Advances in Intelligent Systems and Computing (AISC)
Volume 1247, 2021, Pages 668–680

Experimental Evaluation of Phishing Attack on High School Students (Conference Paper)

Marusenko, R.[a], Sokolov, V.[b], Buriachok, V.[b]

[a]Taras Shevchenko National University of Kyiv, Kiev, Ukraine
[b]Borys Grinchenko Kyiv University, Kiev, Ukraine

Abstract

The effectiveness of phishing attacks is being analyzed by many researchers. At the same time, researches often deal with the random sample of people suffered a phishing attack and are limited with analysis of consequences of unrelated cases without conducting an actual phishing experiment. Experiments typically involve a small number of respondents. The novelty of present study is to analyze the educational institution' susceptibility to phishing attack. Authors demonstrate a methodology of creating a group of targets homogeneous in age, place of study, level of knowledge and to conduct an experiment on a large group of respondents (3,661 people). The methodology of gathering and filtering of email addresses using open sources of information is explained. Emotionally neutral text of a phishing email to minimize the deceptive effect of the letter was formulated. The experiment showed the success rate of the attack on a large sample of students at 10.8%, and demonstrated the vulnerability of the educational institution's infrastructure to the hidden preparation and conduct of the attack. Novelty of methodology includes use of a phishing letter that includes a questionnaire to gather statistics on responders' awareness of phishing nature. It made possible to compare respondents' beliefs with the real susceptibility to phishing based on sensitive data they provided in return to the phishing letter. We show how the data collected by phishing can be personalized and conclude that respondents need further training to detect phishing attacks. We also argue necessary organizational, infrastructural measures, recommendations of necessary mail server configuration changes.

Author keywords

Attack, Fishing, Personal information, Sensitive information, Social engineering

Funding details

Funding sponsor	Funding number	Acronym
Ministry of Education - Singapore	CCNU19TS022	MOE

Funding text

This scientific work was partially supported by RAMECS and self-determined research funds of CCNU from the colleges' primary research and operation of MOE (CCNU19TS022). All experiments were conducted at Borys Grinchenko Kyiv University.

About this paper

https://link.springer.com/chapter/10.1007%2F978-3-030-55506-1_59

ISSN: 2194-5357
Print ISBN: 978-303055505-4
DOI: 10.1007/978-3-030-55506-1_59
EID: 2-s2.0-85089721650

First Online: 06 August 2020
Source Type: Book Series
Document Type: Conference Paper
Publisher: Springer, Cham