016, p. 4).

The need for phishing awareness and knowledge
Cyberattacks can be classified as “syntactic” attacks (which exploits technical vulnerabilities), “semantic” attacks (which exploit social vulnerabilities) or “blended” attacks, where cybercriminals use technical tools to gain access to confidential information (Choo, 2011, p. 724). As phishing represents a blended attack, safeguarding against phishing cannot be achieved through technological measures alone (Vishwanath et al., 2011, p. 576). This is highlighted by Frauenstein and von Solms (2014) and supported by Kirlappos and Sasse (2012), who conclude that improving users’ ability to detect phishing can only be accomplished if aspects relating to the user (the human element) complements other anti-phishing measures (such as technological controls and policies, standards and procedures).

Cybercriminals often exploit the “vulnerable human element” (Frauenstein and von Solms, 2014) when launching phishing attacks (Gupta et al., 2016, p. 3; Khonji et al., 2013, p. 2093). One of the factors that increases users’ vulnerability is a lack of phishing-related awareness and knowledge, which can render them unable to identify phishing attacks (Karakasiliotis et al., 2006; Dhamiya et al., 2006, pp. 582-583; Weber, 2012, p. 63). Users’ behaviour influences computer security and they remain a weak link in the security chain when they are unable to identify a phishing attempt and unknowingly respond (Rhee et al., 2009, p. 817; Davinson and Sillence, 2010, p. 1739).

To improve anti-phishing protection researchers recommend that the human feature be enhanced by means of three distinct matters – security awareness, education and training (Frauenstein and von Solms, 2014; Kirlappos and Sasse, 2012). Awareness aims to attract users’ attention to the phishing problem and helps them to realise their vulnerability, while education efforts intend to equip users with phishing-related knowledge to inter alia assist them in identifying a phishing attack (Kirlappos and Sasse, 2012, p. 30). Training efforts test users’ understanding of the communicated information and correct any misconceptions and extends wider than mere awareness and education (Kirlappos and Sasse, 2012, p. 30).

Studies have confirmed that awareness, education and training efforts can improve users’ behaviour and their susceptibility to phishing attacks (Jansson and Von Solms, 2013, p. 591; Downs, Holbrook and Cranor, 2007, p. 42, Kumaraguru et al., 2007; Sheng et al., 2010; Kruger et al., 2010). If users are more informed about potential threats, more knowledgeable about phishing detection and more proficient in identifying phishing attacks, it reduces the incidence of successful phishing attacks and improves security (Frauenstein and von Solms, 2014, p. 1; Sarel and Marmorstein, 2006, p. 105).

Anti-phishing awareness, education and training initiatives are thus important for organisations often targeted by cybercriminals – such as financial institutions. Financial institutions plays an important role in online security education of their employees as well
as their customers, who are potential phishing victims (Aloul, 2012, p. 181; Redlinghuis and Rensleigh, 2010, p. 6; Purkait, 2012, p. 406). These include informing customers about security threats such as phishing (Purkait, 2012, p. 406).

Most, if not all, financial institutions have an online presence that serves as a major channel of communication with their customers and enables business transactions (Van der Merwe and Bekker, 2003, p. 330; Bose and Leung, 2008, p. 899). Financial institutions often employ their websites as part of their education and security awareness efforts (Redlinghuis and Rensleigh, 2010, p. 5). The quality of phishing-related information that financial institutions make available on their websites is critical to create both awareness of the risk and conveying knowledge to educate online banking users. When effective, this information will reduce user’s susceptibility to phishing, improve users’ ability to identify attacks and assist them to act appropriately to limit negative consequences.

Information quality
To measure the quality of information numerous authors have investigated, developed frameworks and attempted to define information quality (IQ) (Wang and Strong, 1996; Lee et al., 2002). IQ is however a multi-dimensional concept whose attributes will vary based on the philosophical point of view of the author concerned (Knight and Burn, 2005, p. 160). Knight and Burn (2005) analysed IQ and identified and defined the 20 most common IQ dimensions used in research studies (Appendix 1).

Researchers agree that IQ is context-sensitive and that it cannot be described, measured or assured using a single model (Stvilia et al., 2008). IQ needs to be assessed within the context of its generation and its intended purpose or use (Knight and Burn, 2005, p. 162). Thus, expressing an opinion on the IQ of phishing-related information needs to be contextualised for the particular objective.

Problem statement and objective
Although financial institutions frequently use their websites to display information about cyber-related threats, the “actual effectiveness” of this information is uncertain (Redlinghuis and Rensleigh, 2010, p. 6). The primary research question (PRQ) of this study is whether the phishing-related information on the websites of South African financial institutions is fit for purpose, i.e. improves awareness about the risk of phishing and provides relevant information to educate users about phishing.

For researchers, a move beyond the domain on internally-focussed security awareness, education and training programmes, which are very well covered in academic literature, is important. Using the attributes of IQ to assess the effectiveness of phishing-related information on financial institutions’ websites could provide valuable new insights for future research on cyber security using a contextualised IQ construct.

The results of this study will prove useful to financial institutions and SABRIC, who design and implement phishing-related awareness, education and training initiatives in South Africa. Identifying deficiencies in the levels of effectiveness of phishing-related information could assist organisations concerned in designing more appropriate content and mechanisms to improve phishing awareness and educate online consumers to prevent successful phishing attacks.

Research questions and methodology
The PRQ aims to determine whether phishing-related information provided on the websites of South African financial institutions are fit for purpose. To answer the PRQ four research questions (RQ) were formulated (Table I).
As this study aims to determine and examine online banking users’ awareness and education on phishing and not to measure, a qualitative research design was adopted. However, a combination of research methods was deemed appropriate to answer the research questions (Table I). These methods included developing a contextualised model from IQ literature, a survey among the users on online financial services as well as analysing the content of the phishing-related information published on the websites of South African financial institutions (content analysis).

**Appropriate information quality model**
A contextualised IQ model, which could be used to determine the quality of phishing-related information, was developed using the IQ dimensions found in literature. Not all of the dimensions of IQ identified by Knight and Burn (2005) and listed in Appendix 1 are applicable when assessing the quality of phishing-related information available on the websites of financial institutions. Using the context of phishing-related information and the display thereof on websites, a list of IQ dimensions at a higher level of granularity was developed from Appendix 1. Table II summarises the five IQ dimensions, as well as the contextualised description of each attribute, as it relates to this study.

Given that the information to be assessed is published on the websites of trusted entities, the intrinsic IQ attributes (accuracy, consistency, reliability, objectivity, believability and reputation) were not included in the analysis. Similarly, as security controls were not assessed, the attribute security was not included in this study.

**User exposure and information perception (RQ1, RQ2 and RQ3)**
The use of surveys is regarded as an appropriate research method when researching human computer interaction (Ozok, 2009, p. 1152). A survey, containing questions about consumers’ phishing exposure (RQ1), methods used to obtain phishing information (RQ2) and their perception of the quality of phishing information (RQ3) was designed, pilot tested and validated. The survey was designed based on instruments developed by Liang and Xue (2010) and Arachchilage and Love (2014). Although the instruments were updated for phishing, the constructs developed by Liang and Xue (2010) and Arachchilage and Love (2014) were respected.

To prevent participants from becoming more suspicious (increasing their security-consciousness) when answering the survey and creating bias (Parsons et al., 2015),

<table>
<thead>
<tr>
<th>Research question (RQ)</th>
<th>Method used to answer research question</th>
</tr>
</thead>
<tbody>
<tr>
<td>RQ1 Extent of exposure</td>
<td>Are South African online consumers exposed to email phishing attacks and the associated negative consequences? Survey of online users to determine exposure</td>
</tr>
<tr>
<td>RQ2 Sources of information</td>
<td>What are the sources of anti-phishing information used by South African online consumers? Survey of online users to determine sources of information</td>
</tr>
<tr>
<td>RQ3 Perceived phishing IQ</td>
<td>What is users’ perception of the quality of phishing information available on websites? Survey of online users to determine perceived IQ</td>
</tr>
<tr>
<td>RQ4 Measured phishing IQ</td>
<td>What is the measured quality of the phishing information on the websites of financial institutions? Content analysis of websites to determine IQ deficiencies</td>
</tr>
</tbody>
</table>

Table I. Research questions and methodology

ICS 518
participants were not informed that this was a “phishing” study. Instead, the survey was attached to an article on the increased level of cyberattacks experienced by South Africans, explaining how the new South African Cybercrimes and Cybersecurity Bill will attempt to address the risks posed by threats such as phishing. Respondents could click on a hyperlink that appeared below the article to take part in the online survey.

The online survey was refined via two iterations of pilot testing, first with academic experts to check for construct validation and secondly with online consumers in a focus group to ensure clear statement of questions and no forced answers. The survey contained 17 questions that included both structured and open-ended questions and used a four- and five-point Likert scale, respectively. Besides demographical information, the survey also contained questions to determine respondents’ phishing awareness and knowledge levels. Participants were also asked about phishing-related information provided by their financial institutions. A total of 177 respondents started the survey but 26 exited the survey, leaving 151 completed responses for analysis.

The respondents who took part in the survey represented customers from 10 different financial institutions. Less than 7 per cent of respondents preferred not to disclose which financial institutions’ online banking facility they use. The top six institutions indicated were FNB (30.9 per cent), ABSA (25.3 per cent), Standard Bank (25.3 per cent), Investec (17.4 per cent) Nedbank (11.2 per cent) and Capitec (7.9 per cent). As these represent the major retail banks in South Africa, they were used in the analysis.

**Measured phishing information quality (RQ4)**

Content analysis was used to assess the phishing-related information available on financial institutions’ websites, using the IQ construct to measure the extent to which these institutions provide quality information to increase phishing awareness and educate users. Content analysis is a research technique that can be used to analyse the content of observable communication whether in written, verbal or electronic format (Sarel and Marmorstein, 2006, p. 107). The “content” can refer to aspects such as words, pictures, symbols or any message that can be communicated (Mouton, 2001, p. 165).

Hsieh and Shannon (2005) explain that a summative content analysis involves counting and comparisons, usually of keywords or content, followed by the interpretation of the
underlying context. This method was deemed appropriate to analyse some of the more complex constructs. The technique has previously been applied to research on financial services industry websites to assess privacy statements (Kabanda et al., 2010) as well as corporate social responsibility communication (Boateng, 2016; Sujana, 2015; Branco and Rodrigues, 2006).

The five dimensions of IQ defined in Table II were assessed for the six financial institutions indicated by survey respondents, using the measures defined by the authors and described in Appendix 2. Clarity (the IQ dimension Clear) proved challenging and required moving beyond coding for conditions. Hence it was decided to use the Flesch Reading Ease Score, a well-known measure used to determine readability – i.e. the ease or difficulty of comprehending written material (Sallis and Kassabova, 2000, p. 48). The Flesch Reading Ease method’s use has been validated as reliable by various authors (Singh et al., 2011; Paasche-Orlow et al., 2003). It has been used in various fields of study, including to assess the readability of email messages (Sallis and Kassabova, 2000) and privacy policies on websites (Singh et al., 2011; Proctor et al., 2008), including those in the financial services industry (Kabanda et al., 2010). This score was calculated for the phishing-related information that appears on each website as a measure to assess the IQ dimension Clear.

Limitations of study
This study assesses the quality of phishing-related information on financial institution’s websites. No technological security measures implemented by financial institutions as anti-phishing measures or otherwise, nor the protection of communication and transactions between financial institutions and their online banking customers, were assessed.

Although effective anti-phishing education include three distinct steps, namely awareness, education and training (Kirlappos and Sasse, 2012), this study only assesses aspects related to awareness and education and does not test whether users are able to apply their phishing-related knowledge to successfully distinguish email phishing attacks and react appropriately (i.e. training).

Finally, making a comparison between specific financial institutions and responses from online banking customers fell outside the scope of the research for which ethical approval was obtained. This could represent an area for further research.

Research ethics
Ethical clearance for the research was obtained from the researchers’ academic institution. All data were treated as sensitive and no respondent was identified or any banking account number or password collected during the study. To ensure anonymity, the six financial institutions used in the analysis were merely identified as Banks A-F in the sections where the results of the study are discussed.

Research results
Extent of exposure (RQ1)
It is evident that respondents have been exposed to email phishing attacks as almost 75 per cent of respondents indicated that they had “definitely” received such emails. However, not all respondents were able to distinguish email phishing attacks as 15.5 per cent indicated that they had “possibly” received such emails and 7.7 per cent indicated “I don’t think so” when asked if they have ever received a phishing email.

While almost 62 per cent of respondents were sure that they had definitely not responded to phishing emails, almost 5 per cent have definitely responded, while almost 34 per cent were uncertain (Table III). This “uncertain”-trend among respondents was also evident.
when asked about their reaction to and experience with the consequences of successful phishing attacks (Table III). More than 5 per cent have “definitely” had their personal information compromised and 6 per cent have “definitely” suffered losses as a result of phishing.

Encouragingly respondents view the consequences of successful phishing attacks in a serious light. More than 80 per cent understood and “strongly agreed” or “agreed” that phishing poses a danger to their personal information. While 71.9 per cent “strongly agreed” that it would be severely damaging if their personal information was compromised via phishing, another 21 per cent “agreed” with this statement. When asked how they would rate the impact of a number of other phishing-related consequences, “devastating” was the response from the majority of the respondents (Table IV).

These results serve to indicate that there are high levels of awareness of phishing among South African online consumers as well as a clear appreciation of the negative consequences associated with it. As users seem to realize their vulnerability, this awareness should contribute to reduce the success of phishing attacks (Kirlappos and Sasse, 2012, p. 30; Gupta et al., 2016, p. 3).

Concerning is respondents’ perception about their financial institution’s liability in case of successful phishing attacks. The Banking Association South Africa’s Code of Banking Practice 2012 determines that banking customers may be held liable for losses if they acted negligently or without reasonable care (such as disclosing personal information like account numbers, passwords and PINs) and this has caused or contributed to losses suffered (The Banking Association South Africa, 2012). Yet, almost 30 per cent of the respondents to this study “strongly agreed” or “agreed” that their financial institutions will be fully liable for losses that they may personally suffer as a result of phishing (Figure 2).

This incorrect perception among online users may potentially contribute to users underestimating the seriousness of this threat and the potential financial implication it could hold for them personally should they become victims of successful phishing attacks. In

<table>
<thead>
<tr>
<th>Responded to phishing email</th>
<th>Yes, definitely (%)</th>
<th>Uncertain (%)</th>
<th>Definitely not (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Had personal information compromised due to phishing</td>
<td>4.2</td>
<td>33.9</td>
<td>61.9</td>
</tr>
<tr>
<td>Suffered losses as result of phishing</td>
<td>5.4</td>
<td>44.1</td>
<td>50.6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accounts are opened and online purchase made in your name</th>
<th>Not serious at all (%)</th>
<th>Moderately serious (%)</th>
<th>Serious (%)</th>
<th>Deva-stating (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access is gained to your bank account number and or credit card number</td>
<td>1.2</td>
<td>3.0</td>
<td>35.1</td>
<td>60.7</td>
</tr>
<tr>
<td>Your online banking username and password are compromised</td>
<td>0.6</td>
<td>4.2</td>
<td>19.0</td>
<td>76.2</td>
</tr>
<tr>
<td>Your internet bank settings (account limits/notifications) are changed</td>
<td>0</td>
<td>1.2</td>
<td>19.0</td>
<td>79.8</td>
</tr>
</tbody>
</table>

Table III. Respondents’ exposure to phishing attacks

Table IV. Respondents’ view of consequences associated with phishing
addition, it may make users less security-motivated and contribute to users who underestimate the necessity to acquire and apply anti-phishing knowledge.

**Sources of information (RQ2)**

More than 86 per cent of respondents “strongly agreed” or “agreed” that phishing-related knowledge is crucial to detect phishing emails. Despite this, almost 35 per cent of respondents “agreed” or “strongly agreed” that they do not know where to obtain phishing knowledge and less than 14 per cent of the respondents felt confident that they know the tell-tale signs of phishing and would be able to successfully identify a phishing attack. As there is a direct correlation between relevant anti-phishing knowledge and the success of phishing attacks (Karakasiliotis et al., 2006; Dhamija et al., 2006, pp. 582-583; Weber, 2012, p. 63), not possessing the relevant knowledge may make users more vulnerable.

Financial institutions’ websites and communication from financial institutions were indicated as the primary sources of phishing-related information among respondents (Figure 3), confirming the relevance of this research to determine the quality of the information deemed as users’ most important source of phishing knowledge. Their own voluntary research as well as conversations with friends, family and colleagues were also regarded as main sources of phishing knowledge. Television and radio discussions and infomercials, pamphlets and posters did contribute “some” or “very limited” information or made no contribution to respondents’ knowledge levels.

**Perceived phishing IQ (RO3)**

Although respondents use various sources to obtain phishing knowledge (Figure 3), a major constraint is that not all online users know where to acquire phishing-related information (Figure 4). This deficiency relates to the IQ dimensions of availability and accessibility. Relevant information can either be available or not be readily accessible – i.e. it may be available on the websites of financial institutions, but users do not know where to find it.

Importantly, anti-phishing material can only be effective in reducing successful phishing attacks “when users actually read them” (Sheng et al., 2010, p. 374). Studies have found that users seldom seek out education materials and that they tend to ignore communication recommending that they read these materials (Kumaraguru et al., 2010, p. 5). However, reading also relates to the IQ dimensions Clear and Purposeful – unless the message is clear, reading it will not improve awareness and educate users.

Almost 65 per cent of respondents indicated that they have previously read phishing information made available by their financial institutions. The top motivations were to learn more about the issue of phishing (76.5 per cent) because they regard computer security as important (71.4 per cent) and because they thought that the information “might come in
handy one day” (67.4 per cent). Almost 45 per cent of respondents indicated that they have read this information as people they know have been phishing victims or because they have personally been victims of phishing (11.2 per cent).

However, it is clear that not all respondents use the potential valuable source of information provided by their financial institutions. More than 35 per cent of respondents indicated that they have not read the phishing-related information made available by their financial institutions. Reasons for this included that financial institutions do not provide such information, that it is too time-consuming and too much to read, that it looked too technical and complicated and that users felt that they “already know what there is to know” about phishing and that the information was “not applicable” to them. They did not find the information really effective in increasing their knowledge and ability to enable them to avoid becoming phishing victims. These deficiencies could relate to any of the IQ dimensions available, accessible, clear and purposeful as used in this study.

As cybercriminals continuously find new methods and techniques of attack (Choo, 2011, p. 725), it was encouraging to note that respondents seem to understand the importance of updating anti-phishing knowledge regularly. More than 85 per cent of the respondents “disagreed” or “strongly disagreed” with the statement that updating anti-phishing knowledge regularly is not very important. The anti-phishing knowledge that respondents...
have obtained also made them more security-conscious, as 37.8 per cent “strongly agreed” and 51.7 per cent “agreed” that it made them more careful when reacting to emails. These results support the concept that increased knowledge levels increases users’ motivation to behave more securely (Sheng et al., 2010; Kruger et al., 2010; Wang, 2013).

Despite the majority of the respondents indicating that “my financial institution’s website” was their primary source of phishing-related information (Figure 3), some users remain largely uncertain about the availability and nature of phishing-related information on their financial institution’s website (Table V). This uncertainty could stem from deficiencies in any of the five IQ dimensions used in this study and required further scrutiny.

**Quality of phishing-related information available on website (RQ4)**

The quality of phishing-related information available on the websites of financial institutions was assessed for each of the IQ dimensions defined in Table II, using the measures explained in Appendix 2. Figure 5 contains the quantified comparison between the five dimensions of IQ for the six financial institutions as measured.

<table>
<thead>
<tr>
<th>Table V. Respondents’ perception of phishing-related information on websites of their financial institutions</th>
<th>Yes (%)</th>
<th>Not sure or don’t know (%)</th>
<th>No (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines/describes what phishing is</td>
<td>61.6</td>
<td>35.8</td>
<td>2.6</td>
</tr>
<tr>
<td>Describe the tell-tale signs of a phishing attack</td>
<td>53.0</td>
<td>43.0</td>
<td>4.0</td>
</tr>
<tr>
<td>Tells me how to react when I receive a phishing attack</td>
<td>53.0</td>
<td>41.7</td>
<td>5.3</td>
</tr>
<tr>
<td>Provide examples of what phishing looks like</td>
<td>40.7</td>
<td>50.7</td>
<td>8.6</td>
</tr>
</tbody>
</table>

**Figure 5.** Information quality of phishing-related content on the websites of financial institutions
Except for the IQ dimension of Available, deficiencies concerning all four the other IQ dimensions measured (Accessible, current, clear and purposeful), were noticed for all six financial institutions. Clear variances in the performance of the different financial institutions were also evident. Although all the financial institutions addressed availability, the overall performance of one particular financial institution (Bank B) was significantly better for all the other dimensions of IQ (Figure 5). The worst performing IQ dimensions were current and purposeful. Two financial institutions (Bank C and Bank D) scored the lowest overall scores in all dimensions of IQ.

Available. Being the industry whose brands are most targeted in phishing attacks (APWG, 2016; Lagazio et al., 2014, p. 59) and their websites representing the primary source of phishing information used by online consumers (Figure 3), clearly places an obligation on financial services institutions to have phishing information available. Availability was the easiest dimension of IQ to establish. From the analysis it was evident that phishing information is indeed available on the normal online portal used by customers for all six financial institutions. This is in contradiction to users’ uncertain perception about the availability of phishing information on their financial institutions websites (Table V).

Accessible. Beside users not being sure about the content available on the websites (Table V), almost 35 per cent of respondents “agreed” or “strongly agreed” that they do not know where to obtain phishing information (Figure 4). One of the reasons may be that users have trouble in accessing this information due to its lack of prominence on the website.

According to Sarel and Marmorstein (2006) some financial institutions follow “a low-key approach” concerning security issues on their websites and only make security-information available deeper on their websites for customers who search for this information in particular, while others are “more direct and upfront” about security and may put such information on their website landing page. When measuring both the depth (number of clicks) and prominence and ease of access via cross-posting, there was indeed a significant difference between the different financial institutions. Inconsistencies in the levels of accessibility of information made available by the different financial institutions were noted. At least two of the financial institutions (Bank D and Bank F) performed significantly below the norm, with information being difficult to access unless a user knows exactly where to search for phishing-related information or follow a very specific sequence of clicks from the landing page to get to that information.

Current. As it establishes relevance, information being current (such as links to events in popular media, for example) can be an important “tool” to convince users that it is in their best interest to access, read and apply the information. If users are more informed about current security threats and the latest avenues of attacks this could improve awareness and highlight users’ need for education.

By analysing whether the most recent phishing-related information, including examples of the latest phishing attacks, variations on ordinary phishing (such as spear-phishing) and links to major security events are mentioned in the information, an assessment of whether the information is current was made. This dimension was the single worst performance area for IQ for all the financial institutions. By not using recent examples and links to well-known security breaches covered in popular media, financial services institutions are clearly missing a key factor in the anti-phishing awareness and education space. Significant room for improvement exists on this dimension for five of the six financial institutions analysed.

Clear. Supported by analysing the content to ensure it is not unnecessarily unwieldly (will not be read in full), the Flesch Reading Ease Score was the basis for the analysis of this IQ dimension. Across all financial institutions, the information on the websites was mostly
Some financial institutions' information was however found to be slightly more cluttered than others by, for example, using embedded scrolling. The higher the Flesch Reading Ease score, the easier the text is regarded to be read and understood. The Flesch Reading Ease scores for the financial institutions varied between 43.1 and 53, which, although not regarded as easy to read, would be readable by online banking customers. Taking into account that phishing is a rather complex concept, financial institutions should take care to make this complex concept understandable to users in text that is easy to read and not too technical or complicated.

**Purposeful.** The IQ dimension of Purposeful was analysed on two different levels, assessing whether the content displayed on the website would raise awareness about phishing and determining whether the information have educational value in that there are clear calls for action and instructions on what to do if users receive or have responded to an email phishing message. This would include ways to report phishing and contact their financial institution should their details have been compromised.

On average, the financial institutions did not perform very well in this analysis. This supports user’s perceptions about the purposefulness of phishing information. While more than 60 per cent of respondents indicated that their financial institutions defined or described what phishing is, almost 50 per cent were unsure or indicated that their financial institutions do not provide education by describing the tell-tale signs of a phishing attack and telling them how to react when they receive a phishing attack (Table V). Two financial institutions (Bank C and Bank D) however stood out in particular as not nearly achieving the intended purpose by mostly failing on both of the sub-dimensions tested.

**Conclusion and recommendations**

Phishing poses a significant threat to online computer users and can have severe negative consequences for both online users and organisations, such as financial institutions, whose brands are often targeted in such attacks. This study found that although South African users are exposed to email phishing attacks there is a lack of anti-phishing knowledge among online banking users, which increases their vulnerability to email phishing attacks. In addition, this study found that users often underestimate the threat that phishing poses to their personal financial information and the possible associated financial liability. Underestimating the phishing threat or the liability for losses in case of successful phishing could further increase users’ susceptibility.

Education and awareness about risks such as these are crucial to make users aware of security threats they may be exposed to and to improve security-consciousness and knowledge, resulting in more secure behaviour. Studies have confirmed that awareness and education initiatives can improve users’ ability to not become phishing victims (Frauenstein and Von Solms, 2014; Kirlappos and Sasse, 2012). It is recommended that financial institutions design appropriate interventions specifically aimed at reducing phishing and use appropriate mediums of communication to deliver these “messages” to the correct target audience groups. However, Furnell (2008, p. 9) warns against a “build it and they will come” approach. Further research therefore needs to be conducted to align the message with the medium and audience demographics. Various mediums such as emails, flyers, discussions on radio and television as well as advertisements on radio, television and billboards can for example be used to bring across tailored educational messages.

Although the websites of financial institutions are the major source of anti-phishing knowledge among South African users, users often do not read this information. Anti-phishing information can only be effective if users actually read the information (Sheng et al., 2010, p. 374). Given the significance of the threat, financial institutions should make
more effective use of existing communication with customers, by for example making the relevant information more accessible and easier to understand when placed on existing communication artefacts. Furthermore, it is recommended that financial institutions increase their efforts to ensure that customers do read this information, by for example using an acknowledgement indicator, a common practice in the online space. Multi-factor acknowledgment, using for example mobile devices to both prompt and acknowledge reading, will ensure closed loop communication to customers. Financial institutions should also ensure that the information made available stays current by including relevant information on the latest security threats, including the tell-tale signs of such attacks and how to prevent falling victim.

Financial institutions in South Africa differ in the quality of phishing-related information that they make available. A discrepancy between users’ perceptions on what is available on websites and the actual information available was evident. While all major financial institutions did indeed make phishing information available on their websites, they vary in the accessibility, currency, clarity and purposefulness of their anti-phishing information. Except for availability, the websites of all major financial institutions displayed deficiencies in all other dimensions of IQ for phishing information.

While continuous educational efforts by financial institutions are necessary to improve online security (Sarel and Marmorstein, 2006, p. 104), user education and awareness alone is not sufficient to address the phishing problem (Khonji et al., 2013, p. 2114). Given the magnitude of the challenge, it is recommended that inter-institutional structures, such as SABRIC, be used to a greater extent in the process to educate South African online banking customers, using pooled resources. Parties responsible for designing phishing-related awareness and education initiatives in South Africa, such as financial institutions and SABRIC, should take note of the findings of this study to improve the effectiveness of phishing awareness and training efforts. Deliberate and committed efforts to educate consumers will reduce the number of successful email phishing attacks, improve computer security in South Africa and reduce the cost of phishing.

References


Appendix 1

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accuracy</td>
<td>Extent to which data are correct, reliable and certified error free</td>
</tr>
<tr>
<td>Consistency</td>
<td>Extent to which information is presented in the same format and compatible with previous data</td>
</tr>
<tr>
<td>Security</td>
<td>Extent to which access to the information is restricted appropriately to maintain its security</td>
</tr>
<tr>
<td>Timeliness</td>
<td>Extent to which information is sufficiently up-to-date for the task at hand</td>
</tr>
<tr>
<td>Completeness</td>
<td>Extent to which information is not missing and is of sufficient breadth and depth for the task at hand</td>
</tr>
<tr>
<td>Concise</td>
<td>Extent to which information is compactly represented without being overwhelming</td>
</tr>
<tr>
<td>Reliability</td>
<td>Extent to which information is correct and reliable</td>
</tr>
<tr>
<td>Accessibility</td>
<td>Extent to which information is available, or easily and quickly retrievable</td>
</tr>
<tr>
<td>Availability</td>
<td>Extent to which information is physically accessible</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Extent to which information is unbiased, unprejudiced and impartial</td>
</tr>
<tr>
<td>Relevancy</td>
<td>Extent to which information is applicable and helpful for the task at hand</td>
</tr>
<tr>
<td>Useability</td>
<td>Extent to which information is clear and easily used</td>
</tr>
<tr>
<td>Understandability</td>
<td>Extent to which data are clear without ambiguity and easily comprehended</td>
</tr>
<tr>
<td>Amount of data</td>
<td>Extent to which the quantity or volume of available data is appropriate</td>
</tr>
<tr>
<td>Believability</td>
<td>Extent to which information is regarded as true and credible</td>
</tr>
<tr>
<td>Navigation</td>
<td>Extent to which information are easily found and linked to</td>
</tr>
<tr>
<td>Reputation</td>
<td>Extent to which information is highly regarded in terms of source or content</td>
</tr>
<tr>
<td>Usefulness</td>
<td>Extent to which information is applicable and helpful for the task at hand</td>
</tr>
<tr>
<td>Efficiency</td>
<td>Extent to which data are available to quickly meet the information needs for the task at hand</td>
</tr>
<tr>
<td>Value-added</td>
<td>Extent to which information is beneficial, provides advantages from its use</td>
</tr>
</tbody>
</table>

Source: Knight and Burn (2005, p. 162)
Appendix 2

<table>
<thead>
<tr>
<th>IQ Dimension</th>
<th>Measure used for assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Available: Information on phishing is available on the website. Mute: Phishing is not mentioned/discussed on the website.</td>
</tr>
<tr>
<td>Accessible</td>
<td>Prominent: The word 'Phishing' appears on the landing page of the website. Non-prominent: For non-prominent accessibility, a count of the number of clicks required to reach 'Phishing' information was performed.</td>
</tr>
<tr>
<td>Current</td>
<td>Information concerning the latest phishing incidents/attacks are provided by either including the topics used in the latest phishing emails scams or providing examples of recent phishing emails.</td>
</tr>
<tr>
<td>Clear</td>
<td>Information is clear, easy to understand and does not contain lengthy texts, crowded and cluttered information and too many links. In addition, the Flesch Reading Ease score was calculated for the phishing information that appears on the website.</td>
</tr>
<tr>
<td>Purposeful</td>
<td>To assess awareness it was determined whether the website contains the following: Describes what phishing is. Explains the consequences of successful phishing attacks. Provides an indication of the magnitude of the problem. To measure the information's educational value it was determined whether the following were indicated on the website: Describe the tell-tale signs of a phishing attack. Warns that the bank won’t ask for sensitive personal information in emails. Advise users what not to do (eg. not to click on links in emails) and what action to take (eg. reporting). An option to report phishing (eg. email address, hotline number).</td>
</tr>
</tbody>
</table>

Table AII. Measures used to assess the quality of phishing-related information

Corresponding author
Rika Butler can be contacted at: rbutler@sun.ac.za

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm Or contact us for further details: permissions@emeraldinsight.com