JAN
Informing Practice and Policy Worldwide through Research and Scholarship

Editorial

New types of fraud in the academic world by cyber criminals

Introduction

In recent years, the academic world has faced many challenges such as a move towards online open access publishing, and researchers have tried to accommodate them. However, this has also created problems. For example, Dadkhah *et al.* (2015a) covered unethical behaviours in the academic world, including plagiarism, article sale, forced joint authorship, conversion of a journal in to a 'print machine', and invitations to invalid conferences. I believe that the main reasons for the above mentioned challenges do not belong to the publishers alone; unethical behaviour of some researchers is also to blame and can be effective in creating such challenges (Christova-Bagdassarian 2014, Shashikiran 2014). Valuable insights regarding journal quality in relation to these challenges, specifically 'predatory publishing' have been provided by Beall (2010a,b). There is not much research on the types of cybercrime in the academic world but there are 31 papers in Google Scholar, six papers in Scopus, and a paper in PubMed investigating hijacked journals. However, these types of 'scams' are increasing and it is necessary to expose them. Most of these frauds are clearly unknown to many researchers. In this paper, I discuss new types of fraud in the academic world and present general guidelines for preventing them. Most of these frauds are complex and require knowledge about information security and thus many researchers cannot detect them.

New Frauds in the Academic World

Hijacked journals

Hijacked journals are fake websites that use the name and ISSN of authentic journals to cheat authors. These journals publish authors' papers without review by receiving money. There is some research regarding hijacked journals, but it seems that this is insufficient because the number of victims of hijacked journals is growing. Some authors (Jalalian & Mahboobi 2014, Dadkhah *et al.* 2015c) discuss hijacked journals and define general guidelines for authors to detect this fraud. Also, there are editorials that expose specific hijacked journals with evidence of their fraud (Jalalian 2014a, Dadkhah & Sutikno 2015). Some of the research focuses on the ways forgers cheat authors, including bogus impact factors (Jalalian 2015), fake conferences (Dadkhah *et al.* 2015b), and social engineering (Dadkhah & Quliyeva 2014). There were 20 known hijacked journals in 2014 (Jalalian 2014b), but approximately 90 hijacked journals were detected in June 2015 (Jalalian & Dadkhah 2015). This shows that the prevalence of hijacked journals is growing. Also, in the initial hijacked journals, hijackers used simple methods for hijacking and, in most cases, they use a content management system to create the website. However, in 2015, we saw complex types of hijacking, where hijackers create hijacked websites similar to the original ones and use complex social engineering techniques to cheat scientific databases, such as Thomson Reuters, and index the fake website in these databases. Two examples are *Allgemeine Forst und Jagdzeitung* (Fake URL: http://www.sauerlander-verlag.com; accessed 08 October 2015) and *GMP Review* (Fake URL: http://www.euromed.uk.com; accessed 08 October 2015). Forgers cheat Thomson Reuters and indexed fake URLs by using some vulnerabilities in this scientific database.

Hijacking old domains of reputable journals

Currently, we observe a new type of hijacking. In previous hijacking methods, forgers used similar URLs to authentic journal URLs or created the website for journals that did not have a website. In the new hijacking method, forgers search in Thomson Reuters to find expired domains, which previously belonged to actual journals, then register them. When these expired domains are re-registered, authors will find the hijacked version of the journal in Thomson Reuters and think that it is the authentic version of journal. We list some examples of hijacked journals that forgers are using in this way: *Journal of Veterinary Dentistry*- ISSN: 0898-7564, Hijacked and indexed URL in Thomson Reuters (Fake URL: http://www.pspcommunications.com; accessed 08 October

2015; Authentic Version URL: http://www.jvdonline.org; accessed 08 October 2015); *Intelligent Automation and Soft Computing* – ISSN: 1079-8587 (Fake URL: http://autosoftjournal.org, Authentic Version URL: http://wacong.org/autosoft/auto/index.php); *GMP Review* – ISSN: 1476-4547 (Fake URL: euromed.uk.com, Authentic Version URL: http://www.euromedcommunications.com; accessed 08 October 2015).

These types of hijacking will lead to other challenges with the quality of academic resources. First, databases such as Scopus and Google Scholar may index published papers in the hijacked journal because these databases consider the old domain as the authentic domain for the journal. Second, the number of hijacked journal victims will increase exponentially because hijackers will use available URLs in Thomson Reuters to claim that their journal is authentic and reputable. The process of hijacking with this method is:

1 Hijackers check Thomson Reuter's journals list to find a linked URL, which is expired, then register the expired domain.
2 Forgers create a fake website and use names and ISSNs similar to authentic versions of the journals, and the hijacked version of the journal is ready.
3 After creating a hijacked journal, forgers need to invite authors to submit their papers, thus they must send calls for papers to prospective authors. They suggest fast publishing in reputable journals in the call for papers. There is software that gather lists of authors' email from websites, and they gather list of emails from authors in small journals (or conferences) then send repeated calls for papers to authors and suggest fast publishing papers in Thomson Reuters indexed (or Scopus, PubMed) journals. They use the available links from Thomson Reuters and impact factors to claim victims. For example, they use this link: http://science.thomsonreuters.com/cgi-bin/jrnlst/jlresults.cgi?PC=MASTER&ISSN=0898-7564 (accessed 08 October 2015), mentioning the old URL of the reputable journal that is now available but registered by forgers. http://www.pspcommunications.com (accessed 08 October 2015) is the URL of a hijacked version of a journal and the authentic version is available at http://www.jvdonline.org (accessed 08 October 2015).

For detection of journals hijacked by this type of hijacking method, authors can use the Whois database (http://whois.domaintools.com/; accessed 08 October 2015). If the domain creation date does not match the years in which a journal has issues, the reviewed URL is fake because when an expired URL has been registered again by another person, the domain creation data will be changed to the most recent registration date. Also, editors of journals must inform scientific databases, such as Thomson Reuters, of any change in their journals' URL.

Attacking authors in open access journals for financial goals

Currently, forgers are attacking researchers for financial reasons. They gather list of emails addresses related to authors and send deceptive emails. They gather these email lists from open access journals with the use of specialized software. After collecting authors' email addresses, they send emails to authors and try to cheat them by sending fake PayPal invoices or phishing (Martino & Perramon 2010) websites. In most of these fraudulent emails, forgers promise a big prize or speak about new business opportunities and try to collect more information about their victims, then use this information to cheat authors in the next round of fraudulent emails. In this new type of fraud, authors think that they have received an original payment website or a subscription invoice from journals. To combat this type of fraud, I recommended authors do not answer such emails and ignore them completely. Also, authors must be careful about email attachments and not open suspicious file types, such as: .html, .jar, .exe, .xml etc. Phisher may create malware and infect victims' operation system to steal information (Dadkhah & Jazi 2014).

Invasion of privacy by selling of private information

In the current century, privacy is of the utmost concern and in the academic world we can see some types of privacy invasion through the selling of private information. Some questionable journals or conferences sell their participants' information (Lukiæ *et al.* 2014), including email addresses, telephone number and expertise to people who seek this information for advertisement. For example, many researchers receive calls for papers from predatory journals after participation in conferences or receive spam emails about some company. The best approach for dealing with this type of invasion of privacy is detection of fake conferences from authentic ones. Fake conferences often have unknown scientific committees, use independent URLs and general mail services such as Yahoo and Gmail.

Paper Hijacking

Recently, hijackers have created fake proof reading sites to hijack unpublished papers and sell them to people who seek such papers. Most of these fake proof reading sites promise fast, high quality and cheap proof reading to persuade their victims to send papers. After hijacking and selling the papers, we can find the same paper published with different authors. The answer to: 'which authors are the real authors of paper?' is very hard to determine. For detection of these fake proof reading sites, we suggest that authors use the Whois database and the Google page ranking algorithm (http://www.whatsmypr.net; accessed 08 October 2015). By using the Whois database, an author can search the domain and receive related information; if the domain registration time is less than a year, the reviewed site is suspicious. According our inspection, an authentic proof reading site has more than one page ranking.

Conclusion

I have introduced the types of cybercrime in the academic world and presented general guidelines for detecting them because I find that there is a lack of knowledge in the academic world regarding cybercrime. It is necessary that researchers know about cybercrime, otherwise they may themselves become victims. In addition, cybercrime has an adverse effect on the quality of academic resources. For example, published papers in hijacked journals may be indexed in scientific bases and be cited in future papers. Working to assess other aspects of cybercrime continues.

Mehdi Dadkhah

Mehdi Dadkhah MSc
Lecturer
Department of Computer and Information Technology,
Foulad Institute of Technology, Foulad Shahr, Isfahan, Iran
e-mails: dadkhah80@gmail.com, m.dadkhah@iautiran.ac.ir

References

Beall J. (2010a) Predatory open-access scholarly publishers. *The Charleston Advisor* **11**(4), 10–17. doi:10.5260/chara.12.1.50.

Beall J. (2010b) Update: predatory open-access scholarly publishers. *The Charleston Advisor* **12**(1), 50. doi:10.5260/chara.12.1.50.

Christova-Bagdassarian V. (2014) Plagiarism and academic ethic. *Mintage journal of Pharmaceutical & Medical Sciences* **3**(2), 1–3.

Dadkhah M. & Jazi M.D. (2014) Secure payment in E-commerce: Deal with Keyloggers and Phishings. *International Journal of Electronics Communication and Computer Engineering* **5**(3), 656–660.

Dadkhah M. & Quliyeva A. (2014) Social engineering in academic world. *Journal of Contemporary Applied Mathematics* **4**(2), 3–5.

Dadkhah M. & Sutikno T. (2015) Phishing or Hijacking? Forgers Hijacked DU Journal by Copying Content of Another Authenticate Journal. *Indonesian Journal of Electrical Engineering and Informatics* **3**(3), 119–120.

Dadkhah M., Jazi M.D. & Pacukaj S. (2015a) Fake conferences for earning real money. *Mediterranean Journal of Social Sciences* **6**(2), 11–12. doi:10.5901/mjss.2015.v6n2p11.

Dadkhah M., Elias N., Jazi M.D., Christova-Bagdassarian V. & Abu-Elteen K.H. (2015b) A new challenge in the academic world: earning real money and eminence by paper publishing. *Jordan Journal of Biological Sciences* **8**(2), 73–75.

Dadkhah M., Obeidat M.M., Jazi M.D., Sutikno T. & Riyadi M.A. (2015c) How can we identify hijacked journals? *Bulletin of Electrical Engineering and Informatics* **4**(2), 83–87. doi:10.12928/eei.v4i2.449.

Jalalian M. (2014a) Hijacked journals are attacking the reliability and validity of medical research. *Electronic Physician* **6**(4), 925–926. doi:10.14661/2014.925-926.

Jalalian M. (2014b). *Hijacked Journal List: List of Hijacked Journals and Fake Publishers*, 1st edn. Retrieved from http://mehrdadjalalian.com/1.pdf on 18 July 2015.

Jalalian M. (2015) The story of fake impact factor companies and how we detected them. *Electronic Physician* **7**(2), 1069–1072. doi:10.14661/2015.1069-1072.

Jalalian M. & Dadkhah M. (2015) The full story of 90 hijacked journals from August 2011 to June 2015. *Geographica Pannonica* **19**(2), 73–87.

Jalalian M. & Mahboobi H. (2014) Hijacked journals and predatory publishers: is there a need to re-think how to assess the quality of academic research? *Walailak Journal of Science and Technology* **11**(5), 389–94. doi:10.14456/wjst.2014.16.

Lukiæ T., Blešiæ I., Basarin B., Ivanoviæ B.L., Miloševiæ D. & Sakulski D. (2014) Predatory and fake scientific journals/publishers – a global outbreak with rising trend: a review. *Geographica Pannonica* **18**(3), 69–81.

Martino A.S. & Perramon X. (2010) Phishing secrets: history, effects, and countermeasures. *International Journal of Network Security* **11**(3), 163–171.

Shashikiran N.D. (2014) Plagiarism and academic integrity. *Journal of Indian Society of Pedodontics and Preventive Dentistry* **32**(1), 1–2. doi:10.4103/0970-4388.126989.