Letter

Victimizing Researchers by Phishing

Mehdi Dadkhah,[1,*] and Glenn Borchardt[2]

[1]Information Science Scientist, Isfahan, IR Iran
[2]Progressive Science Institute, Berkeley, California, USA

[*]*Corresponding author*: Mehdi Dadkhah, Information Science Scientist, Isfahan, IR Iran. E-mail: Dadkhah80@gmail.com

Dear Editor,

We read the brief report by Khadem-Rezaiyan and Moghadam, "Hijacking by Email: A New Fraud Method" (1), and would like to present some details and correct some issues in their report. We applaud these authors for increasing awareness of the problem. It appears that the phenomenon is growing faster than attempts to expose it and eliminate it.

In paragraph two, the authors used the word "high-jack," while the correct word is "hijack," which according to the Oxford dictionary (2), includes three different meanings:

1. Illegally seize (an aircraft, ship, or vehicle) while in transit and force it to go to a different destination or use it for one's own purposes.

2. Steal (goods) by seizing them in transit.

3. Takeover (something) and use it for a different purpose

In the academic world, we usually use the term "hijack," to reflect the third concept. For instance, we use it for exposing hijacked journals. These appear as websites produced under a slightly different name than the websites of the legitimate journals from which they were copied. Researchers are encouraged to submit papers that receive little or no review, have exorbitant page charges, are seldom read or cited, and disappear after the legitimate journals take legal action.

This may seem like a mere quibble, but we suggest that this particular fraudulent practice involving scam emails, might better be designated by the term "phishing" instead of "Hijacking by Email." The authors presented two examples that they believe are a type of "Hijacking by Email." Actually, they really do not involve hijacking, as no papers are ever published. Indeed, they are clearly phishing attacks. In phishing attacks, hackers use fraudulent emails to lure responders to their fake websites (3). Any sensitive information entered at the fake websites becomes the prop-

erty of the phishers, as mentioned in the example given by Khadem-Rezaiyan and Moghadam. Phishers then use such data in their subsequent attacks, which contain exact information about researchers once again directing them to a phishing website. Most of these phishing attacks have financial goals, with the gathered information being used for hacking credit cards.

Nowadays, a new type of scam is appearing. Some sites and companies claim that they can share authors' publications such as eBooks and papers between many researchers. They state that their main goal is to promote the books and papers. They list authors' books as free ebooks, always say there have been more downloads already, and have one-word reviews that are always the same for each of them. They get the credit card numbers from authors and others who sign up, charge them monthly, but seldom have any eBooks. They do not stop the monthly charges after complaints, so applicants are forced have to close their credit card accounts.

As mentioned in the report, there are many frauds affecting scholarly publication. Among these are: faked declarations, tempting impact factors, email spoofing, cheating publishers, fake editorial boards, and fake conferences (4). These frauds are proliferating, and researchers should be aware of all of them.

References

1. Khadem-Rezaiyan M, Dadgar Moghadam M. Hijacking By Email: A New Fraud Method. *Razavi Int J Med.* 2016;**4**(2):37366. doi: 10.17795/rijm37366.
2. Oxford Dictionary . Oxford Dictionary UK: Oxford University Press; 2016. Available from: http://www.oxforddictionaries.com/definition/english/hijack.
3. Fette I, Sadeh N, Tomasic A. Learning to detect phishing emails. The 16th international conference on World Wide Web. New York. ACM Publication; 2007. pp. 649–56.
4. Dadkhah M, Quliyeva A. Social engineering in academic world. *J Contemp Appl Math.* 2014;**4**(2).