THE AMERICAN JOURNAL of MEDICINE®

Fraud in Academic Publishing: Researchers Under Cyber-Attacks

Mehdi Dadkhah, MSc,[a] Glenn Borchardt, PhD,[b] Tomasz Maliszewski, PhD[c]

[a]Information Science Scientist, Isfahan, Iran; [b]Progressive Science Institute, Berkeley, Calif; [c]Department of Social Sciences, Pomeranian University in Słupsk, Poland.

ABSTRACT

Day by day, researchers receive new suspicious e-mails in their inboxes. Many of them do not have sufficient information about these types of e-mails, and may become victims of cyber-attacks. In this short communication, we review current cyber threats in academic publishing and try to present general guidelines for authors.

• *The American Journal of Medicine (2017) 130, 27-30*

KEYWORDS: Bogus metric; Fraud; Predatory journal; Spam e-mail

Nowadays, researchers often receive suspicious e-mails inviting them to publish the results of their research. The inviting parties use various marketing tricks, eventually disclosing the financial conditions for publishing with them. We decided to count the number of such suspicious e-mails that we received from May 2015 to May 2016. One of us (first author) received about 400 of them and the other (third author) received about 650. We classified them in three categories: Calls for submitting a paper to questionable journals, scam e-mails, and phishing e-mails. Figure 1 shows the percentage for each of the categories. The calls for papers are easily detected, because they use their journals' name in their e-mails and present their URLs. Scam e-mails request sensitive information and promise a big prize or business opportunity. Phishing e-mails use URLs and request that prospective victims log in to suspicious web sites.

TOP SCAM IN THE SCHOLARLY WORLD AND HOW TO AVOID IT

As can be seen from the graph, researchers receive many e-mails that "call for papers" from the journals that promise fast review and publishing,[1] claiming that they are indexed and have a high impact factor. One can assume that almost every researcher who has published in recent years has received such calls for papers from a questionable journal

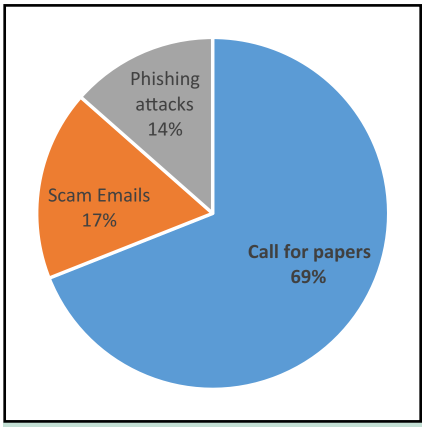


Figure 1 Percentage of suspicious e-mails that we received from May 2015 to May 2016.

Funding: None.

Conflict of Interest: There are no conflicts of interest for any of the authors.

Authorship: I certify that all authors had access to the data and a role in writing the manuscript.

Requests for reprints should be addressed to Mehdi Dadkhah, MSc, Independent Scientist on Information Science, Foulad Institute of Technology, Foulad Shahr, Isfahan 8491663763, Iran.

E-mail address: dadkhah1992@gmail.com

0002-9343/$ -see front matter © 2016 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.amjmed.2016.08.030

soon afterwards. These fraudulent journals have the following tactics:

1. Cybercriminals want to earn money from unaware researchers, so they register a web site and launch a journal by using content management systems. It is, unfortunately, neither complicated nor takes long to prepare such a site. People with basic skills in web design can set up such a web site within 2 or 3 days.
2. After launching a web site, they try to index their journals in indexing centers. *Thomson Reuters Impact Factor* and *Scimago Journal Ranking*[2] are the popular recognized and transparently operating entities for ranking journals. Failing that, they often use bogus metrics and indexing companies. These generally have no clear ranking methods and will assign ranks to journals—for a price.
3. The last step is to send a huge number of calls for papers to researchers from all over the world. Cyber criminals can easily collect lists of e-mails for this purpose from web sites by using readily available web tools. Cyber criminals can also scan a legitimate journal's web site to gather lists of e-mail addresses of researchers who might be amenable victims.

CLINICAL SIGNIFICANCE

- Day by day, researchers receive new suspicious e-mails in their inboxes. Many of them do not have sufficient information about these types of e-mails and may become victims of cyber-attacks. This article will increase researchers' awareness.
- We show importance of cyber-attacks issues in the academic world.
- Authors can use general guidelines in this article and detect emerging fraud in the academic world.

Any "call for papers" that uses misleading metrics should be avoided out of hand. The **Table** shows a list of these bogus metrics.[3,4]

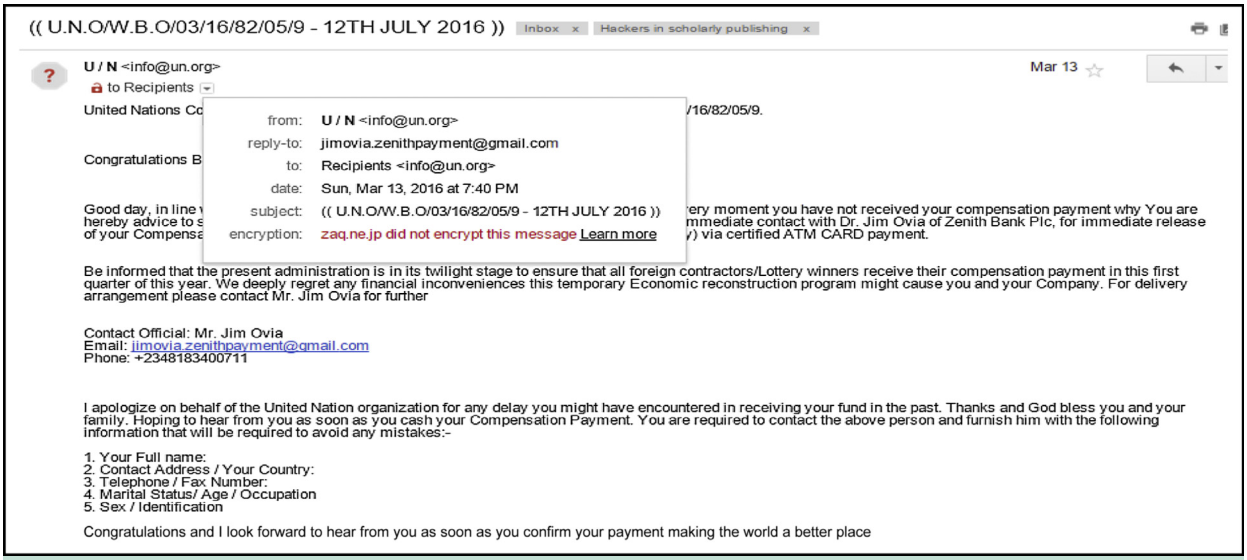
We also recommend using the *Alexa database* (http://www.alexa.com) to detect fraudulent journals. Most of these introduce themselves as reputable international journals. Alexa lists the countries of the visitors to each journal web site. According to our observations, reputable journals have visitors from more than 3 countries. Questionable journals generally have visitors from only one country. Often, their details are not even available in Alexa. So using Alexa can help researchers detect reputable journals as long as one remembers that the result is not always correct for legitimate journals that are just starting out.

The second category of suspicious e-mails involves scams. The e-mails promise big awards, business opportunities, jobs,

Table List of Misleading Metrics*

No.	Bogus Metric Name	Web Site URL
1	Advanced Science Index	http://journal-index.org
2	African Quality Centre for Journals (AQCJ)	http://www.aqcj.org
3	Cite Factor	http://www.citefactor.org
4	Council for Innovative Research	http://cirworld.org
5	Directory of Indexing and IF	http://www.diif.org
6	Einstein Inst. for Scientific Information	http://journalimpactfactor.co.in
7	General Impact Factor (GIF)	http://generalimpactfactor.com
8	The Global Impact & Quality Factor (GIF)	http://globalimpactfactor.com
9	Impact Factor (JCC)	http://www.journal-metrics.com
10	Impact Factor Journals	http://www.impactfactorjournals.com
11	Institute for Science Information	http://isi-thomsonreuters.com
12	International Impact Factor Services (IIFS)	http://impactfactorservice.com
13	International Scientific Indexing (ISI)	http://isindexing.com
14	International Scientific Institute (ISI)	http://www.scijournal.org
15	ISRA: Journal Impact Factor (JIF)	http://www.israjif.org
16	Journal Impact Factor (JIF)	http://jifactor.com
17	Journal Influence Factor	http://www.journalsconsortium.org
18	The Journals Impact Factor (JIF)	http://jifactor.org
19	Open Academic Journals Index	http://oaji.net
20	Scientific Indexing Services	http://sindexs.org
21	Scientific Journal Impact Factor (SJIF)	http://www.sjifactor.com http://www.sjifactor.inno-space.net
22	Universal Impact Factor (UIF)	http://www.uifactor.org

*Extracted from reference[3,4] with some additions.



((U.N.O/W.B.O/03/16/82/05/9 - 12TH JULY 2016))

U / N <info@un.org>

United Nations Co /16/82/05/9.

from: U / N <info@un.org>
reply-to: jimovia.zenithpayment@gmail.com
to: Recipients <info@un.org>
date: Sun, Mar 13, 2016 at 7:40 PM
subject: ((U.N.O/W.B.O/03/16/82/05/9 - 12TH JULY 2016))
encryption: zaq.ne.jp did not encrypt this message Learn more

Congratulations B

Good day, in line ery moment you have not received your compensation payment why You are
hereby advice to s mmediate contact with Dr. Jim Ovia of Zenith Bank Plc, for immediate release
of your Compensa y) via certified ATM CARD payment.

Be informed that the present administration is in its twilight stage to ensure that all foreign contractors/Lottery winners receive their compensation payment in this first quarter of this year. We deeply regret any financial inconveniences this temporary Economic reconstruction program might cause you and your Company. For delivery arrangement please contact Mr. Jim Ovia for further

Contact Official: Mr. Jim Ovia
Email: jimovia.zenithpayment@gmail.com
Phone: +2348183400711

I apologize on behalf of the United Nation organization for any delay you might have encountered in receiving your fund in the past. Thanks and God bless you and your family. Hoping to hear from you as soon as you cash your Compensation Payment. You are required to contact the above person and furnish him with the following information that will be required to avoid any mistakes:-

1. Your Full name:
2. Contact Address / Your Country:
3. Telephone / Fax Number:
4. Marital Status/ Age / Occupation
5. Sex / Identification

Congratulations and I look forward to hear from you as soon as you confirm your payment making the world a better place

Figure 2 A scam e-mail that was sent by e-mail spoofing techniques involving a counterfeited United Nations e-mail address.

or request an urgent reply. Such messages stand a bigger chance of cheating researchers because cyber criminals use advanced information technology techniques. They send their scam e-mails from official e-mail addresses, such as international organizations, standout universities, or recognizable research corporations. These e-mails request personal information such as full name, contact address, telephone, marital status, age, occupation, and academic position. Having gathered all the information, they try to cheat researchers in various ways.

The question that should be asked here is: how can cyber criminals send e-mails by using official e-mail addresses? There are 2 hypotheses about that. The first one: cyber criminals steal e-mail credentials of editors, students, and researchers to make their scam e-mails seem official. Of course, this increases the effectiveness of their attacks.

The second one uses e-mail spoofing techniques. In this technique, cyber criminals send e-mails by using official e-mail addresses, but cannot receive any answers.[5] They embed malicious URLs that infect the receiving computer with malware when the link is clicked. Some of these e-mails request the receiver to answer another e-mail address instead of replying to such e-mails directly. Figure 2 shows the type of scam e-mails that cyber criminals use. We received this e-mail on the 13th of March 2016.

Scams of this type can be detected relatively easily. The sender of the e-mail in Figure 2 requested that replies be sent to another e-mail address instead of the e-mail address the message came from.

Other suspicious e-mails may not use counterfeit addresses. These e-mails from nondescript addresses belong to phishing attacks, whose sole purpose is to get private information. In phishing attacks, cyber criminals create fake web sites that are similar to legitimate sites. Victims are directed to the fake sites by the deceptive e-mails.[6] Some of these warn the recipients of the "low security" of their accounts, requesting them to update their information. Experts use various, sometimes complex methods for detecting phishing attacks. The simplest method is this:

> *"Authors must search for the title of each web site embedded in e-mails requesting sensitive information. If a search engine (such as Google) returns a similar, but not identical web site, it is likely that it is not legitimate."*

Researchers also can use *Phish Tank database* (https://www.phishtank.com). This is an updated international database that people can use to register phishing web sites they uncover. In addition, some updated security software is designed to counteract this threat.

CONCLUSION

In this short article, we divulged 3 types of cyber-attacks that threaten researchers in scholarly publishing and presented guidelines for confronting them. As in the case of ordinary computer viruses, the numbers and types of such threats continue to increase. Cyber criminals are developing ever-more sophisticated techniques to entrap not only young researchers, but also experienced academics unaware of the threats focused on scholarly publishing. Such attacks remind us—in a way—of *Jurassic Park*, a film by Steven Spielberg in which researchers were attacked by predators. As in that movie, one must be aware of the threats, constantly developing the skills to cope with them. We name the current age of the academic world as the "Jurassic age of the academic world."

References

1. Moher D, Srivastava A. You are invited to submit. *BMC Med.* 2015;13:180.
2. Bornmann L, Marx W, Gasparyan AY, Kitas GD. Diversity, value and limitations of the journal impact factor and alternative metrics. *Rheumatol Int.* 2012;32(7):1861-1867.

3. Gutierrez FR, Beall J, Forero DA. Spurious alternative impact factors: the scale of the problem from an academic perspective. *Bioessays*. 2015;37(5):474-476.
4. Jalalian M. The story of fake impact factor companies and how we detected them. *Electron Physician*. 2015;7(2):1069.
5. Mooloo D, Fowdur TP. *An SSL-based client-oriented anti-spoofing email application*. Pointe-aux-Piments, Mauritius: AFRICON; 2013:1-5.
6. Harrison B, Svetieva E, Vishwanath A. Individual processing of phishing emails: How attention and elaboration protect against phishing. *Online Inf Rev*. 2016;40(2):265-281.