Awareness of Scam E-Mails: An Exploratory Research Study – Part 2

Kelly A. Cole, Tejashree D. Datar(✉), and Marcus K. Rogers

Knoy Hall of Technology, Room # 255, 401 N. Grant Street,
West Lafayette, IN 47907, USA
{colek, tdatar, rogersmk}@purdue.edu

Abstract. This paper is the second part of an entire study conducted regarding general awareness of email scams. The goal of this particular part of research was to check the awareness level and knowledge gap among email users with respect to the actions that need to be taken in case of scam email victimization, and awareness regarding common practices that are used in identifying scam email and types of online scam media. Most common actions mentioned by respondents in case of financial scams and clicking on a malicious link were to contact their banks to close their accounts and cancel their credit cards (41.17 %) and running an anti-virus scan (20.83 %) respectively. The most frequently mentioned online scam media other than email was online ads with pop-ups, while the most common practice employed to identify email scam was to check for emails asking for or giving away money. A definite lack of awareness was found among the users with respect to the actions that need to be taken in case of financial scam victimization. In conclusion, the researchers suggest a need for formal education regarding email scam awareness and best email usage practices.

Keywords: Email scam · Financial scam · Scam victimization · Email scam awareness

1 Introduction

Worldwide spam traffic is increasing on a daily basis. Spohos's Security Threat Report 2014 mentioned that 2013 saw an increase in the spam activity level in terms of email [1]. According to Securelist [2, 3], the average worldwide spam traffic in January 2014 among all email traffic was 65.7 %, and in February 2014 was 69.9 %. In February 2014, the U.S. ranked second in the distribution of this traffic by distributing 19.1 % of the worldwide spam [3]. Increase in scam activity has increased the likelihood of a user falling victim to email scam.

With scam emails becoming more sophisticated day-by-day, it becomes harder for email users to differentiate between scam and legitimate emails. These sophisticated emails increase the chances of an individual falling prey to scam emails. This makes it imperative to examine common practices used in identifying scam emails and the awareness of required actions that need to be taken by users in case of scam email victimization. Depending on technical proficiency, various methods can be employed

J.I. James and F. Breitinger (Eds.): ICDF2C 2015, LNICST 157, pp. 115–125, 2015.
DOI: 10.1007/978-3-319-25512-5_9

by email users to identify a given email as scam or legitimate. Some of the common practices to identify email scams are verifying the sender, checking email headers, checking hyperlinks within the email without clicking them, checking for digital certificates, and looking for cue words in the email body (e.g., urgent, money/information request, hyperlinks, typos) [4, 5].

Various actions are advised in case of financial scam victimization, and email scam victimization. In case, and individual clicks on a malicious link, different actions need to be taken to protect the computer. Agencies such as OnGuardOnline [6, 7], Michigan State Police [8], and Microsoft [9] have stated on their respective websites that potential victims of phishing email should take the following steps in cases of financial scam victimization:

- Put fraud alert on credit cards.
- File an identity theft report with the Federal Trade Commission (FTC). The FTC will provide the complainant with an affidavit.
- Take the affidavit from the FTC and file a report with the police.

These agencies believe that victims of phishing could possibly become victims of identity theft. The Federal Bureau of Investigation asks the victims to register a compliant with the Internet Crime Complaint Center (IC3) [10]. Microsoft [9] also asks the victims to contact their bank officials, and to change passwords and PINs. In addition to following all the above actions, victims of scam emails also need to update the anti-virus software and run a scan on their computer, and change passwords to any compromised accounts [11]. In case an individual clicked on a malicious link in an email, closing the pop-up window is not a good option, as it does not ensure that the malware is removed from the browser. A safer approach is to immediately disconnect from the Internet and to reboot the machine, and perform an antivirus scan [12, 13].

Online scams take place through various media. Email scam forms a small percentage of online scams. A lot of phishing attacks take place on social networking sites [14]. The other media for online scam include social networking sites (such as quizzes, or fake messages/alerts), SMS, fake online ads (such as lotteries, tech support, money offers, investment schemes), to name a few [15–19]. It is important to examine whether users of email have awareness of other online scam media.

This paper is the second part of an entire study conducted regarding general awareness of email scams. The aim of this part of research is to understand the awareness of email users regarding actions that need to be taken if they are victimized by scam email, common practices of identifying email, and awareness of different scam media. This research is important in understanding user approach and awareness to email scam and in finding the knowledge gap of these users regarding email scam awareness. Examining the different actions taken by the users in case of scam victimization and comparing them to suggested actions discussed earlier would throw light on users' knowledge about these actions. As mentioned earlier, different users are likely to employ variety of methods to identify email scams. It is helpful in understanding the most common practices that are used in identifying email scams. These results combined with the results from the first paper of the email research series will then help determine any need for workshops related to scam emails awareness.

2 Previous Research

Several studies have been conducted in the past to check if participants are able to identify scam emails. Jakobsson et al. conducted a study to identify email scam. Participants were shown emails on a screen and were asked to verbally identify the shown emails [20]. Shannon and Bennett [21] conducted a study on a university campus where they asked 109 students to identify a single email as scam or legitimate. Wang et al. studied the indicators or visual triggers that helped individuals in identifying scam emails. They found that individual with prior knowledge of scam emails were less susceptible to phishing scams as they paid more attention to visual triggers. They also found that participant's likelihood of responding to an email was dependent on visual triggers such as typos [22].

In his paper, Freiermuth described the red flags such as convincing storyline, soliciting offers, credentials, and salutations that can be used in identifying 419 scams [23]. Ragucci and Robila conducted a study to help businesses overcome their bad business email practices by avoiding red flags in email content [24].

The previous paper in the email scam series focused on identifying variables that influenced a user's ability to identify scam email. It was found that only the Frequency of Email Usage influenced a person's ability to identify emails, while 'awareness of common practices to identify email scam' was not found to be an influencing factor towards a user's ability in email scam detection [25]. Participants were also given four emails (2 scam and 2 legitimate), and were asked to identify these emails and to point out the indicators that aided them. The most common indicators used by respondents in email identification were: requesting personal, confidential, and financial information, giving away large sum of money, embedded links, asking to log into account, sender credentials, and generic email format. It was also found that 64.5 % of respondents were correctly able to identify 3 or more emails out of the given for emails [25].

3 Methodology

The study was aimed to check the awareness level and knowledge gap among email users with respect to scam email victimization. This was done with the help of following four questions that were asked to the participants with the help of the survey:

1. Question 1: What are the possible actions that individuals will take if they fall prey to a financial email scam or clicked on a malicious link?
2. Question 2: If users were victimized by a scam email, what actions did they take?
3. Question 3: Are the participants aware of other types of online scam media apart from email?
4. Question 4: What are the common practices to identify email scams?

The first question was included so as to understand whether users had any knowledge with respect to actions that need to be taken in case they are victimized by a financial scam or clicked on a malicious link in an email. The second question was included to get an insight into the action steps that were taken by the respondents after they were actually victimized by scam email. This will prove to be of help for any

future studies regarding email scam victimization by providing a gap in the knowledge as to what actions were actually taken as opposed to what actions need to be taken. The third question was included to understand if the respondents were aware of other online scam media. In the first part of scam email research study series, awareness of common practices to identify scam was used as one of the factors influencing a user's ability in email scam detection. The fourth question was included as the researchers were interested in knowing if the participants could name these common practices used to identify email scam.

A stratified random sample of N = 163 participants from Purdue University was used for the study. Researchers received approval from the Institutional Review Board (IRB) of Purdue University for administration of the survey at the university during the fall of 2011. The survey collected data for two different studies on email scam. As mentioned earlier, this research is the second between the two studies and uses a subset of the entire dataset. Participants were asked to answer a twelve-question survey as well as identify the four given emails as scam or legitimate. The survey was a combination of close-ended and open-ended questions. It asked for information such as demographics, frequency of email usage, participant's awareness of scam emails and other online scamming media apart from emails, participant's ability to identify email scam, common practices used to identify scam emails, actions taken if victimized by scam emails, and likely actions that will be taken if victimized by a financial scam. Participants had to identify four emails, two of which were scam while the remaining two were legitimate emails received by the researchers.

4 Results

The study used a sample size of N = 163, out of which 72 entries were not complete in entirety. The incomplete items included identifying the emails as scam or legitimate, common practices to identify email scams, listing other scam media, actions that were taken by victims after falling for financial scam, and possible actions that would be taken in case of financial scam of clicking on malicious link. The incomplete entries were retained in the dataset as all the research questions were independent of each other and did not necessitate a survey completed in entirety. For this particular paper only partial data from the entire data set was used. The demographics of the participants is as follows: Out of the 163 participants, 90.2 % participants were between the 18–30 years age group, 6.1 % between 31–45 years age group, and 3.7 % between 46–65 years age group. Of all the participants, 44.8 % of the participants were females, while 55.2 % were males (see Appendix, Table 5).

88.7 % of the participants replied receiving an e-mail scam, while 10.1 % replied never receiving any email scam. 1.3 % of the participants were unsure if they had ever received an e-mail scam. 90.5 % of the participants replied to never have been a scam victim, while 9.5 % replied with an affirmative (see Appendix, Table 6).

Participants took a variety of actions after receiving scam e-mail. 73.1 % replied that they deleted or ignored the e-mail, followed by 15 % of the respondents indicating that they researched online and deleted/ignored the e-mail. Only 1.9 % reported it to the authorities. Refer to Table 7 in the Appendix for a detailed list of all actions taken by

respondents. 72.3 % of the respondents replied they were aware of other online scam media, 23.8 % replied in the negative, and 3.8 % were unsure (see Appendix, Table 8).

Question 1. What are the possible actions that individuals will take if they fall prey to a financial email scam or clicked on a malicious link?

A hypothetical question was asked in the questionnaire asking the participants to specify any actions they will take in either of the situations. With respect to the financial scam question, most frequently suggested action by the respondents was 'contacting the bank to cancel cards and to close accounts' (35)[1], and the action that was least frequently specified was 'running a credit score check' (1). Most common action mentioned by respondents after clicking on a malicious link was 'running an anti-virus software' (25), and the least common action mentioned was 'ignoring it' (8). For an entire list of all the actions specified by the respondents see Table 1.

Question 2. If users were victimized by a scam email, what actions did they take?

Only 9.2 % of the respondents replied to being a victim of scam email. Most common action that was taken by the respondents after being victimized by an email scam was to 'delete and/or mark the email as spam' (4), while the least common actions that were taken by the respondents after being victimized were: block the sender (1), and report it to the authorities (1) (see Table 2). Respondents did not specify which authorities were reported about the incident.

Question 3. Are the participants aware of other types of online scam media apart from email?

57.7 % of respondents replied that they were aware of other types of online scam media. Many of the respondents mentioned more than one type of scam media. Most frequently mentioned scam media was 'online ads with pop-ups' (82), while least frequently mentioned scam media was 'applications' (1). For a complete list of other online media, please refer to Table 3.

Question 4. What are the common practices to identify email scams?

52.8 % of the participants responded that they were aware of the common practices to identify email scams. Of these, many respondents mentioned more than one practice. Most frequently mentioned common practice was 'emails asking for or giving out money, emails informing about rewards, sales or business offers, or advertising emails' (44), while the least frequently mentioned common practices were: 'looking for headers and email address source' (4), and 'looking for secure sites' (4). Table 4 lists a complete list of practices employed by the respondents.

[1] Bracketed numbers indicate frequency.

Table 1. Frequency of the likely actions taken by respondents if they fall prey to financial scam or click on a malicious link

	Likely actions taken	Frequency
Actions for financial scam	Contact bank to cancel cards and to close account	35
	Notify the authorities	23
	Ask for help	3
	Take legal action	2
	Run a credit check	1
Actions for malicious link	Run anti-virus	25
	Close pop-up message	16
	Delete email with malicious link and change password	17
	Ask help from IT services	11
	Shut down/restart the computer and/or restore it	9
	Ignore it	8
	Delete cookies and temporary files	5
	Mark email as spam	1
	Call anti-virus company	1
	Unsubscribe	1
	Call server to cancel link	1
	No authorities to report to	1
	Irrelevant response	8
	Not sure	21
	Did not respond	26

Table 2. Actions taken after being email scam victim

Actions taken	Frequency	Valid frequency
Delete and/or mark the email as spam	4	16
Use and/or update anti-virus program	2	8
Change the password and/or email address	2	8
Block the sender	1	4
Report it to the authorities	1	4
Did not respond	7	28
Irrelevant answer	8	32
Total	25	100

5 Discussion

As students form a large part of the dataset, large number of participants from the 18–30 years age group was expected. The gender of the participants is fairly balanced with 44.8 % participants being females and 55.2 % participants being males. Majority of the participants (88.7 %) answered positive to receiving email scams. This is consistent with the figures from Spohos (2014) and Securelist (2014a, b), which were mentioned

Table 3. Other scam media apart from email

Online scam medium	Frequency
Online ads with pop-ups	82
Social media	24
Fake websites	16
Cell phone calls and/or texts	16
Hyperlinks	12
Spam and phishing	9
Online bots	4
Cookies	3
Malware/Adware and attacks	3
Unsecured login	2
Website tracking	2
Applications	1
Did not respond	37

Table 4. Common practices employed by the respondents to identify email scam

Common practices used	Frequency
Emails asking for or giving out money, emails informing about rewards, sales or business offers, or advertising emails	44
Looking for email sender either known or unknown	38
Emails asking for personal/private information such passwords, social security number, or ID number	29
Emails with hyperlinks that ask the recipient to go to a specific website	17
Typos or misspelling in the email content, bad grammar, big words in the email, emails sounding too good to be true, unknown content	15
Financial or banking information	13
Email subject heading such as heading in capital letters, generic heading, or informing about monetary gain, generic email greetings	13
Emails from Nigeria or 419 phishing emails	9
Looking for headers and email address source	4
Looking for secure sites	4
Did not respond	23
Irrelevant answer	12

at the beginning. Some participants (10.1 %) mentioned to never having received email scams, which could be due to stringent mailbox rules, extremely less email usage, or lack of awareness of scam emails. A few participants (1.3 %) were unsure if they had ever received scam email, which indicates a lack of awareness in identifying scam emails. Majority of the participants (90.5 %) who had received email scams reported of not being victimized from the scam emails. A fairly large number of participants (23.8 %) replied of not knowing any other online scam media other than email,

indicating a lack of awareness of popular online scams media such as social networking sites, where a lot of phishing attacks take place (Gudkova 2014).

The first research question talked about possible actions that need to be taken in the case of financial scam victimization or clicking on a malicious link. The responses for this question (see Table 1) do not match any of the suggested actions that need to be taken in case of either financial victimization (creating a fraud alert, filing a theft report, and running a credit check) or clicking on a malicious link (rebooting the machine to clear the cache, and running an anti-virus scan for the full machine). The second research question focused on actions that were taken by the actual victims of email scams. The responses to this question (see Table 2) also do not match with the recommended actions that should have been taken after falling victim to a financial scam.

The third research question focused on the knowledge of other types of scam media apart from email. None of the respondents mentioned legitimate websites such as Craigslist as one of the other scam media, while a few users mentioned options such as spam and phishing (9), cookies (3), unsecured login (2), and malware/adware attacks (3) that cannot be called as online scamming media (see Table 3). The fourth question focused on some of the common practices used to identify email scam. Participants were able to identify a number of different practices to identify scam email (see Table 4), and seemed fairly aware of the practices that should be used to check email legitimacy.

User awareness of the common practices employed in identifying scam email, but lack of awareness of different scamming media, shows a partial awareness regarding preventive measures towards email scam victimization. This lack of awareness could prove dangerous to email users; as such users will not be vigilant while using other online services and could fall victims to popular scam not implemented via email. Though the responses provided by the participants are partially correct, a huge gap in knowledge is still visible in regards with actions that need to be taken in case of financial scam victimization or clicking on a malicious link, as well as computing and different types of online scamming media. Users lacked awareness about the proper legal or safety actions that need to be taken after falling prey to an email scam. Financial scams are a popular type of scam, and the possibility of users encountering these scams is high. Lack of awareness of financial scams can lead users to lose valuable financial as well as personal information, monetary loss, and in worst cases adversely affect their financial reputation. This gap the knowledge suggests a need for some type of intervention/education to make users aware of different scamming media, and the proper legal actions that need to be taken in the unfortunate event of email scam or financial scam victimization.

6 Limitations

A reliability test for the survey was not deemed necessary due to the exploratory nature of the research. Participants did not receive any compensation for being part of the study, which resulted in participants not filling out the survey completely. As the study was conducted on a university campus, most of the data was limited to the 18–30 year age group.

7 Conclusion

There is a definite knowledge gap among the users with respect to actual actions that need to be taken after email or financial scam victimization and the actions that the users were aware of. Financial scams are one the most popular types of scam and this lack of awareness can prove dangerous to email users. The lack of knowledge gap points that users need to be educated in matters of actions that should be followed in cases of email scam victimization, or financial scam victimization. Increase of email usage is inevitable, and the recent surge in scam email traffic indicates possible future victimization of users. A formal awareness education regarding email scams and their victimizations should be developed to help users stay safe and aware while using email.

Appendix: Tables

See Tables 5, 6, 7, 8.

Table 5. Demographics of the respondents

		Frequency	Percent
Age (in years)	18–30	147	90.2
	31–45	10	6.1
	46–65	6	3.7
	Total	163	100.0
Gender	Females	73	44.8
	Males	90	55.2
	Total	163	100.0

Table 6. Frequency of receipt of scam email, and email scam victimization

		Frequency	Valid percent
Ever received scam email	Yes	141	88.7
	No	16	10.1
	Unsure	2	1.3
	Total	159	100.0
Email scam victimization	Yes	15	9.5
	No	143	90.5
	Total	158	100.0

Table 7. Frequency of actions taken after receiving a scam email

	Frequency	Valid percent
Research online if mail is scam	3	1.9
Delete it/Ignore it	117	73.1
Report to authorities	3	1.9
Research online, and Delete/Ignore it	24	15
Research online, and Report to authorities	2	1.3
Delete it/Ignore it, and Report it to authorities	4	2.5
Research online, Delete it, and Report to authorities	5	3.1
None of the above	2	1.3
Total	160	100.0

Table 8. Frequency of awareness of other scam media

	Frequency	Valid percent
Yes	4	2.5
No	5	3.1
Unsure	2	1.3
Total	160	100.0

References

1. Sophos: the security threat report 2014 (2014). http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-security-threat-report-2014.pdf
2. Securelist: spam report: January 2014 (2014). https://www.securelist.com/en/analysis/204792327/Spam_report_January_2014
3. Securelist: spam report: February 2014 (2014). https://www.securelist.com/en/analysis/204792328/Spam_report_February_2014#09
4. Office: identify fraudulent email and phishing schemes (n.d.). http://office.microsoft.com/en-us/outlook-help/identify-fraudulent-e-mail-and-phishing-schemes-HA001140002.aspx
5. Apple: identifying fraudulent “phishing” email (n.d.). http://support.apple.com/kb/ht4933
6. OnGuardOnline: identity theft. (n.d.) http://www.onguardonline.gov/articles/0005-identity-theft
7. OnGuardOnline: phishing (n.d.). http://www.onguardonline.gov/phishing#action%20steps
8. Michgan State Police: victim action steps (n.d.). http://www.michigan.gov/msp/0,4643,7-123-1589_35832_38137—,00.html
9. Microsoft: email and web scams: how to help protect yourself (n.d.). http://www.microsoft.com/en-GB/security/online-privacy/phishing-scams.aspx
10. Federal Bureau of Investigation: new e-scams and warnings (n.d.). http://www.fbi.gov/scams-safety/e-scams
11. Acohido: USA Today, 3 must-do steps to recover from a phishing scam (17 May 2013). http://www.usatoday.com/story/cybertruth/2013/05/17/phishing-scams-steps-to-recover-privacy/2193105/
12. Computer world: don’t click that link, but if you do… (11 April 2014). http://blogs.computerworld.com/15907/dont_click_that_link_but_if_you_do

13. Fortinet: you clicked on that (malicious) link: from panic to peace of mind (20 April 2012). https://blog.fortinet.com/you-clicked-on-that-malicious-link-from-panic-to-peace-of-mind/
14. Gudkova, D: Kaspersky Security Bulletin. Spam evolution 2013 (2014). http://securelist.com/analysis/kaspersky-security-bulletin/58274/kaspersky-security-bulletin-spam-evolution-2013/
15. Internet crime complaint center: internet crime schemes (n.d.). http://www.ic3.gov/crimeschemes.aspx#item-17
16. Internet crime complaint center: scam alerts (March 2014). http://www.ic3.gov/media/2014/140321.aspx
17. Norton: your security resource (n.d.). http://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams
18. Norton: social networking scam (n.d.). http://us.norton.com/social-networking-scams/article
19. OnGuardOnline: common online scams (n.d.). https://www.onguardonline.gov/articles/0002-common-online-scams
20. Jakobsson, M., Tsow, A., Shah, A., Blevis, E., Lim, Y.-k.: What Instills trust? A qualitative study of phishing. In: Dietrich, S., Dhamija, R. (eds.) FC 2007 and USEC 2007. LNCS, vol. 4886, pp. 356–361. Springer, Heidelberg (2007)
21. Shannon, L., Bennett, J.: A case study: applying critical thinking skills to computer science and technology. In: Information Systems Educators Conference, vol. 28 (2011)
22. Wang, J., Herath, T., Chen, R., Vishwanath, A., Rao, H.R.: Phishing susceptibility: an investigation into the processing of a targeted spear phishing email. IEEE Trans. Prof. Commun. **99** (2012). doi:10.1109/TPC.2012.2208392
23. Freiermuth, M.: Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. Discourse Commun. **5**, 123–125 (2011). doi:10.1177/1750481310395448
24. Ragucci, J., Robila, S.: Societal aspects of phishing. IEEE, pp. 1–5 (2006). doi:10.1109/ISTAS.2006.4375893
25. Datar, T.D., Cole, K.A., Rogers, M.K.: Awareness of scam e-mails: an exploratory research study. In: Proceedings of the Conference on Digital Forensics, Security and Law, pp. 11–34 (May 2014)