ISSN 2278-3091
Volume 10, No.3, May - June 2021
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse851032021.pdf
https://doi.org/10.30534/ijatcse/2021/861032021

Empirical Evidence of Socially-Engineered Attack Menace Among Undergraduate Smartphone Users in Selected Universities in Nigeria

Arnold Adimabua Ojugo[1], Andrew Okonji Eboka[2]
[1]Department of Computer Science, Federal University of Petroleum Resources Effurun, Delta State, Nigeria
ojugo.arnold@fupre.edu.ng, arnoldojugo@gmail.com, maryarnoldojugo@gmail.com
[2]Department of Computer Science, Federal College of Education (Technical), Asaba Delta State,
ebokaandrew@fcetasaba.edu.ng

ABSTRACT
Smartphone proliferation today, have up-scaled user adoption of Internet-based processing activities. These include (not limited to) e-learning, e-commerce, mobile-banking and others – all aimed at better performance, service delivery at improved execution speed, greater portability, flexibility and accessibility ease. Thus, necessitating growth expansion in mobile-app development across varying platforms that are poised to help users accomplish processing tasks while harnessing the benefits of the technology. Conversely, these techs have also allowed users to be constantly besieged by threats and security breaches. In lieu of residence, sensitive and proprietary – users have become bothered with smartphone exposure to possible data loss and theft – if they are to further adopt these new paradigms. With doubt in their minds, trust levels in user adoption continues to reduce. We seek to investigate social-engineered threats and attacks amongst undergraduates in Nigerian Universities. Result shows that phishing hits a higher success rate against smartphone users in Nigeria, which has decreased client's trust level in Internet-based services.

Key words: Social engineering, Phishing, Fraud, Education, CyberSecurity, Transactions, Spam

1. INTRODUCTION

Information and communication technology (ICT) as a new paradigm – continues its rise with sophisticated improvements as well as its poise to ease exponentially today, our society's dependence and reliance on it. Its adoption, reliance and heavy dependence can be attributed to its ease of use, ubiquity in nature, low transaction cost, portability, ease in accessibility, mobility, flexibility and trust-level in the communication channel and/or medium. All of these, continues to advance their popularity, flexibility in adaptation, and ease in adoption cum usage [1]. These adoption have further eased transaction between clients, permeated into our lives via its use in personal, biz and recreational feats. A sine-qua-non effect is the myriad of breaches that seeks to exploit the inherent challenges and vulnerabilities in ICT, which manifests in various forms presenting itself as misleading items of benefits to unsuspecting users, aimed at defrauding a user [2-3]. These, have attracted adversaries who eavesdrop on user transaction(s) and hijacks such for personal gains. Many adversaries have successfully perpetrated and continues to do so via the social engineering techniques called spam [4-6].

Spams are well-organized, carefully crafted and unsolicited messages sent to a network user without their consent, whose merchandise is unsolicited adverts aimed at making money. Its risen trend continues to pose concern to security experts the world over [7, 8, 9]. When spams are targeted at personal gains, it is simply fraud. Criminals seek to exploit potential victims since they are aware that businesses heavily depends on trust. Though, the high investment in security addresses some issues, it fails to adequately curb vulnerability threats and deception of network users – as criminals evolve their techniques to evade detection and the control measures in place as they successfully trick unsuspecting victims [10].

Spams have been defined by many researchers in relation to how they differ from genuine messages (or hams). The shortest among these, describes the spam as unsolicited bulk message [11]. They are 'unsolicited messages sent indiscriminately, and often where the sender has no relationship with the unsuspecting user [12]. One of the widely accepted definitions is that spams are unsolicited messages sent as part of a larger collection, having substantially identical content. They aim to advertise goods and services with dedicated percentage that change over time [13]. This changeability has become a big challenge used by social engineers, especially in the local nature relating to concept drift in spam [14]. This issue has become an imperative concern as spams constitute over 80% of total messages in form of emails and SMS received by users. This consequently result in direct financial

losses via the misuse of traffic, storage space, and computational power [15, 16, 17].

Spams wastes processor time, leads to the loss in productivity and violation of privacy rights. It also has caused various legal issues via pornographic advert, Ponzi-schemes etc [18]. Total worldwide financial losses caused by spam estimated by Ferris Research Analyzer Information Service were over $50 billion as of 2018 [19]. Phishing are special cases of spamming activity found to be dangerous and difficult to control – because it particularly hunts for sensitive data (such as passwords, credit card numbers, etc.) by imitating requests from trusted authorities such as banks, server administrators or service providers [10]. Social engineering attack is on the rise, and this calls for a growth finding(s) to address the features of spamming and offer feasible controls.

2. LITERATURE REVIEW

Social engineering threats is not a new paradigm. But, it has steadily grown with no-end-in-sight. Its continued growth, borders on human nature of trust instincts and emotions, which adversaries manipulate and ultimately exploit to steal user data. Common methods adopted here includes (not limited to) phishing, vishing, etc [20-24]. These attacks are mostly targeted at Internet-based connected devices, which has tripled with the adoption of smartphone. Smartphones have increased user access to Internet from 42.5% in 2013 to about 92% by 2018 [25]. Its choice over the personal computers is due to its portability, functionality, design, mobility etc. In turn, it has significantly increased the threats with a range of complications to work-related and business issues that often exposes sensitive data to adversaries [26-27, 3].

Social engineering threat simply employ technical subterfuge to defraud an online account holder of their financial data by posing as a trusted identity. Phishing employs multiple means like spoofed emails, web link manipulation and forgeries, man-in-middle chat, phone calls, covert redirect etc – to convince a user to divulge confidential data or indulge in fraudulent transactions. A more effective favored variant of phishing is spear phishing – in which targeted mails are sent to a victim, whom are cleverly persuaded via access links redirecting them to spoofed websites containing malware that aim to siphoned and compromise a user data. Another variant of phishing is the short messages (SMS) phishing also called Smishing that tricks a user into downloading a malware unto his cellular phone or other mobile device [10].

Vishing seeks to steal payment card data via calls or SMS with the fraudster posing as a bank's representative in order to convince victims into divulging their data, which is either used for card-not-present transactions (e.g. online shopping), or data is re-coded onto new card for card-present transactions (e.g. purchase goods or cash withdrawal from teller machines). Other attacks redirect a site's traffic to another fake site, by either changing the hosts file on a victim's device, or by exploiting the vulnerability in the domain name service server software. Thus, it allows an adversary install malware unto a user device and redirects the user to a fraudulent site without their consent and/or knowledge [3].

Zaini et al [28] investigated the effectiveness of machine learning in the classification of phishing attacks. Their study compared five classifiers to find the best machine learning classifiers in detecting phishing attacks. In identifying the phishing attacks, it demonstrates that random forest is able to achieve high detection accuracy with true positive rate value of 94.79% using website features. Their results indicate that random forest is the most effective classifiers for detecting phishing attacks. Many other studies have been reported to examine the increasingly, sophisticated tactic of deception fraud – so as to proffer actionable suggestions for effective risk mitigation.

2.1. The University Frontiers, Footprints and Experience

Undergraduates in Nigeria, have both become the target of phishing and also, the perpetrators of these social engineering attacks. Crave for wealth, continues to bedevil Nigeria with sprees of fraudulent practices robbing her of opportunities and progress. Fraud is a criminal act, perpetrated via embezzlement, and theft in which a criminal uses falsehood to benefit from an unassuming victim (usually aimed at a financial transaction). Transaction is the exchange of goods and services for gains or money deliverables [29-31]. With advances in ICT beaming continually its potentials on users across the world, its sine-qua-non effect is the myriad of threats that exploit inherent vulnerabilities in the associated techs. These threats manifest in various forms or ways – presenting itself as misleading items of benefits to unsuspecting users, aimed at defrauding them [2, 5].

[23] examined threats people experience by focusing on the comparison between the effectiveness of phishing and vishing methods, sampling 772-Thai undergrad students with age ranges between 18-to-23 years old. Their result suggests that phishing problem tends to get higher success rate than vishing. Some other factors, such as gender also has an impact on the success rate of each technique.

[32] deployed a client-trusted detection framework for e-banking on the android smartphone platform as it sought for a dependable, mobile banking to address threats via transaction authenticity and message authorization. The framework notably increased clients' trust level against social engineering threats targeted at smartphones with about 72percent for mobile online-banking applications (ported on a community-cloud). They attempted to examine threats experienced by smartphone users by focusing on the comparison between the effectiveness of phishing and vishing techniques. He sampled 600-respondents in the South-South and South-East Geo-Zone of Nigeria. Results indicated that phishing poses more of a problem with higher success rate than vishing.

3. METHODOLOGY

3.1. Data Gathering and Sampling

The study adopts a survey design with chosen samples (biased with the knowledge of social engineering attacks) to help analyze selected data. Dataset was collected through stratified sampling across the six (6) Geo-Political zones in Nigeria. Selected targets includes: The University of Abuja (North-North zone), Federal University of Petroleum Resources Effurun (South-South), University of Lagos (South-West), University of Nigeria Nssukka (East zone), the randomly selected targets. 3-Universities, 3-Polytechnics and 2-Colleges of Education were selected at random from the six (6) geo-zones in Nigeria. Samples retrieved from the Nigeria Universities Commission, Nigeria Board of Technical Commission and The Nigerian Commission for Colleges of Education website. A hundred and twenty (120) students were each chosen from various department(s) in the selected institutions. The study design had about 5,760-questionnaires administered. The achieved co-efficient r = 0.73, accounts for the reliability of instrument (questionnaire) used; while, the figures 1 – 3 depicts a summary of the collected data.

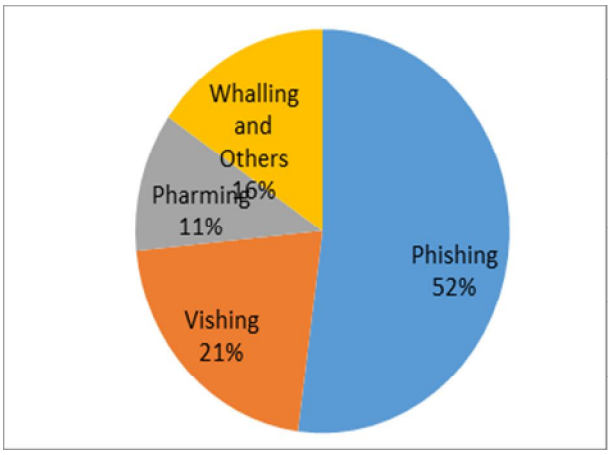

Fig. 1. Target list by Social Engineering Attacks

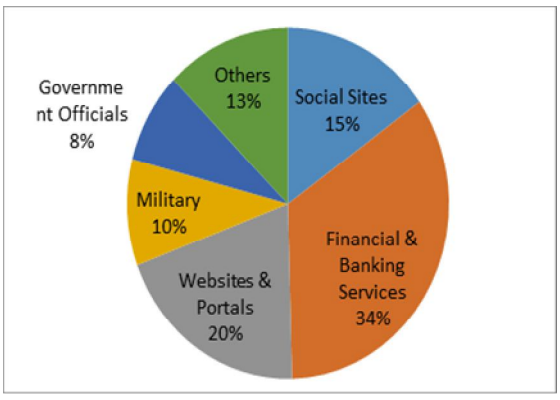

Fig. 2. Targeted Biz by Social Engineering Attacks

3.2. Procedure for Data Collection

In a phishing experiment, it is important to make interaction look like phishing, without actually compromising credentials. A conductive study such as carrying out phishing attacks, in the academic environ is especially difficult for reasons that include attaining the University's approval and for her ICT personnel(s) to carry out such attacks. In our experiments, we illustrated methods to avoid having to handle credentials, but still being able to verify whether they were correctly entered. This was achieved by obtaining feedback from a server log files we had access to. Undergraduates in the selected tertiary institutions were invited via email to participate in a short-web survey about student message usage and info on their future plan to pursue a graduate studies. Webpage was designed and used to collect the data [33-39]. We provided a link to webpage with misspelt URL (Uniform Resource Locator) to the targets. Web pages were designed similar to the genuine site and replicated from the official institution website were designed. All menus and functions are similar to the official institution website. We used the *dot.com* domain as it is cheaper than other host; And, it seems to be the most effective for phishing as adopted from Chanvarasuth [23] and Ojugo and Eboka [10].

Step of phishing technique appears when the targets receive phishing e-mail that contains the link to the phisher website. First, the targets will see the login page on this page, the targets are asked to login by using their own student ID and password on the registration page. The website also asks each student to fill their information such as name, last name, age, e-mail, and others. Our questionnaire is adapted from Wang et al [30] dividing the survey into: demographic, scale of awareness, and risk caused by phishers. After acquiring the data from social engineering techniques, we use victim's data to analyze/compare the effectiveness of these techniques. This study seeks to compare effectiveness between phishing and vishing techniques among other techniques. Then, use a paired sample *t*-test to compare means of same for comparison between 2-sample groups; And, One-Way ANOVA to analyze the data which has more than two groups of sample results.

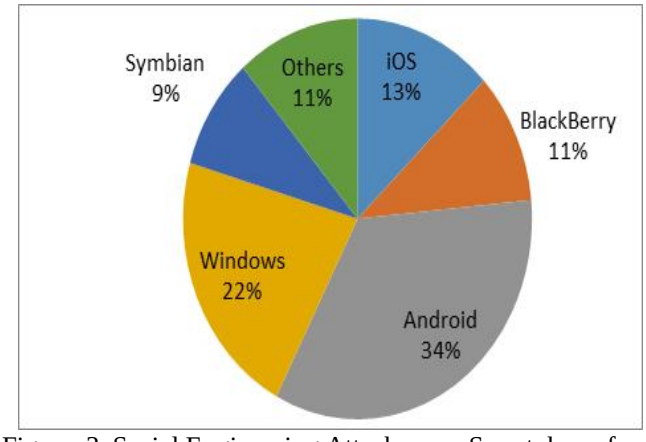

Figure. 3. Social Engineering Attacks over Smartphone from 2011 – 2019

3.3. Statement of Problem

Money serves as great motivation. It mobilizes the mind to great inventions, helping it allocate various resources to productive uses, facilitates exchange and risk management. The hypotheses for the study includes:

a. H_o1: Is phishing is the most effective of all the social engineering technique available?
b. H_o2: What is the success rate of phishing?

The ***objective*** of this study is to: (a) compare the effectiveness between phishing, vishing, pharming and whaling techniques of social engineering threats on Nigeria Undergraduates in relation to exploring how human traits affect these threats and the use of specific techniques.

4. FINDINGS / DISCUSSION

The study obtained responses from 5,231-participants. For phishing, email was sent to all 5,760-participnts and 5,231-respondents were attained to represent approximately 91% of sample population. In table 1, we retrieved 3714-respondents (representing 71%) of the total population of 5231-respondents as obtained for phishing data were male; while 1517 (about 29%) of the sample population for phished clients were female. Conversely, 3766-respondents representing 72% of vished-respondents are male; while, 1465-respondents representing 38% of the vished-respondents were female; And so on.

Table 1. Number of Respondents by Gender

Attacks	Sex	Percent	Count	Total
Phishing	Male	71	3714	5231
	Female	29	1517	
Vishing	Male	72	3766	5231
	Female	28	1465	
Pharming etc	Male	67	3504	5231
	Female	33	1727	
Whalling	Male	67	3504	5231
	Female	33	1727	
Smishing	Male	82	4289	5231
	Female	18	942	

On the hypothesis: we used an awareness factor to ascertain if students are more aware of phishing than any other technique. Our result notes that respondents (undergraduate students) are more familiar with phishing than any other social engineering attack. From our finding, it can be concluded that undergraduate students are more vulnerable to phishing than vishing. Thus, we note that success rate of phishing is higher than vishing, pharming and whaling. We obtained students' first-name, last name, and some other details, to count as ***success***; While, for vishing and others, the needed info is name, last name, and student ID. The study unveils that undergraduate students are more vulnerable to phishing technique than any other technique and thus, it agrees with the works in [40-43].

Table 2. Comparison on Effectiveness of Attacks

No	*Hypothesis*	*F-critical*	*F-Statistics*	*Significance*
$H_0$3	Home	1.732	1.360	0.688
	Private	1.437	1.360	0.647
	Mobile	2.716	1.360	0.070

$p < 0.05$

5. CONCLUSION

Some recommendations and actionable suggestions to mitigate risks of deception and fraud losses [10, 44-47]:

1. Training: (a) keep employees informed on type of scams being perpetrated, (b) provide anti-fraud training on how to recognize attacks and report suspicious activities that violate coy policies and procedures, (c) train employees on what information is confidential and what should never be released unless approved by management, (d) train employees to slow down if the message conveys a sense of urgency, intimidation, or high pressure sales tactics, (e) train employees not to forward, respond to, or access attachments or links within unsolicited emails, (f) hold employees accountable but also create a culture where they are rewarded for verifying suspicious activity.
2. Provide Internal Controls by: (a) authenticating changes to users' contact and internal bank data, (b) require supervisor sign-off on any changes to vendor and client information, (c) validate requests from users, (d) validate all internal requests to transfer data, (e) limit transfer permissions to specific employees, (f) guard against unauthorized physical access (theft of keys, access cards, ID badges etc.), (g) keep physical documents locked and secured and shred documents not in use, (h) monitor the use of social media, (i) develop reporting and tracking programs that document incidences of deception fraud or attempts of deception fraud, (j) keep cyber security software up to date, (k) implement mobile device security procedures, (l) use 2-factor authentications on your organizations computer platform(s).
3. Organizations should continually monitor effectiveness of their education, training, and internal controls by conducting third party penetration testing. These fake hacks provide valuable information on how to focus training and educational efforts.
4. The client-trusted security model for smartphones in mobile banking [23] yields a dependable framework to help with transaction authenticity and message authorization. Result of study shows framework is capable of increasing client's trust level in relation to social engineering attacks with 72% as implemented over their firewall by the banks (ported on a community-cloud) for user access.
5. Exchange of fraud detection data is a prerequisite for curbing the menace and though, these data if often limited and sometimes, experts deem it unwise to describe as well as share such data over public domain (since an extensive knowledge of fraud detection techniques in great detail) will consequently arm

intruders on evasive techniques to curb detection. Thus, as a dual effect, it will further equip users and hackers with adequate data required to combat as well as evade significant detection (for hackers).

The increasing and evolved sophistication in the methods that phishers use to attack clients and evade detection is quite alarming. As phishers continues to develop new means to execute their attacks, research must stay ahead of scammers in terms of the phishing strategies implemented for detection – to proffer up-to-date knowledge defense against these attacks; And in turn, protect both users and their data [1, 23, 33-38].

The study examines the differences on phishing technique from spoofing website, vishing and other social engineering attacks. Result reveals that no matter the method employed, both techniques notes that the targets always loses sensitivity data amongst other properties. Thus, user awareness is a safe haven to combat against phishing. Also, phishing is more effective than any other technique as it yields a higher response and success rate. Women are easier to get phished more than men. Also, an academic major is not a factor affecting the effectiveness of phishing technique. We also found that the type of incoming phone call seems to have an impact on phishing's success rate. Our finding agrees with [24] that women are phished easier than men, but disagree with [39-42] that gender does not have any effect on phishing. Finally, our findings also agree with the study by [21] that academic majors do not have any effect on phishing at all.

REFERENCES

1. A.A. Ojugo., R.E. Yoro., **Forging a deep learning neural network intrusion detection framework to curb distributed denial of service attack**, Int. J. Elect. Computer Engr., Vol. 11, No. 2, pp 128-138, 2021
2. E.O. Yeboah-Boateng, P.M. **Amanor.,** ***Phishing, SMiShing & Vishing: An Assessment of Threats against Mobile Devices***, *Journal of Emerging Trends in Computing and Information Sciences*, 5(4): pp297-307, 2014
3. A.A. Ojugo., A. Eboka., R.E. Yoro., M. Yerokun., F.N. Efozia., **Hybrid model for early diabetes diagnosis**, *Mathematics and Computers in Science & Industry*, 50, pp207-217, 2015
4. A.A. Ojugo, A.O. Eboka, **Signature-based malware detection using approximate Boyer Moore string matching algorithm**, *Int. J. of Mathematical Sciences and Computing*, 3(5): pp49-62, doi: 10.5815/ijmsc.2019.03.05, 2019
5. A.A. Ojugo, A.O. Eboka, **Memetic algorithm for short messaging service spam filter text normalization and semantic approach,** *Int. J. of Info. & Comm. Tech*., 9(1): pp13 – 27, doi: 10.11591/ijict.v9i1.pp9-18, 2020
6. V. Paxson, **An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks**. 31 (3), 38-47, 2001
7. T.M. Nuruzzaman, C. Lee, M.F. Abdullah, D. Choi, **Simple SMS spam filtering on independent mobile phone**. *Journal of Security and Communication Networks*, 5(10): pp 1209–1220, 2012
8. M. Dadkhah, T. Sutikno, **Phishing or hijacking? Forgers hijacked DU journal by copying content of another authenticate journal**. *Indonesian Journal of Elect. Engr., & Informatics*, 3(3): 119-120, 2015
9. A.A. Ojugo., A.O. Eboka., **Empirical evaluation on comparative study of machine learning technique in detection of denial of service attack**, *J. Applied Sci. Eng. Tech. & Edu.*, 2020, 2(1): pp18 – 27, doi: 10.35877/454RI.asci2192
10. A.A. Ojugo, A.O. Eboka, **A social engineering detection model for the mobile smartphone clients**, *African J. of Computing & ICT*, 7(3): pp52-64, 2014
11. I. Androutsopoulos, J. Koutsias, V. Konstantinos., D. Constantine, **An experimental comparison of naïve bayesian and keyword-based anti-spam filtering with personal e-mail messages**, *Proc. of 23rd annual ACM SIGIR Conf. on research and development in information retrieval*, SIGIR '00, pp. 160-167, 2005
12. G. Cormack, T. Lynam, **Spam corpus creation for TREC**. *In Proceedings of Second Conference on Email and Anti-Spam, CEAS'2005*. 2005. [web]: http://ceas.cc/2005/
13. L. Lorenzo, M. Mari, A. Poggi, **Cafe collaborative agents for filtering e-mails**, *Proc. of 14th IEEE Int. Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise, WETICE'05*, pp356-361, 2005.
14. S. Delany, C. Padraig, T. Alexey, C. Lorcan, **A case-based technique for tracking concept drift in spam filtering**, *Knowledge-based systems*, pp 187-195, 2004
15. MAAWG. Messaging anti-abuse working group, ***Email metrics report for third & fourth quarter 2006***, 2006. [web]: www.maawg.org/about/MAAWGMetric200634report.pdf.
16. D. Christine, J. Oliver, E. Koontz, ***Anatomy of a phishing email***. *In Proceedings of the First Conference on Email and Anti-Spam, CEAS'2004*, 2004.
17. O.B. Longe, A.B.C Robert, S.C. Chiemeke, Ojo. F.O., **Feature outliers and their effects on the efficiencies of text classifiers in electronic mail**, *The Journal of Computer Science and Its Applications*, 25(2): pp24-38, 2018
18. L. Daniel, M. Christopher, **Good word attacks on statistical spam filters**, *In Proc. of Second Conference on Email and Anti-Spam, CEAS'2005*, 2005.
19. Ferris Research (2015). ***The global economic impact of spam***, report #409. http://www.ferris.com/get content file.php?id=364
20. E.M. Baker, W.H. Baker, J.C. Tedesco, **Organizations respond to phishing: exploring the public relations tackle box**, *Communication Res. Reports*, 24(4): pp.327-339, 2007
21. C.J. Case, D.L. King, **Phishing for Undergraduate Students**, *Res. in Higher Education Journal*. pp. 100-106, 2006
22. A. Castiglione, R. De Prisco, A. De Santis, **Do you trust your phone**?" In T. Di Noia and F. Buccafurri (Eds.), E-Commerce and Web Technologies, 2009, pp. 50-61.
23. P. Chanvarasuth., **Knowledge on Phishing and Vishing: An Empirical Study on Thai Students**, *International Journal of Humanities and Applied Sciences*, Vol. 2, No. 3, pp 58 – 62, ISSN 2277 – 4386, 2013
24. A. Colley, J. Maltby, **Impact of the Internet on our lives: Male and Female Personal Perspectives**, *Computers in Human Behavior*, 24(5): 2005-2013, 2008
25. D. Harley, A. Lee, **Phish phodder: is user education helping or hindering?**, Virus Bulletin Conf., pp.1-7, 2007
26. D. Irani, S. Webb, J. Giffin., **Evolutionary Study of Phishing**, *eCrime Researchers Summit*, 2008, pp. 1-10.
27. R. Manning, ***Phishing activity trends report: 2nd Quarter/2010***, APWG, pp. 1-11, 2010

28. N.S. Zaini, D. Stiawan, M.F. Ab Razak, A. Firdaus, W.I.S. Wan Din, S. Kasim, T. Sutikno., **Phishing detection system using machine learning classifiers**, *Indonesian J. of Elect. Engr. & Computer Science*, 17(3): pp 1165-1171, doi: 10.11591/ijeecs.v17.i3.pp1165-1171, 2020
29. S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, J. Downs., **Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions**, Proc. SIGCHI Conf. on Human Factors in Computing Systems, pp. 373-382, 2010.
30. J. Wang., T. Herath., H.R. Rao. **An empirical exploration of the design pattern of phishing attacks**, in: S.J. Upadhyaya, H.R. Rao (Eds.), *Annals of Emerging Research in Information Assurance, Security and Privacy Services*, Emerald Publishers, 2009.
31. A.A. Ojugo., A.O. Eboka., **Comparative evaluation for high intelligent performance adaptive model for spam phishing detection**, *Digital Technologies*, 3(1): 9-15, doi: 10.1269/dt-3-1-1, 2018
32. A.A. Ojugo., R.E. Yoro., **Empirical solution for an optimized machine learning framework for anomaly-based network intrusion detection**, *Technology Report of Kansai University*., TRKU-13-08-2020-10996, 2020, 62(10): pp6353-6364
33. T. Jagatic., N.A. Johnson., M. Jakobsson., F. Menczer., **Social Phishing**, *Communications of ACM*, 50(10): 94-100, 2005.
34. S. Hasib, M. Motwani., A. Saxena., **Anti-Spam Methodologies: A Comparative Study**. *Int. J. Computer Sci. Information Technologies*, 2012, 3(6): 5341-5345, [web]: http://www.cs.nmt.edu/~janbob/SPAM
35. A.A. Ojugo., E. Ben-Iwhiwhu, O.D. Kekeje., M.O. Yerokun., I.J.B. Iyawah., **Malware propagation on social time varying networks: a comparative study of machine learning frameworks**, *Int. J. of Modern Education Comp. Science*., 6(8): pp25-33, doi: 10.5815/ijmecs.2014.08.04, 2014. [web]: http://www.mecs-press.org/ijmecs/v6n8.html
36. D. Cook, **Catching Spam before it arrives: Domain Specific Dynamic Blacklists**, *Australian Computer Society*, 2006
37. A.A. Ojugo, A.O. Eboka., E.O. Okonta., R.E. Yoro., F.O. Aghware., **Genetic algorithm rule-based intrusion detection system**, Journal of Emerging Trends in Computing Information Sys., 3(8): pp1182-1194, 2012
38. A.A. Ojugo., R.E. Yoro., **Extending three-tier constructivist learning model for alternative delivery: ahead covid-19 pandemic in Nigeria**. *Indonesian J. of Elect. Engineering & Computer Science*, 21(3), pp1673-1682, doi: 10.11591/ijeecs.v21.i3.pp1673-1682, 2021
39. I.P. Okobah., A.A. Ojugo., **Evolutionary memetic models for malware intrusion detection: a comparative quest for computational solution and convergence**, *IJCAOnline Int. Journal of Computer Application*, 179(39): pp34–43, 2018.
40. A.A. Ojugo., O.D. Otakore., **Mitigating social engineering menace in Nigerian Universities**, *Journal of Comp. Science & Application*, 6(2): pp64–68, doi: 10.12691/jcsa-6-2-2, [web]: www.sciepub.com/jcsa/content/6/2, 2018
41. A.A. Ojugo., A.O. Eboka., **Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: a logical view**, *Int. J. of Modern Education & Computer Science*, 6, pp29-45, 2020, doi: 10.5815/ijmecs.2020.06.03
42. D.A. Oyemade., A.A. Ojugo., **A property oriented pandemic surviving trading model**, *International Journal of Advanced Trends in Computer Science and Engineering*, 9(5): pp7397-7404, 2021
43. A.A. Ojugo., D. Oyemade., **Predicting diffusion dynamics of coronavirus in Nigeria through ties-strength threshold on a cascading SI-graph**, *Tech. Report of Kansai University*., TRKU-13-08-2020-10998, 2020, 62(8): pp4313-4323.
44. A.A. Ojugo., D.O. Otakore., **Intelligent cluster connectionist recommender using implicit graph friendship algorithm for social networks**, Int. J. of Artificial Intelligence, 9(3): pp497~506, doi: 10.11591/ijai.v9.i3.pp497~506, 2020
45. A.A. Ojugo., O.D. Otakore., **Forging a smart dependable data integrity and protection framework via integration of honeypots to web-servers**, *Tech. Report of Kansai University*, TRKU-24-08-2020-11040, 2020, 62(8): pp5933-5947
46. A.A. Ojugo., A.O. Eboka., **An intelligent Bayesian network to improve performance and dependability analysis of a campus network**, *International Journal of Artificial Intelligence*, 10(3), pp [web]: http://ijai.iaescore.com/index.php/IJAI/article/view/20923
47. A.A. Ojugo., D.A. Oyemade., **Boyer Moore string-match framework for a hybrid short messaging service spam filtering technique**, *International Journal of Artificial Intelligence*, 10(3), doi: 10.11591/ijai.v10.i3.pp519-527