Original Research Paper | Vol. 04 Issue 06 June - 2021 | Manuscript ID: #0451

UTILISATION OF INFORMATION SECURITY MECHANISMS FOR COMBATING PHARMING ON UNIVERSITY WEBSITES IN NORTHERN REGIONS OF NIGERIA

ABDULRASHID ABUBAKAR
Department of Library and Information Science, Federal University, Dutsinma-Nigeria.
e-mail:abubakarabdulrashid@rocketmail.com Phone number: 08065570839
Zakari Mohammed
Department of Library and Information Science Ahmadu Bello University, Zaria, Kaduna State-Nigeria.
E-mail address:zakmoh2000@yahoo.com
Umar Babangida Dangani
Department of Library and Information Science Ahmadu Bello University, Zaria-Nigeria, email address : nadangani44@gmail.com

Corresponding author: *ABDULRASHID ABUBAKAR
Email : abubakarabdulrashid@rocketmail.com

ABSTRACT

This paper investigates the "utilisation of information security mechanisms for combating pharming on University Websites in Northern Regions of Nigeria". Two objectives were formulated: to identify the "type of information security mechanisms employed for combating pharming on University Websites in Northern Regions of Nigeria"; and to determine the "effectiveness of the information security mechanisms employed for combating pharming on University Websites in Northern Regions of Nigeria". Quantitative research methodology was used for the study. 9 Universities in Northern Regions of Nigeria with 127 ICT personnel were selected. Questionnaire was used as an instrument in collecting the data. Mean and standard deviation were used to present and analyse the data collected in the study. The research found that "detectives, preventive and mitigative mechanisms"were the types of "mechanisms employed for combating pharming on Universities studied"; it was also found that "mitigative and detective information security mechanisms employed are more effective than preventive mechanisms in combating pharming on University studied". The paper concludes that, if security safeguards are not adequate, pharmers affect the "functionality of University websites undetected". They can attack a websites using skills the software developers never imagined. The study recommended that, to guarantee information effective information security therefore, ICT personnel need to establish strong preventive measures and quality management practices that will protect data during collection, processing and storage from pharmers.

KEYWORDS

Information Security; Pharming Attacks; Detective, Preventive and Mitigative Mechanisms.

INTRODUCTION

Pharming is a fraudulent attempt to manipulate the Domain Name System (DNS) information and redirects victims to unwanted websites under the control of the attacker. Johansen (2019) posits that "pharming is a form of Internet based attack involving malicious code and fraudulent websites. Cybercriminals install malicious code on user's computer or server. The code automatically directs user to sham websites without their consent or permission. The goal is to get user's sensitive information, like payment card data or passwords, on the false websites".

The popularity of the Internet allows universal methods of connectivity that offers tremendous opportunities; allowing average people to make e-transaction, mingle, conduct research and be entertained remotely from their offices or homes through the use of personal computers (PC). As individuals or organisations depend largely on Internet technology for day to day activities, so the likely of pharming attacks and other emerging security threats escalates. As the volume of information grows and continues to be increasingly stored and communicated electronically, it is mandatory for educational institutions, especially Universities and indeed other establishments, to take certain measures to ensure the security of their vital information. Schneider (2013) viewed information security as "a way of safeguarding information and information systems from illicit access, usage, expose, distraction, alteration, read-through, assessment, copy or damage. Information security involved the confidentiality, integrity and availability of data irrespective of the nature the data: be it in storage, processing or transit".

An aspect of information security is Security Mechanism. It is a method, means, tool, system, instrument, device or procedure for enforcing security. Stallings (2005) opined that "Security Mechanism is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of Security Mechanisms are encryption algorithms, digital signatures and authentication protocols among others". There are numerous Security Mechanisms to combat pharming attacks. They include: cryptographic techniques, authentication, authorisation, accounting (auditing), physical security, packet filters, firewalls, and intrusion detection and prevention system to mention a few.

Pharming is one of the devastating cybercrimes today demanding slight talent on the part of the impostors. The task of protecting vital information of users such as usernames and passwords from pharmers becomes essential day in day out. The best way to keep individual and organization safe and secured against these pharming attacks is by following the best practices of information security. Internet users should be regularly informed about the pharming phenomena. That Pharming is seemingly an evolving organism. Thus, there is need to have security up-to-date on system and websites. An unsecured website is vulnerable to users: private, public or government sites. It permits rapid growth of pharming attacks against sensitive assets and organisational infrastructures. To this end, Universities and indeed other establishments should develop a strong website security architecture and robust risk and disaster management policy and framework to enhance network security and prevent data breaches on their websites.

Statement of the Problem

It is important to emphasise that the loss of data assets in a University is a serious and huge loss capable of affecting its progress. It will also portend a gloomy picture and a terrible pointer to a University's reputational crises. Individuals and Organisations should be cautious in providing

effective information security mechanisms to detect, prevent and mitigate fraud as a result of pharming attacks such as Domain Hijacking, DNS Cache Poisoning and Registration of Similar Sounding Domains among others. It can be argued that pharming attacks as major crimes are escalating universally, frightening individuals and organisations.

Spammers, Skimmers and malicious apply numerous methods of pharming to get organisations and individuals crucial information. The aforementioned necessitated the need to examine the utilisation of information security mechanisms for combating pharming on University websites in Northern Regions of Nigeria.

Objectives of the Study

This study has the following objectives:

1. To identify the "type of information security mechanisms employed for combating pharming on University websites in Northern Regions of Nigeria".
2. To determine the "effectiveness of the information security mechanisms employed for combating pharming on University websites in Northern Regions of Nigeria".

Literature Review

Pharming attacks are treacherous to internet users; they are fraudulent ways to obtain vital information such as users' credentials like bank account details, social security numbers etc. Symantec (2016) remarked that "the key technique to fight against pharming is being performed by the Internet Service Providers (ISPs). They sift out as many of the fake redirects as possible. Nonetheless, it is likely to upturn system guard from office/home with some modest stages and protections. It is essential to embrace the use of trustworthy ISPs. The URL is also an important place to check. Constantly ensuring that, as soon as a page has been loaded, the URL is spelt properly so that it is not readdressed to a slightly dissimilar spelling". Kessler (2013) asserts that "prevention, detection, and mitigation of pharming include constant enhancements to incorporate security measures".

Detection:

Detection is the process of identifying the presence of something concealed. According to Sheng, Holbrook, Kumaragus, Cranor & Downs (2009) "an effective methods to detect pharming falls between the victim and the pharmers. The logic is that by stooping/preventing the nasty email sent to the victim, it will stop the victim from being pharmed".

Prevention:

Prevention is the process of stopping something from happening. Banday&Qadri (2007) posited that "pharming is relatively new, complex and continuously evolving phenomenon that includes social engineering as well as malicious technology. There is no fool proof technology or legislative system that can protect against or prevent pharming attacks from getting through. However, properly deployed combinations of technology coupled with employee education and diligence can significantly reduce the likelihood that a business or a customer will succumb and fall victim to this growing threat. Further, public reporting mechanisms established by governments and the law enforcement community."

On the other alternative, the initiative by Google should be emulated by other giant industries and Universities so as to lessen the effect of pharming. Paladin (2016) outlined various mitigation security mechanisms to combat pharming attacks such as:"USE of SSS certificate to help establish the true Identity of websites; making sure that the Domain Name System software is properly protected; Use

of freely accessible internet services to observe any modifications on Domain Name System configuration (e.g. Markmornitor.com, Mark Alert); Visual cue e.g. identity cues; Anti-pharming tool; Multifactor and Token based Authentication; Educating Website users; Keep simple names for domain; SfoofStick and Cloud Mark Anti-fraud Toolbar".

Mitigation:

Mitigation is the process of making something less severe, dangerous or damaging. Individuals and Organisations should be cautious in providing effective information security mechanisms to detect, prevent and mitigate fraud as a result of pharming attacks such as Domain Hijacking, DNS Cache Poisoning and Registration of Similar Sounding Domains among others. Pharming attacks as major crimes are growing rapidly in every nook cranny of cyberspace, intimidating private and public sectors. Cybercriminals use different methods of pharming to get organisations and individuals vital information. Thus, organisations should endeavor to implement the latest and sophisticated information security mechanisms to curtail the effects of pharming attacks on their websites.

Methodology of Conducting the Research

Quantitative research methodology was adopted in this research. The target population of the study comprised of all the 61 Universities in the Northern States of Nigeria recognised by the National University Commission (NUC). However, the study population (subjects of this study) were the ICT personnel of the Universities studied. The personnel comprised of the Directors, the staff of the Software Development Units and the staff of the Networks Infrastructure and Security Units. This gives a total number of seven hundred and thirteen (713) personnel. Using multistage sampling technique (i.e. purposive, stratification, cluster, proportionate and simple random sampling),a sample of 9 Universities was used for the study with 127 respondents (ICT personnel). Quantitative technique (Mean and Standard Deviation) was used in analysing the data in the study.

Findings and Discussions

The data collected and analysed were presented and discussed under the following subheadings:

Types of Information Security Mechanisms employed for Combating Pharming on University websites Studied in Northern Regions of Nigeria

The first research question was aimed at identifying the "types of information security mechanisms employed to combat pharming attacks on the websites of the Universities studied in Northern States of Nigeria". In order to answer the research question, the researcher categorised the information security mechanisms into: "detective", "preventive" and "mitigative mechanisms" for the respondents to tick as applicable to their respective Universities as shown in table 1. The acceptance benchmark is 3.0 mean score. Thus, any item less than 3.0 response mean score was not accepted as being an ultimate "information security mechanism employed to combat pharming attacks on the Universities studied".

Table 1: "Type of Information Security Mechanisms employed for Combating Pharming on University Websites Studied in Northern Regions of Nigeria"

"Type of Information Security Mechanisms"	N	Mean	Standard Error	Standard Deviation	Remarks
Detective Mechanisms	40	4.31	.050	.559	Accepted
Preventive Mechanisms	13	4.03	.059	.666	Accepted
Mitigating Mechanisms	60	4.29	.040	.456	Accepted
Total	**113**				

Table 1 depicts the mean scores and standard deviation of the "type of information security mechanisms employed to combat pharming attacks on the websites of the Universities studied in Northern Regions of Nigeria". From the table, it can be seen that "detective mechanisms" with mean scores of 4.31, and standard deviation = .559 were identified as the most employed information security mechanisms. This is followed by "mitigative mechanisms" with mean scores of 4.29 and standard deviation = .456. The 'preventive mechanisms' were found to be the least employed "information security mechanisms" with mean scores of 4.03 and standard deviation =.666 response scores.

This implies that all the items ("detective, preventive and mitigative mechanisms") have mean scores and standard deviation above the acceptable benchmark of 3.00. It therefore means that the Universities studied accepted them as the type of "information security mechanisms employed for combating pharming on their various websites".

From the analysis it can be concluded that "detective mechanisms are the information security mechanisms mostly employed to combat pharming attacks in the Universities". This is closely followed by mitigating mechanisms. The least employed mechanisms are the "preventive mechanisms on the websites of the Universities studied in Northern Regions of Nigeria". This finding agrees with the earlier findings of Sheng et al (2009), and Sumathi& Prakash (2012). In their separate studies, "they found detective mechanisms as important in reducing the number of pharming attacks on websites. This finding is plausible because the effective means of detective mechanism lies between the user and the pharmers". This is because the idea of blocking the malicious email directed at a user and will hinder the malicious email from a victim and will have a least chance of being pharmed. It may also be that many email providers such as Google have integrated pharming 'detection and notification' into their email services that play important role in reducing the number of pharming attacks on websites.

The implication of this finding is that the Universities should take holistic measures from people and process standpoint to detect, prevent and mitigate security breaches on their websites. This should involve auditing all operator/administrator access and actions, have zero standing permission for administrators in the service, have "Just-In-Time (JIT) access and elevation" of ICT personnel especially Network Security and Infrastructure personnel privileges to troubleshoot the service and ensure segregation of the employee email environment from the production access environment.

The second research question sought to examine the "effectiveness of the information security mechanisms employed to combat pharming attacks on the websites of the Universities in Northern States of Nigeria studied".

The respondents were presented with a list of types of "effectiveness of information security mechanisms (i.e. detective, preventive and mitigative mechanisms)" to indicate the effectiveness of the mechanisms employed against the ones that are applicable to them. The table 4.9 portrayed the responses of the respondents. The acceptable response benchmark was 3.0 mean scores. Hence, any item less than 3.0 means score was not accepted as really being effective.

Table 2: "Effectiveness of Information Security Mechanisms employed to Combat Pharming Attacks on the Websites of the Universities Studied in Northern States of Nigeria "

"Effectiveness of Information Security Mechanisms"	**N**	**Mean**	**Standard Error**	**Standard Deviation**	**Remarks**
"Detective Mechanisms"	40	3.25	.044	.499	Accepted
"Preventive Mechanisms"	13	2.95	.053	.602	Rejected
"Mitigative Mechanisms"	60	3.39	.074	.837	Accepted
Cluster Mean		**3.30**	**.057**	**.646**	
Total	**113**				

Table2 shows the mean scores and standard deviation of the "effectiveness of the information security mechanisms employed to combat pharming attacks on the websites of the Universities studied in Northern States of Nigeria". It indicated that 'detective mechanisms' with mean scores of 3.55 and standard deviation = .044; and 'mitigative mechanisms' with mean scores of 3.39 and standard deviation = .074 have mean scores and standard deviation above the acceptable benchmark of 3.00. They are thus accepted as being effective with the cluster mean scores of 3.30 and standard deviation of .057. On the contrary, 'preventive mechanisms' with mean scores of 2.95 and standard deviation = .053 below the acceptable benchmark of 3.00 are not accepted as being effective From the forgoing analysis, it can be deduced that "mitigative and detective information security mechanisms employed are more effective than the preventive mechanisms in combating pharming attacks on the websites of the Universities studied in Northern States of Nigeria". This finding corroborates with the findings of Banday&Qadri (2007) and Paladin (2016). In their separate findings, they reported the use of "detective and mitigative information security mechanisms as being effective for combating pharming attacks on the websites of organisations". This finding may be that the Universities' websites managers have to take holistic approach to critical technologies such as DNS to ensure that they are designed and maintained securely.

The major findings of the study include:

1. "Detectives, preventive and mitigative mechanisms are the types of information security mechanisms employed for combating pharming on University websites studied in Northern Regions of Nigeria".
2. "Mitigative and detective information security mechanisms employed are more effective than preventive mechanisms in combating pharming on University websites studied in Northern Regions of Nigeria".

CONCLUSION

From the analysis and research findings, it can said that the "ICT staff of the Universities studied have realised the need for application of mitigative and detective mechanisms as part of defense-in-depth strategy for providing reasonable protection of sensitive information vis-à-vis the means of detection and remediation of security breaches". However, the ICT staff does not seemingly explore, to a large extent, the advantages of preventive mechanisms to prevent the occurrences of most pharming on the websites of their Universities. This paved way for cyber-crimes. Generally, when security safeguards aren't adequate, intruders could escape undetected. They can attack a website using methods the designers are unaware of. Hence, the need for constant improvement on securing the vital information.

Recommendations

The study recommended the followings:

1. "Ensure that robust information security mechanisms such as: third-party host resolution verification, suitable change regulator, regular checking and warning/caution mechanisms are available in order to effectively protect pharming on websites".

2. "Intensify the use of preventive information security mechanisms such as provisions of Secure Token Service (STS); and Use of Site Seal in combating pharming attacks".

References

Banday, M.T., &Qadri, J.A. (2007). "Phishing - A Growing Threat to E-Commerce," The Business Review, ISSN: 0972-8384, 12(2), pp. 76-83

Johansen, G.A. (2019). What is pharming and how to protect yourself. Retrieved on 16th February, 2021 from https://us.norton.com/internetsecurity-online-scams-what-is-pharming.html

Kessler, G. (2013). An Overview of Cryptography. Retrieved 8th May, 2018 from http://www.garykessler.net/kumquat_pubkey.html.

Schneider, L. (2013). Information Security - Learn about Information Security. Retrieved on 16th March, 2018. From http://www.about.com/.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L.F. & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. Proc. of the 28th International Conference on Human Factors in Computing Systems, USA.

Stallings, W. (2005). Cryptography and Network Security, Principles and Practices. Third Edition. USA: Pearson Education, Inc.

Symantec (2016). Online fraud: pharming. Retrieved on 15th April, 2018 from http:// us.norton.com/.