Did you know that during a single day, there are about 507 billion emails that are sent out and out of those, 80% are more than likely to be spam, malware and phishing messages [2]. What exactly is Phishing? Phishing is the process in which a phisher sends out a single message to a large population in the hope that some part of the population will respond to the message. This message can be in the form of an email message that people receive in their inboxes, and the email message can direct people to provide their personal information, click on a link to a fraudulent website, download malicious software or open an attachment which contains malware [2]. After people are lured into visiting these fraudulent websites, they are tricked into providing their personal sensitive and financial information, which the phisher can use for his personal gain [1]. Organizations have tried using technical methods to protect themselves from phishing, which include filtering phishing messages, automatic detection of fake websites and installing anti-phishing warning systems, but technical methods alone cannot protect people against phishing attacks. Phishers use valid communications channels such as email to send messages, therefore it can become complicated to separate deceptive messages from authenticated messages, and that is why it is very important for people who use email to know how to detect whether a message is from a phisher [2]. Phishing messages use diverse set of persuasion elements and influence techniques to make the user respond to fake messages or download malicious software on computer that will in return let the phishers gain access to the user’s personal information, and it is very important as users to know what these techniques are [2]. This paper has been divided into two parts, where the first part discusses the persuasive elements that phishers use, and the second part discusses the influence techniques that phishers use to lure users into providing sensitive personal information about themselves, which jeopardizes their security.

When phishers send out fake messages, their main goal is to entice the user to respond to the fake message or download malicious software on computer in order to steal sensitive personal information. In order for a message to be believable and persuasive, it must come from a credible source, must present a quality argument and must use certain structure elements such as repetition [1]. For a source to be credible, the messages must look exactly like the messages that people would expect to receive [2], and if the message has spelling mistakes or looks different in its
layout than the expected message, then it is more likely to raise suspicion and the receiver is less likely to respond
[2]. Phishers also use graphics, logos, contact methods, and forged security seals from financial institutions or other
trusted institutions to make the recipient believe that the message is from a legitimate source [2]. According to past
studies, recipients are more likely to respond messages that show urgency and require the recipient to respond as
soon as possible or within a certain time frame, and messages that use elements such as repetition and a certain order
can also increase the persuasiveness of a message [1].

The paper “Understanding persuasive elements in phishing e-mails”, which has been written by Daejoong
Kim and Jang Hyun Kim, performed a study in which the authors examined the different persuasive elements
present in e-mail messages, and this was done by combining categorical content analysis and semantic network
analysis. In this study a total of 2608 emails were collected from the archives of Anti-Phishing Working Group
website, and 285 e-mails were randomly selected and 30 phishing e-mails were assigned to three coders and a
coding reliability test was performed and the data was found to be satisfactory [1].

For categorical content analysis, source credibility, argument quality of the message and the structure of the
message were the three areas that were analyzed. There were five markers that were used to measure source
credibility, and they included sender’s domain name, sender’s e-mail address prefix, if the sender was mentioned in
the email or not, if contact information was present and if a company logo was present. To analyze the quality of
the argument presented in the message, rational appeals, emotional appeals, motivational appeals and time pressure
were analyzed. In rational appeals, the three types of reasoning that were analyzed included cause, sign and
analogy. Reasoning from cause in a message shows that one event caused the second event to happen. For
example, the message can contain something that says a new security system has been developed and the user’s
information needs to be updated [1]. Reasoning from sign indirectly indicates that the occurrence of one event is a
sign that another event will occur. Reasoning from analogy basically presents an analogy to explain the situation, so
that it is easier for the recipient of the e-mail to understand what is going on. In emotional appeals, there were seven
types of emotions that were analyzed and they included fear, being sad, feeling guilty, angry, happy, and
affectionate and being humorous. Messages can use fear appeals to make the recipient perform a certain task.
Motivational appeals were analyzed based on the five level hierarchy of Maslow, which included human needs,
safety needs, the need to belong, self-esteem needs, and self-actualization needs. Time pressure refers to how much
time the phisher gives the recipient to respond to the message. Structure of message can be analyzed based on
whether the message sent was explicit or implicit and whether repetition of information was present. Explicit
messages tell recipients what they should conclude from the message; whereas implicit messages let the recipients
make their own conclusions. In semantic network analysis, the relationships between words were analyzed, and
CATPAC, which is software that analyzes based on frequency of words, was used to analyze the distance between
words and the coexistence of words and the repetitiveness of words in phishing messages [1].

For categorical content analysis, the study found that when it comes to phishing attacks, financial
institutions have the highest rate for getting targeted by a phisher. Online retailers such as eBay, Amazon and
PayPal came in second place in terms of getting targeted by phishers. For source credibility, it was found that
phishing e-mails used legitimate sender prefixes, domain names and company logos, and there were also few e-
mails that provided telephone numbers or e-mail addresses. When it came to argument quality of a message, it was
found that in rational appeals reasoning from cause succeeded reasoning from sign and reasoning from analogy.
Emotional appeals mostly employed fear appeals, with affection appeals in second place and happiness appeals in
third place. Motivational appeals mostly employed safety needs, with self-esteem appeals in second place and the
need to belong in third place. When it came to time pressure, it was found that 63 e-mails asked the recipient to
respond immediately, 78 asked the recipient to respond within 24 hours, 13 asked the recipient to respond within 48
hours, three asked to respond within 72 hours and seven e-mails gave more than 72 hours to respond. There were
121 messages that did not ask the recipient to respond within a certain period of time. When it came to the structure
of the message, it was found that most messages employed explicit conclusions over implicit conclusions and used
non-repetitive messages over repetitive messages [1].

For semantic analysis, the study found that some of the most occurring words were account, please, eBay,
banking, security, update, access, customer, PayPal, click, and link among others. Based on the most occurring
words it was indeed found that the main purpose of phishing is to trick people into providing their personal
information by telling them their online accounts are having security problems and personal information needs to be
updated. CATPAC also performed cluster analysis and two main clusters were found based on distance between the
repetitive words and coexistence of words. The first cluster was the security cluster, and the second cluster was the
privacy cluster. In the first cluster, a bulk of the words had to do with updating or verifying personal information,
and in the second cluster most of words had to do with having recipients click on links that could present privacy
problems [1].
Based on the results of this study it can be seen that most phishing e-mails have high credibility since they include company logos and domain names and very few emails have direct contact information, which could be due to the fact that having such information would give recipients the choice to request additional information, which in return could decrease the success rate of the phishing e-mail. Phishing messages also employ variety of appeals in order to pressure the recipient into doing what the phisher wants, and earlier studies had assumed that there were very clear differences between phishing and authentic messages, but in reality there is not that much difference between the two, instead phishing messages are exactly like authentic messages with minor changes. There were three important patterns that were observed through this study. Firstly, it was found that contrary to popular belief, phishing messages do not include time pressures because 42 percent of the e-mails did not even mention a certain time frame in which the message had to be returned. This suggests that more research needs to be done in this area. Secondly, it was found that phishing messages use both rational and emotional appeals, which differs from past studies, which showed that phishing messages mostly employed emotional appeals such as fear. Thirdly, it was found security and privacy concerns are the two strategies that phishers use to lure the recipients into providing personal information to fraudulent websites or to click on malicious links [1]. It is very important for people to realize when they are being tricked into compromising their security and the security of their computer and knowing the kind of techniques that phishers use is very important. This paper talked about the different persuasive elements that phishers use, but there are other techniques like influence techniques that phishers use as well.

The paper “Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance” analyzed the different influence techniques that phishers use and why certain techniques when used in phishing messages are very dangerous. When people see phishing messages, they will likely respond to them like they do to other authentic messages because they are usually using system 1 thinking, which can be seen as automatic thinking, and people do not think that a message will be harmful unless they have been notified to be careful regarding phishing [2]. This study formed three hypotheses regarding influence techniques used by phishers. The first hypothesis was that messages that contain influence techniques such as likeability, reciprocity, consistency, social proof, references to authority and scarcity increase the chances of a recipient responding to a phishing message. The technique of liking takes into consideration the fact that people are more likely to respond to a message that is coming from someone they like. The second hypothesis was that recipients are less likely to respond to messages that contain influence techniques regarding prior shared experiences than messages that contain no shared
experiences. The reason for this is that if a phisher uses past shared experience in the message, and if the details of the experience do not match, then the recipient is more likely to be alerted that the message is fraudulent. The third hypothesis takes into consideration motivation and self-determination. It hypothesizes that influence techniques that arouse a high level of self-determination behavior are more likely to have a higher rate of return for phishing messages than techniques that arouse low level of self-determination behavior. For example, techniques such as liking, social proof and scarcity will cause people to respond to a higher extent because people will think they want to respond, and techniques such as consistency, reciprocity and authority will cause less people to respond because people will think they have to respond due to other’s expectations [2].

A field experiment was performed to test the three hypotheses, and it was conducted at a university in the Midwestern United States. 2624 participants were selected at random from the university population, and the university provided the e-mail address and gender of the participants, with 53 percent being females. For each hypothesis, the participants received the same phishing message asking them to visit a fake website and provide their username and password. A fictional employee of the university signed the phishing message in question, and it was delivered from a fake university e-mail address. The phishing messages were modified to fit the criteria of the three hypotheses, and after visiting the fake website, the usernames of the participants were recorded but their passwords were deleted, and when the participants logged into the website they received the message that the site was under construction and to come back at a later time. The duration for the phishing attack was four days, and the researchers also informed the IT helpdesk of the experiment as well [2].

The results of the experiment showed that out of the 2624 participants, 178 participants provided their login information. In order to test the first hypothesis, a logistic regression was performed in which the influence techniques, liking, reciprocity, social proof, authority, consistency and scarcity were used as the predictor categorical variables, and the outcome variable was whether the participants responded to the phishing message or not by logging into the fake website. The gender of the participants was included in the regression as a control variable. The results of the test were consistent with the first hypothesis for four influence techniques, which included liking, scarcity, reciprocity and social proof, while consistency did not show any influence in responding to phishing messages and authority showed influence but in the opposite direction to the hypothesis. It was also observed that females were more likely to respond to phishing messages than males. To test the second and third hypotheses, the marginal effects for each of the influence techniques were plotted against the reference probabilities,
which are probabilities that a participant will respond to a phishing message [2]. The results were compatible with the second and third hypotheses and proved that phishing messages that aroused a high-level of self-determination and did not include any made-up prior shared experiences had the highest rate of return for phishing messages, with messages that had made-up prior shared experiences and aroused a little bit of self-determination being in second place. The messages that did not present any self-determination and did not have any fictitious shared experiences were found to be least dangerous types of messages. A second linear regression was performed in which the three different influence techniques categories, self-determined and no fabricated shared experiences, self-determined and fabricated shared experiences, and non-self-determined and no fabricated shared experience were used as predictor categorical variables and the outcome variable was whether the participants responded to the phishing message or not, with gender serving as the control variable. It was found that the category that did not require any fabricated shared experiences and presented self-determination was the only category that impacted whether a participant responded the phishing message or not. This test was in line with the first, second and third hypotheses [2].

Phishing has been around for a long time and is something that organizations and ordinary people have to deal with everyday. People are tricked into giving away their personal information by visiting a fraudulent website or they are tricked into downloading malicious software on their computer, which comprises their personal and computer security. The two papers that were discussed in this paper shed light on how to differentiate between authentic and deceptive messages, and what persuasive elements and influence techniques phishers use that make people want to respond to a phishing message. I feel that it is very important for individuals and organizations to train people so that they know how to identify a phishing message by analyzing it based on different techniques being used in the message [2]. Unknowingly responding to phishing messages not only compromises a user’s personal security but also the security of the computer system because a phishing message might have persuaded the user to download malicious software, which would give the phisher power to access information on the computer and change the security settings.
Works Cited
