## عنوان مقاله:
Victimizing Researchers by Phishing

## محل انتشار:
مجله بین المللی پزشکی رضوی, دوره 4, شماره 3 (سال: 1395)

تعداد صفحات اصل مقاله: 1

## نویسندگان:
Mehdi Dadkhah - *Information Science Scientist, Isfahan, IR Iran*

Glenn Borchardt - *Progressive Science Institute, Berkeley, California, USA*

## خلاصه مقاله:
We read the brief report by Khadem-Rezaiyan andMoghadam, Hijacking by Email: A New Fraud Method (1),and would like to present some details and correct someissues in their report. We applaud these authors for increasingawareness of the problem. It appears that the phenomenonis growing faster than attempts to expose it andeliminate it.In paragraph two, the authors used the word highjack, while the correct word is hijack, which accordingto the Oxford dictionary (2), includes three different meanings:1. Illegally seize (an aircraft, ship, or vehicle) while intransit and force it to go to a different destination or use itfor one's own purposes.2. Steal (goods) by seizing them in transit.3. Takeover (something) and use it for a different purposeIn the academic world, we usually use the term hijack, to reflect the third concept. For instance, weuse it forexposing hijacked journals. These appear as websites producedunder a slightly different name than the websites ofthe legitimate journals from which they were copied. Researchersare encouraged to submit papers that receive littleor no review, have exorbitant page charges, are seldomread or cited, and disappear after the legitimate journalstake legal action.This may seem like a mere quibble, but we suggest thatthis particular fraudulent practice involving scam emails,might better be designated by the term phishing insteadof Hijacking by Email. The authors presented two examplesthat they believe are a type of Hijacking by Email. Actually, they really do not involve hijacking, as no papersare ever published. Indeed, they are clearly phishing attacks.In phishing attacks, hackers use fraudulent emails tolure responders to their fake websites (3). Any sensitive informationentered at the fake websites becomes the propertyof the phishers, as mentioned in the example given byKhadem-Rezaiyan and Moghadam. Phishers then use suchdata in their subsequent attacks, which contain exact informationabout researchers once again directing them toa phishing website. Most of these phishing attacks have financialgoals, with the gathered information being usedfor hacking credit cards.Nowadays, a new type of scam is appearing. Somesites 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 thebooks and papers. They list authors' books as free ebooks,always say there have been more downloads already, andhave one-word reviews that ... are always the same for eachof them. They get the credit card numbers from authorsand others who sign up, c

## کلمات کلیدی:
Fraud, Spam Emails, Review