MEDINFO 2019: Health and Wellbeing e-Networks for All
L. Ohno-Machado and B. Séroussi (Eds.)

doi:10.3233/SHTI190732

Result and Effectiveness of Malicious E-mail Response Training in a Hospital

Hye Sook Lee, Da Na Jeong, Su In Lee, Shin Hae Lee, Kyung Hwan Kim, Hae Young Lee, Hyun Jai Cho, Sae Won Choi, Taehoon Ko

Office of Hospital Information, Seoul National University Hospital

Abstract

Malicious e-mails sent intentionally to institutions have caused an increase in data breaches. Measures against these methods must be taken by healthcare institutions to prevent leakage of sensitive personal medical information. As a form of training, we conducted a phishing simulation to gauge the response of the hospital staff to similar email attacks, and to raise awareness about information security protocols.

Keywords:
Education, Electronic mail, Hospital.

Introduction

In recent years, risk of personal information leakage has increased due to malicious e-mails sent intentionally by hackers. [1] These malicious e-mails are usually sent to staff accounts [2] and can infect the employee's computer to compromise and damage important data when opened. The infected computer can then be used to spread to other computers through the intranet and cause secondary damages. Because personal health information is extremely sensitive information, data leak involving hospital records may result in serious harm to the patients involved and damage the reputation of the hospital. For these reasons, Seoul National University Hospital (SNUH) has preemptively conducted malicious e-mail simulation training. This training is designed not only to understand the level of security awareness of the hospital employees, but also to prevent information leakage by raising the awareness of the employees.

Methods

Malicious e-mail response training was organized by the Office of Hospital Information of Seoul National University Hospital and was conducted with support from an external security consulting company. Employees who have intranet accounts with access to hospital information system, general staff of the information office and human resources department, system administrators of other departments, and clinical fellows were selected as the target group.

Response training was organized in three stages: preparation, training, and analysis. In the preparation stage, the target group was selected after setting up a response training plan. Information protection and personal information protection campaigns were conducted through banners and notices on the hospital intranet to raise employee's awareness. In the training stage, a fake phishing mail was randomly sent to the subjects in three different scenarios: modification guide of personal information from a shopping mall, penalty payment from Seoul Gangnam police station, and notice about certificate leakage by malicious code. The reaction information was collected and divided into cases of just reading, clicking on a link, or downloading an attachment. All cases were considered to be infected by malicious code and subjects were notified via a pop-up to contact information security officer of the information/system security team. In the analysis stage, the results of the response training were analyzed to derive future security strategy.

Results

Among 405 employees targeted, 222 people (55%) viewed the malicious mail, 63 people (16%) of the viewers clicked on the link, and 66 (16%) people downloaded the attachment. Of the 222 people required to report malicious mail, 70 (32%) reported the incident to the information/system security team.

The details of the training, risk of malicious code infection, and compliance were shared through intranet with the entire hospital staff.

Conclusions

The number of reports of suspected malicious mail to the information security team increased after the malicious email response training. It is expected that the awareness of personal information protection will be improved by expanding the number of trainees in the future and periodically conducting malicious e-mail response training with scenarios modified to better suit the hospital's characteristics.

References

[1] Eom Jungho, *the improvement Plan of a Customized Cyber-Training Structure for enhancing the Capability of Cyber Security*, Journal of Security Engineering, 2015

[2] Moon Jeayeon, Chang Younghyun, *Ransomware Analysis and Method for Minimize the Damage*, the Journal of the Convergence on Culture Technology, 2018

Address for correspondence

Hye Sook Lee

Mailing Address: Office of Hospital Information, Seoul National University Hospital, 101, Daehak-ro, Jongno-gu, Seoul, Republic of Korea

E-mail:amaranth@snuh.org

Phone: +82 2 2072 2774, Fax number: 82 2 2072 0050