science editing
pISSN 2288-8063
eISSN 2288-7474

Sci Ed 2017;4(2):76-79
https://doi.org/10.6087/kcse.99

Case Study

Impersonation of *Journal of Electrical Engineering & Technology* journal website

Jaeseok Choi

Department of Electrical Engineering, Gyeongsang National University, Jinju, Korea

Abstract

The website of *Journal of Electrical Engineering & Technology* (JEET, http://www.jeet.or.kr) published by Korean Institute Electrical Engineers was found to be impugned in March 2017. The purpose of this case study article was to describe the case of phishing and suggest the measures to prevent it. In June 29, 2016, informant submitted his manuscript to phishing e-mail jeet@jeet.us, because he misunderstood the phishing site as that of JEET. After that he received the confirmation mail of acceptance and expected date of publication. However, there was no further progress, he inquired official e-mail of JEET on his manuscript. During the correspondence with journal secretary, he found that it was the phishing. There was no request of publication fee from phisher. It is difficult to know what is the purpose of this phishing. Probably, it may be an initial inducement to deceive the contributor. If the manuscript is published in the phishing web site, phisher may be able to request publication fee as next fraudulent action. Besides of announcement of precaution on phishing, regrettably there is no way to punish phishers or more active protective action. It was not possible to ask the investigation of the case to police because there was no monetary loss. Also it was impossible to shut down the phishing web site http://www.jeet.us because server was located in the United States. The international cooperation, enactment of international law on phishing, and its enforcement is necessary to eradicate this kind of criminal action.

Keywords

Criminals; International law; Journal website; Phishing; Republic of Korea

Introduction

In March 2017, we received a report that the website (http://www.jeet.or.kr) of the *Journal of Electrical Engineering & Technology* (JEET; pISSN 1975-0102, eISSN 2093-7423, indexed in Science Citation Index Expanded, Scopus, and the Korea Citation Index), which is the official journal of the Korea Institute Electrical Engineers (KIEE), one of the 4 major engineering academic societies in Korea, was being impersonated. By summarizing, disclosing, and sharing this case of website impersonation, this paper aims 1) to help protect domestic scientific jour-

Received: July 29, 2017
Accepted: August 1, 2017

Correspondence to Jaeseok Choi
jschoi@gnu.ac.kr

ORCID
Jaeseok Choi
http://orcid.org/0000-0003-0867-6251

nals in advance, 2) to protect authors (contributors) who submit high-quality articles from being harmed by fraudulent websites that steal their work, 3) to issue a warning to phishers and other scammers that there is no benefit to be gained from such activities, and finally 4) to help the journal websites published by various academic societies to develop countermeasures to ensure that they are not victimized in the future.

Informant and the Report

The informant's name and affiliate were closed. It is not necessary to expose the name and affiliation although it is treated as anonymity. The informant submitted his paper to the fake e-mail address 'editor@jeet.us' by following the instructions on the impersonated website (http://www.jeet.us), not the official JEET website (http://www.jeet.or.kr). Domain information of the phishing website was available in Suppl. 1. This case of fraud was discovered when the informant (the author) thought that his submitted paper had been accepted and made an inquiry to the JEET secretariat regarding the publication status of his paper. Comparison of the official e-submission site and fake submission site of JEET was presented in Fig. 1.

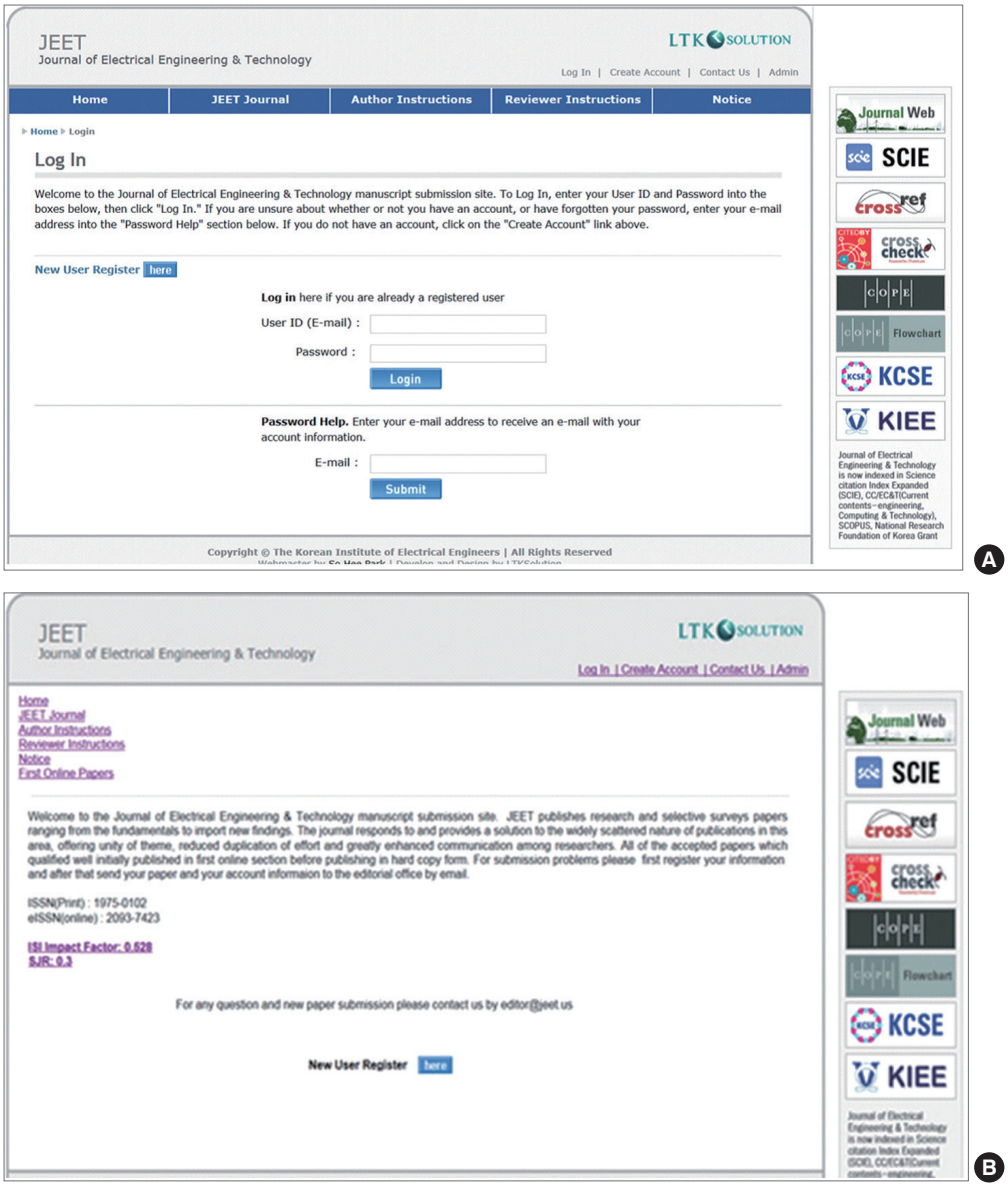

Fig. 1. Comparison of the official *Journal of Electrical Engineering & Technology* (JEET) website and the fake website. (A) Official JEET website: http://www.jeet.or.kr and (B) fake JEET website: http://www.jeet.us.

Case Timeline

June 29, 2016
The informant submitted his paper according to the instructions on the fraudulent website.
Kunihiko Hidaka, who is an honorary editor-in-chief of JEET and a professor at Tokyo University, was impersonated, and the informant received a confirmation mail sent from 'editor@jeet.us.'

August 30, 2016
The author received a confirmation number (#RP2509-0834) and copyright file from 'editor@jeet.us.'

September 17, 2016
An acceptance e-mail was sent to the informant from 'editor@jeet.us.'

September 24, 2016
The informant inquired with 'editor@jeet.us' about the date of publication.

September 28, 2016
The informant did not receive a reply, and therefore sent another inquiry about the date of publication to 'editor@jeet.us.'

October 10, 2016
The informant received a reply from 'editor@jeet.us' that the paper would be published by March 2017.

November 29, 2016
The informant inquired about the publication fee.

December 7, 2016
The informant received a reply from 'editor@jeet.us' stating that no fee would be required.

March 27, 2017
Since the informant did not receive any further correspondence from 'editor@jeet.us' after the last reply, he inquired about the publication date of his paper with 'jeet@kiee.or.kr,' which is the official secretariat of JEET.

Case Analysis

The informant submitted his manuscript to the fake website following their submission guidelines. Since the website contained a list of already published and forthcoming JEET papers linked to the official JEET website, the informant had no reason to be suspicious. After that, regarding the peer review process, peer review results, and the acceptance letter, he was only in contact with the e-mail address impersonating the honorary editor of JEET. For this reason, the JEET secretariat was not aware of the issue at all. Based on our analysis of this incident, the following is a brief presentation of the damages caused in terms of the phisher, the informant, and JEET.

First, the phisher's purpose in this incident does not seem to have been monetary. However, this may have been an initial inducement to deceive the contributor. If the paper had been published successfully in this case, the phisher might have asked for a publication fee as the next fraudulent act. If not, another possible purpose would be to confound the academic publishing process for its own sake. However, the likelihood that this was the motive is extremely low. In fact, as of June 2017, phishing websites have evolved and are requesting contributors to pay journal subscription fees; that is, they require an annual subscription fee instead a publication fee. Thus, their intention definitely seems to have been monetary.

Meanwhile, the contributor (informant) was informed of the "acceptance decision" and "free publication." As such, he suffered no monetary loss, but he must have suffered considerable psychological damage because this incident affected the review of his PhD thesis.

In terms of JEET itself, this incident did not affect the journal by causing it to lose credibility among contributors. Instead, this incident suggests that JEET is well known and valued highly enough to be used for impersonation. After this experience, JEET plans to revamp its publication process by enhancing security measures and developing new ways of accepting and evaluating manuscripts. However, many journals, including JEET, need to be aware of these dangers in advance and to develop preventive measures against phishing.

This incident was a case of phishing in which an academic journal website was impersonated, unlike typical phishing, in which monetary requests are made. On the fake website, information is provided via links to the official website of JEET; however, the fraudulent website states that manuscript submission and other correspondence should be conducted only by e-mail. Since this is the first case of fraud that JEET has experienced, no formal countermeasures have yet been taken, and information regarding this case is still being collected and verified. JEET informed the Korean Council of Science Editors about this incident and made an official request for their consultation. After sharing this incident with the board of directors of KIEE and journal editorial board of JEET, it was learned that similar incidents have occurred in other academic societies as well.

Handling of This Case and Measures

Like many fakes, this fake was very crude also. The crudeness of this impersonation can be identified easily on the fraudulent website, which is still up. As the number of reported phishing incidents increases, we need ways to prevent them; potential measures include legislation, user education, and fraud protection technology. In addition to phishing using computers, phishing can be carried out over the phone, which

is known as voice phishing. The following are examples of preventive measures: 1) Do not click on links in untrustworthy e-mails; 2) If in doubt, visit the site directly. 3) Check the mail header. 4) Check whether the address of the link is an IP address or a domain name. It may be a phishing site if it is an IP.

After being informed of the incident, The KIEE took the following measures: 1) The society reported it to the Cyber Police (https://www.police.go.kr/eng/main.do), but they did not investigate the case because there was no monetary loss. 2) Since the site had an overseas URL, it was impossible to shut down the site immediately. 3) The society sent an e-mail to the contributor informing him that he had submitted his manuscript to a fraudulent site and sent an e-mail alerting other members of the society. 4) The society put a pop-up message on their official website warning their members to be wary of scams.

Nonetheless, the above measures are passive protective actions and precautions that focus on the potential victims, and there is regrettably no way to punish phishers through active protective actions. JEET is issued bimonthly (in odd-numbered months), listed in Science Citation Index Expanded, and had an impact factor of 0.679 in 2015. The papers published in JEET can be verified on JEET's official website http://home.jeet.or.kr/. The society decided to regularly provide authors submitting manuscripts with the precautions against phishing sites to allow them to take extra precautions against fraudulent sites.

Conclusion

This incident involved the impersonation of the website of JEET. Regrettably, this fraud is still ongoing, because we have been unable to compel this website to be taken down. The following is a brief summary of the incident. 1) This incident started when the informant communicated with the fraudulent site and submitted his paper through e-mail. The fake website is still up, and it is evident that the submission guidelines are crude. 2) Fakes also evolve. Journal website impersonation is becoming a vicious scam. The fraudulent website, which first directly referred to itself as JEET, evolved to present itself as the purported online publication of the *Journal of Electrical Engineering* & *Technology and Interface Utilities*. Furthermore, it is expected that these fake journals will start requiring journal subscription fees and manuscript submission fees (peer review fees) from the beginning of the process. 3) Meanwhile, there are no clear preventive measures to be taken against this phenomenon. In particular, there seems to be no international statute for detecting and punishing phishers. Therefore, contributors (authors) need to pay special attention. It is easy to distinguish whether a website is official or fake by paying close attention when submitting a paper.

Finally, Korean academic journals are mostly published by academic societies, and they have purely academic goals. Therefore, it is unlikely that they will take effective measures based on a discussion of this issue. Moreover, almost all the measures that can be taken are passive protective actions and precautions in terms of the contributors, with no way to punish the phishers. Therefore, in order to develop effective countermeasures, it is essential that broad-based professional organizations such as the Korean Council of Science Editors should be more actively supported by the government. In addition, as we can see from this impersonation incident, the world is now bound together through the internet. Therefore, it is urgently necessary to discuss countermeasures against online impersonation through various international councils of editors. Publishing high-quality journals is extremely important not only for the scientific development and national growth of an individual country, but also for the scientific development of the world. Ultimately, we need to establish clear countermeasures to ensure that phishers clearly understand that they can gain no benefit from impersonating academic journals.

Conflict of Interest

No potential conflict of interest relevant to this article was reported.

Acknowledgments

The editorial board of *Journal of Electrical Engineering & Technology* is acknowledged for providing the relevant data, as is Mr. Woonkyeong Choi for arranging, and revising this article.

Supplementary Material

Supplementary file is available from: https://doi.org/10.6087/kcse.99

Suppl. 1. Domain information of the phishing web site of the *Journal of Electrical Engineering* & *Technology*.