Game Theoretic Aspect of Phishing and Virtual Websites.

C.C. Nwobi-Okoye

Anambra State University, Uli, Anambra State, Nigeria.

E-mail: nwobi@ansu.edu.ng
chidozien@yahoo.com

ABSTRACT

Phishing, a virtual strategy, is analyzed in the context of a virtual game. In the analysis it is shown that phishing increases the rank of the phishing web page, and hence, the optimum or equilibrium strategy for the strategist. In addition to this it is shown that phishing decreases the page rank of non phishing pages and possible payoff from such pages. Similarly, it is shown that designing virtual pages whose traffic is redirected to the genuine page reduces the rank of the phishing page, and phishing becomes the non equilibrium strategy. In continuation, it is shown that with proper law enforcement and awareness, phishing would equally no longer be optimum or equilibrium strategy for the strategist. Finally, the positive use of virtual web pages especially for market entrants is highlighted. This work will be very useful to information managers, game theorists, operations researchers, system scientists etc involved in the regulation of the internet and design of e-business systems.

(Keywords: phishing, game, equilibrium, web pages, virtual strategy, virtual web pages)

INTRODUCTION

There has been an explosive rise in the use of the internet in the last five years. More and more people are going online to conduct information searchers and routine transactions. In recent years, developing nations have witnessed an ever increasing number of internet users. In China alone there is an estimated 350 million internet users (BBC 2010a). One reason responsible for more and more people being connected to the internet is the increased availability of cheap internet enabled mobile phones. Currently, the internet has become the primary source of information for vast majority of people both in developed and developing countries.

The internet, however, is not with its attendant problems. Computer viruses, worms, Trojan horses, scam mails, spam mails, phishing websites, etc. are all problems associated with the internet. A recent survey revealed that more than 2 million web pages on the web are infected with malicious programs.

Phishing websites are fake websites designed to look exactly like the original site. Visitors to such sites are tricked into revealing their confidential information such as credit card details, bank account details, email passwords, etc. Every year thousands of people fall victim to such websites and millions of dollars are lost annually by these victims. Recently, the British Broadcasting Corporation (BBC) reported that the International Carbon Market was hit by a phishing attack which saw an estimated 250,000 permits worth over 3 million Euros stolen in the first week of February 2010. It reported further that 7 out of 2000 German companies targeted were known to have fallen victim of the scam (BBC 2010b). The BBC equally reported that 22.6 million pounds were lost in 2007 to phishing scams in the UK (BBC 2008).

In light of the revelations above, it is imperative that phishing must be studied scientifically in order to understand better the mechanisms of its occurrence and increase awareness of its existence among academics and web users. By so doing the chances of web users falling victim to it would be drastically reduced.

One possible salient scientific method of studying phishing is through the application of game theoretic modeling to understand the scientific basis to phishing website successes. The appropriate game theoretic model is based on the theory of virtual games developed by Nwobi-Okoye (Nwobi-Okoye 2009, Nwobi-

Okoye 2010a, Nwobi-Okoye 2010b, Nwobi-Okoye 2010c).

Of course designing web pages to be identical or similar to other pages is not entirely for diabolic purposes. The designed identical page is regarded as a virtual page. Such virtual web pages could be used by market entrants who wish to popularize their products or services in the shortest possible time (Nwobi-Okoye 2010a).

Let us not forget that adopting web addresses very similar to existing web addresses is a very powerful virtual strategy, and whenever virtual or phishing web page designs are mentioned as strategies, such strategies are an intrinsic part of it. In fact most phishing websites have web addresses very similar to the original sites.

In order to expatiate on this, when I was trying to visit the website of the Nobel Foundation, I visited the web address: www.nobel.org shown in Figure 1. When I visited the site, I discovered that the site was not that of the Nobel foundation. The site designers had no criminal intent hence they directed me to the actual site of the Nobel Foundation whose address is: www.nobelprize.org as shown in Figure 2.

By choosing a web address that is almost identical to that of the Nobel Foundation, a well known and popular organization, the imitators increased the number of possible visitors to their site. Had it been that they imitated the site of the Nobel Foundation; visitors would be under the illusion that they are in the website of the Nobel Foundation but in reality they are not.

The imitating website I discussed above was not used for diabolical purposes; hence I regard such websites as a virtual website in order to distinguish it from the phishing websites which are used for diabolic purposes.

The objective of this paper, therefore, is to use the theory of virtual games to model and scientifically study the basis and motivation for phishing and virtual website creation and development. This will help researchers recommend palliative measures aimed at limiting the ugly effects of phishing, as well as explore the possible use of virtual sites for positive uses.

THEORETICAL BACKGROUND

Virtual Games

Virtual games are games where the competitors use strategies known as virtual strategies (Nwobi-Okoye 2009, Nwobi-Okoye 2010a). Virtual reality occurs when the payoff determining factors assume certain conditions exist which in fact do not. Virtual reality strategies use deceptive perceptions to improve payoffs for the strategist (Nwobi-Okoye 2009, Nwobi-Okoye 2010a). By definition a virtual game is defined as:

Definition: A virtual game is defined as a game with a finite set of players i Є J, a grand/secondary payoff matrix, GG, a set of virtual strategies, $V = (V_1, V_2, V_3, V_4 \ldots V_n)$ for each player with each strategy tied to a virtual payoff matrix, G_n, an associated probability matrix/vector, E (v), and an effective virtual payoff matrix, G_{ev}, where $G_{ev} = E(v) \cdot G_n$.

The Model

The game theoretic model used to model phishing is Markov queue game model developed by Nwobi-Okoye (2009). The following assumptions are made for the purpose of the modeling:

Game Characteristics and Assumptions: The game model used in the analysis in this work is based on the following characteristics and assumptions:

1. The game corresponds to model/variant 2 of the game developed by Nwobi-Okoye (2009).

2. An infinite population source (Hamdy 2004, Asmussen 2003) which represents possible browsers of the web pages is assumed.

3. There is possibility of moving from a higher state to a lower state, hence web surfers could move from virtually any page to the other.

Figure 1: A Virtual Website (Imitating Website).

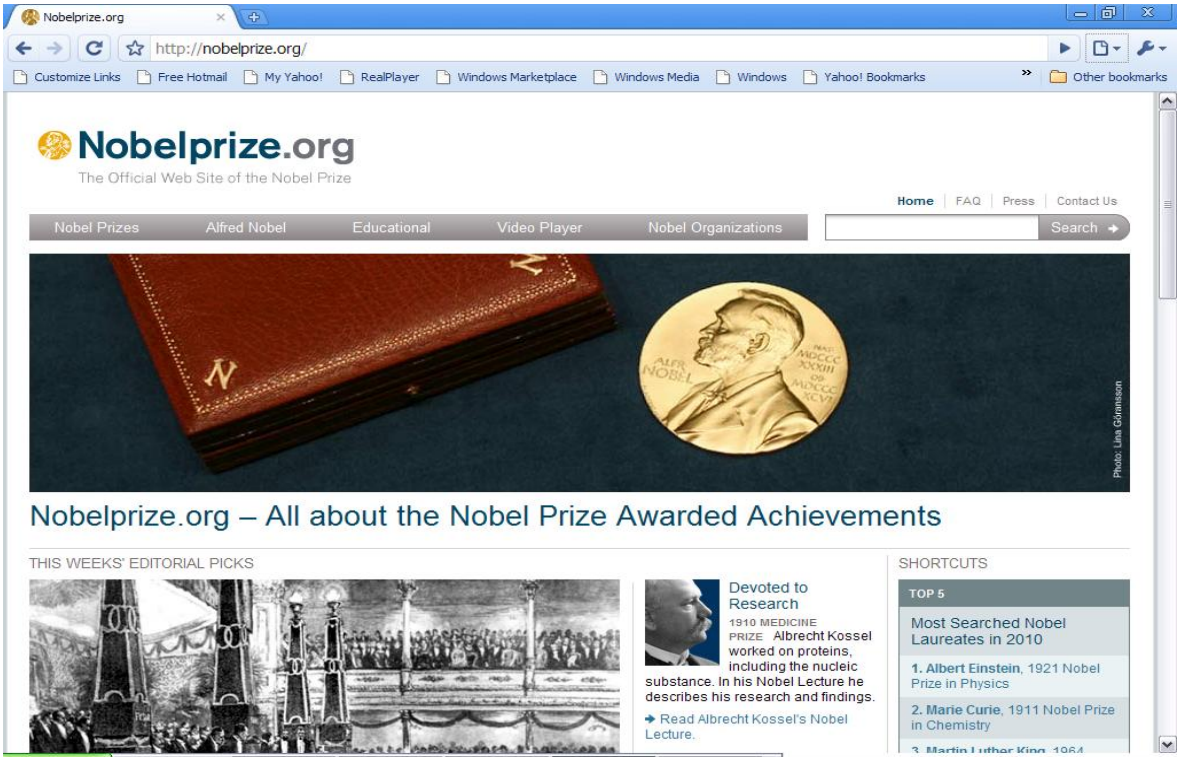

Figure 2: Imitated Website.

Mathematical Analysis

Here it is assumed that competitors try to use strategies that would attract customers (visitors) to their websites. The web users could queue behind (visit) any website they wish to do business with its owner(s). The entire mathematical analysis is entirely based on the model developed by Nwobi-Okoye (2009).

Since the game corresponds to variant 2 as has earlier been mentioned, the applicable equations for modeling the game theoretic aspect of phishing are:

EG = P·G **(1)**

The dot operator in equation 1 carries out the operation of multiplying each payoff by its associated probability of occurrence.

GT=G– R **(2)**

Here R is the payoff reduction.

R represents the extra cost incurred due to the incorporation of flow features.

$$GT_{IXJX} = G_{IXJX} - R_X \quad \textbf{(3)}$$

$$GT_{IYJY} = G_{IYJY} - R_Y \quad \textbf{(4)}$$

EG=PT·GT **(5)**

The grand payoff matrix, GG, is shown in Figure 3.

	0	1	…	N
0	$GG_{1X,1X}, GG_{1Y,1Y}$	$GG_{1X,1X}, GG_{1Y,1Y}$	$\ldots GG_{1X,NX}, GG_{1Y,NY}$
1	$GG_{2X,1X}, GG_{2Y,1Y}$	$GG_{2X,2X}, GG_{2Y,2Y}$	$\ldots GG_{2X,NX}, GG_{2Y,NY}$
.	.	.	.
.	.	.	.
.	.	.	.
N	$GG_{NX,1X}, GG_{NY,1Y}$	$GG_{NX,2X}, GG_{NY,2Y}$	$\ldots GG_{NX,NX}, GG_{NY,NY}$

Figure 3: Grand Payoff Matrix, GG.

Here:

$GG_{iX,jX}$ = the cumulative payoff for player X in the effective payoff matrix, EG, when X uses strategy i-1.
$GG_{iY,jY}$ = the cumulative payoff for player Y in the effective payoff matrix, EG, when Y uses strategy j-1.

$$GG_{IYJY} = \sum_{I=1}^{N} \sum_{J=1}^{N} EG_{IYJY} \cdots \quad \textbf{(6)}$$

$$GG_{IXJX} = \sum_{I=1}^{N} \sum_{J=1}^{N} EG_{IXJX} \quad \textbf{(7)}$$

N= maximum value of strategies i.e. possible number of phishing/virtual strategies.

METHODOLOGY

The appropriate class of virtual games to be used for the modeling as I have said earlier is the Markov Queue Game. In this game the matrix P is a Markov transition matrix whose nature is shown in Figure 4. In matrix P, $P_{iX,jX}$ represents elements for competitor x, while $P_{iY,jY}$ represents elements for competitor x assuming a 2-persons game.

	0	1	… N
0	$P_{1X,1X}$, $P_{1Y,1Y}$	$P_{1X,2X}$, $P_{1Y,2Y}$	… $P_{1X,NX}$,$P_{1Y,NY}$
1	$P_{2X,1X}$, $P_{2Y,1Y}$	$P_{2X,2X}$, $P_{2Y,2Y}$	… $P_{2X,NX}$,$P_{2Y,NY}$
.	.	.	.
.	.	.	.
.	.	.	.
N	$P_{NX,NX}$,$P_{NY,1Y}$	$P_{NX,2X}$, $P_{NY,2Y}$	… $P_{NX,NX}$,$P_{NY,NY}$

Figure 4: Transition Matrix, P.

Proposition 1

Consider a set of web pages given by:

W= {1, 2, 3 …n}

Let R_i be the rank of web page i.

Consider a scenario where i became a phishing page. Let R_j be the rank of i after this change. It follows that $R_j > R_i$.

Proof

Consider the matrix P. let the set F given by:
$F = \{F1, F_2, F_3 \dots F_n\}$

F represents the set of probabilities of visit to web page i. Let sum of these probabilities be given by:

$$\mathrm{Sum1} = \sum_{i=1}^{n} F_i$$

Consider the matrix Pv after a virtual strategy, phishing, was introduced. Let the set V given by:
$V = \{V1, V_2, V_3 \dots V_n\}$

V represents the set of probabilities of visit to web page j. Let sum of these probabilities be given by:

$$\mathrm{Sum2} = \sum_{j=1}^{n} V_j$$

It follows from virtual strategy theorem (Nwobi-Okoye 2010) that Sum2 > Sum1, hence $R_j > R_i$.

Proposition 2

Phishing/virtual web page design would always be the optimum strategy provided no counter strategy is employed by an opponent, hence the equilibrium point in matrix GG must correspond to a position where i≠0 or j≠0.

Proof

From proposition 1, $R_j > R_i$. It follows from matrix GG that for any competitor i or j,

$$GG_{IXJX} > GG_{0X0X}$$

and

$$GG_{IYJY} > GG_{0Y0Y}$$

provided i≠0 or j≠0, hence phishing would always be the optimum strategy.

□

Application Case Study

Consider a Markov process which has state space S such that:

S = {0, 1, 2 … n}

The states are:
M = {0, 1, 2, 3 … n}

The states represent web pages. State 0 assumes that no page is visited, state 1 assumes web page 1 is visited, state 2 assumes web page 2 is visited, state 3 assumes web page 3 is visited, etc.

The transition diagram for the system is shown in Figure 5 below;

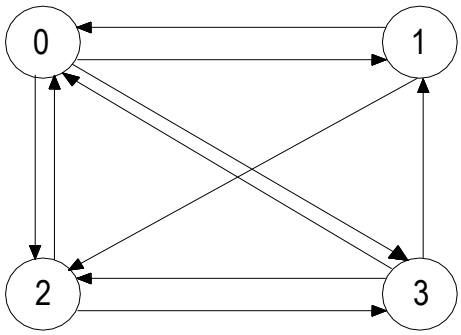

Figure 5: Transition Diagram for the Web Browsing.

The transition matrix is shown below:

$$P_0 = \text{Current State}\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c}\text{Next State}\\ \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array}\\ \left|\begin{array}{cccc} 0.00 & 0.10 & 0.50 & 0.40 \\ 0.10 & 0.10 & 0.30 & 0.50 \\ 0.20 & 0.00 & 0.20 & 0.60 \\ 0.30 & 0.10 & 0.50 & 0.10 \end{array}\right| \end{array}$$

For the transition matrix P_0 above, at equilibrium the proportion of visits to the web pages is shown in matrix V_a below:

$$\begin{array}{c} 1 \quad 2 \quad 3 \\ V_a = \left| 0.0625 \; 0.3750 \; 0.3702 \right| \end{array}$$

Hence, the rank for the web pages is 0.0625, 0.3750 and 0.3702 for web pages 1, 2, and 3, respectively.

For the above transition matrix P_0, it is assumed that the probability of moving from a higher state to a lower state is not zero (0) since a web surfer could move from one page to another or could stop surfing entirely. This is a slight modification from the model of the typical Markov queue game developed by Nwobi-Okoye (2009) where it is assumed that the probability of moving from a higher state to a lower state is zero (0).

The transition matrix Px above represents the natural state of the game. Assuming web page 1 becomes a phishing page designed to look like web page 3, the strategy is a virtual strategy and from virtual strategy theorem, the attached probability matrix P must change due to increased traffic to web page 1. Hence, matrix P would change to matrix PT as shown below:

$$PT = \text{Current State}\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\begin{array}{c}\text{Next State}\\ \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array}\\ \left|\begin{array}{cccc} 0.00 & 0.20 & 0.50 & 0.30 \\ 0.10 & 0.10 & 0.30 & 0.50 \\ 0.20 & 0.00 & 0.20 & 0.60 \\ 0.30 & 0.10 & 0.50 & 0.10 \end{array}\right| \end{array}$$

For the transition matrix PT above, at equilibrium the proportion of visits to the web pages is shown in matrix V_b below:

$$\begin{array}{c} 1 \quad 2 \quad 3 \\ V_b = \left| 0.0818 \; 0.3720 \; 0.3566 \right| \end{array}$$

Hence, the rank for the web pages is 0.0818, 0.3720 and 0.3566 for web pages 1, 2, and 3, respectively.

Assuming that the payoff matrix $\mathbf{G_0}$ is as shown below and the elements represent the payoff or possible gain per visit to each web page.

$$\begin{array}{c} 1 \quad 2 \quad 3 \\ G_0 = \left| 200 \; 500 \; 300 \right| \end{array}$$

The effective payoff matrix for the game, EG_0, is given by:

$EG_0 = G_0 \cdot V_a$

Here $V_a \equiv P_0$ in Equation 1.

$$EG_0 = \begin{vmatrix} 12.50 & 187.50 & 111.06 \end{vmatrix}$$

Possible total payoff for player 1 = 12.50
Possible total payoff for player 2 = 187.50
Possible total payoff for player 3 = 111.06

The transition and payoff matrices P_0 and G_0 above represent the natural state of the game.

Assuming that the payoff matrix after the introduction of the phishing page represented by **GT** is as shown below and the elements represent the payoff or possible gain per visit to each web page.

$$GT = \begin{array}{c} 1 \quad 2 \quad 3 \\ \begin{vmatrix} 200 & 500 & 300 \end{vmatrix} \end{array}$$

Note that G_0 and GT are equivalent because it is assumed that the cost of introducing the phishing page is negligible for the purposes of the analysis here. The effective payoff matrix, EG_1, is given by:

$EG_1 = GT \cdot V_b$

Here $V_b \equiv$ PT in Equation 5.

$$EG_1 = \begin{vmatrix} 16.36 & 186.00 & 106.98 \end{vmatrix}$$

Possible total payoff for player 1 = 16.36
Possible total payoff for player 2 = 186.00
Possible total payoff for player 3 = 106.98

Excluding players 2 and 3, let us consider the one person game represented by GG.

$$GG = \begin{array}{c} 0 \quad 1 \\ \begin{vmatrix} 12.50 & 16.36 \end{vmatrix} \end{array}$$

A look at the payoff matrix, GG, above shows that the optimum strategy for player 1 corresponds to strategy 1, which is the virtual strategy, hence, Nash equilibrium point corresponds to strategy 1.

Assuming a virtual web page, page 4, designed to resemble page 3 is introduced into the system. Let all traffic to web page 4 be redirected to page 3. The strategy is a virtual strategy and from virtual strategy theorem, the attached probability matrix P must change due to increased traffic to web page 4. Hence, matrix P would change to matrix PT as shown below:

$$PT = \begin{array}{c} \\ \text{Current State} \end{array} \begin{array}{c} \text{Next State} \\ \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \end{array} \\ \begin{vmatrix} 0.00 & 0.10 & 0.50 & 0.20 & 0.20 \\ 0.10 & 0.10 & 0.30 & 0.50 & 0.00 \\ 0.20 & 0.00 & 0.20 & 0.60 & 0.00 \\ 0.30 & 0.10 & 0.50 & 0.10 & 0.00 \\ 0.10 & 0.00 & 0.00 & 0.80 & 0.10 \end{vmatrix} \end{array} \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{array}$$

For the transition matrix PT above, at equilibrium the proportion of visits to the web pages is shown in matrix V_b below:

$$V_b = \begin{array}{c} 1 \quad 2 \quad 3 \quad 4 \\ \begin{vmatrix} 0.05986 & 0.359375 & 0.351563 & 0.041667 \end{vmatrix} \end{array}$$

Hence, the rank for the web pages is 0.05986, 0.359375, 0.351563, and 0.041667 for web pages 1, 2, 3, and 4, respectively.

Assuming that the payoff matrix after the introduction of the virtual page represented by **GT** is as shown below and the elements represent the payoff or possible gain per visit to each web page.

$$GT = \begin{array}{c} 1 \quad 2 \quad 3 \quad 4 \\ \begin{vmatrix} 200 & 500 & 300 & 000 \end{vmatrix} \end{array}$$

Note that G_0 and GT are equivalent because it is assumed that the cost of introducing the virtual page is negligible for the purposes of the analysis here.

The effective payoff matrix, EG_1, is given by:

$EG_1 = GT \cdot V_b$

Here $V_b \equiv$ PT in Equation 5.

$$EG_1 = \begin{vmatrix} 11.97916 & 179.6874 & 109.4688 & 00.0000 \end{vmatrix}$$

Possible total payoff for player 1 = 11.97916
Possible total payoff for player 2 = 179.6874
Possible total payoff for player 3 = 109.4688
Possible total payoff for player 4 (Dummy player) = 00.0000

Excluding player 2 and the dummy player 4, let us consider the two-person game represented by GG.

$$GG = \begin{array}{c} \\ Player1 \\ \\ \end{array} \begin{array}{c} \quad\quad Player3 \\ \quad 0 \qquad\qquad\quad 1 \\ \begin{array}{c} 0 \\ 1 \end{array} \begin{vmatrix} 12.500,106.980 & 12.500,109.111 \\ 11.979,106.980 & 11.979,109.111 \end{vmatrix} \end{array}$$

A look at the payoff matrix GG above shows that the best strategy for player 1 is to play strategy 0 which is a non virtual strategy. For player 3, the best strategy is to play strategy 1, the virtual strategy. Hence, Nash equilibrium point corresponds to point (0, 1).

The analysis above assumed that the virtual strategy worked perfectly well. What happens if the virtual strategy is imperfect? The strategy could be imperfect in this case if there is law against phishing which stipulates penalty for offenders, or if there is increased awareness among web users on the dangers of phishing.

Assuming there is penalty for phishing, and the extensive form representation of the one person game above is shown in Figure 6.

Figure 4 could be used to construct a one person virtual game GG shown below:

$$GG = \begin{array}{c} \quad 0 \qquad 1 \\ \begin{vmatrix} 12.50 & 8.18 \end{vmatrix} \end{array}$$

A look at the payoff matrix, GG, above shows that the optimum strategy for player 1 corresponds to strategy 0, which is the non virtual strategy, hence, Nash equilibrium point corresponds to strategy 0.

Assuming there is increased awareness among web users on the dangers of phishing, in this case the probability of success is some value less than one i.e. P(Success)<1 as shown in Figure 7, below.

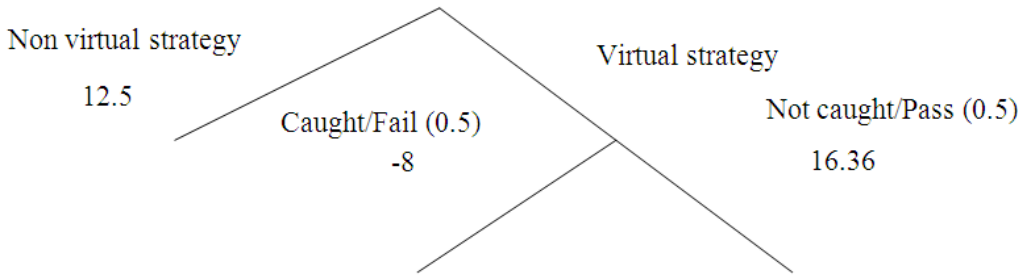

Figure 6: Virtual Strategy Construction Technique 2.

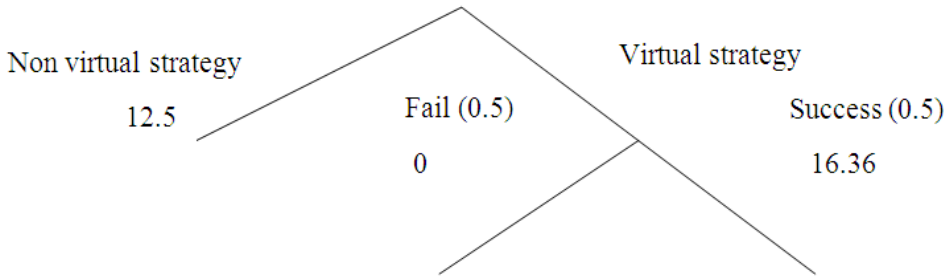

Figure 7: Virtual Strategy Construction Technique 3.

Figure 5 could be used to construct a one person virtual game GG in strategic form which is shown below:

$$GG = \begin{array}{cc} 0 & 1 \\ \left| 12.50 \quad 8.18 \right| \end{array}$$

A look at the payoff matrix, GG, above shows that the optimum strategy for player 1 corresponds to strategy 0, which is the non virtual strategy, hence, Nash equilibrium point corresponds to strategy 0.

RESULTS AND DISCUSSION

From the analysis above, it is obvious that making a web page a phishing page would improve/increase the page rank. Increasing the page rank results to increased payoff for the player using phishing, a virtual strategy. Hence, phishing would always be optimum for players using such strategies. From the results it could be seen that the page rank reduction affected all the web pages except web page 1, the phishing page, but the reduction affected more the web page that was imitated. This could be explained from the fact that there is a general market share reduction of the non phishing pages due to phishing. Similarly, from the above analysis, it could easily be deduced that designing virtual pages and redirecting the traffic to the actual page, reduces the rank of phishing pages and possible payoffs from such pages.

Penalizing phishing introduces an element of risk to the virtual strategist; hence, if the strategist is risk loving, he could brave it and use the virtual strategy which is not optimum for him. On the other hand if the strategist is risk averse, he would most probably play the equilibrium strategy which is the non virtual strategy.

Increased awareness among web users reduces the payoff from using the virtual strategy; hence the virtual strategy is not the equilibrium strategy for the player using the virtual strategy. This could be explained from the fact that increased awareness reduces the number of visits to the phishing web pages.

Using search engines to link to websites could be another way to reduce the possibility of a phishing attack. This is because genuine sites are often ranked higher than fake ones in search engines.

Of course as I have earlier stated, designing web pages to look similar to others may not necessarily be for diabolic purposes. It could be an appropriate strategy for market entrants (Nwobi-Okoye 2010a). Business organizations entering a market newly with a new product or service might be better off (attract possible customers quickly) choosing a web address similar to the web address of an existing business organization on the same market.

CONCLUSIONS

Phishing alters the perception of would be web surfers and increases the possibility of web surfers being swindled. This is a powerful virtual

strategy which could be exploited to the maximum by criminals. The mathematical/analytical basis for its successful exploitation by criminals has been laid down in this work. This will help regulators better understand and fight the menace of scam sites. At the same time designing sites to be similar to popular existing ones could be an appropriate strategy to create awareness very quickly for the existence of a new product or service.

The analysis done in this work will be very useful to game theorists, information managers/technologists, systems scientists and operations researchers who help in the regulation of the activities on the internet or design e-business sites.

REFERENCES

1. Asmussen, S. 2003. *Applied Probability and Queues*. Springer Publications: New York, NY.

2. BBC News. 2008. Available from: http://www.news.bbc.co.uk [Accessed 1/23/10].

3. BBC News. 2010a. Available from: http://www.news.bbc.co.uk [Accessed 1/15/10].

4. BBC News. 2010b. Available from: http://www.news.bbc.co.uk [Accessed 2/16/10].

5. Ching, W. and Ng, M. 2006. *Markov Chains: Models, Algorithms and Applications*. Springer Science + Business Media, Inc.: New York, NY.

6. Fudenberg, D. and Tirole J. 1991. *Game Theory.* MIT Press: Cambridge, MA.

7. Hamdy, T. 2004. *Operations Research*. Prentice Hall of India: New Delhi, India.

8. Nash, J. 1950. *Equilibrium Points in n-Person Games*. National Academy of Sciences: Washington, D.C.36:48-49.

9. Nwobi-Okoye, C.C. 2009. "Markov Queue Game with Virtual Reality Strategies". *Science World Journal*. 4(3):35-40. http://www.scienceworldjournal.org/article/viewFile/5352/3673 [Accessed 1/23/10].

10. Nwobi-Okoye, C.C. 2010a. "General Theory of Games with Virtual Strategies". *Pacific Journal of Science and Technology*. 11(1):317-327. Available from: http://www.akamaiuniversity.us/PJST11_1_317.pdf [Accessed 5/28/10].

11. Nwobi-Okoye, C. 2010b. "Game Theoretic Aspects of Crowd Renting". *Science World Journal,* 5(2):35-40. Available from: http://www.scienceworldjournal.org/article/viewFile/5352/3673 [Accessed 6/22/10].

12. Nwobi-Okoye, C.C. 2010c. "Equilibrium Points in Games with Virtual Strategies". *Pacific Journal of Science and Technology*. 11(2):332-341. Available from: http://www.akamaiuniversity.us/PJST11_2_332.pdf [Accessed 5/28/10]

ABOUT THE AUTHOR

Chidozie Chukwuemeka Nwobi-Okoye teaches at Anambra State University, in Uli, Nigeria with research interests in operations research, game theory, and virtual systems.

SUGGESTED CITATION

Nwobi-Okoye, C.C. 2011. "Game Theoretic Aspect of Phishing and Virtual Websites". *Pacific Journal of Science and Technology*. 12(1): 260-269.