COMMENTARY

Publication phishing: a growing challenge for researchers and scientific societies

Shahryar Sorooshian

Publication phishing has the potential to develop further into a serious gainful enterprise if effective security measures are not in place. Be that as it may, there is growing concern over the erosion of users' trust towards journals, conferences and other channels of publication stemming from the rise in scam cases involving users' money, research articles and personal identifications. Phishing is becoming a major issue for users and will be making an ever greater and prominent issue for good scientific societies who need to devise anti-journal hijacking measures to mitigate the impacts of phishing to their operations. Researchers and scientific societies need to design adequate technical security systems to mitigate phishing threat to users. This note highlights some issues and basic steps to anti-phishing educators and scientific societies to ensure the viability of anti-phishing initiatives.

Publication phishing has been attracting a lot of interest and receiving serious concerns[1], in light of the fact that such attacks have been expanding and escalating in operations, number and sophistication. The term 'phishing' originated from the analogy where cyber identity predators employ alluring information typically in such forms like e-mails to 'fish' for or steal delicate personal identifiers and finance-related information from the 'sea' of web users[2]. In mid-2003, most internet identity thefts were in the form of e-mails, often embedding website designs into the e-mails containing logos of focused companies, including return addresses that were spoofed to appear as though they originated from the companies. In any case, by mid-2004, 'phishers' (predators or fraudsters) started utilizing novel programming strategies to modify the appearance of the victim's address bar by supplanting the 'URL' of the phishing site, with the goal to impersonate the company[2]. However, the activities became more prominent in 2012 when cyber criminals began massively engaging in publishing numerous counterfeit scientific journals[2,3]. This was a major breakthrough for these phishers who are currently ready to swindle a large number of users worldwide, as it is presently hard to discern between the genuine and the fake. In 2004, an estimate of 57 million American adults received e-mail attacks from phishers[2]. It must be emphasized that phishing is not limited to the most well-known activities in which targets are sent spoofed messages alluring them to divulge private information. Rather and as of late reported both in academic and criminal perspectives, phishing is a multifaceted techno-social issue for which predatory publishers attempt to take advantage of authors who are seeking a home for their findings in the scholarly publishing world. They have turned their websites into money-making systems that ultimately publish large volumes of non-reviewed papers on their fake websites[4]. These non-peer reviewed papers published and circulated will appear in search results and will be used for future research. This, however, undermines the reliability and validity of published scientific papers as well as future research[5]. As a result, an increasing number of researchers and experts are trying to measure dangers and degrees of vulnerabilities with a specific goal to understand where to focus anti-phishing and protective measures[2]. However, this note highlights some basic steps to inform researchers on how they can handle these phishers in today's environment of emerging and intense social engineering innovations.

Specifically, hijacked journals are those that scam researchers using identifiers and reputation of their original counterpart[1]. These fraudsters present themselves as the principal journal editors by designing an on-line website for existing journals that offers print-only access, but lacks on-line or electronic access[6]. Generally, they use the conventional techniques for social engineering to exploit gullible research brains who are trying to publish their findings in journals and other media. As such, these fraudsters have hijacked a number of legitimate and prestigious sites of indexing journals. Among these indexed sites, we can refer to Cite Factor (http://www.citefactor.org), which has put together almost all hijacked journals as well as their fake addresses[5]. Primarily, those journals with wide scope or topics (for

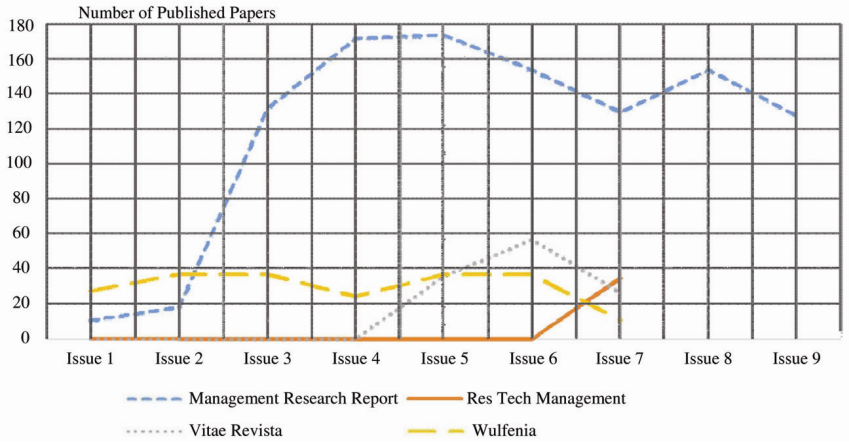

Figure 1. Number of published papers per issue in some hijacked journals[5].

instance, *The Journal of Technology*) are targeted and attacked[5]. Figure 1 shows the tendency of journal hijacking in relation to journal issue; it indicates the number of papers published per issue in some hijacked journals. From the figure, the number of paper(s) had a tendency to increase in every issue in light of the fact that hijackers used numerous deceptive strategies for swindling authors and for every issue they will get more papers from authors. Nonetheless, after some time the authors realize that these journals are scams and as a result, the number of paper(s) in the subsequent issues eventually begins to diminish[5].

By and large, the proliferation of publication centres, scientific communities and multifaceted techno-social innovations has witnessed the emergence of various kinds of phishing activities on the internet. These activities are incorporated in the form of deceptive phishing, phishing using destructive software, web Trojans, pharming, phishing injection, phishing based on fake applications and domain hijacking, among others. To handle these predatory activities, numerous techniques and systems have been designed, including Sign-in Seal, web page-based design systems to detect phishing websites, genetic algorithm, data mining algorithm, categorization of super link techniques, etc.[6]. Nonetheless, some basic steps have been provided below to inform researchers on how to detect hijacked journals based on their activities. It is expected that when these steps are used together with technical counter measures, the concerns arising from publication phishing, specifically journal hijacking, will be effectively avoided.

Domain page ranking: Page Rank is an algorithm used by Google to rank websites based on the result from search engines. It has to do with an assessment of the quality and number of links to a page to check the rough approximation of the significance and impact of the website. Websites that are more important are likely to be connected to other websites. Hijacked journals mostly have no or very low ranking. Therefore, if the assessed website does not have high ranking, then it is necessary for researchers to question its authenticity (refer to the following website for page ranking: http://www.whatsmypr.net)[5,6].

Availability of previous numbers: Hijacked journals typically ask for usernames and passwords to obtain information from the previous journal issues or just to index abstract of articles. If a journal employs this feature, then a critical investigation needs to be undertaken by authors to avoid any case of fraud[5,6].

Website domain lifetime: Counterfeit journals usually register their website domain shortly before designing the website. Hence, site domain of counterfeit journals might have been registered in recent years. However, the existing papers in the list of archives date back several years ago. Suitable domain lifetime is measured in relation to the first issue in the journal archive. This feature is also suspicious and authors will have to assess the credibility of those journals before providing any financial or personal identification to them. The WHIOS databases can be used to obtain information on this feature, (http://whois.domaintools.com)[6].

Call for papers: Counterfeit journals normally endeavour to send persistent e-mail messages to entice their victims. They get the victims e-mail through existing articles in low-quality journals and conferences. They also seek e-mail addresses of authors from some commercial websites and non-peer review journals. The prospective victims are anticipated to respond positively to calls for papers through e-mail messages received from these hijackers. They are smart in using e-mail marketing (spam marketing) to lure their victims[1,7].

Mostly, victims of hijacked journals are from the developing countries where there several conferences are held by private companies instead of scientific societies or universities. Generally, reputable journal's have visitors geographically spread across the globe and are not limited to few or certain countries. Therefore, if a journal's visitors are limited to few or certain countries, then authors should be circumspect about their validity and reliability. For instance, 40 websites in relation to hijacked journals showed that the victims usually belong to the developing countries. The Alexa website can be used to verify information about the journal website visitors (http://www.alexa.com)[5,6].

Thus there is a growing concern to evaluate and design appropriate technical security systems and educational programmes to mitigate phishing threat posed to scientific societies. A global anti-journal hijacking strategy should disseminate information about such scams and provide fundamental knowledge of this issue to researchers and practitioners. Therefore, if an author is considering publishing a research paper, there are a couple of critical factors to consider in the pre-submission process. For instance, be cautious about unfamiliar journals whose promises sound too good to be true, or ignore spontaneous calls for papers or e-mails asking you to submit a paper or that your paper has already been selected for publication. Likewise, verify information on these journals through different *Web of Science* databases and various indexes. Also, use their papers to search for more information.

1. Jalalian, M. and Mahboobi, H., *Walailak J. Sci. Technol.*, 2014, **11**(5), 389–394.
2. Gerald Goh, G. G., Tan, N. L., Goh, C. Y., and Uchenna, C. E., *Commun. IBIMA*, 2008, **5**, 133–142.
3. Jalalian, M. and Mahboobi, *Electron. Phys.*, 2013, **5**(3), 685–686.
4. Jalalian. M., Publication ethics report, 2014; www:mehrdadjalalian.com, http://www.mehrdadjalalian.com/index.php/list-of-hijacked-journals-and-fake-publishers/30-hiajcked-journal-list-2014-first-edition-june-2014 (retrieved on 18 May 2015).
5. Dadkhah, M., Obeitat, M., Davarpanah Jazi, M., Sutikno, T. and Riyad, M., *Bull. Elect. Eng. Inform.*, 2015, **4**(2), 83–87.
6. Dadkhah, M., Tole, S., Davarpanah Jazi, M. and Deris, S., *Telkomnika*, 2015, **13**(2), 373–380.
7. Kolahi, J. and Khazaei, S., *Dent. Hypotheses*, 2015, **6**(1), 3–5.

Shahryar Sorooshian is in the Faculty of Industrial Management, Universiti Malaysia Pahang, Malaysia.
e-mail: sorooshian@gmail.com