Innovare
Academic Sciences

International Journal of Pharmacy and Pharmaceutical Sciences

ISSN- 0975-1491 Vol 7, Issue 10, 2015

Letter to Editor

PHISHERS ATTACK ON THE RESEARCHERS FOR FINANCIAL GOALS IN PHARMACEUTICAL AND MEDICAL OPEN ACCESS JOURNALS

MEHDI DADKHAH[1]*, ALI TARHINI[2]

[1]Department of Computer and Information Technology, Foulad Institute of Technology, Fouladshahr, Isfahan, Iran, [2]Department of Information Systems, Brunel University London, Uxbridge, Middlesex, United Kingdom
Email: dadkhah80@gmail.com

Received: 10 Jul 2015 Revised and Accepted: 24 Aug 2015

We and other researchers introduced some types of frauds in the academic world such as hijacked journals [1-3], fake conferences [4], social engineering [5] and etc. The mentioned frauds are committed by forgers, but recently, we observed new type of fraud that is committed by phishers who are mainly attacking the researching authors. Information security literature defined phishers as those who create the fake website which is similar to the original one, and consequently they end up stealing victim's user names and passwords for financial goals. In other words, phishing is the action of attacking researchers for stealing their sensitive information by means of social engineering techniques [6]. There are different types of phishing attacks, and some techniques have been introduced for the sake of their detection. Nowadays, Phishers are attacking researchers for financial goals. They search for authors' email addresses in open access journals that mainly charge authors for publishing, and then they collect a list of authors' emails. In a later stage, the phishers start sending deception emails to the victim authors in order to cheat them and eventually steal their credit card information. In some cases, Phishers create fake PayPal invoice or fake payment website and redirect authors to it, then steal their credit card information. Other examples of phishers attack is the use of email spoofing technique that consists of sending emails to authors with the contact address of famous journals or editors without having the ability of receiving any kind of acknowledgments or replies. In this new type of fraud, authors think that they are interacting with the original payment website or received subscription invoice from journals. To confront with this kind of fraud, we recommended following the below steps:

– If you receive an email from journal that request payment, make sure to check the sender email address and their corresponding names. This is followed by sending an inquiry email to the editor of the journal for the purpose of detecting whether the attack is done by the email spoofing technique.

– Check websites against phishing attacks by using available and well-known anti-phishing tools. This can be greatly assisted by the fact that many browsers are equipped with supported anti-phishing tools.

– Check email attachment file type and make sure not to open or download suspicious file type such as html, jar, exe, xml and etc. Phishers maycreate malware and infect victims' operation system and accordingly steal sensitive credential information.

– If the email contains links that redirect users to a website, carefully check the website URL by retrieving its hosting database for the sake of identifying its originality. It should be noted that Phishers may use similar URL to the original website for deceiving authors.

– Some emails request urgent reply and promise the researchers with big prizes when they answer the emails. In first, these emails request some personal information such as age, full name, address, telephone number and etc. After that, the phisher send fake invitation or invoice for victims and cheat them. In this case, we recommend ignoring such emails.

– Make sure to search for the sender email address and contact information in popular search engines, if it belongs to editor or journals, you can find similar results.

By doing the above mentioned steps, this new fraud can be easily detected. However, Phishers may change their techniques, and the author must be careful every time he/she receives an email requesting sensitive information. Indeed, this fraud is considered as a kind of phishing attacks that is called "spear phishing" as it contains information related to a specific group of authors and conceives them.

REFERENCES

1. Jalalian M, Mahboobi H. Hijacked journals and predatory publishers: is there a need to re-think how to assess the quality of academic research? Walailak J Sci Tech 2014;11:389-94.
2. Jalalian M. Hijacked journals are attacking the reliability and validity of medical research. E-Physician 2014;6:925-6.
3. Dadkhah M, Obeidat MM, Jazi MD, Sutikno T, Riyadi MA. How can we identify hijacked journals? Bull Electrical Eng Inf 2015:83-7.
4. Dadkhah M, Jazi MD, Pacukaj S. Fake conferences for earning real money. Med J Soc Sci 2015:6;11-2.
5. Dadkhah M, Quliyeva A. Social engineering in academic world. J Contemporary Appl Mathematics 2014;4:3-5.
6. Martinoand AS, Perramon X. Phishing Secrets: History, Effects, and Countermeasures. Int J Network Sec 2010;11:163-71.