WALAILAK JOURNAL
http://wjst.wu.ac.th Special Article

Hijacked Journals and Predatory Publishers: Is There a Need to Re-Think How to Assess the Quality of Academic Research?

Mehrdad JALALIAN[1,*] and Hamidreza MAHBOOBI[2]

[1]*Editor In Chief, Electronic Physician, Mashhad, Iran*
[2]*Infectious and Topical Diseases Research Center, Hormozgan University of Medical Sciences (HUMS), Hormozgan, Iran*

([*]Corresponding author's e-mail: mehrdad.medic@gmail.com)

Received: 2 February 2014, Revised: 4 February 2014, Accepted: 6 February 2014

Abstract

During the last 2 years, there has been extensive discussion about "hijacked journals being imposed on the academic world by the huge increase in the number of bogus publishers and spurious websites". Hijackers make money by stealing the identities of legitimate journals and collecting the article processing charges on the papers that are submitted to journals. The cybercriminals have cheated thousands of professors and Ph.D. scholars mostly from developing countries and those who were in the urgent need of publishing their articles in journals that are covered by the Journal Citation Report (a Thomson Reuters' product). The fake journals targeted their victims using smart ideas both in web development step and victim selection. This paper introduces some simple methods that can be used easily to identify the fake publishers as a short to midterm solution and recommends establishing a movement for designing a new model for assessing the quality of academic research.

Keywords: Research, journal, publisher, impact factor, fake

Introduction

We read with great interest the paper in the journal "Nature" in which Declan Butler reported 2 sham journals that were scamming authors [1]. According to Butler (and our own experience as well), 2 print-only journals that do not offer electronic versions were hijacked by cyber criminals. The hijackers set up fake websites and took money from authors who were attempting to publish their research work in one of the journals indexed by Science Citation Index Expanded (SCIE), a Thomson Reuters' metric product that compiles impact factors for covered journals. A similar story entitled "Scientific Articles Accepted (Personal Checks, Too)" was published in The New York Times recently [2], warning about fake conferences and the unethical business practices of some predatory publishers.

While there was a substantial increase in the number of fake publishers and hijacked journals in 2012, we have being trying to draw attention to this predatory practice for several years. Indeed, we identified the signs of a growing movement toward such misconduct in the early 2000s, when some of the "American Journals" based in Asia were established. The so-called "American Journals" (with no American authors publishing their work in them) began to publish thousands of articles written by authors from developing countries. These authors, who were unknowingly defrauded, were very excited to see their research published in the prestigious "American Journals". A journal editor for a reputable publishing company in Iran told us about a recent incident in which an author submitted an article for publication in the journal. After reading the article, the journal's reviewers provided a long list of constructive comments that required the author to make major revisions. The author had obviously been defrauded earlier by either "American Journals" or similar bogus publishing companies, and he responded to the journal editor: "I have published numerous articles in prestigious American journals before without

any need to revise the manuscript; why is your non-reputable, regional journal so demanding?" We know of literally hundreds of such incidents during last 10 years, and we have expended considerable effort to warn academic researchers about the low-quality, non-reviewed journals those days and to caution them about being fooled by some of the so-called "prestigious journals" that work only on a "pay and get published model". The result of efforts, which were well-intentioned, was that thousands of excited authors turned against us, especially those who had received academic upgrades by publishing in commercial journals. This story reminds us an old, Persian proverb that says "One hand clapping produces no sound!" After these introductory remarks about this issue, first, we discuss the overt misconduct that threatens the academic world, i.e., fake publishers and scam websites and introduce some practical, short-term solutions for avoiding fake publishers and hijacked journals. Finally, we address the issue of questionable and nefarious, open-access publishers to depict the magnitude of the threat they pose, and close the paper by emphasizing the emergent and pressing need to re-think how we assess the models of evaluating academic research.

The problem: real money from fake journals

Stories about fake websites that con people into paying for goods that are never delivered have been told for many years. Today, the facts that we consider research 'a work' only if it is published in journals that have a high impact factor and that academic publishers have shifted from a traditional business model to an open-access model have made it profitable enough for scammers to add a new line in their business: "Real Money from Fake Journals" [1,3]. During the last 2 years, cyber criminals have started to imitate the names of reputable journals that publish only printed versions of articles. During these 2 years, we observed almost all of the fake publishers and hijacked journals, and there were almost one hundred of them. By saying "one hundred" fake journals, readers may think we are referring to the predatory journals that could easily number in the hundreds these days; however, what we are really referring to are the tens of cases similar to the "Vulfenia Journal" and "Archives des Sciences," not the predatory, open-access journals. In our updating of these kinds of spurious journals, we found evidence of the hijacking of "Jokul Journal" from Iceland, a South African-based journal entitled "Bothalia," and an old French journal "Pensee Journal", all of which have their impact factor compiled by Journal Citation Report (JCR). Moreover, we have diagnosed some signs of the fake institutes (registered by no one at nowhere) that began to assign fake impact factor values to journals recently [4]. Actually, paying for real, open-access publications is a reasonable thing to do, but the money should go to reputable, not bogus, journals. The extent to which thousands of authors have incurred strong negative impacts as the result of having been duped into publishing in fake journals is sad, both for those authors and the scientific community at large. The sadder story was that we found some lecturers who opted to submit their manuscripts to Vulfenia Journal even though they were fully aware that it was a fake journal. They did so because they were going for their academic upgrade procedure, and they knew that the university evaluators/reviewers were not aware of the fake-journal scam and would approve their academic upgrade.

Unfortunately, such fake websites can be created by almost anyone who has even minimal knowledge of how to design a website can do so by using open-source Content Management Systems (CMSs). However, we believe that the academic cyber criminals who are responsible for the propagation of hijacked journals are completely familiar with the academic rules of upgrading lecturers, qualifying Ph.D. candidates, and applying for admission to postgraduate programs or any professorship positions. These criminals may be ghost writers or they may be the experts who used to help scholars write and publish their research work before they decided to become full-scale "ghost publishers". Whoever they are, it is apparent that they have the knowledge required to design a website and to hide their identities on the Internet. In addition, they definitely are familiar with authors' behaviors, and they know that many of authors are in urgent need of publishing a couple of "ISI papers" (i.e. articles published in journals that are indexed by Thomson Reuters/Institute for Scientific Information-ISI) within a limited time. Therefore, the new version of academic cyber criminals knows what to do and how to organize a completely fake conference or hijack a printed journal. According to our observations, the main techniques and rules these criminals have used to cheat high-intellect academics are categorized below.

Target (journal) selection

1. Finding some reputable, but non-famous, journals as their potential targets, especially individual publishers with single journals.

2. Journals based in non-English-speaking countries are preferred. It is really a difficult job even for authors who are skeptical about a journal to find the phone numbers of authentic journals that are based in non-English-speaking countries.

3. Since only the Thomson Reuters' (ISI) indexed journals matter to most universities when someone is applying for an academic upgrade or a Ph.D. opportunity, the criminals know that the victim journal should be covered by the Web of Science (WOS) and have an impact factor compiled by the JCR, a product of Thomson Reuters.

4. The target journal should not have a website. When searching Thomson Reuters for print-only journals using their ISSN, their titles will appear in the search results. However, no links to the journals' websites exist because they do not have websites.

5. The target journal should not have a high impact-factor value because it would be difficult for the hijackers to convince the authors that a high impact-factor journal invited them to publish their work in 2 weeks. However, claiming a low (but greater than zero) impact factor on the fake website is good enough for authors who are trying to get their work published in a Thomson Reuters' indexed journal in the shortest possible time.

Web development

1. Anonymous registering of a .COM or .ORG domain name for the affected journal to imitate the website of an authentic journal or maliciously setting up a duplicate website for the hijacked journal.

2. Avoiding the country-name domains (such as .US and .IR) because their registration procedures usually require a check of the identity of the domain owner or verification of a valid address.

3. Misusing of famous editors and real people's names in the list of the journal's editorial board without their permission. It seems to be an easy job to set up a fake journal listing "editors" who know nothing about the job they purportedly are doing or listing fake names of people with titles such as "Dr." or "Ph.D."

4. Creating fake impact factors or falsely stating that they have earned an impact factor is a good technique to pretend to be a prestigious journal. This technique applies for the completely fake publishers, not for the websites of real journals that have been hijacked, because they have a verified impact factor compiled by the JCR.

5. Providing a link from a fake website to the authentic journal's profile in the master journal list of Thomson Reuters. Sometimes, authors know that there should be a link between the Thomson Reuters' website and the Journal's website, but they forget that this link should be from Thomson Reuters to the Journal, not from the Journal to Thomson Reuters.

6. Having no contact detail provided in the "Contact us" page of the website of a hijacked or fake publisher.

7. Providing full contact information in the hijacked journal! As we stated previously, in their very earliest work, cyber criminals used a simple contact/feedback form instead of providing real contact details. However, authors' being unaware of how to differentiate between fake journals and real journals increased the confidence of the hijackers to a level that encouraged them to introduce their masterpieces, i.e., fake websites with complete details concerning how to contact the editorial office, including "real" postal addresses and "real" but invalid phone numbers, which, in some cases, were virtual VOIP-based phone numbers, to make sure nothing was questionable in their websites so that even skeptical authors might not suspect that they were being scammed.

8. Including a fake log-in gateway for accessing the archive of the past issues that will never work.

9. Perhaps (in their future innovations) providing a real access portal to double their money by selling subscriptions.

10. Misusing of the names of invalid organizations, indicating that they are scientific supporters or publishers of the fake journals. Examples can be the use of prestigious terms used in academic publishing

with slight modifications, such as "International Association of X", "American Society of X", "World Association of X" and "British Committee of X".

Victimology and marketing

1. The selection of victims among certain high-risk academic groups is key to success for academic cyber criminals. By introducing the term "selection of victims" we mean that academic cyber criminals are proficient at analyzing the behaviors of people and the phenomena that occur in the academic world. Thus, they focus their marketing campaign on selected groups of authors who they identify as potential victims. They find the email addresses of the authors from the websites of commercial, non-peer-reviewed journals that are listed in Thomson Reuters or Scopus (A metric product of Elsevier). These authors (potential victims) are expected to respond positively to any call-for-paper emails they receive from an ISI journal, because they have already published earlier articles in commercial journals that work on a "pay and get published" basis. Again, we believe that the cyber criminals are intelligent enough to avoid recruiting their victims from the websites of real, high-quality journals that follow a strict model in their peer-review procedure.

2. Email marketing (better categorized as spam marketing) for the legitimate journal on the website of a hijacked or junk journal. Technically, the cyber criminals also may use some email extractor software and an automated, large-scale spam broadcaster machine.

3. Using pseudo names and titles such as Dr., Ph.D., and Professor in all of the unsolicited emails they broadcast.

4. Mentioning the journal's ISI impact factor and clearly pointing out the rapid acceptance of manuscripts within 2 weeks or less time.

Finally, making money from non-reviewed research articles. In a week or 2, the "lucky" authors will receive an acceptance letter and, of course, an invoice.

Short- to mid-term solutions

Disclosing the unethical and criminal practices of hijacked journals and bogus publishers is the only existing action against this type of academic cybercrime. Some universities also have announced a long list of banned or black-listed journals. Unfortunately, only short-term effects are expected from these knee-jerk reactions, because they are usually based on some superficial investigation rather than on logical reasoning. Instead, familiarizing the authors with methods of avoiding the scammers' sites could be considered a better short- to mid-term choice. The goal of a short- to mid-term strategy should be to "disseminate knowledge/awareness about such scams and to train authors so they will have the basic skills required to avoid fake publishers and hijacked journals. Based on our practical knowledge, experience, and observations, we have prepared the following "to-do/not-to-do" list to explain how to identify and avoid fake journals:

1. Ignore all call-for-papers solicitations emailed directly to you. Indeed, broadcasting unsolicited calls for papers is not the way high-quality publishers do their jobs unless an author's name is already of their list of newsletter recipients. Therefore, without hesitation, mark them all as spam.

2. Do not open any unsolicited email saying that your work has already been selected for publication. They are all scams.

3. If a website claims to be the authentic website of a prestigious journal that is listed in an indexing or abstracting database, such as Thomson Reuters, Pubmed/Medline, Index Copernicus, Scopus, SCImago (A free access tool created by Scopus), or the Directory of Open Access Journals (DOAJ), investigate the respective websites of these databases for any link to the website of the journal and make sure they are matched.

4. In case there is no direct link from the investigated indexing portal (such as Thomson Reuters) to the journal, check the other indexing or abstracting services (such as SCImago) for any valid link to the journal's website.

5. Check the "Whois" profile of the website through InterNIC (http://www.internic.com), Domain Tools (http://www.domaintools.com), GoDaddy (http://www.godaddy.com), or OnlineNIC

(http://www.onlinenic.com). In the Whois data section of the investigated website, search for the "date created." This value refers to the exact day the domain was registered by its owner. You may find that the fake website of a hijacked journal was registered just a few days ago! However, a very old and reputable, print-only journal may decide to go online and, therefore, also would have a recent "date created." Therefore, this technique is not a stand-alone method for determining a fake website.

6. Double check the journal's website for everything, including the access to past issues, the peer-review flowchart, the guide to authors section, and the other journals that might be hosted by the same website.

7. The content of fake journals tends to be copied from other websites and pasted on the fake website. For example, we checked the property of the Microsoft Office Word file of the "Journal Template" in the hijacked Vulfenia Journal and found that the file was copied from a publisher in Canada. A similar file on the website of the hijacked Jokul Journal was copied from a conference of the "Institute of Electrical and Electronics Engineers" (IEEE). To check the property of a Microsoft Office Word file, simply right click on it (in Microsoft Windows) and choose "Properties." Then, double check all of the tabs, especially the tab "Details," where you may find even more exciting information, such as the address of the website of the original journal from which the file was stolen. Usually, cyber criminals either do not have time to fix all of these details or they are sure no one will check them. In the "Author" box in the "Details" tab, you will find the log-in name of the cyber criminals' computer when they turn on their computer and log in to Microsoft Windows! To illustrate how significant this capability is, suffice it to say that we found that the hijacker of "Vulfenia Journal" and "Archive des Science" was the same person!

8. Evaluate the overall design of the website and check it thoroughly for any shady picture or misspelled words. Cheap-looking websites that are masquerading as prestigious publishers do not have the time dedicated to them that the real thing does.

9. Email both the indexing service and the journal editor for the purpose of further verification, but this method usually does not produce any useful results. However, authors might want to give it a try knowing that a "No response" sometimes is a good parameter that can help them get a distinct image of the journal in their mind. If any response is received from the journal, then it might provide some information to determine how trustworthy the journal is.

10. To an inexperienced person, all websites look legitimate; therefore, it is difficult to tell whether they are fake or real. Inexperienced authors or those who have any doubt after doing all of the recommended investigations should consult expert. They may simply decide to forget about it and stick to the high-quality journals they know from their experience.

11. If someone claims she can publish your article in a prestigious journal fast, reject her offer with no doubt. One of the constant marketing strategies of the fake publishers is to do business with some people who can work for them on commission to recruit hundreds of authors for them and take their commissions. In most cases, it seems that even the intermediate people who work with journal hijackers are unaware that they are doing business with fake publishers.

12. Some people may suggest authors submitting their articles only to a limited list of the most famous publishers and ignoring all of the other journals. We do not suggest that authors do so, because there are many great, high-quality journals that are new but have not developed their reputations because they have yet to be indexed. For example, if a prestigious university decides to launch a new journal, the journal initially will not be deemed to be reputable because the repute of a journal is calculated using some numerical values, and, for the most part, those values come from the citation of metric data. No matter how reputable the journal may be according to the quantitative value that is blinking at you on its website's homepage, be careful when there is a lack of transparency about the journal's publishing processes.

Long-term strategy

Due to the huge explosion in the numbers of academic cyber criminals during the last 2 years and the upcoming academic cyber crime (Fake institutes that introduce new but fake impact factors values) we call the years 2012 and 2013 the years of Fake Journals and we will call the year 2014 the year of Fake Impact Factors. Fake publishers and impact factors reminded us of the urgent need to evaluate the methods that currently are used to assess academic research. Doing a thorough retrospective assessment definitely is an urgent need in today's academic world. Perhaps switching from quantitative methods to qualitative approaches for assessing the quality of academic research is the only long-term strategy that would be effective in protecting academia from all of the obvious misconduct of fake publishers, hijacked journals, and, of course, the predatory, non-reviewed, low-quality publications that are great threats to the validity and integrity of science. To be more precise, we believe that numerical values are not ideal indicators for use in assessing the quality of scientific efforts to fill the gaps in our knowledge. To put it into practical terms, numerical values simply are not the gold standard for determining the quality of journals. There are many low-quality journals in the market that do not even use a review process, while their websites provide several numerical values proclaiming that they are reputable. We even have heard many stories about intelligent students who sent stupid papers to some of the journals, and they were accepted for publication. We hope the stories we shared have clearly depicted the weakness of the current quantitative methods that are used to evaluate the quality of academic research. Honestly, however, we also recognize that it will be difficult to design and implement new models, especially qualitative models. Now that we understand that a journal's repute is based on a questionable numerical value, we conclude this appeal with a question: Do the terms "reputable journal" and "high-quality journal" have the same meaning?

References

[1] D Butler. Sham journals scam authors. *Nature* 2013; **495**, 421-2.
[2] G Kolata. Scientific Articles Accepted (Personal Checks, Too), The New York Times, Available online at: http://www.nytimes.com/2013/04/08/health/for-scientists-an-exploding-world-of-pseudo-academia.html?_r=2&, accessed April 2013.
[3] J Beall. Predatory publishers are corrupting open access. *Nature* 2012; **489**, 179.
[4] M Jalalian and H Mahboobi. New corruption detected: Bogus impact factors compiled by fake organizations. *Electron. Physician* 2013; **5**, 685-6.