Special Issue, Vols. 6 & 7, 2016-2017
East West Journal of Humanities

Legitimization in Phishing: A CDA Perspective

Tanzina Tahereen
East West University

Abstract

This paper mainly aims at analyzing how various discursive strategies legitimizing different requests and assertions in phishing emails are exploited to exercise the social power abuse and influence cognitive knowledge of the users. This study attempts to interlock Van Leeuwen and Wodak's (1999) four legitimization strategies and Van Dijk's (1998, 2001, 2006) 'triangulation approach' of discourse-society-cognition cycle in order to analyze the legitimization strategies in phishing from a critical discourse perspective. The discursive approach includes the discursive strategies in legitimation, the social approach shows the social power abuse engaged in legitimization, and the cognitive approach presents the manipulation of the user's beliefs influencing their actions. In order to conduct this study, qualitative method is applied in randomly selected 25 phishing emails as textual data.

Keywords

Legitimization, discourse, power, cognition, phishing.

Introduction

Bose & Leung (2008) define phishing email as a deceptive email where an executor (phisher) attempts to masquerade the form of email in such a way that it appears to the recipient as a legitimate request for personal and sensitive information (as cited in Vishwanath, Herath, Chen, Wang & Rao, 2011). Moreover, according to the Anti-Phishing working group, phishing is a kind of online identity theft trick which tries to deceive consumers by filching their information on personal identity and financial account credentials through the use of social engineering and technical maneuvers (Vittal, 2005). They exploit some credible identity or name, show their associations with renowned organizations, and use some persuasive techniques to establish their claims, advices, requests as valid and legitimate to the recipients. These seem trustworthy to many and lead them to follow the actions instructed in the emails. Because of these fraudulent activities, people are losing their confidence on online interfaces, and in the long run, it augments the economic loss every year (Belanger et al., 2006, cited in Vishwanath et al., 2011). There are many studies conducted from different perspectives regarding the question how these phishing emails make others entrapped. Consequently, this paper concentrates on the analysis of phishing strategies from critical perspective. Among all the strategies, legitimization is one of the most significant tactics to enable phishers earning people's trust, and convincing them to respond. It usually comes in the form of a request, an advice, a command, an instruction, or an assertion which is as legitimized as possible through many different tactics in order to make it more credible and trustworthy to the recipients.

By applying Van Dijk's (1998, 2001, 2006) 'triangulation approach', this study shows how social power is abused through legitimization in order to deceive the recipients. Moreover, four strategies of legitimization promoted by Van Leeuwen & Wodak (1999) are applied in order to illustrate the discursive strategies used in phishing. The legitimization strategies are incorporated in the 'triangulation framework' as discursive strategies to show how legitimization is considered as a power tool to exercise control over individuals, and to manipulate their beliefs, opinion and actions. Moreover, cognitive approach shows how individuals evaluate and process legitimization, and how this evaluation, in-turn, affects the individuals' susceptibility in phishing (Vishwanath et al., 2011). Not many researches are done on the discursive strategies of legitimization and their manifestation in social power control and social cognition.

Concept of Legitimization

Legitimacy and legitimization are crucial to operating social action in general and organizational action in particular (Vaara, Tienary & Laurila, 2006, p 789). According to Weber (1964), "Every system of authority attempts to establish and to cultivate the belief in its legitimacy" (as cited in Van Leeuwen, 2007, p1).

Suchman (1995) states, legitimacy is a major concept in institutional theory, and it is defined as a generalized concept or theory of the acceptance, desirability and appropriateness of any actions of an entity by the norms, values, beliefs and definitions of any social structures (as cited in Whittle, Carter & Mueller, 2014). Also, Suchman (1995) adds that legitimacy or sense of legitimacy is based on pragmatic, moral and cognitive analyses. The pragmatic one refers to the estimation of egotistical meaning; the moral refers to the social acceptance of norms and rules, and the cognitive part relies on 'comprehensibility' and 'taken for grant-ed-ness' (cited in Vaara et al., 2006, p 791). Moreover, according to Berger and Luckmann (1966), Legitimation provides the 'explanations' and justifications of the salient elements of the institutional tradition. (It) 'explains' the institutional order by ascribing cognitive validity to its objectivated meanings and (...) justifies the institutional order by giving a normative dignity to its practical imperatives. (as cited in Van Leeuwen, 2007, p 92).

Therefore, justification, acceptance and explanation provide a pragmatic standard and rationale to accord with the institutional order (Krause & Nielsen, 2014). The organizations which are highly dependent on the support and resources of other actors, requires legitimacy to a higher degree for their organizational actions (Oliver, 1991, cited in Whittle et al., 2014).

Furthermore, Van Leeuwen (2007) has illustrated language as the most important tool for carrying such legitimization attempts. Therefore, institutional vocabularies are considered a fundamental tool for legitimization explanations (Berger and Luckman, 1966, cited in Van Leeuwen, 2007; Suddaby & Greenwood, 2005), and these 'vocabulary of motive' vary from situation to situation apt to institutional-pertinent attitudes (Mills, 1940, cited in Whittel et al., 2014)

Phishing emails are also called a kind of 'pastiche', a form of imitation of the legitimate style or structure of a particular genre, especially business emails of banks, financial organizations or other well known international organizations (Blythe & Clark, 2010). There are apparently credible, trustworthy attempts to persuade or manipulate the recipients through the fake legitimacy in discourse.

Another significant phenomenon which is brought in this paper along with legitimacy that Rocco, Finholt & Herbsleb (2000), Bose et al. (2002) & Ridings, Gefen & Arinze (2002)

emphasize is 'trust', a social keystone for computer-mediated communication (CMC) which augments social collaboration, cooperation and lubricates information exchange (as cited in Vasalou, Hopfensitz & Pitt, 2008). Moreover, Corritore, Kracher & Weidenbeck (2003) delineate that online trust refers to a confident approach to a vulnerable online context believing that it does not threat one's susceptibility (as cited in Vasalou et al., 2008). Among two types of trusts, cognitive trust, that Rocco et al., (2000), Corritore et al., (2003), Riegelsberger, Sasse & McCarthy, (2005a) define as a change in belief and attitude because of rationalization of reliability factors (as cited in Vasalou, et al., 2008), is focused in phishing to form user's social cognition. Therefore, factors that construct and engender cognitive trust are reliability, authenticity, competence and responsibilities. Moreover, shared group identity reputation system enhances the trustworthiness of online interfaces more, especially in anonymous environment (Vasalou et al., 2008). Thus, phishers' strategy is being pretentious of possessing these features, and legitimizations work as a trust indicator for the users in this case.

Theoretical Framework

Critical discourse analysis is based on the concept of how discourse plays a significant role in legitimizing the inequality, injustice and dominance in the society (Van Leeuwen, 2009). Accordingly, this paper is based on two major theoretical ideas: Van Dijk's 'triangulation approach' of critical discourse analysis (CDA) (1998, 2001, 2006), and Van Leeuwen and Wodak's (1999) concept of 'legitimization'. In this paper, the former theory includes the latter for attending to the research questions.

Triangulation Approach

Van Dijk's (2001) multidisciplinary approach of CDA concentrates on socio-cognitive interface of discourse analysis. It focuses on various forms of social power abuse, dominance and inequality which are reflected through various discourses in different contexts (1998). His theoretical 'discourse-cognition-society' triangle or 'triangulation approach' describes these three terms in broader sense:

> 'Discourse' is here meant in the broad sense of a 'communicative event', including conversational interaction, written text, as well as associated gestures, facework, typographical layout, images and any other 'semiotic' or multimedia dimension of signification. Similarly, 'cognition' here involves personal as well as social cognition, beliefs and goals as well as evaluations and emotions, and any other 'mental' or 'memory' structures, representations or processes involved in discourse and interaction. And 'society' is meant to include both the local, microstructures of situated face-to-face interactions, as well as the more global, societal and political structures variously defined in terms of groups, group-relations (such as dominance and inequality), movements, institutions, organizations, social processes, political systems and more abstract properties of societies and cultures" (Van Dijk, 2001, p 98).

Thus, CDA indicates the integration of these three approaches into the critical analysis of any social problems. First, society is analyzed in CDA at micro-level e.g. social interaction, social situations, and at macro level e.g. group, organization or social structure. The macro notions of power exercised in the broader realm of the social structure and institutions is accountable for the apparent domination and subjugation, and internalization of that dominated behavior observed into the micro level of social discourses and practices.

Therefore, every discursive interaction, a part of a specific social structure (Van Dijk, 1998), reflects the social asymmetrical relationship between different social groups and represents

social hierarchies. Moreover, the central focus of CDA is the discourse of power, e.g. social power of groups or institutions. By power he refers to social power which is realized in terms of the control social actors or groups exercise over others. According to Max Weber (1946), power is a capability of a person or a group to compel its will on others against their interests (as cited in Servaes, 2013). Therefore, a specific group or institution exercises social power by controlling other's actions, beliefs and mental cognition based on the scarce resources in the society, such as money, knowledge, status, fame, force, information, culture or forms of public discourse or communications (1998). Van Dijk adds, "Those groups who control most influential discourse also have more chances to control the minds and actions of others" (1998, p 355). All types of power are not equally exercised. Power control can be more or less depending on the situation and domain, and even it can appear in an accepted, legitimated or natural form to the dominated (1998).

Second, Van Dijk (2001) talks about social cognition, which is a set of mental abilities, such as knowledge, attitudes, ideologies, norms and values. He adds that social representations are particularized in mental models, and it is through the mental models of every day discourse that we construct our knowledge, social attitudes and ideologies and fundamental norms and values, and finally social representations. This is how social power affects our cognition. Controlling people's knowledge and belief is also a fundamental way to reproduce dominance and hegemony. This is called 'mind control', e.g. control of people's belief and actions by Van Dijk (1998, p 356). There are contextual and discursive conditions to construct such 'mental model'. Authoritative, trustworthy and credible sources of knowledge, specific situation of knowledge, lack of alternative sources of information and ignorance of appropriate knowledge work as contextual conditions to influence one's cognition. Moreover, structural strategies of text and talk as discursive conditions exercise control over others' 'mental model'. In other words, "given a specific context, certain meanings and forms of discourse have more influence on people's minds than others" (Van Dijk, 1998, p 357). This cognitive dimension involves the persistence process of information evolving from various types of discourse structures effecting the basic understanding process in short term memory to the formation, activation and enhancement of 'mental model' in episodic memory of LTM (long term memory), and finally, leading to more stable, permanent construction of social representation, such as knowledge, beliefs, attitudes, ideologies, norms and values (Van Dijk, 2006). This is how someone perceives and comprehends a specific kind of text and talk.

Third, it is obvious that all the power control and cognitive advancement are accomplished through the means of discourse. There are various kinds of discursive features Van Dijk talks about, such as word selection, the structures of propositions, and coherence and other relations between propositions, topic selection, ideological polarization, positive self representation, legitimization, structures of text, rhetoric features, features of spontaneous talk like turn taking, repairs, pauses, hesitation, and so on. Discourse having a strong connection to legitimacy always provides the 'frame' for the establishment of legitimacy which helps people to interpret particular issues around them (Van Dijk 1998, Van Leeuween & Wodak, 1999). In this paper, the discursive strategies include the legitimization strategies significantly in order to show how these legitimizations exercise power and constructs cognitive trust in one's 'mental model' to influence one's actions.

Legitimization Strategies

According to Van Leeuwen & Wodak (1999), there are four types of 'legitimizations' based on the form and content: (i) authorization, (ii) moral evaluation, (iii) rationalization, and (iv) mythopoesis. They can occur in isolation or in combination. These four categories are explained as:

1. *Authorization,* that is, legitimation by reference to the authority of tradition, custom and law, and of persons in whom institutional authority of some kind is vested;
2. *Moral evaluation,* that is, legitimation by (often very oblique) reference to value systems;
3. *Rationalization,* that is, legitimation by reference to the goals and uses of institutionalized social action, and to the knowledge society has constructed to endow them with cognitive validity;
4. *Mythopoesis,* that is, legitimation conveyed through narratives whose outcomes reward legitimate actions and punish non-legitimate actions (1999, p 92).

There are some sub categories of these major categories. Five legitimization strategies derived from these four categories are developed into a model by Vaara et al. (2006). These are: (1) normalization, (2) authorization, (3) rationalization, (4) moralization, and (5) narrativization (p 790). This paper connects the micro level of discursive strategies used in legitimization in deceptive emails to the macro level of deception and power abuse study in the society.

Methodology

Research Questions

This study is based on two major research questions:

a. What are the discursive strategies used as legitimization strategies in phishing emails?
b. How are the social power abuse and the cognitive trust construction connected to discursive legitimacy in phishing?

These two questions are interlinked with each other and thus, addressing these two questions together adjoins two theoretical approaches in this study. First, the 'triangulation approach' includes the area of discursive strategies in the study of the social power abuse and cognition construction. Second, the study of legitimization strategies mainly cover the discursive strategies.

Data Collection

In order to address these two research questions and conduct this study, 25 phishing emails are chosen as textual data. These emails are selected randomly from www.millersmiles.co.uk- an anti phishing service which archives phishing emails. Among these emails, there are 15 bank emails, 3 payPal emails, and 7 yahoo and facebook emails. The topics of these emails are mainly account verification, account re-activation, money transfer, problem in payment, account updating or upgrading.

Data Analysis

Qualitative methodology is applied in order to analyze the data. In order to identify the legitimization in the emails, the vocabularies, sentence structures, the beginning of the email, the suggestion for the solution, the statement of the problem are analyzed. Moreover, narrative analysis approach is used in order to examine the texts of the emails, and to create

a connection between the propositions of this study and the narratives of the emails. This analysis is believed to open a gateway to a better understanding of this topic. Furthermore, the analyses are done at three levels: discursive, social and cognitive. At first level, the discursive strategies used in these 25 emails are analyzed and identified under the category of four legitimization strategies promoted by Van Leeuwen & Wodak (1999). At second level, the analysis elucidates the connection between legitimization and social power abuse. It analyzes what kind of power this legitimization possesses, and how it exercises the power in the narratives. At the final level, legitimization, social power and cognition become intertwined. The analysis illustrates how the power control of legitimization influences the knowledge and belief of individuals, and how constructing new knowledge and trust leads one to respond to the phishers' commands.

Analysis and Results

Discourse & Legitimization

All the discursive features which are applied to legitimize the narratives are analyzed under four categories of legitimizations:

Authorization

"Authorization is legitimation by reference to authority" (Vaara et al., 2006, p 799). These authorities can be vested in a person based on their institutionalized role or expertise, or it can be in the form of impersonal authority of law, rules and regulations (Van Leeuwen, 2007). The selected materials of this paper have used a great amount of references to the authority of various recognized institutions (banks), established laws or rules, the high officials, the experts of the industry, etc. for establishing the legitimacy of their claim in the text.

First, the analyses of the texts reveal that the impersonal authority legitimization is prominently employed in order to make the requests or claims trustworthy and valid. Therefore, the names of various banks, organizations are used in order to establish legitimization, such as the *Federal Reserve Bank Board, First Community Bank, Transfer Laws of United States of America, First Quarter Annual Audit, Sterling Bank PLC, Yahoo Mail, Facebook.* In example 1, the reference of two banks and two institutional terminologies are used in order to legitimize their activities so that the users trust them easily.

1. The Federal Reserve Bank have called off your payment file from Africa and have it sent to the newly government approved bank for international debt cancellation (Sterlink Bank PLC). (Federal Reserve Bank, 23 April, 2012).

Moreover, these applications show how the impersonal laws or rules are personified in the selected texts by associating human attributes with them to establish their authoritative function. For example:

2. Fifth Third Customer Service requests you to complete Commercial Banking Online form. (Fifth Third Bank, 28 February 2008)
3. The system will automatically send you a new notification message. (Fifth Third Bank, 13 January 2009)
4. Nigerian Financial Intelligence Unit sends and requests…. (First National Bank, 20 April 2011)

Second, the names of the high officials of any big organization along with their designations are employed as the senders of the emails, such as *Dr. Benny Okoh, (Director of Financial Intelligence/Operations), Alex Bennet, (Senior Digital Marketing Manager).* These names

along with the designations may enforce the recipients being cautious straight away even if the names do not sound familiar to them. These names and designations imply their power and status which do not require any further justifications (Van Leeuwen, 2007) in the texts. Moreover, logos, slogan embedded in the emails or spoof website instill trust in the users as these often provide a mirror image of legitimate email or site (Wright & Marret, 2010). The confusions and arguments regarding the requests, the assertions or the service offered in the emails are resolved automatically through such impersonal authority references. Therefore, a whole message from such an authority containing 'some forms of obligation modality' is adequate itself to legitimize the text (Van Leeuwen, 2007, p 94).

Third, in some messages, the expert authority is also referred. For example, *carbon trust standard* is an expertise of *First Security Bank* through which they claim to provide the most secured service. Here, the *carbon trust standard* feature is personified as an expert whose expertise can take care of one's security issue. This is a kind of an assurance in the form of 'verbal process clause' or 'mental process clause' to legitimize the advice specified in the email (Van Leeuwen, 2007, p 95).

Fourth, the authority of conformity is also used in some cases in order to convince the recipients that s/he is not the only one who has to go through the specific process suggested in the email. "Contemporary law makers increasingly believe that, if most people are doing it, it cannot be wrong, and should be legalized" (Van Leeuwen, 2007, p 97).

5. Every Fifth Third Direct customer has to complete a Fifth Third Direct Customer form. (Fifth Third Bank, 13 January 2009)
6. The instruction has been sent to all bank customers on same issue. (First Direct Bank, 20 July, 2001)

So, these sentences in example 5&6 convey the message that "Everybody else is doing it, and so should you" (Van Leeuwen, 2007, p 97).

Moralization

'Moralization' or moral evaluation mainly refers to the moral values which are manifested in specific moral discourses. These are mostly implicit in the text, and cultural knowledge is required in order to understand such references of loyalty and morality. Evaluative adjectives, abstraction and analogies are significantly applied in the texts to establish moral legitimization (Van Leeuwen, 2007). It is quite natural that 'moralization' easily can create a sense of trust among the recipients about the claims in the emails which can easily control people's beliefs and actions consequently. The selected phishing emails contain a range of examples of 'moralization' or moral evaluation in the forms of references associated with diverse practices or qualities which are allied to the discourse of moral values (Van Leeuwen, 2007). For example:

7. We wish to let you know that all difficulties have been removed for the success of this contract fund to be credited into your personal account. (Federal Reserve Bank, 10th September 2009)
8. The information provided will be treated in confidence and stored in our secure data base. (Franklin Bank, 13 April 2008).
9. In order to protect your sensitive information, we temporarily have suspended your account for further investigation. (First Merit Bank, 18th September 2005).
10. For security purpose and clarity, we advise that you keep your winning information confidential until your claims have been processed and your money remitted to you. (British Lottery Headquarters, 6 August 2005).

11. ….our continuing commitment to protect your account and to reduce the instance of fraud on our website. (PayPal, 3 February 2011)

We can see above, using appropriate analogy is a common method of expressing moral evaluation which has a legitimatory function (Van Leeuwen, 2007). In the above examples (7-11), the phishers tried to establish that their intention and attempts are always for doing something good to the users; even it is done in the form of temporary account suspension or identity verification. Therefore, they want to 'protect', 'advise', or 'secure', and thus these chosen analogies provide the recipients with a situation where they compare it with the situation which is unprotected, and insecure. Thus, this 'moralization' legitimizes their actions and claims which receive a moral identity through this process of establishing and enhancing the trust and credibility. The recipients' responses are attracted mostly because of the reference of moralized attempts.

Rationalization

'Moralization' and 'rationalization' are closely connected to each other. No 'rationalization' is possible without 'moralization' (Van Leeuwen, 2007). Also, he mentions two types of 'rationalizations': (i) instrumental, in reference to goals, uses and effects, and theoretical, in reference to natural order of things or practices (2007). The materials of this study mostly have applied instrumental rationalization as the phishers have purpose construction with an element of 'moralization'. Therefore, the 'instrumental rationalization' focuses on the benefits, purposes, functions, or outcomes (Vaara et al., 2006) that the phishers create in order to legitimize and validate their actions. Habermas (1976) characterizes the institutions that regulate different kinds of social actions in terms of the validity claims, or 'kinds of truth' which underlie and legitimize them (as cited in Van Leeuwen, 2007, p 101).

12. We wish to let you know that all difficulties have been removed for the success of this contract fund to be credited into your personal account. (Federal Reserve Bank. 28 June 2009)

13. We noticed irregular activity on your Barclays debit card. For your protection, you are required to answer the verification questions correctly as the primary owner before we can re-open your debit card for use. (Barclays Bank Plc, 14 August 2013)

14. We have also received information to re-route the fund to your bank account immediately. (First National Bank, 20 April 2011)

15. The Classic version of BT Yahoo! Mail will be replaced by our new version on 16 Aug 2013. So, it's time to upgrade, before you lose your email access. (BT Yahoo, 14 August 2013)

All these purposes in the above examples (12-15) are based on moral and ethical behaviors. These show the purposes of the actions taken by the phishers which are a tool to legitimize the texts. Apparently, the phishers want to establish that their main objectives in the emails (12, 13, 14 and15) are to take the steps for the smooth transfer of the money to their account, or account verification or upgradation. It is user's money, user's account or user's protection; however, it seems to be the sender's moral purpose to address them all. Their rationales coated with moral values sound legitimized enough to the account users to attend to their (phishers') advices.

Mythopoesis

Van Leeuwen (2007) mentioned that storytelling can be a good criterion to legitimize the message that one wants to convey. He shows how telling a story can make someone's message or assertion acceptable, appropriate and preferable to others (Vaara et al., 2006). There are two kinds of stories in legitimization: moral tale, where the central characters are rewarded for his/her noble engagement in lawful social practices, and refurbishment of social order, and cautionary tale, where they suffer because of their deviant engagement against the social practices. These are shown in order to convey the message for the consequences of going against the social practices and laws (Van Leeuwen, 2007). Therefore, the selected materials of the study mostly tell the cautionary tale to make the recipients vigilant about their negative consequences of what if they do not follow the way showed by the content of the emails. Though the stories told in these emails are not like the conventional storytelling, the phishers mostly come up with a problem in the form of warnings indicating the consequences, for example, account deactivation, or suspension if the recipients ignore the suggested solutions or advices. Moreover, these narrativizations mostly have quite dramatic openings. They fabricate their openings with either 'congratulations' or 'attention' or 'beware' or 'warning' note which has a dramatic impact on the recipients. Therefore, the phishers can attract the recipients' attentions even if they are kind of aware of the 'phishing'. The dramatic openings often become the only one option for the recipients to consider. Consequently, failing to understand the intention of the sender, and attending to the story's call, the recipients often find themselves hooked up at phishers' baits.

16. Subject line: "Your online service is expired"
Dear First United Bank & Trust Cardholder,
Your online service is expired. You must renew it immediately or account will be closed. If you intend to use this service in the future, you must take action at once!
To continue click here, log in to your online banking and follow the steps.
Thank you.
First United Bank and Online Center. (First United Bank, 7 April 2007)

This email has started with the consequence of something that is the expiration of the recipient's bank account. So, the problem arises with a 'warning' if he does not renew the account immediately, it will be closed, and s/he will not be able to get his/her access to this anymore. Later on, the solutions are provided with which he can renew the service. There is always a link leading the person to a spoof website which requires some personal information. This kind of 'narrativization' with such alert makes the message legitimized to those who have accounts with them. So, being convinced, most of them automatically follow the instruction as it appears to be a valid and trustworthy message. Thus, they become the victim.

Moreover, some of the emails convey this caution implicitly. The risk and the insecurity of the issue are mentioned repeatedly, however, the type of risk is not explicitly mentioned. This kind of message employs positive self representation that Van Dijk (2001) mentioned as one of the discursive strategies to manipulate others in which there are a great amount of emphasizes on the positive images of the self representations. These often work to make the messages acceptable and trustworthy. These emails always come with specific solutions though these start with problems at the very beginning. In the middle, they try to portray a positive image of themselves through series of legitimized motives.

17. Confirmation of your Apple ID gives you easy access to a variety of Apple services, including the iTune Store, Apple Online Store, iChat, and more. We will not share your information with anyone else unless you authorize us to do so. (Apple Alert, 22 August 2013)

18. What we do to keep you safe… (First Direct Bank, 6 May 2011)

In example 17 & 18, the senders try to show how many good features they can offer in service, and how trustworthy (17) and moral (18) they are.

Legitimization & Social Cognition

Discursive legitimization is a tool of manipulation, and persuasion influencing how the recipients' beliefs, opinions, knowledge, evolve into a new cognitive knowledge or belief and constructs cognitive trust which, in turn, makes them perform or act accordingly. In other words, the cognitive analysis shows how understanding can be influenced or manipulated by various contextual forms of legitimization in discourse. This process involves three stages: short term memory, long term memory and social cognition or social representations.

Legitimization in Short Term Memory

According to van Dijk, discourses generally "involve processing information in short term memory (STM), basically resulting in 'understanding' (of words, clauses, sentences, utterances and non-verbal signals) for instance in terms of propositional 'meanings' or 'actions'" (2006, p 365). This hypothetical understanding includes some guesses and shortcut comprehension. Using some specific discursive strategies can control such understanding in STM:

First, the subject line (Headlines or titles) of the emails, the sender information and the topic as conventional text category can function to express the 'semantic macrostructure' that represents what the discourse is all about (Van Dijk, 2001, p 101-102; 2006, p365). The global meaning of the text is comprehended in STM, and thus the main idea of the text can be recalled later. Some subject lines of phishing are 'Information regarding your fund', 'Fifth Third Bank: Confirmation required', 'First Community Bank update', 'About you online service', 'DEAR BENEFICIARY WE HAVE RECIEVED YOUR TRANSFERRED FUND', 'New Member $90 Reward Survey, 'VERY URGENT CONGRATULATIONS' which are better represented in short term memory, and recalled later. Moreover, bold fonts, the salient position of the title in the text attract more attention and require more time to process. Second, the legitimized reference to the authority (Yahoo mail, Federal Reserve Bank, First Merit Bank) as a sender or a contact person functions in the same way. Third, the imitated structure of a business email, logo, slogans used in phishing and the spoof website for legitimization draw the attention of the reader more than others as the visual representation always has a greater effect (Van Dijk, 2006). All of these morphological and syntactic strategies in discourse are used to influence the understanding process in STM and to gear towards the more efficient understanding. The phishers as a dominant group in phishing want to control the understanding of the information provided in the emails in favor of their interest and try to deviate the readers' comprehension against their interest. In order to achieve that control, they employ these discourses based legitimization strategies which exploit STM based understanding.

Legitimization in Episodic Memory

Understanding a text involves the construction of a subjective 'mental model' in episodic memory by the recipients. This understanding does not mean only the meaning The positive self representation by moral superiority is a significant discursive strategy to manipulate episodic memory (Van Dijk, 2006, 2001). Therefore, presenting themselves as an authoritative trustworthy figure or a part of a renowned organization is nothing but an effort to portray their positive self-representation. Usually, there are some descriptions or

explanations of the phishers' good intentions or objectives to 'rescue', 'advise', 'protect' or 'secure' the recipients from some negative consequences in the emails. The 'moralization' strategies applied by referring to their intentions or activities to some moral values are actually 'the positive self-representation' which are consistent with the positive 'mental model' of the recipients. If the legitimacy of the moralization process in phishing resembles the users' personal opinions and emotions, they try to reconstruct the 'mental model' through the existing knowledge. Moreover, the phishers usually intend to create an authentic image of their actions, and portray apparently a moral support by providing a solution. For example:

19. As part of our drive to offer you better banking, we've rolled out a new Online Banking service. The new service is packed full of helpful features and functionality making it even easier and secure. (Halifax, 14 May 2012)

20. In order to protect your sensitive information, we temporarily have suspended your account. (First Merit Bank, 18 September 2005)

21. What we do to keep you safe….(First Direct Bank, 6 May, 2011)

Positive self representations are also done in the form of referring to a role model authority (Bill Gates, Sultan of Brunei) in the text (22) which the recipients comprehend corresponding to their positive mental model. Nesler & Fivush (1994) state, "Recipients tend to accept beliefs, knowledge, and opinions (unless they are inconsistent with their personal beliefs and experiences) through discourse from what they see as authoritative, trustworthy, or credible sources, such as scholars, experts, professionals, or reliable media" (cited in Van Dijk. 2006, p 200).

22. Note: ALL participants in this lottery program have been selected randomly through a computer ballot system drawn from over 20,000 companies and 30,000,000 individual names, email addresses from all search engines and web sites. This promotional program takes place every year, and is promoted and sponsored by eminent personalities like the Sultan of Brunei, Bill Gates Have Microsoft Inc, Multi Choice- China site and other corporate organizations. This is to encourage the use of the internet and computers worldwide. (British Lottery Headquarters, 6 August 2005)

Moreover, the threats or the cautions implied in 'attention', 'beware', 'flagged as spam', 'It is time to upgrade before you lose your email access' in emails create a sense fear for losing money, or losing access to the account or losing a big offered fortune/opportunity.

23. Warning!!! Account owner that refuses to update his/her account after receiving this warning will lose the account permanently. (Yahoo Alert, 4 November 2009)

This message (23) with an exact logo legitimizes the 'warning', and evokes a true sense of fear, and that leads the recipients to interpret it the way the phishers want them to do. So, legitimacy and fear are connected, and thus controlling people's action is a consequence of this connection.

Cognitive Trust in Social Representation

The formation of 'mental model' is not the only goal here, rather the target is to influence more general and abstract belief and knowledge that will lead to perform the actions according to the phishers. The new belief and stable knowledge of a recipient allow him/her to act, interact and communicate accordingly. After the positive correspondence of the personal 'mental model' of opinions and beliefs of the users with the legitimacy of the

emails, the phishers target to control or develop cognitive trust, which make them to act or interact consequently. The 'rationalization' of the legitimacy presented in the discourse finally earns and constructs a shared belief of cognitive trust in the society among the recipients (social actors) which make them to follow the instructions in the email.

Legitimization & Social Power Abuse

Rojo & Van Dijk (1997) argue, in CDA, discursive legitimization is associated with power relation (as cited in Vaara & Monin, 2010; Van Leeuwen & Wodak, 1999) and the connection between legitimacy of specific actions and the power status of social actors are significantly discussed (as cited in Vaara & Monin, 2010). In these emails, the ability to control the recipients' actions and decisions presuppose a power base of knowledge and information in the word of providing security and fortune. Mostly power control appears in the form of abusive acts. Legitimization is a working tool for the phishers as a dominant group to control the acts and beliefs of the recipients, and the power abuse is related to the concept of controlling people's action in taking some detrimental steps against their best interest. According to Van Dijk (2006), if peoples' knowledge or opinions can be influenced, the indirect control over their actions is also possible. This control is reflected in these phishing emails. Among all the strategies, legitimization is the most influential as it makes the text or message credible and acceptable to others. For example:

24. Dear Valued Customer,
YAHOO ACCOUNT VERIFICATION ALERT!!!
(KMM69467VL055834KM)
Yahoo mail has discovered series of illegal attempts on your yahoo account from a bad IP location and will shut your account as it has been flagged as a spam account. You are immediately required to secure your online access by manually filling the form below by clicking on the Reply-To button on your page, filling correct information carefully and sending to yahoo alert center: (Yahoo Alert, 4 November 2009)

First, power lies in group membership, institutional position, profession, material or symbolic resources and other factors. So, a high official from an institution, or a group from an institution can have power control in phishing emails. Here, the phishers are in the power role by faking the power position, and authoritative legitimization has validated it. Moreover, getting access to one's inbox provides the phishers a base for nurturing the power control and dominance. Being unaware of the intention of the phishers and authenticity of the emails, the recipients become a victim if they respond to their instructions. The phishers exercise the power control here in the form of manipulation which violates social norm and rules. Through these 'special' kinds of emails, the phishers are controlling their illegitimate power over the recipients by legitimizing their discourses of claims and actions. These appear in an authentic and legitimate form of institutional communication to the recipients and some of them who are connected to the organizations find it authentic and logical to follow their instructions. An alert from yahoo mail in (24) says, the recipient's account security is in danger that creates a fear in the recipient's mind as it sounds and appears legitimized to him/her. The structure, logo, analogies ('secure', 'illegitimate', 'verification') of the email legitimize every single claim here. Moreover, the moralization along with rationalization (identifying the illegal attempts to log in from alien location that might close the account and providing a solution to that problem) and the impersonal authorization (Yahoo Mail Alert Center & verification code) legitimize the alert made in the email as well. Furthermore, using fake request and claim (suspension of account), forging one's identity (Yahoo mail),

providing counterfeit instruction (filling the form in a provided link), using spoof website and capturing user's personal information are parts of the social wrong doings considering these illegal attempts of manipulation and deception. These illegal attempts produce inequality and domination in the society which make the less powerful group (users as victim) suffer, and serve the interest of the more powerful group (phishers).

Discussion

Addressing the research questions, few issues have been made clear in this paper through the incorporation of legitimization strategies into the 'triangulation approach' of Van Dijk:

First, the phishing emails have one main intention which is to grab the attention of the recipients and make them respond to their requests. It is not that everybody responds to their requests but even if one or two attends to their emails, their purpose is served. Only clicking into the link may disclose the user's personal information, and cause identity theft.

Second, the connection between discourse and legitimization is established through the strategies applied in phishing. Discourse is the main tool to legitimize the claim. Authorization, moralization, rationalization, and mythopoesis are analyzed in the phishing emails and shown through some examples included in the texts. Application of one or two strategies may legitimize the text.

Third, the legitimization is found as a social lubricant in the 'discourse-power-cognition triangle' which exercises a power control over the people's beliefs and actions. The analysis shows how legitimization strategies can be medium of social power abuses and cognitive manipulation in phishing discourses. The phishing email business is a part of social illegitimate actions which fakes the legitimacy, and deceives people. An overview of the entire analytical process has been shown in table 1.

Table 1: Legitimizing Strategies

Legitimization	Discursive strategies	Social Power control	Cognition-constructing trust and response
Authorization	Reference of various organizations, institutions, laws, committees, meetings as impersonal authority;	These references indicate inherent power of their statuses and roles. No other justifications are required, and all the arguments are resolved by such references.	Primary influence on people's knowledge and opinion is operated by the power implied in this authorization.
	Reference of famous personalities, experts, conformity action		
Moralization	By using some analogies which have some moral implications;	Moralization of the texts has more power of manipulating user's beliefs and activities.	Positive self- representation of the phishers constructs positive mental model of knowledge and belief in episodic memory.
	By referring the actions or motives of the phishers to some moral activities;		
Rationalization	By providing the moral purposes of their requests and claims, phishers rationalize their discourses;	Power of rational behavior and claim is stronger to exercise its control over the recipients.	Combination of moralization and rationalization construct stable mental model and cognitive trust.
Mythopoesis	Narrating the negative consequences of not following the steps shown by the phishers often legitimizes the message.	The story teller phishers appear here as a dominant group and the listener recipients as dominated.	The trust on the narratives leads them to follow the phishers.

Conclusion

To summarize, this paper analyzes the phishing email discourse from critical discourse analysis perspective to show how legitimization of the discourse in the emails can exercise the power abuse of manipulation and develop a new attitude or belief in social cognition to trust the claims made in the emails. This represents the illegitimate power abuse exercised by

shown here at the micro level discussion of phishers' deceiving the users. This whole process, from legitimization to response making, has been explained through the 'triangulation framework' of Van Dijk (2001). The framework also includes the legitimization categories or strategies of Van Leeuwen & Wodak (1999). This framework discloses how legitimization constructs cognitive trust to entrap the users in their deceptive actions through the empirical data analysis.

References

Blythe, M., & Clark, J. (2010). The Phish in the pond: Scam emails as literature. *CHI.*

Krause, T., & Nielsen, T. D. (2014). The legitimacy of incentive-based conservation and a critical account of social safeguards. *Environmental Science & Policy, 41,* 44-51.

Servaes, J. (2013). The many faces of (soft) power, democracy and the Internet. *Telematics and Informatics, 30*(4), 322-330.

Suddaby, R., & Greenwood, R. (2005). Rhetorical strategies of legitimacy. *Administrative science quarterly, 50*(1), 35-67.

Vaara, E., & Monin, P. (2010). A recursive perspective on discursive legitimation and organizational action in mergers and acquisitions. *Organization Science, 21*(1), 3-22.

Vaara, E., Tienari, J., & Laurila, J. (2006). Pulp and paper fiction: On the discursive legitimation of global industrial restructuring. Organization studies, 27(6), 789-813.

Van Dijk, T. A. (2006). Discourse and manipulation. *Discourse & Society, 17*(3), 359-383.

Van Dijk, T. (2001). Multidisciplinary CDA: A plea for diversity. In R. Wodak & M. Meyer

Van Dijk, T.(1998). 18 Critical discourse analysis, viewed 25 February 2012, http://www.discourses.org/OldArticles/Critical%20discourse%20analysis.pdf

Van Leeuwen, T. (2009). Critical discourse analysis. *Discourse, of Course. An Overview of Research in Discourse Studies,* 277-292.

Van Leeuwen, T., & Wodak, R. (1999). Legitimizing immigration control: a discourse -historical analysis. *Discourse Studies, 1*(1), 83-118.

Van Leeuwen, T. (2009). Critical discourse analysis. In J. Renkema (Ed.), *Discourse, of course: An overview of research in discourse studies* (pp. 277-292). Amsterdam [u.a.: Benjamins.

Van Leeuwen, T. (2007). Legitimation in discourse and communication. *Discourse & course: An overview of research in discourse studies* (pp. 277-292). Amsterdam [u.a.: Benjamins.

Vasalou, A., Hopfensitz, A., & Pitt, J. V. (2008). In praise of forgiveness: Ways for repairing trust breakdowns in one-off online interactions. *International Journal of Human-Computer Studies, 66*(6), 466-480.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Vittal, A. (2005). Phishing, Pharming, and Other Scams. GP*Solo, A 22*(8), 26-32.

Whittle, A., Carter, C., & Mueller, F. (2013). 'Above the fray': Interests, discourse and legitimacy in the audit field. *Critical Perspectives on Accounting.*

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273-303.