Phishing in the System of Systems Settings: Mobile Technology

Alta van der Merwe
School of Computing
University of South Africa
Pretoria, South Africa
vdmeraj@unisa.ac.za

Remzi Seker
Computer Science Department
University of Arkansas at Little Rock
Little Rock, Arkansas, U.S.A
rxseker@ualr.edu

Aurona Gerber
School of Computing
University of South Africa
Pretoria, South Africa
gerbeaj@unisa.ac.za

Abstract - *The immense growth in mobile technology has opened various opportunities, both in marketing and in M-Commerce applications. The growth in these applications is according to the system of systems concept through which technologies such as cell phone networks are becoming integrated with other systems such as the Internet. Unfortunately, this may also lead to a new security risk, the use of mobile technology, more specifically the distribution of Short Message Service (SMS) messages, to conduct phishing attacks. We demonstrate four types of phishing activities that can take place via mobile technology and provide a specific example on one of the introduced types.*

Keywords: Phishing, Security risk, mobile phishing, mobile security risk.

1 Introduction

According to the 2004 CSI/FBI Computer Crime and Security Survey [1], the unauthorized use of computer systems is on the decline in the USA. This may be true for reported intrusions, but a significant growth may be experienced in unreported intrusions, especially the intrusions related to financial institutions as reporting intrusions may lead to negative publicity.

The growth in the use of the Internet and the World Wide Web has lead to new types of security risks. From the moment a business obtains a web presence, there is the potential for the business systems in the organization to be exposed to security and confidentiality breaches across the entire Internet [2]. Any link to the Internet makes the business vulnerable and creates a potential intrusion risk.

Historically most of the crimes committed over the Internet were either the result of curiosity or malicious technical attack, performed by *crackers*. A *cracker* is the person who breaks security on a system. The immense growth of the Internet population using financial applications led to the introduction of two other computer criminals, called *spammers* and *fraudsters* [3]. Spam is defined as "Unsolicited commercial e-mail messages" [4] and is created by a spammer. Fraudsters are people involved in Internet fraud, a practice used by individuals who spam potential victims. These criminals cause significant damage to different role players. In 2003 alone, there were more than 200 million dollars of personal losses due to fraudulent intrusions [5]. In recent years spammers and fraudsters were joined by phishers. A phisher is involved in a fraud activity called phishing or spoofing, where phishing is defined as luring of sensitive information and *spoofing* is creation of a replica of an existing web page to fool a user into submitting personal, financial, or password data [4].

Phishing was first reported when America Online users were lured in the mid 1990's by phishers to part with their user names and passwords. One intrusion technique used by phishers is the deployment of worms [6]. The W32.Mimail.I and W32.Mimail.S worms attempted to fool users into handing over credit-card information while posing as either a PayPal application or Microsoft Windows expiration notice [3].

Based on the monthly report issued by the Anti-Phishing Working Group [7] for the month of May 2004, 1,197 unique phishing attacks were reported to the anti-phishing organization. The organization that was targeted the most was Citibank with 370 attacks. eBay South Africa was targeted in July 2004. A database was discovered with more than 1,000 active logins, passwords and credit card information that could be used to purchase items on eBay's site [8]. These kinds of attacks are categorized as *identity theft* [9], where the phisher after stealing the personal information, uses this information for account takeover or application fraud [10].

There are various guidelines for prevention of phishing attacks. The Anti-Phishing Working Group [7] frequently publishes reports on phishing activities. Victims of identity theft may use the APWG's web-site to report phishing attacks. The newest strategy that financial services implement in prevention of phishing attacks is the verification of financial transactions via mobile technology. The financial institution will send a unique code to the user of the account, which must be entered together with the transaction for verification purposes [11]. The problem with

this strategy is the cost involved with each transaction verification for the financial institution [12]. Sending one SMS may be reasonable, but sending thousands of messages on a daily basis will add to the expenditure of a financial institution and may not be feasible for small transactions.

Traditionally, Short Message Service (SMS) communication was limited to personal communication between two mobile phone users. However, SMS technology is no longer limited to personal communication between two users only. A report published by Ovum [13] predicts that by 2005, twenty percent of all Internet advertising will be wireless. The benefit businesses see in sending SMS' to potential customers is even if it is more expensive. For an SMS recipient, this kind of marketing is not easy to ignore.

Using mobile technology for marketing purposes is closely related to M-Commerce, which refers to all forms of e-commerce that take place when consumers make online purchases using mobile devices. It is already possible to use a mobile phone to pay for parking services [14] or to transfer money from an existing contract phone to a pre-paid phone [15].

Using SMS technology for financial transactions and marketing purposes introduce a number of security risks. Due to increasing publicity of spamming and phishing victims and advancing spam filters, the risk of being a victim of an *e-mail* phishing activity is decreasing. The average user is getting more careful about clicking links included in incoming e-mails. We do believe that phishers, sooner or later will utilize SMS based phishing activities to keep their fraudulent activities continuing. One of the reasons that SMS can be a powerful tool in phishing activities is that SMS is still perceived as a more personal medium of communication when compared to e-mail. The main goal of this paper is to warn the stakeholders about two possible phishing activities and start the first steps towards preparing against phishing activities that can take place via SMS.

The paper is structured as follows: In section 2, we give a brief introduction to the characteristics of a phishing attack, followed by a discussion of the use of mobile technology as a phishing instrument in section 3. In section 4, we discuss *Education, Preparation, Avoidance, Intervention,* and *Treatment* issues related to mobile phishing followed by a conclusion in section 5.

2 The characteristics of a traditional phishing attack

Phishing traditionally involves fraudulent e-mails that fraudsters send to random e-mail addresses. The fraudulent e-mail contains information that usually requires the individual receiving the e-mail to follow a link within the e-mail (usually to a spoofed website) and enter their personal details, be it ID numbers, banking details, passwords, etc. As soon as the form with this information is submitted, it sends the data to the fraudster [16]. The following similarities are found in fraudulent e-mails:

- There is always some kind of company that is imitated, often from the financial sector.
- The e-mail often includes a security breach, warning customers to login and verify or renew their details.
- There is always a link the user (potential victim) needs to follow in order to complete the process.
- The graphics used are often identical to the original website.

After clicking on the link provided, the user will be taken to a spoofed web site. The difference between the original website and the spoofed website are not easily spotted by the inexperienced user. The graphics used on the spoofed web site are similar to those on the original site and often the fraudsters use relevant website addresses. It is also possible for fraudsters to use the "same website address" by using JavaScript code to replace the victim's browser's address bar with a fake bar. Moreover, fraudsters will use logos and footers similar to those on the original website. Furthermore, the fraudsters may promise "worry-free protection" to lure individuals into submitting personal information on the spoofed website. In the CitiBank example, a "$0 Liability for Unauthorized Purchases" was promised. The goal is to ease concerned individuals by saying that if something does go wrong, the Citibank client will not be held liable, instead Citibank will take care of the losses [17]. Table 1 gives a summary of the different characteristics one will encounter between the original website and the spoofed website [18].

3 Mobile technology: the "new" playfield for phishers

We could not find any reports on phishing attacks where phishers used mobile technology and more specifically, SMS communication. As mentioned previously, we believe that with the rapid growth in the use of SMS technology as a M-Commerce communication medium [19], the question is not *if* phishing via SMS technology will happen, but rather *when* it will happen. All the information we have observed is public domain and we just put the pieces together, hopefully faster than a fraudster has done. Our goal is to warn the stake holders and have them take necessary measures to be prepared against phishing attacks.

Table 1. Difference between the original site and the spoofed website

Character-istic	Original website	Spoofed website
URL	https://www.citi.com	http://www.mycitibank.net/
Graphics	Original web site graphics used for business	Identical to original website
Digitally signed	Yes–using services such as Verisign	No
Logo	Uses original business logo's	Identical to original website
Footer	Uses a footer to represent business information	Almost identical

A mobile phish may, similar to a phish in the Internet community, be sent out by a phisher with identity theft as goal. This can be dangerous in numerous application domains, with financial applications probably being the most vulnerable.

There are a number combinations by which phishing can take place via mobile technology. In order to provide more insight, we will comment on some of the weaknesses we have observed. An SMS message may be created and sent using an existing pre-paid phone or from a web service provided by the prepaid phone company (the user can take advantage of the convenience of a computer keyboard in sending and receiving SMS messages). For both these options, a pre-paid amount of SMS message credits are purchased. After a successful phishing activity, the pre-paid package (e.g. the SIM card) can be discarded and a new service option can be acquired at minimal prices.

In most countries, pre-paid phones are bought without registration of the buyer. Top-up packages are also available without any identification. Moreover, there are readily available web services that will let anyone send SMS messages worldwide. Some of these services are registration based (but free) and some are on pre-paid basis. There are also programs that let someone send and receive SMS messages through a computer without having to go to a website or use a cell phone. For example Mailfreeonline provides a free SMS service without identification (http://www.mailfreeonline.com/.)

Most mobile service carriers provide a web service through which anyone can send an SMS message to a number serviced by that carrier, at no cost to sender e.g. T-Mobile in the USA will allow the user to send such an SMS (http://www.t-mobile.com/messaging/default.asp?nav=hm). The cost associated with the SMS message sent through the mobile service providers website is charged to the number which receives the message. A person can go randomly to any of those sites by using a web browser and send SMS messages to any number on that network. For the sake of simplicity, we have not considered automating the SMS sending process by abusing the "free" service provided by most carriers. There does not seem to be any measure on those web services to prevent automated SMS sending. In general, most online service providers (e.g. Google e-mail service) use image-based measure to prevent automated registration or brute force attacks.

In order to show some of the combinations of how phishing can take place, we use a pair of binary variables, M and W, where M denotes the use of a mobile device and W denotes a World Wide Web service (W can be an SMS message service or a spoofed website). In any ordered pair of M and W, the first variable represents the spawning medium and the second variable represents the harvesting medium. For example, MM would mean the phish is spawned (sent out) via a mobile device and the information is harvested via arriving SMS message. Table 2 shows the possible combinations for spawn-harvest pairs in phishing activities involving SMS technology.

Table 2. Four possible scenarios utilizing mobile technology for phishing

Type	Origin	Harvest Point	Property
MM	The phish is sent via SMS on a mobile device	The information is collected via SMS on a mobile device	Cyclic activity in Fig. 1 takes place
WM	• Dedicated web interface from the prepaid mobile service provider • Local executable using prepaid SMS service is utilized • Web interface from customer's mobile service provider (the recipient is billed for received SMS)	• Information received at the mobile device or • Internet-based software providing SMS service	
MW	Information sent via mobile	User directed to a spoofed web site to submit information	Traditional phishing activity takes place
WW	• Dedicated web interface from the prepaid mobile service provider • Local executable for prepaid SMS service is utilized • Web interface from customer's mobile service provider (the recipient is billed for received SMS)	User directed to a spoofed web site to submit information	

Note that the phishing activity could also combine two or more of the scenarios shown in Table 2. In such a case an SMS message would ask a potential victim either to reply to the SMS or visit a spoofed website through which information will be stolen. In MW and WW types of phishing, as seen in Table 2, the role of mobile technology replaces that of e-mail in traditional phishing activities.

A phishing attack using mobile technology thoroughly (MM type in Table 2) can be modeled as a cyclic activity, presented by us as a spiral model with three phases (Figure 1). In the first phase, the phisher sends out his phishing messages to a number of selected recipients. He/she then

receives a number of replies to the phish. In the next step, the phisher requests information from the potential victims. Those recipients who trust this request and submit confidential information become victims of the phishing activity.

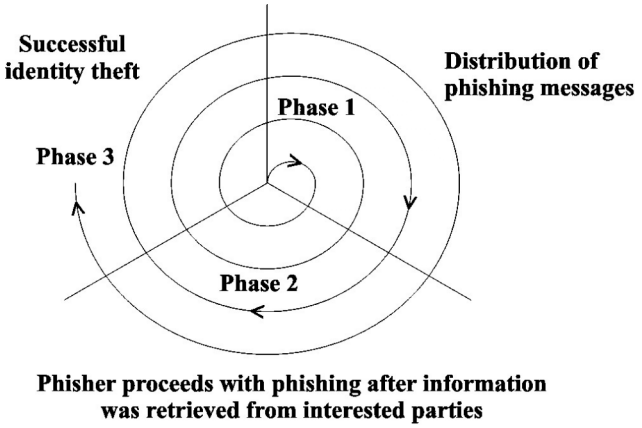

Figure 1. Cyclic nature of the MM and WM-type mobile phishing activity

We elaborate on the three phases, which take place in MM type phishing, in the remainder of section 3, by presenting the MM type phishing scenario in which spawning the phish and harvesting the phished information are done on a mobile device. This example is also useful to show the cyclic activity that takes place with MM and WM types of phishing.

Phase 1: Distribution of phishing messages

The following are typical steps that a phisher will be involved in before he sends his phish to a selected list of mobile numbers (not necessarily in this order):

1. Determining the number of phishing messages of the phishing attack.
2. Determining the numbers that will be phished (we are assuming the phisher has not acquired a database of mobile phone numbers). In contrast with e-mail address generation this is easy to do. A phisher may use a known service provider, with the first three digits known to the phisher.
3. Selection of the service the phisher wants to access, e.g. Fraudulent Bank in our example.
4. Compiling the phishing message.
5. Sending out the phish to different numbers.

In Figure 2, we give an example of an SMS message that may be used to phish information from cell phones users. For illustration purposes we use a fictitious financial service, called Fraudulent Bank. The phisher creates the message on his phone (or on an Internet web service) and then sends this copy to a number of potential victims.

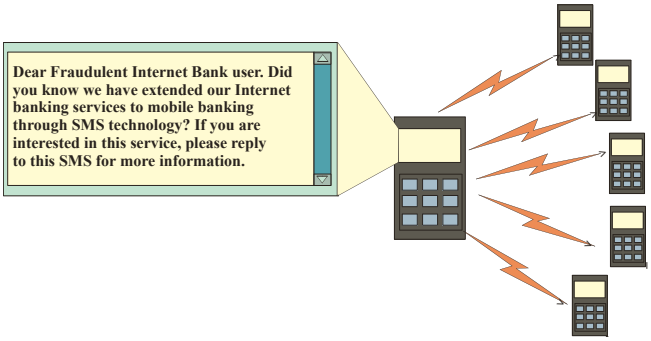

Figure 2. An example of a phishing attack using mobile technology

Phase 2: Phisher's reaction to first cycle phished information.

According to the Anti-Phishing Work Group [20], data suggests that in traditional phishing activities (e-mail and web-based), phishers are able to convince up to 5% of recipients to respond to them. The result of these scams is that consumers suffer identity theft, credit card fraud, and financial loss. We predict that the percentage of SMS recipients who respond to a phish will be much higher due to the more personal nature of mobile settings and the fact that it is harder for the users to ignore an SMS message.

As soon as the phisher has received replies from his/her first round of phishing, where nothing has been revealed except interest, he/she can proceed to send his/her request for personal information. The request will be determined by the goal of the phish. If his goal is to misuse information for credit card fraud, he may request personal and credit card information. If the goal is to access a bank account, the online banking details will be requested (e.g. users may be tricked into believing they are doing banking via SMS). In our Fraudulent Bank example, the phisher requests information used by recipients to log into Internet services provided by the bank. Figure 3 gives an example of a second SMS message to be sent to potential victims.

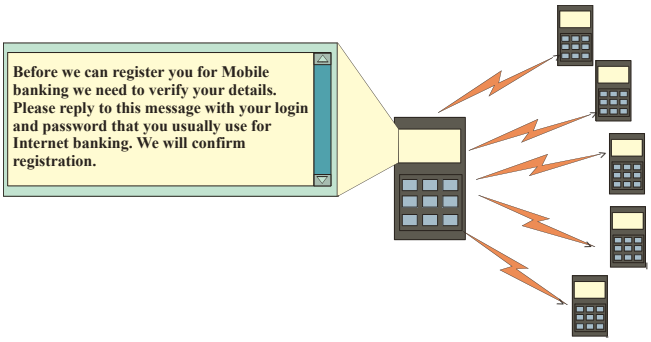

Figure 3. Phase 2 – phisher sends SMS to obtain information from potential victims

Phase 3: Successful identity theft

In the last phase the phisher will, if successful, receive the information phished from the recipients. Depending on the goal of the phishing activity, the phisher may miss-use the information for personal gain [21]. For example:

1. Phishers can use the data to access existing accounts.
2. Phishers can use the data to open "false" accounts in someone else's name, which may only be discovered when creditors contact the "account holder".
3. Phishers can use the data to harm the trust customers have in various institutions providing online services.

There are several issues involved in phishing via mobile technology for the recipient of the phish and the business whose name was used in the phishing activity. These issues are geared towards removing or minimizing the effects of phishing via mobile technology and are discussed in section 4.

4 Issues involved in a mobile phishing attack

Van der Merwe *et.al* (2005) identified the issues involved in an e-mail phishing attack to include *Education, Preparation, Avoidance, Intervention,* and *Treatment* (Table 3). The authors also emphasize the responsibility shift for prevention of identity theft from the business to user level. Previously, it was the responsibility of a financial institution to ensure the client that his/her information is secure during a valid Internet transaction. For legitimate transactions this is still the case. However, in order to prevent a phish from being successful, an additional step at user level is necessary namely, authentication of the web-service.

The five issues related to website phishing attacks are also relevant for mobile phishing (Table 3).

1. The users need to be *educated* and made aware of the possibility of a phishing attack via mobile technology. The types of attacks stated in Table 2 can constitute the initial step towards awareness.
2. Even if no *preparation* strategy is possible for the user, businesses need to establish guidelines to follow when a client is the victim of a mobile phishing attack besides taking necessary measures to minimize the risk of a phishing attack taking place or becoming successful. In SMS communication, the recipient doesn't have a choice in receiving the spammed message. In contrast with spammed e-mail, it is difficult to block spammed SMS messages. Blocking of spammed e-mails is possible after a sender's e-mail has been identified as a spammer and blacklisted. In mobile phishing, the phisher will probably not re-use the cell phone number after the first attack. Even if we consider blocking a number from which phishing originated, a whole set of new issues appear. One of the issues to be addressed is that permanently blocking the numbers will pose the challenge of running out of numbers. Thus, a measure based on blocking numbers, if chosen to be implemented, must be done so with considerations of limited number space.
3. Phishers disposing the used cell phone limits the options for the recipient to *avoid* unwanted SMS messages based on history. We envision that adaptive methods that interpret the content of SMS messages can be used in helping a user avoid such attacks.
4. The user may *intervene* after the first SMS is received from the phisher by deleting the messages or contacting the business to which he thinks he is supplying information. Consequently, the servers that relay SMS messages can possibly block the SMS messages coming from a specific source for a certain amount of time. Another strategy could be to delay the SMS message that is interpreted as fraudulent. The amount of delay should be long enough to give the user enough time to doubt authenticity of the request.
5. When a user suspects that he/she has been victim of a mobile phishing activity and supplied information to an untrustworthy source, the user should immediately contact the business. The business then should try and work toward *treatment* of the situation and take necessary actions to prevent misuse of the supplied information.

In Table 3 we summarize the issues related in both a website phishing attack and a SMS attack.

Table 3. Issues in a mobile and SMS phishing attack

Issue	Website phishing attack	SMS phishing
Education	Educate the users with regard to prevention techniques and a strategy on preparing to avoid phishing attacks.	Educate users with regard to the possibility of phishing attacks through mobile technology.
Preparation	Preparation consists of the process of thinking and stipulating what you will do in the event a phishing attack.	Businesses need to establish guidelines that stipulate what they will do in case of a phishing attack. Build mechanisms to minimize the risk of an attack taking place and becoming successful.
Avoidance	Avoidance includes activities that evade the onset of an attack.	Avoidance of becoming a recipient of phishing SMS's.
Intervention	Intervention involves activities where the person/business involved in a phishing attack intervenes or step in to affect the outcome of the attack.	Intervene after the recipient has received the first SMS by deleting it or contacting the applicable business.
Treatment	Treatment includes the activities to recover after a phishing attack.	Contact appropriate role players to prevent misuse of information.

5 Reeling in a phisher

A phisher is vulnerable during two different phases of a mobile phishing scenario. The first is during the phishing attack. When a cell phone is used, it is possible for the service provider of the pre-paid package to detect the position of transmission. The strength is measured and compared between different cell phone transmitters, which enable the service provider to determine the exact location of the cell phone. This service is already available as a tracing mechanism from different cell phone companies and mostly used by parents to "keep an eye" on their children's activities.

The only problem with finding the cell phone location is that the user of a phone must first give permission that this information may be available to other users. Obviously a phisher will not give this kind of permission. This implies that if a phishing activity is identified, a warrant for access to this information must first be provided to the service provider before he will make the information available. In most countries this is a time consuming process, which provides the phisher with enough time to discard his/her pre-paid phone after a phishing activity.

The second phase in which a phisher is vulnerable is when he/she is using the phished information for personal gain or to create discomfort for others. Unfortunately, there is a lot of collaboration between criminals in different sectors that almost nobody is safe from information misuse. Phishers may attempt to use personal information for different activities including creation of accounts. There must be necessary measures implemented to catch a phisher during this phase, when the phishing activity has been identified.

6 Conclusion

Threats are best handled if they are known in advance and necessary measures to weather them are in place. In dealing with any threat, education of the potential victims is one of the key elements. Therefore, this paper can be considered as the first attempt geared towards increasing the awareness of mobile phishing attacks and educating the potential victims.

Identity theft is the ultimate goal of any phisher. The phished information can be used in different application domains, with financial applications probably the most vulnerable. It is advised that cell phone users are very selective when sharing cell phone information. If mobile phishing achieves the same success rate with the traditional e-mail-based phishing, which is 5%, one can see that the possible loss from phishing activities has the potential to double. However, due to the more personal nature of mobile technology and the difficulties in ignoring the incoming SMS messages, we predict that the success rate of mobile phishing may be much higher than that of traditional, e-mail-based phishing.

SMS message misuse is made possible especially by pre-paid phones. In most countries, the service providers do not require identification when a pre-paid cell-phone option is sold. A phisher may also use the web services we mentioned in the paper to conduct mobile phishing attacks. Having access to compromised networks or conducting such an attack from an Internet café is the situations in favor of potential phishers.

In this paper, we introduced four types of mobile phishing. We provided a scenario based on the MM type mobile phishing and presented its cyclic nature with the details of activities that can take place in every phase of a this type of phishing attack.

Although we believe that education is still the key to prevent phishing attacks, we also listed other issues that should be considered by both mobile technology users and the organizations affected by a phishing attack. These issues include *Education, Preparation, Avoidance, Intervention,* and *Treatment*. Where applicable, we have provided some ideas on possible measures including those to be used in weathering phishing attacks and rendering them useless. We do believe that the institutions that are affected in phishing activities need to work on procedural changes in order to minimize the risk associated with such attacks, including locating the phishers during the various phases of an attack or after an attack when the stolen information is used to cause harm to users.

References

[1] Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson, *2004 CSI/FBI Computer Crime and Security Survey*, CSI/FBI Computer Crime and Security Institute, San Fransisco, 2004.

[2] Lawrence, E., B. Corbitt, J. Fisher, J. Lawrence, and A. Tidwell, *Internet Commerce, 2nd Edition*, John Wiley & Sons, Queensland, Australia, 1999.

[3] Levy, E. and I. Arce, "Criminals become Tech Savvy," *IEEE Security & Privacy*, Vol 2, No 2, pp. 65-68, 2004.

[4] McFedries, P., "The Word Spy", Electronically available at http://www.wordspy.com/words/, Accessed July 2004.

[5] FTC, "Total Number of Fraud Complaints & Amount paid", Electronically available at http://www.consumer.gov/sentinel/states03/fraud_complaint_trends.pdf, Accessed July 2004.

[6] Stallings, W., *Network and Internetworked Security*, Prentice Hall, Englewood Cliffs, New Jersey, 1995.

[7] APWG, "Proposed Solutions to Address the Threat of Email Spoofing Scams (White Paper)", Electronically available at http://www.antiphishing.org/, Accessed July 2004.

[8] Porter, B., *It was 'Phishing' - eBay*, 28 July 2004 ed, News 24, South Africa, 2004.

[9] McLaughlin, L., "Online Fraud Gets Sophisticated," *IEEE Internet Computing*, Vol 7, No 5, pp. 6-8, 2003.

[10] Clearinghouse, *Reducing the Risk of Identity Theft*, Clearinghouse / UCAN, San Diego, CA, 1995.

[11] Tuliani, J., "Bugwatch: The Future of Phishing", Electronically available at http://ad.uk.doubleclick.net/jump/mpu.vnunet.uk/hacking;cat=hacking;sec=news;page=article;artid=1154803;tile=3;sz=1x1;ord=123456789?, Accessed September 2004.

[12] Lebihan, R., "Still Fishing for Answers to Internet Scams", Electronically available at http://afr.com/articles/2004/08/25/1093246607260.html, Accessed September 2004.

[13] Davison, J., D. Brown, and A. Walsh, "Mobile E-Commerce: Market strategies", Electronically available at www.ovum.com, Accessed September 2004.

[14] VIP.parking, "VIP Parking", Electronically available at Accessed September.

[15] Vodacom, "Vodacom Transfer", Electronically available at http://www.vodacom4me.co.za/servlet/homepage, Accessed September 2004.

[16] FSTC, *FSTC Counter-Phishing Initiative*, Financial Services Technology Consortium, New York, 2004.

[17] APWG, "The Anti-Phishing Working Group (APWG): Citi-Bank update", Electronically available at http://www.antiphishing.org/phishing_archive/07-21-04_Citibank_(Attn_Citibank_Update).html, Accessed July 2004.

[18] Van der Merwe, A., M. Loock, and M. Dabrowski, "Characteristics and Responsibilities involved in a Phishing Attack," Proc. Winter International Symposium on Information and Communication Technologies, Cape Town, 2005.

[19] Rettie, R. and M. Brum, "M-Commerce: The Role of SMS Text Messages," Proc. COTIM-2001: From E-commerce to M-Commerce, Karlsruhe, Germany, 2001.

[20] APWG, "The Anti-Phishing Working Group (APWG): Phishing Attack Trends Report", Electronically available at http://www.antiphishing.org/APWG_Phishing_Attack_Report-May2004.pdf, Accessed July 2004.

[21] APWG, "The Anti-Phishing Working Group (APWG)", Electronically available at http://www.antiphishing.org/, Accessed July 2004.