Vol. 5, No. 4 April 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences
©2009-2014 CIS Journal. All rights reserved.
http://www.cisjournal.org

Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices

[1] Ezer Osei Yeboah-Boateng, [2] Priscilla Mateko Amanor
[1] Center for Communications, Media & Information technologies (CMI), dept. of Electronic Systems, Aalborg University, Copenhagen
[2] Coventry University, Accra Campus and a database administrator

ABSTRACT

This study is an exploratory assessment of Phishing, SMiShing and Vishing attacks against mobile devices. It examines the implications of end-user behavior towards mitigating the risks posed by using mobile devices for online services and facilities. Phishing is that socially engineered attack aimed at enticing unsuspecting users with familiar websites spoofed and purported to come from a legitimate organization or source. It lures the user to furnish the assailant with the user's access credentials, for which privileged access would be gained to harm the user. SMiShing attacks also happen whenever text messages are sent for the user to either click on a link provided, which leads to a fraudulent website or for the attacker to get access to the user's contacts and/or any other confidential information. Vishing is a voice phishing attack, whereby a voice call received from an assailant lures the target into providing personal information with the intention to use that information to cause harm. With the proliferation of smart phones, tablets and hotspots, these social engineering attacks on mobile devices are now prevalent. The study observed and strategically interviewed 20 end-users for their knowledge, perceptions and behavior when confronted with phishing attack situations. The results show that men are more comfortable and trusting on the cyber-space and thus more susceptible to phishing attacks than women. The results also indicate that most users are either slightly aware or not at all aware of Phishing, SMiShing and Vishing threats against their mobile devices. Interestingly, 55% would occasionally examine the messages received as perceived threats, whilst 35% would never or almost never scrutinize any messages. A taxonomy of 'alluring" and "decoying" words used in phishing attacks is provided as a benchmark to end-users to guard against becoming cyber-victims. Of the most commonly used operating systems, the iOS was found to be the most susceptible to phishing attacks.

Keywords: *Phishing, SMiShing, Vishing, Mobile Devices, Attacks, Cyber-victims, Social Engineering*

1. INTRODUCTION

Innovation with information and communications technologies (ICTs) has permeated our lives, be it for business, for personal or for recreation purposes. We especially rely on the Internet for business, personal, finance and investment decision making, etc. Coupled with these advancements are myriad of threats which exploit the inherent vulnerabilities on the Internet and its associated technologies [1]. Some of these threats manifest in various ways, such as pretentious items offered for sale on eBay, with the aim to swindle unsuspecting patrons, or assuring victims of great returns, if the victim will help a foreign financial transaction through his own bank account, etc.

Phishing, in particular, has been in existence for a long time. Phishing is a pretentious way of causing an end-user into revealing his/her sensitive information to an attacker online, such as passwords or credit accounts, other personal information or sensitive financial data [2]. Another attack that comes close to Phishing is SMiShing. Instead of the attack occurring through emails it comes as short messaging services (SMS) or text messages. The term "Vishing" is derived from a combination of "voice" and "Phishing"[3]. Here, a phone call is received with the attacker luring the receiver into providing personal information with the intention to cause harm. For instance, a customer receives a call on weekend and off-banking hours, purported to come from the contact center of his bank. The information gathered by the attacker can be used for criminal activities such as identity theft or fraud. Generally, customers and/or users, heretofore referred to as target victims, are misled into revealing this information either by providing it through a web form or by downloading and installing malicious software.

A mobile device (or a handheld embedded computer or simply handheld) is defined as a small computing device, usually with a small output screen, which may have touch input or miniaturized keyboard [4]. It performs the basic functions of a computer, such as control, data processing, data movement and data storage. Examples of mobile devices are Palm and other PDAs, tablet PC and smart phones [5].

Today, with ubiquitous computing, the use of mobile devices to access and browse the Internet and various computing applications have become commonplace; be it for business or personal use. Mobile device utility is partly due to its portability and long battery life. Coupled with numerous applications, the use of mobile devices present a myriad of cyber-security challenges due to its utility and interconnectivity. The threats posed to these emerging embedded computing technologies is the subject of this research paper. Specifically, we seek to establish the enormity of the mobile devices threats and to create the awareness on Phishing, SMiShing and Vishing threats and their associated impact upon exploitation.

1.1 Problem Formulation

According to [6] the trend of Phishing, SMiShing and Vishing against mobile devices have been increasing without any signs of the attacks abating. For two consecutive years, the reported cases of these attacks per

©2009-2014 CIS Journal. All rights reserved.

month increased by more than 160 times, whilst the number of unique reported phishing websites progressed by about 16 times, with over 100 well-known brands being under attacks[6].

Typical attacks emanate as genuine emails purported to originate from the "spoofed" originator or sender. This email message may request the recipient to furnish some sensitive user credentials or personal information or click on a link for further actions. For example, an email purported to originate from your systems administrator may ask you to furnish the administrator with personal details including your password, by a certain deadline or you risk losing your account. Once the user responds to the message with the requisite information, the attacker can then seize the opportunity to harm one's systems or misuse the stolen identity profile. Until recent times, mobile devices had only been susceptible to viruses and worms, but there are indications of Phishing, SMiShing and Vishing attacks.

Studies into threats against mobile devices seem to suggest that many users disregard security concerns whenever they visit or carry out transactions online [7][8]. This study seeks to assess the mobile user behavior and ascertain the extent of attacks and their impact. The key issues of concern are as follows:

i. What is the extent of Phishing attacks on mobile device users?
ii. What are the characteristics of Phishing, SMiShing and Vishing which confront mobile devices?
iii. How do mobile device users fall prey or become victims of Phishing attacks?

This study endeavors to assess the level of understanding and awareness of mobile device users on Phishing attacks, in general. We seek to create taxonomy of Phishing, SMiShing and Vishing characteristics that usually confront most mobile users. Also, we shall evaluate the impact of Phishing, SMiShing and Vishing in respect of identity theft as user profile or access credentials are stolen. This study enumerates some key characteristics of Phishing, SMiShing and Vishing threats as "Click Here", "download", "documents", "View", "Password", "Account" and "Transactions" etc. The study also discovered that generally men use the Internet more than women, and that men are also more prone to Phishing, SMiShing and Vishing attacks than women.

This paper is organized as follows: this introductory section deals with the background followed by related works and state-of-the-art literature on those threats. The methodology adopted is presented next, and it's followed by the results and findings, whilst the implications of the findings are discussed in the conclusion.

2. LITERATURE REVIEW

This section deals with the state-of-the-art and related works on Phishing, SMiShing and Vishing as threats against Mobile Devices and the awareness and implications on end-users as the threats exploit the human-centric vulnerabilities. There are some vulnerabilities with mobile devices as well as the end-users, which are manifested through E-mails, text messages or short messaging service (SMS), Web browsing and listening to voice mail that may be fraudulent or may be attacks seeking to exploit the inherent weaknesses of end-users.

Here, we discuss social engineering as a major threat or technique by which most Phishing, SMiShing and Vishing attacks are employed against mobile devices.

2.1 Social Engineering

Social engineering is the ability of deceiving or enticing someone to disclose his or her sensitive or security information [9][1]. This includes the means or capability of getting entry to premises, networks or databases by exploiting individual mindset, instead of breaking into or using specialized hacking methods.

Social engineering attacks is usually achieve by manipulating victims to perform actions that they don't intent doing and which may be to their detriment [10]. Social engineering is usually used to describe trickery or deception for the purpose of information gathering, fraud or gaining computing system access. In the book "The Art of Deception: Controlling the Human Element of Security"[11], social engineering is defined as follows:

> "Using influence and persuasion to deceive people by convincing them that the attacker is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information, or to persuade them to perform an action item, with or without the use of technology."

The social engineer, thus, employs deception, influence and persuasion in collecting business and/or personal information [11] by exploiting the susceptibilities of the victims. The key motive here is to acquire relevant information that may permit him/her to gain unauthorized access to a valued system and the information that dwells on it. Literature has various definitions of what constitutes social engineering; for example [12][13], have their own versions of social engineering definitions and techniques. Here is one good classifications of social engineering into the following categories [13].

i. Social engineering by phone (i.e. via telephone communication), which is characteristic of SMiShing and Vishing in this study;
ii. Dumpster diving (i.e. office or electronic waste);
iii. Online social engineering (i.e. on the web through browsing), which is characteristic of Phishing in this study.

©2009-2014 CIS Journal. All rights reserved.

iv. Persuasion (face-to-face communication); and
v. Reverse social engineering

This classification is based purely on the techniques rather than the nature of the attacks. For this study, social engineering is defined as the act of luring or manipulating people to disclose their computing user credentials and/or any valuable information that may be technically detrimental to the end-user and his systems and data. The purpose of the social engineering activity is to defraud or gain access to the user's systems. It must be noted that this study alludes to the following classifications in line with [13] social engineering via telephony – hereinafter referred to as SMiShing and Vishing, Online social engineering and reverse social engineering, which are forms of Phishing.

Typically, social engineering is a threat to all computer users. It is normally used in conjunction with other attack vectors and mainly exploits the vulnerability of ignorance or lack of diligence on the part human users. It has the potential to cause serious harm to computer systems and networks. The stakes are high as very confidential information may be disclosed through social engineering approaches. According to [6], there has been an increase in security attacks against mobile devices since the year 2006; most of these security attacks occur due to flaws and weaknesses within web browsers. Also, the web is full of malicious codes that can be downloaded easily and used as Spam or Phishing attack vectors to lure users into disclosing their user profiles and credentials as well as sensitive corporate information. The proliferation of mobile devices and applications has also exacerbated the situation with Phishing, SMiShing and Vishing attacks on mobile users.

2.2 Phishing, SMiShing and Vishing

In this section, we review the definitions and techniques of Phishing, SMiShing and Vishing. Phishing, SMiShing and Vishing continue to be prominent among cyber-criminal communities or the underground economy of malwares for the following reasons [14];

- The implementation cost to carry out an attack is incredibly low which considerably decreases the obstacles or hurdles posed to new criminals initiating attacks;
- Minimal specialized expertise is necessary to initiate an attack. The launching operation turned out to be totally automated and a Phishing attack can be launched with a few clicks.
- Although the act of social engineering with Phishing, SMiShing and Vishing are age-old scams, they remain prevalent and effective; especially, with mobile devices and users. The techniques employed by the scammers may vary, end-users are lured into disclosing or revealing key and sensitive information on the Internet and also over the phone.

2.2.1 Phishing

When an online user is deceived into disclosing his/her confidential information such as password or PIN (personal identification number) or account number, this is known as Phishing [15]. When a fake login page of a popular social web site, for example Face book, Yahoo, Faces.com, Fet life, Face party, auction sites and online payment processors is sent by an attacker to an unwary individual in a form of an email or WebPages for his\her response then it marks the beginning of an attack. These messages or websites are crafted to resemble the actual site making it almost impossible for the victim to make it out. An email message may purport to come from the system administrator or IT services support, which asks the user to take some actions, such as "you're about to exceed your storage capacity, please click here to remain active". As soon as the user clicks or provides the needed information, the criminal hacker (or cracker) will use that information to hack into the victim's account and/or systems. There is also a case of Phishing by the use of the man-in-the-middle (MITM) attack; this is where the victim visits an honest website and unknowingly fills in his details in the login page which has been substituted with a fake login page. Immediately this is done the user's details are captured and diverted to the criminal's webpage.

This study affirms that Phishing is a social engineering technique whereby unsuspecting users are lured into disclosing personal and sensitive information, through solicitation via email, instant messaging (IM), Online chats, and other social network chats, etc.

2.2.2 SMiShing

Here, we take a look at SMiShing which is a form of Phishing that uses short messaging services (SMS) or text messages on mobile phones and Smartphone's [16]. SMiShing derived its name from the test messaging technology SMS (Short Message Service). There are two main processes for the SMiShing scams; one involves receiving a text message which is purported to have originated from a known and trusted source, such as your bankers or your system administrator. The second one involves you receiving a vital text message about your identity been stolen or account number been frozen, it then goes ahead to direct you to a website or a phone number for the verification of the account information. The thieves upon receiving the information go ahead to withdraw money from the account or open a new credit card in the victim's name. In a similar instance, a vital text message is received by the victim from probably a known or trusted source, which may come along with an attachment. The attachment downloads a virus or malware unto the victim's device which in turn installs a root kit or backdoor for the scammers to have access to everything (contacts, inbox messages and application on the phone etc. etc.) on the victim's phone and sometimes even have control over it.

©2009-2014 CIS Journal. All rights reserved.

2.2.3 Vishing

"Vishing is the practice of leveraging IP-based voice messaging technologies (primarily Voice over Internet Protocol, or VoIP) to socially engineer the intended victim into providing personal, financial or other confidential information for the purpose of financial reward. The term "Vishing" is derived from a combination of "voice" and "Phishing."[3]

Vishing capitalizes on a person's confidence in the telephone service, as the target is usually not aware of scammer's ability to use techniques such as caller ID spoofing and advanced automated systems to commit this kind of scam [14]. However, as the yield on traditional Phishing attacks continues to reduce, scammers have resorted to Vishing in an effort to acquire user's financial account numbers, passwords and other personal data.

Years ago, children could just call an unknown landline and play a prank on them. However, even with circuit switching, digital and/or electromechanical, technologies, the call could be traced back to the telephone bill-payer once the prank was reported to the Telco. But with the recent advancement in the IP telephony system, it means that there is a possibility that a telephone call could originate and/or terminate at a computer anywhere in the world. Besides, the amount to be paid is also negligible, thus making it more likely to engage in Vishing scams.

2.3 Mobile Devices

Mobile devices are typically handheld computing devices, often used in making and receiving phone calls and text messages, as well as for numerous computing applications and services.

For the purposes of this research, mobile devices include personal digital assistants (PDAs), smart phones, portable computers such as Laptops, Notebooks, Net books, iPADs, Tablets, etc. These could run on any operating system, especially Android and iOS[17]. Quite apart from the physical size and weight, most mobile devices today are evaluated based on their computing capabilities, including processing power and storage. Another binding parameter amongst mobile devices is their capability to connect from anywhere anytime via hotspot services. A typical classroom today has students with all sorts of mobile computing devices, from Laptops to Net books to iPADs.

Laptops have been referred to as a mobile device in this study, because of its portability and mobility of use which is often carried around to coffee shops, cafes, at the poolside, around on university campuses, in the airplanes, in moving buses, etc. The user interfaces of mobile devices are small in size and lack appropriate application identity indicators that are available in desktop operating systems and browsers as only one mobile application can control the screen at a time.

To this end, security policies on use and protection of laptops and (traditional) mobile devices are usually lumped together in some studies. This adopted definition for mobile devices is in agreement with similar research works in Information Security. For example,[18] and [19] defined mobile devices as including PDAs, mobile phones, laptops, and smart phones that can expose organizational assets to threats if not properly safeguarded.

2.4 Threats to Mobile Devices

The problem of Phishing, SMiShing and Vishing is much broader than just what has been used in the financial sector or in projects involving money. It is imperative and worth noting, that a reliable mutual authentication mechanism be put in place to resolve the issues militating against identity management. Looking at the current trends [20][21], Phishing attacks are likely to go beyond merely acquiring personal IDs and gathering identity credentials to exploiting other information on the wider cyber-space.

There are various security challenges that occur as a result of users being online; these may result from the use of the HTTP redirection function, as there is some form of danger with the control of an Open ID [21]. The Open ID as an open standard allows end-users to have digital identities which are authenticated by third-party services or agents called the Relying Party (RP). The Open ID is susceptible to Phishing attacks, as a malicious relaying party can re-direct an end-user's visit to a bogus website, which in turn, collects the access credentials (Open ID) of that user. The hacker who also controls the bogus website can then use the credentials to log into any web services.

To mitigate this vulnerability,[20] posited that "successful mutual authentication should not require users to use the same computer all the time, nor to install special software". It seems from the foregoing that, there are numerous approaches to tackling the mobile device menace. In this review, we seek to highlight on key threats exploiting vulnerabilities with mobile devices, be they used for online data, web browsing or voice communications. This section seeks to discuss more on threats due to Phishing, SMiShing and Vishing attack vectors.

2.4.1 Possible Factors of Vulnerabilities

There are a number of theories from researchers on the argument of why people fall prey to computer scammers. The subjects of Phishing, SMiShing and Vishing have been with us for some time now, especially Phishing which can be said to have been with us many years now. Some of the reasons include people being more interested and trusting in web sites based on its visual appearance and not necessarily on the know-how of an entire web sites; this weakness is often and easily exploited by scammers or crackers[22]. Secondly, the lack of knowledge on the various security features available on websites, credit cards, ATMs, for example, is

©2009-2014 CIS Journal. All rights reserved.

another source of vulnerability. This creates a sense of fear, uncertainty and doubt (FUD) [23][24]. Also, the proliferation of Smartphone users, which stores numerous data, could be a source of vulnerability. When the Smartphone is compromised any of the following actions could be taken by the scammers: steal data, launch attacks, install malware on servers, etc. [25].

Users are adamant to handling security issues and may therefore decide to stick to their old fashion way of handling security. Most end-users seldom change or adapt security measures when engaging in the cyber-space. They tend to have all sorts of perceptions on security, which are myths. For instance, that their online protection is perceived to be adequate, some abhor interferences or pop-ups by way of warnings, as well as finding the end-users manuals complicated to read and to understand. Furthermore, end-users are clueless regarding security of a website or its genuineness, and though many websites are spoofed by phishers [26]. Studies have shown that although some end-users are familiar with terms like "virus", "worms", "online scams" and "computer fraud", they are oblivious of Phishing, SMiShing and Vishing [27]. Yet again, for those with some awareness, they sometimes also perceive that there is high stakes for only the corporate entities such as banks and Telcos, and not for personal data.

2.4.2 Cyber-Victims Vulnerabilities

Here we examine some of the vulnerabilities and cyber-victim theories that render the mobile devices susceptible to Phishing, SMiShing and Vishing attacks. Incidentally, as many more connect with their mobiles, the extent of mobile attacks also increase and become more sophisticated[28]. As observed by[29], knowing the factors that instigated or influenced end-users to be cyber-victims may assist in designing appropriate mitigation measures to minimize risks as well as to create the necessary awareness. In their study[29] explored the behavioural patterns of subjects on their prior knowledge and appreciation or otherwise on web environments, such as the URLs, security icons and features. Their past experiences with any cyber-attacks were also taken into consideration. It was revealed that those with some knowledge and/or experiences were less susceptible than those without any prior knowledge [30]. The research also shows that educating (by way of awareness creation) end-users had positive impact on their level of vulnerability, rather than the often not-read service providers' warning messages sent out via emails or SMS[29].

Some theories are used to explain the reasons leading end-users becoming vulnerable to cyber-attacks. For example, the Rational Choice Theory espouses that end-users are "purposive and goal oriented" and make decisions based on a set of alternatives or preferences available to them, with the view to maximize utility[31]. Applying that to cyber-victims vulnerabilities with respect to Phishing, SMiShing and Vishing, the end-users are said to be acting as rational and maximizing utility upon receiving a possible phishing exploit via an email message, text message or a voicemail[31].

Similarly, Technology Acceptance Model (TAM) espouses that users influenced by either the perceived usefulness or the perceived ease-of-use [32] of a particular security measure, to the extent that users may be cyber-victims based on their perceptions on anti-phishing systems (for example). The Unified Theory of Acceptance and Use of Technology (UTAUT), as an upgraded version of TAM, envisages that a user will become a cyber-victim based of his/her expectations, purpose and enabling conditions[33]. It explains that a vulnerable user is less likely to pay any attention to cyber-risk mitigation measures for which he perceives as inconvenience.

Using the Lazy User Theory [34], end-users do not necessarily pay attention to risk mitigation measures, neither do they take any security actions, unless there's as experience or an incidence.

Advances in Internet technologies in the underground economy of malware [1] include URL obfuscation, downloading and installing malicious codes from websites, use of alternate encoding schemes, web browser spoofing vulnerabilities, DNS attacks, cross-site scripting, etc. In view of the above, identifying basic fraudulent messages may be unfortunately difficult for the average user. Obviously, massive security education, training and awareness creation (SETA) is one sure way of mitigating against the threats of Phishing, SMiShing and Vishing. The weakest link in the mobile device security chain is still the mobile users[35].

2.5 Text Data Mining

Generally, data mining is the process of examining data from diverse perspectives and putting it into brief useful information. Data here includes facts, numbers, images, text and voice. Text data mining as a subset of data mining is employing statistical modeling and machine learning techniques in analyzing unstructured data contained in natural language text [36] in order to derive insights for possible business decisions.

A typical analysis using text mining examined various multivariate constructs for the effectiveness of anti-phishing awareness training conducted for various hi-tech firms, revealed that end-users were less likely to be cyber-victims and identified fraudulent websites after the awareness sessions[29]. Interestingly, the study discovered that users rather had difficulties in interpreting long URLs.

Another study uncovered that cyber-security expert opinions varied on the effectiveness of security education used in combating Phishing scams[37]. It also recommended the need to make SETA programs fun and that social networking sites may be utilized in furtherance of security goals.

©2009-2014 CIS Journal. All rights reserved.

3. METHODOLOGY

This section describes the research methods and approaches adopted in this study. It involves the investigation into various forms of attacks on mobile devices. The samples were purposively selected from amongst friends and family, office colleagues, and some students on a university campus. The datasets were analyzed, classified per Telcos operating in Ghana, even though the treatment of results is rendered anonymous. The operating systems for the selected sample mobile devices were restricted to most common ones, which are Microsoft Windows, Android and iOS.

Extensive literature review, by way of gleaning through numerous electronic libraries, online databases, documents, and journals, were carried out. Based on that, the data collection process was embarked upon. It assisted in refining the research questions and assumptions.

Pre-survey briefing with the selected users (samples) was carried out to inform them of the research objectives, to explain key concepts and to assure them of the confidentiality of their responses. Survey administration and strategic follow-up interviews were carried out to collect the datasets used for the analysis. Interviews were employed to elicit the end-users opinions on Phishing, SMiShing and Vishing threats against mobile devices. They also offered insights into issues regarding cyber-victims and their perceptions.

The target samples elicited were twenty (20) and have the various backgrounds in database administration, investment banking, business executives and telecommunications or technology expertise. The selected samples (end-users) were briefed the study's expectations and they were commissioned to report certain cyber incidents form websites, email messages, text messages, Instant messaging, voicemail and calls received during the study period. The threats were categorized into conventional and contemporary phishing attacks, which is in accordance with similar studies[38]. The conventional form involves those email messages and website requests (and pop-ups) intending to lure users to furnish some user credentials. Whilst the contemporary form consists of text messages, Face book chats, WhatsApp messages, Instant Messaging (including Skype, Twitter, MS IM, Yahoo messenger, etc.) and voicemail and calls.

Participants were asked to forward any suspicious messages or incidents to the researchers for validation. Then, they were also required to record or log the incident with brief notes on the attack for further analysis. It must be noted that, Vishing attacks were not validated as they may be calls that can't be forwarded.

Some key characteristics of what the participants were to look for are as follows:

3.1 General Characteristics

i. Click here to view the file account online
ii. Try it now
iii. Click here if you have forgotten your password
iv. You have receive a secure message
v. Click here to upgrade/ update social account password

3.2 Phishing Characteristics

i. Your documents have been completed, to view, download or print the completed document click below. The message was sent to you by administrator
ii. You have receive a secure message from, to decrypt the message provide password
iii. To read the encrypted message complete the following , double click the attachment to download the file to your computer
iv. View recent activity
v. Want to be friends with you on Face book

3.3 SMiShing Characteristics

i. Notice your Face book profile. I love to chart with you
ii. money transfer notification (details of the transaction attached)
iii. full details please visit website
iv. you are advised to send the following information to your agent to facilitate the release of funds to you
v. l've got something to show you

4. FINDINGS

This section presents the results of the study in a systematic manner. The texts, tables and figures are organized in a way to facilitate easy interpretation of the findings.

Data collected from the survey were first preprocessed to create a unified dataset. Also, the interviews were transcribed and preprocessed. The datasets consisted of 60% men and 40% women.

Key metrics examined are user's knowledge of generic online usage, user's online behavior, and user's perceptions of phishing threats against mobile devices.

4.1 User's Knowledge of Online Facilities

Here, we assess the user's level of knowledge in basic online services, such as web browsing, responding to pop-ups and filling in online forms. The extent of technological know-how or "tech-savviness" with respect to web browsing, pop-ups, making use of online facilities, as well as users being comfortable using online services, are as depicted in the chart below (Figure 4-1).

Vol. 5, No. 4 April 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences
©2009-2014 CIS Journal. All rights reserved.
http://www.cisjournal.org

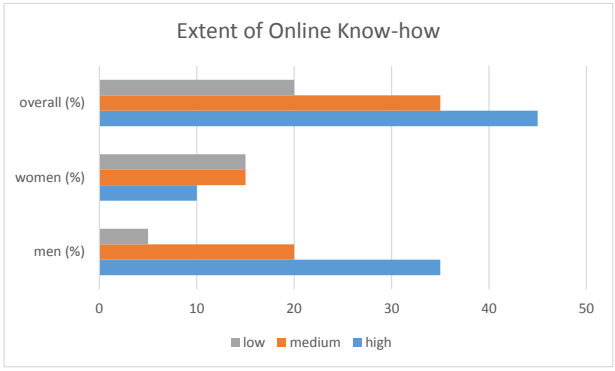

Fig 4.1: Extent of Online Services Know-how

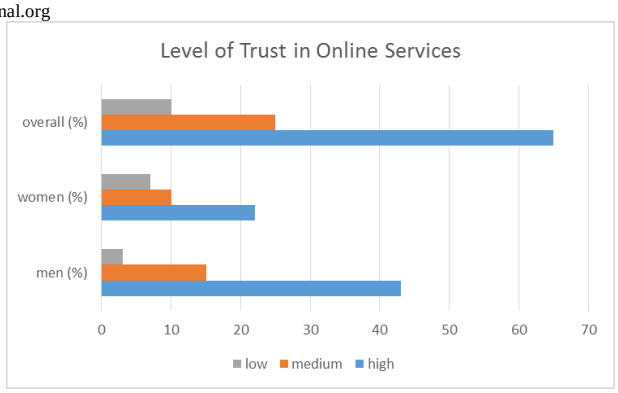

Fig 4.2: Level of Trust in Online Services

This tend to buttress the notion that men are technically savvy than women and are also likely to adopt (and use) new technologies than women.

4.2 User's Online Behavior

Here, we examine user behavior whenever the end-user comes face-to-face with not-well understood messages, opening email attachments (even from unknown sources), responding to online requests (by clicking on links) and threats. According to the Space Transition Theory (STT) [39], users are likely to behave differently in the online environment from their physical space. STT postulates that persons in good societal standing or position, are likely to repress their crminal behavior in physical space, but are highly disposed to commit crime in cyber-space. In essence, a person's concern for his/her status on physical space is not transition to cyber-space, due the dissociative anonymity in cyber-space which gives users (especially victims) the platform to open up to strangers about their personal issues.

We herewith seek to gain some insights into how users fall prey to online fraud or phishing attacks. Figure 4-2 depicts how comfortable and trusting it is for end-users to act on unknown messages and opening any attachments, as well as clicking on any link provided they've been requested to do so. Overall, 65% felt comfortable in providing their personal credentials online, and alluded to being lured by juicy discounts offered on items being purchased. They also indicated that they trusted their banks to be responsible for their unwariness [1] and to protect them from fraudsters. 10% of the users were cautious in giving their information online, whilst 25% were somewhat clueless and apathetic to the happenings online. They assume that no one would hurt them.

4.3 User's Perception of Online Threats

In this sub-section, we examine the end-user's perceptions of Phishing, SMiShing and Vishing attacks against mobile devices. Some key metrics here are perceived awareness of those threats and associated risks, the extent of scrutiny with which users would assess messages received before acting upon them, and the possibility of being a cyber-victim.

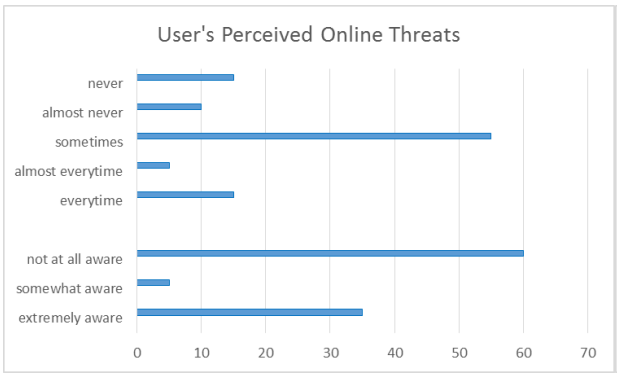

Fig 4.3: User's Perceptions on Online Threats

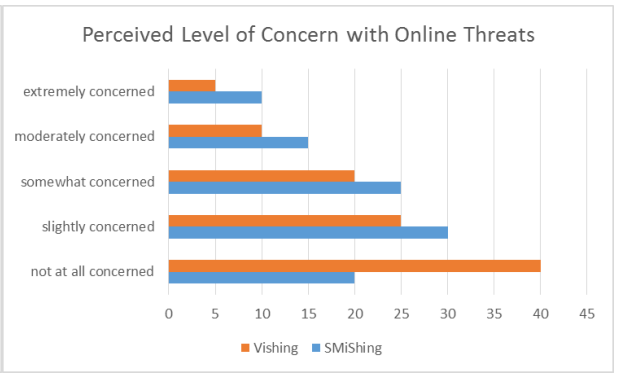

Fig 4.4: Perceived Level of Concern

The results indicate that most users are either slightly aware or not at all aware of Phishing, SMiShing and Vishing threats against their mobile devices. Interestingly, about 35% are moderately to extremely aware of those threats. In terms of perceived scrutiny of messages and/or requests, 55% would occasionally examine the messages as perceived threats, whilst 35% would never or almost never scrutinize any messages.

Vol. 5, No. 4 April 2014 ISSN 2079-8407
Journal of Emerging Trends in Computing and Information Sciences
©2009-2014 CIS Journal. All rights reserved.
http://www.cisjournal.org

Figure 4-4 indicates that the level of concerns perceived on SMiShing and Vishing as mobile threats. Strikingly, there's moderate to extreme low level of concern regarding threats of SMiShing and Vishing against their mobile devices. It was noted that 15% of users succumbed to SMiShing attacks, whilst 5% had been cyber-victims of Vishing attacks.

Using the Text data mining techniques with Wordle.net, the figure 4-5 below depicts the taxonomy of key words and phrases that end-users ought to be aware of in mitigating Phishing, SMiShing and Vishing risks. For instance, **{message; click; password; document; download; link; account; view; etc.}**

Fig 4.5: Taxonomy of Key Words

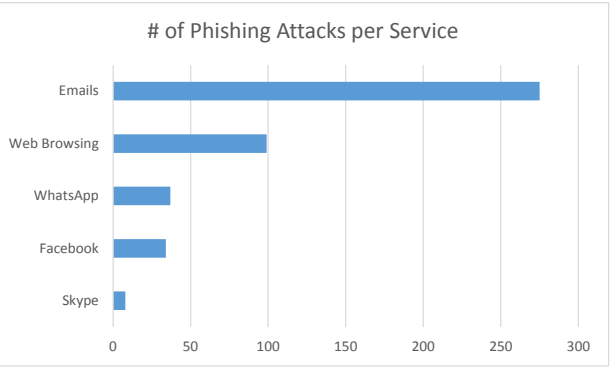

Fig 4.6: # of Phishing Attacks per Service

In addressing the issue of what is the extent of Phishing attacks on mobile devices, we observe the following datasets categorized into type of services used in launching phishing attacks. Figure 4-6 indicates that email messages are most likely to be used for phishing against mobile devices, whilst Skype is very unlikely to be used.

As regards the distribution of the attacks, Figure 4-7 shows that Phishing attacks are most prevalent form of mobile threats, with Vishing being the least.

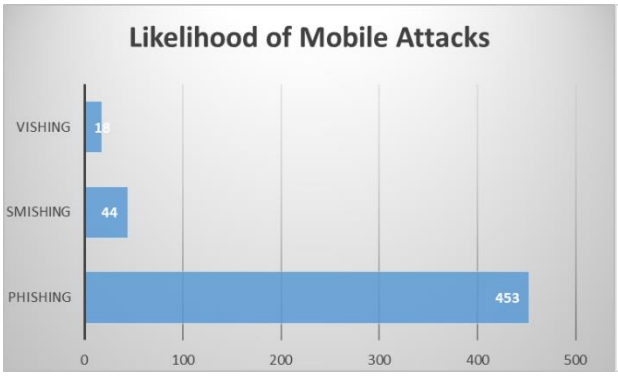

Fig 4.7: Likelihood of Mobile Attacks

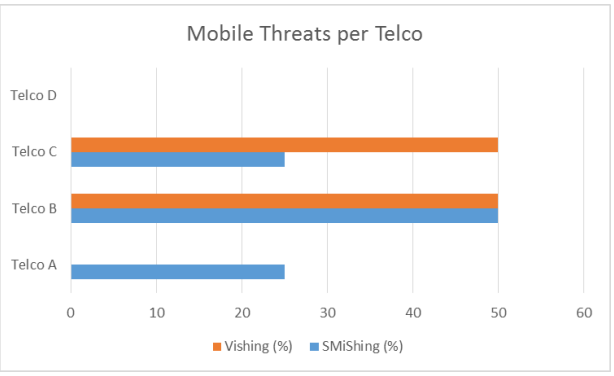

Fig 4.8: Mobile Threats per Telco

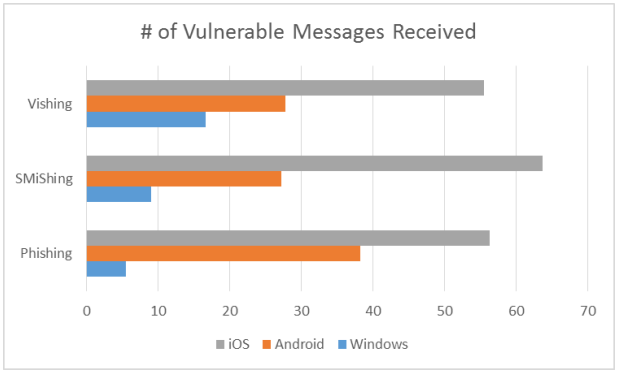

Fig 4.9: # of Vulnerable Messages Received

It is worth noting that the sample users were subscribing mobile communications services from amongst 4 out of the 6 operators. It is observed, from Figure 4-8, that Telco D had neither SMiShing nor Vishing attacks. This could be attributed to either strong security measures filtering customers' messages appropriately or that it had low patronage of services. Conversely, Telco B seems to be the most vulnerable mobile network. The reasons may be high patronage or low security filters for customers or yet, the issue of false negatives intrusion detection, thus allowing suspicious messages.

Finally, Figure 4-9 depicts the extent of susceptibility of mobile device operating systems. As indicated in literature earlier on, the most popular

©2009-2014 CIS Journal. All rights reserved.

operating systems were examined. The results indicate that the iOS is the most vulnerable, with the Windows being the least vulnerable. It could be as a results the samples using more iOS based devices than the rest. The true extent of susceptibility would require further studies beyond this exploratory one.

5. CONCLUSION

This concluding section summarizes the key findings, discusses the study's limitations and makes concluding remarks for future research.

The object of this study was to identify the various threats that militate against mobile devices and the behavior and perceptions of end-users towards those threats. We endeavored to address the extent to which phishing attacks affect mobile devices. Overall, men were perceived to have adequate technological know-how of the operations of the Internet services and facilities. Similarly, they were found to be so comfortable and trusting whenever on the cyber-space, thus making them more susceptible to mobile attacks than their women folks.

We also examined the users' behavior when using mobile online services. Credence was given to the space transition theory, such that cyber-victims dissociate their physical profile from the cyber-space. Users were also found to be unwary or oblivious of the numerous phishing attacks against their mobile devices. It was established that most users were either slightly or not at all concerned with cyber-attacks.

Finally, the taxonomy of 'alluring" and "decoying" words used in phishing attacks could be useful benchmark to end-users to guard against becoming cyber-victims. Though, the findings from this study are empirically deduced, we were, however, handicapped with lots of samples in order to generalize the findings. Obviously, further studies would be appropriate to establish any linkages of vulnerabilities with mobile operating systems and also to ascertain whether or not there's any correlation between mobile network operators and the extent of phishing susceptibilities.

REFERENCES

[1] E.O.Yeboah-Boateng, "Of Social Engineers & Corporate Espionage Agents: How Prepared Are SMEs in Developing Economies?," Journal of Electronics & Communications Engineering Research (JECER), vol. 1, no. 3, pp. 14-22, November 2013.

[2] L. Chen-Wilson, A. Gravell & D. Argles, "Giving You Back Control of Your Data: Digital Signing Practical Issues," in World Congress on Internet Security (WorldCIS), London, 2011.

[3] G. Ollmann, "Understanding X-morphic Exploitation," 2007.

[4] Hu Wen-Chen, Zuo Yanjun, N. Kaabouch & Yang Hung-Jen, "Mobile Data Protection Using Handheld Usage Context Matching," in Mobile Data Management Systems, Services & Middleware MDM'09, Tenth International Conference, Taipei, 2009.

[5] R. Prasad, "Handheld Devices," in Anesthesia Informatics: Health Informatics, Springer, 2009, pp. 409-424.

[6] Zulfikar Ramzan & Candid Wuest, "Phishing Attacks: Analyzing Trends in 2006," in CEAS 2007, 4th Conference on Email and Anti-Spam , Mountain View, CA, 2007.

[7] Min Wu, Samson Garfinkel & Robert Miller, "Secure Web Authentication with Mobile Phones," MIT Computer Science and Artificial Intelligence Lab, Cambridge, MA, 2004.

[8] Rachna Dhamijia, J.D. Tygar & Marti Hearst, "Why Phishing Works," in SIGCHI Conference on Human Factors in Computing Systems, New York, NY, 2006.

[9] E. O. Yeboah-Boateng, "Fuzzy Similarity Measures Approach in Benchmarking Taxonomies of Threats Against SMEs in Developing Economies," Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering & Medicine, vol. 4, no. 1, pp. 34-44, 2013.

[10] X. Dong, "Defending Against Phishing Attacks," University of York, 2009.

[11] Kevin D. Mitnick & William L. Simon, The Art of Deception: Controling the Human Element of Security, John Wiley & Sons, Inc., 2001.

[12] D. Gragg, "A Multi-Level Defense Against Social Engineering," SANS Reading Room, SANS Institute, 2003.

[13] J. Long, No Tech Hacking: A Guide to Social Engineering, Dumpster Diving & Shoulder Surfing, Elsvier, Inc., 2007.

[14] RSA, "Phishing, Vishing and Smishing: Old Threats Present New Risks," RSA Monthly Online Fraud Report, September, October & November

©2009-2014 CIS Journal. All rights reserved.

2009.

[15] C.-W. Argles D, "Healthcare Data Management Issues and the eCert Solution," International Conference on Information Society, June 2011.

[16] IC3/FBI, "IC3/FBI Annual Cyber-security Survey," 2010. [Online]. Available: www.fbi.gov/stories/. [Accessed june 2013].

[17] Canalys Research, "Google's Android Becomes the World Leading Smartphone," Canalys Research Release, 2011.

[18] B. Halpert, "Mobile Device Security," in !st Annual Conference on Information Security Curriculum Development, New York, NY, 2004.

[19] I. Richardson, "Mobile Technosoma: Some Phenomenological Reflections on Itinerant Media Devices," Fibreculture Journal, vol. 6, 2005.

[20] Alphar, G., Hoepman, J.H. & Siljee, J., "The Identity Crisis: Security, Privacy and Usability Issues in Identity Management," Computer Research Repository (CoRR) arXiv: 1101.0427, 2011.

[21] Rachna Dhamijia & Lisa Dusseault, The Seven Flaws of Identity Management: Usability and Security Challenges, IEEE Security and Privacy, 2008.

[22] J. Lin, S. Amini, J.L. Hong, N. Sadeh & J. Lindqvist, "Expectation & Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing," in ACM Conference on Ubiquitous Computing, New York, NY, 2012.

[23] Vivek Anandpare, Andrew Dingman, Markus Jakobsson, Debn Liu & Heather Roinestad, "Phishing IQ Tests Measure Fear, Not Ability," 2007.

[24] W.D. Yu, S. Nargundkar & N. Tiruthani, "A Phishing Vulnerability Analysis of Web-based System," in IEEE Symposium on Computer & Communications (ISCC 2008), Marrakech, Morocco, 2008.

[25] L. Musthaler, "Phishing, SMiShing and Wishing It Would Stop," 2013. [Online]. Available: www.securitybistro.com/?p=5667. [Accessed 17 December 2013].

[26] Vivek Anandpara, Andrew Dingman, Markus Jakobsson, Debin Liu & Heather Roinestad, "Phishing IQ Tests Measure Fear, Not Ability," USEC'07, 2007.

[27] S. Furnell, "An Assessment of Website Password Practices," Computers & Security, vol. 26, no. 7-8, pp. 445-451, 2007.

[28] T. Shaw, "Vishing, Phishing and Smishing - Oh My," USAA's, 2012.

[29] Julie S. Downs, Mandy Holbrook & Lorrie F. Cranor, "Behavioral Response to Phishing Risk," in Anti-Phishing Working Groups, 2nd Annual eCrime Researchers Summit, New York, NY, 2007.

[30] Malcolm Pattinson, Cate Jerram, Kathryn Parsons, Agata McCormac & Marcus Butavicius, "Why do some people manage phishing e-mails better than others?," Information Management & Computer Security, vol. 20, no. 1, pp. 18-28, 2012.

[31] J. Turner, The Structure of Sociological Theory, 1991, p. 354.

[32] Fred D. Davis, Richard P. Bagozzi & Paul R. Warshaw, User Acceptance of Computer Technology: A Comparison of Two Theoretical Models, vol. 35, INFORMS, 1989, pp. 983-1003.

[33] Venkatesh, Viswanath; Morris, Michael G.; Davis, Gordon B. & Davis, Fred D, "Unified Theory of Acceptance and Use of Technology," 2003.

[34] Franck Tétard & Mikael Collan, "Lazy User Theory: A Dynamic Model to Understand User Selection of Products & Services," in 42nd Hawaii International Conference on System Sciences, HICSS '09, Hawaii, 2009.

[35] T. K. Bikson, Understanding the Implementation of the Office Technology, 1987.

[36] Turban, Efraim; Ramesh Sharda & Durun Delen, Decision Support & Business Intelligence Systems, Prentice Hall, Pearson Education, Inc., 2011.

[37] Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L., and Hong, J., "Teaching Johnny Not To Fall for Phish," In Association for Computing Machinery's Transactions on Internet Technology (TOIT), 2009.

[38] Cik Feresa Mohd Foozy, Rabiah Ahmad & Mohd

©2009-2014 CIS Journal. All rights reserved.

Faizal Abdollah, "Phishing Detection Taxonomy for Mobile Device," International Journal of Computer Science Issues, vol. 10, no. 1, 2013.

[39] K. Jaishankar, "Establishing a Theory of Cyber Crimes," International Journal of Cyber Criminology, vol. 1, no. 2, July 2007.