Annual ADFSL Conference on Digital Forensics, Security and Law

2014
Proceedings

May 28th, 9:40 AM

Awareness of Scam E-mails: An Exploratory Research Study

Tejashree D. Datar
Computer and Information Technology Department, Purdue University, tdatar@purdue.edu

Kelly A. Cole
Computer and Information Technology Department, Purdue University, colek@purdue.edu

Marcus K. Rogers
Computer and Information Technology Department, Purdue University, rogersmk@purdue.edu

Scholarly Commons Citation

Datar, Tejashree D.; Cole, Kelly A.; and Rogers, Marcus K., "Awareness of Scam E-mails: An Exploratory Research Study" (2014). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 12.
https://commons.erau.edu/adfsl/2014/wednesday/12

AWARENESS OF SCAM E-MAILS: AN EXPLORATORY RESEARCH STUDY

Tejashree D. Datar
tdatar@purdue.edu

Kelly Anne Cole
colek@purdue.edu

Marcus K. Rogers
rogersmk@purdue.edu

Computer and Information Technology Department
Purdue University
401 North Grant Street, Knoy 255
West Lafayette IN 47907-2021

ABSTRACT

The goal of this research was to find the factors that influence a user's ability to identify e-mail scams. It also aimed to understand user's awareness regarding e-mail scams and actions that need to be taken if and when victimized. This study was conducted on a university campus with 163 participants. This study presented the participants with two scam e-mails and two legitimate e-mails and asked the participants to correctly identify these e-mails as scam or legitimate. The study focused on the ability of people to differentiate between scam and legitimate e-mails. The study attempted to determine factors that influence a user's ability to successfully identify e-mail scams. The results indicated that frequency of e-mail usage was the only factor that influences e-mail scam detection. Only 1.7% of the respondents were able to identify all four e-mails correctly and 64.5% of the respondents were correctly able to identify three of the given four e-mails. Most users tended to delete/ignore the e-mail after receiving a scam e-mail. 59.3% respondents indicated that they were able to identify scam e-mail. Users also tended to trust reputed company names when trying to discern whether the particular e-mail was a scam or was legitimate. It should be noted that this paper is based on a subset of the entire dataset collected.

Keywords: E-mail scam, phishing, e-mail scam identification, awareness of e-mail scam, indicators used in detecting e-mails, phishing attacks, context-aware phishing

1. INTRODUCTION

With the growth in the popularity of the Internet, today, many individuals conduct business online. The credit card information entered online offers new opportunities for criminals to commit theft via the Internet. According to comScore, a global source of digital market intelligence, $49.8 billion dollars was spent through retail e-commerce in the United States for the second quarter in 2013 (comScore, 2013). The high amount of transactions taking place through websites and e-mail provide online criminals with the opportunity to commit financial scams.

Scams and spam can easily be confused. The Spamhaus Project, a well-known company that tracts and prevents spam for corporations, defines an electronic message as spam if "(A) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients; and (B) the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent" (Spamhaus Project, 2012, pg. 1). An e-mail is considered to be spam only if it is both delivered in bulk and is unsolicited, while content is not of importance (Spamhaus Project, 2012). Another way of understanding spam is to look at the Controlling the Assault of Non-Solicited Pornography And Marketing **(**CAN-SPAM) Act of 2003, which addresses the legality of sending commercial e-mails in the United States and is a legislation effort aimed to control spam. According to the Act, e-mails need to match requirements to be considered legal. These requirements are: accurate header, non-deceptive subject line, clear identification as an advertisement, return e-mail address, opt out features, no more contact after choosing to opt out, valid, physical postal address. It needs to be understood that the CAN-SPAM Act addresses only e-mails that are sent commercially. The CAN-SPAM Act requirements unfortunately cannot apply to spam e-mails sent by private users or fraudsters.

According to three popular anti-virus companies spam accounted for somewhere between 70% and 87% of all e-mail traffic (Cisco, 2013; Securelist, 2013; Trustwave, 2013). Looking at these statistics it is safe to say that most everyone with an e-mail account has received spam and scam e-mails at least once. Saberi, Vahidi and Bidgoli (2007) describe Phishing as “a kind of identity theft which tries to steal confidential data such as on-line bank account information through the use of a fake e-mail” (pg 1). Kaspersky (2013) describes phishing as a form of Internet fraud where fake versions of popular websites such as e-mail, social networking sites, or banking sites, are created to lure users. Spam e-mails accounted for 12% of all registered phishing attacks in 2012-2013 (Kaspersky, 2013). According to EMC^2, a popular security company, phishing is here to stay because of the low cost in preparing such attacks, high monetary gain and low risk of detection. From the data reported on EMC^2, 16,000 phishing attacks take place online per month and 70% of them target the United States. Furthermore, there was 1.3 billion in global losses from phishing attacks in 2011. Africa’s notorious Nigerian phishing scams, also called Nigerian 419 scams, cost the United States “$1 billion to $2 billion” per year (FBI, 2010b).

Originally 419 scam attacks were sent through e-mail resembling spam, that is, delivered in bulk and unsolicited. However, phishing has become more advanced turning into what is known as Context-Aware Phishing Attacks (Ragucci & Robila, 2006). For these attacks, the sender gains knowledge of the websites that a victim uses and customizes the attack (e-mail) accordingly (Ragucci & Robila, 2006). The goal of a phishing attack is to attain personal information such as credit card numbers and social security information.

Differentiating between scam e-mail and legitimate e-mail can sometimes be a difficult task. This research is aimed to discover how difficult this task is for users of e-mails. E-mail scams are becoming more sophisticated everyday (Office of Attorney General, California, n.d.). According to the Office of Attorney General of California, these include but are not limited to:

- using names of reputed companies both large and small
- developing more realistic webpages
- mirroring the webpages
- matching the company URL
- matching the format of the e-mail to legitimate e-mails
- erasing the typos in the scam e-mail (pg 1).

Websites such as the Office of Attorney General of California, Microsoft, and many more give information on how to identify scam e-mails. But this information is difficult to use in every situation, especially when the e-mail appears to come from a trusted source such as a well-known bank. For example, if a Bank of America customer receives monthly e-mail statements and suddenly a fraudster sends them a fake e-mail asking them to change their user name and passwords, they may offer up this information without even knowing it was a phishing attempt. Understanding the way users distinguish the e-mail as a scam e-mail or a legitimate e-mail is important, as this will provide an understanding of the indicators that users use when differentiating between scam and legitimate e-mail.

2. PREVIOUS RESEARCH

There have been several previous studies in this area. Freiermuth (2011) describes how a 419 scam can be detected following specific identifying features occurring in the scam e-mail. These features were, soliciting an offer, closing and opening salutations, established credentials, a tale/convincing storyline, and invitation to further contact. Ragucci and Robila (2006) in their study help identify bad business e-mail practices so that customers will be better able to identify the red flags of a possible e-mail scam. In another study Shannon and Bennett (2011) asked 109 students whether a proposed e-mail was a scam or not and why. The scam e-mail warned people to update their Webmail account information within 3 days to avoid cancelation of the account. 80.7% identified at least one item that made the e-mail look suspicious and 7.3% recognized at least two things that made the e-mail suspicious. The students noted e-mail address, message limitation, requesting personal information and the fact that they were to "activate the account" as identifiable scamming techniques (Shannon & Bennett, 2011).

Jakobsson, Tsow, Shah, Blevis, and Lim (2007) conducted a study where 17 participants were verbally asked to announce the answer to whether e-mails shown to them on a computer screen were scams or not. Wang, Herath, Chen, Vishwanath and Rao (2012) developed a survey that contained one scam e-mail. This study focused on indicators or visual triggers that aid individuals toward the identification of a deceptive e-mail. They also found that visual triggers and deception indications such as spelling mistakes affected a participant’s likelihood to respond to the e-mail. They measured the effect of knowledge of scam e-mails on phishing susceptibility and found that the participants with more knowledge surrounding e-mail scams paid more attention to visual triggers and were less susceptible to phishing scams.

3. CURRENT STUDY

The current study is different than previously conducted research in that the study attempts to find indicators that lead to suspicion of scam e-mail, such as unknown sender, or someone requesting personal and financial information. The researchers also aim to discover the variables that help users in identifying scam e-mails, such as age, usage of e-mail frequency, being aware of e-mail scams. This study attempts to find if participants can differentiate between scam e-mails and legitimate e-mails. For this purpose, our study went a step further than Shannon and Bennett (2011) and Wang et. al. (2012). The previous studies only included one scam and one legitimate e-mail. The current study included two scam e-mails and two legitimate e-mails in the survey.

In the current study participants were asked to identify these e-mails as scams or not. Additionally, participants were asked the reasons as to why they thought the particular e-mail was scam or legitimate. The survey also asked several questions to assess participant’s knowledge about phishing, other scam media, and actions that need to be taken in the case of scam victimization.

4. METHODOLOGY

The research questions for the study were as follows:

1. What variables influence a user’s ability to identify a scam e-mail?
    a. Hypothesis 1: Age, Frequency of e-mail usage, Awareness of e-mail scam, and Awareness of common practices to identify an e-mail scam are the variables that will influence a user’s ability to identify an e-mail scam.
2. What indicators were used to identify whether the given e-mail was a scam or not?
    a. Hypothesis 2: Sender credentials, generic e-mail, giving away money, requests for personal information, requests for financial information, and asking to click on an embedded link within the e-mail will be the most common indicators used to identify the given e-mail.
3. How many of the self-reported respondents indicating the ability to identify scam e-mail can

correctly identify the given e-mails?

a. Hypothesis 3: More than 50% of the self-reported respondents indicating the ability to identify scam e-mail will not be able to identify the given e-mails.

The sample consisted of N=163 participants from Purdue University. The participants were a mixture of under graduate students, graduate students, faculty, staff, and some outsiders. The researchers received approval from the Institutional Review Board (IRB) of Purdue University for the administration of the survey to participants at the Purdue University during the fall of 2011.

Data used for this research was collected for two different studies on e-mail scam. This research is the first among the two studies and uses a subset of the entire dataset. Participants were asked to fill out a twelve-question survey. This survey asked for demographic information such as age and gender, frequency of e-mail usage, such as, hourly, daily, weekly, biweekly or never (see Appendix C for the survey). The survey also measured participant's awareness of e-mails being a potential scamming medium and if participants were aware of other scamming methods. Participants were asked if they were able to identify an e-mail scam if they received one and if they were aware of common practices to identify e-mail scams and to name them (see Appendix C for the survey). The survey further asked if participants had ever received e-mail scams and what actions were taken. Participants were also asked if they had ever been a victim of e-mail scam and if yes, to specify what actions were taken (see Appendix C for the survey). Participants were asked to specify actions that need to be taken if they fall victim to a financial scam or if they clicked on a malicious link. Participants were then asked to read through the four presented e-mails and to identify these as scam or not and to circle or mention the identifiers that lead them to this conclusion (see Appendix C for the survey).

The first two e-mails were financial scams that one of the authors had once received. The first of the two scams was a popular 419 Nigerian scam requesting a large sum of money and financial information. The second of the two scams was a Vonage banking scam with many redirects for entering financial information. The other two e-mails (e-mails 3 and 4) were legitimate e-mails. E-mail three was a banking e-statement and e-mail four was a legitimate insurance renewal statement (see Appendix C for the e-mails).

5. RESULTS

The data consisted of a sample size of N=163. Out of 163 entries 72 entries were not complete. The researchers decided to keep the incomplete entries as part of the dataset as all the research questions are independent of each other and do not necessitate the participant to complete the survey completely. For the purpose of this paper, partial data collected from the survey was used. A preliminary descriptive frequency analysis was conducted on all the variables. Of the 163 participants, 90.2% were between the 18-30 years age group, 6.1% of participants were between 31-45 years age group and 3.7% of the participants fell in the 46-65 years age group. This was expected, as the study was undertaken at a university location where undergraduate or graduate students formed the majority of the sample. Of all the participants, 44.8% of the participants were females, while 55.2% were males (see Appendix A, Table 1).

Looking at the frequency of e-mail usage, 47.2% of the participants used e-mail hourly, 49.1% used e-mail daily, and only 3.7% used e-mail on a weekly basis. 95.1% of the participants responded that they were aware of e-mail scams and only 4.9% responded with a negative. When asked if the participants can identify an e-mail scam, 59.3% responded that they are able to identify an e-mail scam, 3.7% responded that they cannot identify an e-mail scam and 37% responded with an unsure/maybe. 68.8% of the participants responded that they are aware of the common practices to identify e-mail scams, while 28.8% responded that they are not aware of the common practices to identify e-mail scams, and 2.4% of the participants were unsure (see Appendix A, Table 2).

When asked if the participants had ever received a scam e-mail, 88.7% of the participants replied that they had received an e-mail scam while 10.1% replied that they had never. 1.3% of the participants were unsure if they had ever received an e-mail scam. From the above percentages, it can be seen that 1.3% of the respondents are not aware of whether they have ever received e-mail scam. This shows a lack of awareness in identifying scam e-mail from legitimate e-mail amongst a small percentage of participants. When asked if the participants had ever fallen victims to 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 A, Table 3). From these percentages it can be seen that a majority of the participants have never been victimized by scam e-mails.

When asked what actions were taken after receiving a 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, while only 1.9% reported it to the authorities. For a detailed list of actions taken by respondents after receiving a scam e-mail, please refer to Appendix A, Table 4. It can be seen from these percentages that most of the users choose to delete or ignore a scam e-mail. Few users choose to research the mail online to check if it is indeed a scam e-mail, and very few users choose to report such incidences to the authorities.

In response to the question if the participants were aware of media other than e-mail for the purpose of scams, 72.3% replied yes, 23.8% replied no, and 3.8% replied, that they were unsure (see Appendix A, Table 5).

5.1 Research Question 1: What variables influence a user's ability to identify a scam e-mail?

Hypothesis 1: Age, Frequency of e-mail usage, Awareness of e-mail scam, and Awareness of common practices to identify e-mail scam are the variables that will influence a user's ability to identify e-mail scam.

Wang et al. (2012) found that users with prior knowledge or e-mail scam paid more attention to visual triggers in the e-mails, were able to identify scam e-mails better, and were less susceptible to e-mail scams. Taking this into consideration, researches decided to include Awareness of e-mail scam, and Awareness of common practices to identify e-mail scam as variables that will help in identification of scam e-mail. Frequency of e-mail usage will make users more aware of e-mail scams and was included as one of the variables to be tested in the hypothesis.

The researchers looked at the Q-Q plots for each variable and found that the sample was not normal and decided to run a binary logistic regression.

The researchers ran a bivariate correlation to find the variables of interest that are the factors that influence a user's ability to identify e-mail scams. The Pearson's Correlation was set to a threshold of 0.2. The following variables were found to be of interest: age, e-mail usage frequency, awareness of scam e-mails, can identify e-mail scams, awareness of common practices to identify e-mail scams, actions taken if victimized by e-mail scam, and other scam media awareness (see Appendix B for the correlation table).

As the nature of this research is exploratory, a forward stepwise method was used for binary logistic regression. Significance level or α of 0.05 was used. Of the above variables of interest only EmailFrequency, that measures the e-mail usage frequency, and AwareOfEmailScam, that measures if a user is aware of scam e-mails were included in the regression model. The rest of the variables were not included in the regression model. Of these two included variables, only EmailFrequency was found to be significant with a p-value of 0.042 and df=1 (see Table 1).

Table 1 Variables Entered in the Regression Equation in a Stepwise Manner

		B	S.E.	Wald	df	p	Exp(B)
Step 1[a]	EmailFrequency	.886	.436	4.137	1	.042	2.425
Step 2[b]	EmailFrequency	.915	.447	4.191	1	.041	2.498
	AwareOfEmailScam	-21.990	27883.416	.000	1	.999	.000
a. Variable(s) entered on step 1: EmailFrequency							
b. Variable(s) entered on step 2: AwareOfEmailScam							

Cox and Snell R-square was found to be 0.047. This means that only 4.7% of the change in the dependent variable, that is, the ability to identify scams can be explained by the variable EmailFrequency.

The factor that influences a user's ability to identify e-mail scams is frequency of e-mail usage. Age, awareness of e-mail scam, and awareness of common practices to identify e-mail scam do not influence a person's ability to identify e-mail scams, thus the first hypothesis was not supported.

5.2 Research Question 2: What indicators were used to identify whether the given e-mail was a scam or not?

Hypothesis 2: Sender credentials, generic e-mail, giving away money, requests for personal information, requests for financial information, asking to click on an embedded link within the e-mail will be the most common indicators used to identify the given e-mail.

Previous research conducted look at the indicators used in identifying scam e-mails and avoiding bad e-mail practices in business (Freiermuth, 2011; Ragucci, & Robila, 2006; Shannon, & Bennett, 2011; Wang et al., 2012). These research suggest sender credentials, soliciting offers, asking personal information, use of hyperlinks, and personalized e-mail format as few of the indicators of scam e-mails. The researchers decided to include these indicators in the hypothesis. Asking for financial information was also added as most of the 419 scams are based on financial element (Freiermuth, 2011).

E-mail 1

This e-mail was a classic case of a 419 Nigerian scam. 23 respondents did not identify the e-mail as scam or not scam and also did not specify the indicators. Out of the participants who answered the question, 97.9% correctly identified this e-mail as a scam, 0.7% incorrectly identified the e-mail as a legitimate e-mail, and 1.4% of the respondents were unsure (see Table 2). 28 respondents indicated whether the e-mail was a scam or not, but did not specify the indicators they used for the e-mail identification, while 28 respondents replied with irrelevant answers.

Table 2 Identification of E-Mails as Scam or Legitimate E-Mail

		Frequency	Valid Percent
E-mail 1	Correct Identification	137	97.9
	Incorrect Identification	1	0.7
	Unsure	2	1.4
	Total	140	100.0
E-mail 2	Correct Identification	17	12.5
	Incorrect Identification	105	77.2
	Unsure	14	10.3
	Total	136	100.0
E-mail 3	Correct Identification	99	72.3
	Incorrect Identification	21	15.3
	Unsure	17	12.4
	Total	137	100.0
E-mail 4	Correct Identification	99	75.0
	Incorrect Identification	14	10.6
	Unsure	19	14.4
	Total	132	100.0

76 respondents mentioned *requesting information* such as personal information, banking details, and confidential information, 47 respondents mentioned *giving away a large sum of money*, and 34 respondents mentioned the word *Nigeria* as an indicator. The other indicators, mentioned by the respondents were: asking for stamped and signed letter head (15)[1], unknown sender or sender's credentials not specified (14), generic greeting (12), unreasonable sounding e-mail (10), subject heading (1), urgency of response (3), and assurance of being risk free (1).

E-mail 2

This e-mail was a scam e-mail that appears to be coming from Vonage and looks like a receipt that asks the recipients to click on various links to provide information. 27 respondents did not identify the e-mail as scam or not scam and also did not specify the indicators. Out of the participants who answered the question, 12.5% correctly identified this e-mail as scam, 77.2% incorrectly identified the e-mail as a legitimate e-mail, and 10.3% of the respondents were unsure (see Table 2). 44 respondents indicated whether the e-mail was a scam or not, but did not specify the indicators they used for the e-mail identification, while 36 respondents replied with irrelevant answers.

Respondents who correctly identified the e-mail as a scam e-mail specified the following indicators: multiple underlined links asking to log into account (10), not a personalized e-mail (2), links not html

[1] Bracketed numbers indicate frequency

(1), unprofessional looking e-mail (1), has no account number (1), grammar issues (1), and billing information is normally given during transactions and not later on (1).

Respondents who incorrectly identified the e-mail as a legitimate e-mail specified the following indicators: doesn't ask for personal or financial information (23), requests to not send confidential information over e-mail (20), secure URL (13), Vonage is a reputed and recognized name (12), looks like an invoice or receipt (6), has 24x7 helpline (4), tells about the services and security features (3), small and realistic amount of money (2), and no typos in the e-mail (1).

E-mail 3

This e-mail was a legitimate bank statement indicating the availability of the credit card statement. 26 respondents did not identify the e-mail and also did not specify the indicators. Out of the participants who answered the question, 72.3% correctly identified this e-mail as a legitimate e-mail, 15.3% incorrectly identified the e-mail as scam, and 12.4% of the respondents were unsure (see Table 2). 56 respondents indicated whether the e-mail was a scam or not, but did not specify the indicators they used for the e-mail identification, while 42 respondents replied with irrelevant answers.

Respondents who identified the e-mail correctly as a legitimate e-mail specified the following indicators: not asking for information or money (26), includes name and account number (7), is a bank statement (7), has copyright, policy, privacy, and security link at bottom (7), to update information need to log into account on bank website (5), HSBC is a trusted source (4), requests not sending confidential information over e-mail (2), and allows to opt out of e-mail (1).

Respondents who identified the e-mail incorrectly as a scam specified the following indicators: in-line ad (4), inconsistencies with Orchard bank being in California and HSBC bank in Nevada (3), links in the e-mail (2), http links hidden (1), unprofessional e-mail (1), and mbeair and Kevin Beair don't match (1).

E-mail 4

This e-mail was a legitimate auto insurance policy renewal reminder. 31 respondents did not identify the e-mail as scam or not scam and also did not specify the indicators. Out of the participants who answered the question, 75% correctly identified this e-mail as a legitimate e-mail, 10.6% incorrectly identified the e-mail as scam, and 14.4% respondents were unsure (see Table 2). 59 respondents indicated whether the e-mail was a scam or not, but did not specify the indicators they used for the e-mail identification, while 44 respondents replied with irrelevant answers.

Respondents who identified the e-mail correctly as a legitimate e-mail specified the following indicators: Progressive is a trusted and reputable company (15), not asking for personal information (11), telephone number provided to contact the organization directly (7), is just a standard renewal invoice (6), has personal identifiable information such as name, policy number, years been with the company (4), sends to company website for payment and information (4), looks official and has trademark logo (4), and doesn't receive reply e-mails (3).

Respondents who identified the e-mail incorrectly as a scam specified the following indicators: wants money and personal information (3), an e-bill is usually sent via paper mail and needs to be in depth (1), bad language and ugly format (1), gives a deadline (1), totals not adding up (1), doesn't receive reply messages (1), and billing renewal 7.2 (1).

In all the four e-mails, the most common indicators used by the respondents to identify the given e-mail as scam in descending order were:

- requesting personal
- confidential and financial information
- giving away large sum of money

- embedded links asking to log into account
- sender credentials
- generic e-mail format.

These indicators were used to identify and differentiate between scam and legitimate e-mail, thus supporting the second hypothesis.

5.3 Research Question 3: How many of the self-reported respondents indicating the ability to identify scam e-mail, can correctly identify the given e-mails?

Hypothesis 3: More that 50% of the self-reported respondents indicating the ability to identify scam e-mail will not be able to identify the given e-mails.

This research question was included to see if the users' confidence in their ability to identify mail scams translates to actually identifying scam e-mails from legitimate e-mails. Researchers decided on 50% in the hypothesis based on prior research by Shannon and Bennett (2011), where 80.7% of the respondents were able to identify at least one suspicious item, and 7.3% were able to identify at least two suspicious items in the given scam e-mail. A very low number of respondents were able to identify two suspicious items compared to respondents identifying one suspicious item. A study conducted by Ballantine, McCourt Larres, and Oyelere (2007) suggests a tendency among students to over-estimate their computer competency irrespective of computer experience. Based on these prior findings, researchers believed that a low percentage of self-reported respondents would be able to identify the given e-mails satisfactorily and decided on 50% as being an appropriate number to test the hypothesis.

As stated earlier, four e-mails (two scam e-mails, and two legitimate e-mails) were included in the questionnaire. The participants identified these e-mails as "scam", "not scam", or "unsure". Participants who were correctly able to identify three or more e-mails were awarded a "Pass", while the remaining participants were awarded a "Fail". 35.5% of the respondents failed to identify e-mail scams and 64.5% of the respondents were able to identify e-mail scams. 1.7% of the respondents correctly identified all four e-mails, 62.8% of the respondents correctly identified three e-mails, 24.8% of the respondents correctly identified two e-mails, 9.9% correctly identified one e-mail, and 0.8% did not identify any e-mails correctly (see Appendix A, Table 6).

E-mail 1

Of the respondents who specified that they are able to identify e-mail scams, 100% were able to identify E-mail 1 as a scam mail (see Appendix A, Table 7).

E-mail 2

7.4% of the respondents who specified that they were able to identify e-mail scam were able to identify E-mail 2 as a scam. 82.7% of the respondents identified this e-mail as not scam, and 9.9% were unsure about this e-mail (see Appendix A, Table 7).

E-mail 3

73.5% of the respondents who specified that they were able to identify e-mail scam were able to identify E-mail 3 as a legitimate e-mail. While 18.1% of the respondents identified this e-mail as a scam, and 8.4% of the respondents were unsure about this e-mail (see Appendix A, Table 7).

E-mail 4

81% of the respondents who specified that they were able to identify e-mail scams were able to identify E-mail 4 as a legitimate e-mail, while 6.3% of the respondents identified this e-mail incorrectly as a scam. 12.7% of the respondents were unsure about this e-mail (see Appendix A, Table 7).

On the whole, 67.1% of the respondents who mentioned that they were able to identify e-mail scams scored a "Pass", and 32.9% scored a "Fail" (see Table 3), thus the third hypothesis was not supported.

Table 3 Frequency of the Respondents That Indicated Ability to Identify Scam E-Mail

		Frequency	Percent	Valid Percent
Valid	Fail	24	25.0	32.9
	Pass	49	51.0	67.1
	Total	73	76.0	100.0
Missing	System	23	24.0	
Total		96	100.0	

6. DISCUSSION

95.1% respondents indicated that they are aware of e-mail scams. 59.3% respondents indicated that they are able to identify scam e-mail while 37% indicated that they are unsure if they are able to identify scam e-mail. 68.8% respondents replied that they are aware of common practices of identifying e-mail scam. 88.7% respondents mentioned that they have received scam e-mail while only 9.5% were ever victimized by the scam e-mail. These respondents who were victimized by an e-mail scam specified taking the following actions after falling for the e-mail scam: delete and/or mark the e-mail as spam and to block the sender, update and use a anti-virus program, change the password and/or e-mail address, and to report it to the authorities. 10.1% of the respondents replied that they have never received an e-mail scam. This could be due to the use of stringent spam protection, extremely low usage of e-mail, or inability in identifying scam e-mail.

Among the factors that influence a user's ability in e-mail scam detection, *frequency of e-mail usage* was found to be the only factor that influences e-mail scam detection (p = 0.041, d = 1). Interestingly, *awareness of e-mail scam*, and *awareness of common practices to identify e-mail scam* did not influence a user's ability to detect e-mail scam. This is inconsistent with the findings of Wang et al. who found that knowledge of scam made users less susceptible to e-mail scam. Among the four e-mails that the respondents were asked to identify as a scam or legitimate e-mail, only 1.7% of the respondents were able to identify all four e-mails correctly. 64.5% of the respondents received a *Pass* with 75% correct identification of the given four e-mails. After receiving a scam e-mail, 73.1% of the respondents tended to delete/ignore the e-mail. Among the respondents who indicated that they are able to identify scam e-mail, 67.1% of the respondents received a *Pass* with 75% or more correct identification of the given four e-mails, while 32.9% of respondents received a *Fail* with less than 75% correct identification of the given four e-mails.

While trying to identify e-mail scams, users tend to trust in the legitimacy of e-mail sent from reputed company names. This can be seen in the second e-mail that the respondents were supposed to identify. The e-mail seemed to originate from Vonage and only 12.5% of the respondents were correctly able to identify the e-mail as scam while 77.2% of the respondents incorrectly identified the e-mail as legitimate e-mail. The respondents also showed faith in the validity of the third and fourth e-mail by identifying the e-mails as legitimate and specifying *originating from a reputed company* as one of the reasons. This could result in people becoming a victim of e-mail scam that use Context-Aware Phishing Attacks, (i.e., fraudsters replicating e-mails from legitimate businesses). Users look for presence of the following in e-mail content as key indicators for the detection of e-mail scam: asking for information, involvement of money, and hyperlinks.

7. LIMITATIONS

Given the exploratory nature of the research, a reliability test for the survey was not deemed necessary. As no compensation was provided to the participants, the researchers assume that participants filled out the survey because they wanted to contribute towards an ongoing study. This resulted in a 72 participants not filling out the survey to completeness. Another limitation to this study was that it was conducted on a university campus because of which the sample was restricted to undergraduate or graduate students in the age group of 18-30 years. This study should be repeated over time, with a wider population from varied age groups. The e-mails were also presented on paper rather than in an e-mail inbox, and the participants were not easily able to research if the given e-mail was a scam or was a legitimate e-mail.

8. CONCLUSIONS

This study provides an understanding on different types of variables that influence users in identifying e-mails as scam and legitimate. It also gives an insight about the various indicators that users rely upon while identifying scam e-mail. Studies have found that intervention could increase phishing detection among individuals through the use of a training e-mail system (Dodge, Coronges, & Rovira, 2012; Kumaraguru, Rhee, Acquisti, Cranor, & Hong, 2007). Phishing prevention training is essential along with phishing software (Saberi, Vahidi & Bidgoli, 2007). The finding of this study could be used in developing an intervention program to detect scam e-mail from legitimate e-mail. As scam e-mails become more sophisticated, businesses can also use this study to educate their employees in identifying e-mail scams and following common precautionary practices such as never clicking on a link within an unknown e-mail, or never disclosing personal information when asked in an unknown e-mail. Following this practice will help businesses in preventing their employees from falling victim to e-mail scam and possible monetary loss. Many people receive e-mails from their banks or other businesses that fraudsters try to replicate (Context-Aware Phishing Attacks). It is important that businesses follow best e-mail practices so that customers can identify scams when they appear in their inbox.

REFERENCES

Ballantine, J. A., McCourt Larres, P., & Oyelere, P. (2007). Computer usage and the validity of self assessed computer competence among first-year business students. *Computers & Education*, *49*(4), 976-990.

Cisco (2013). Cisco IronPort SenderBase Security Network. Retrieved from http://www.senderbase.org/home/detail_spam_volume

comScore (2013). ComScore reports retail e-commerce sales reached $49.8 in 2Q. Retrieved from http://marketingland.com/things-are-looking-good-in-e-commerce-comscore-reports-49-8-billion-in-55264

Cornell University Law School (n.d.). CAN-SPAM Act of 2003: Core requirements. Retrieved from http://www.law.cornell.edu/wex/inbox/can-spam_act_core_requirements

Dodge, R., Coronges, K., & Rovira, E. (2012). Empirical Benefits of Training to Phishing Susceptibility. *IFIP Advances in Information and Communication Technology*, *376*, 457-464.

EMC$^{2.}$ (2012). RSA Online Fraud Resource Center. Retrieved from http://www.emc.com/emc-plus/rsa-thought-leadership/online-fraud/index.htm

FBI (Producer). (2010). Organized Crime. Federal Bureau of Investigation. Retrieved from http://www.fbi.gov/hq/cid/orgcrime/aboutocs.htm

Freiermuth, Mark. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse and Communication, 5*, 123-125. Doi: 10.1177/1750481310395448

Jakobsson, M. Tsow, A., Shah, A., Blevis, E., & Lim, Y. (2007). What instills trust? A qualitative study of phishing. *Financial Cryptography and Data Security, 4866*, 356-361.

Kaspersky. (2013). Kaspersky Lab report: 37.3 million users experienced phishing attacks in the last year. Retrieved from http://www.kaspersky.com/about/news/press/2013/Kaspersky_Lab_report_37_3_million_users_experienced_phishing_attacks_in_the_last_year

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L., Hong, J., & Nunge, E. (2007). Protecting People from Phishing: The design and evaluation of an embedded training email system. *Human-Computer Interaction Institute*, 63.

NACHA. (2012). ACH network statistics. Retrieved from https://www.nacha.org/ACHntwkstats

Office of Attorney General, California (n.d.). Look-alike spam mail keeps surfacing: Don't fall victim to identity thieves. Retrieved from http://oag.ca.gov/consumers/general/spam_phishing

Ragucci, J., & Robila, S. (2006). Societal Aspects of Phishing. *IEEE, 1-5*. Doi: 10.1109/ISTAS.2006.4375893

Saberi, A., Vahidi, M., & Bidgoli, B.M. (2007). Learn to Detect Phishing Scams Using Learning and Ensemble Methods. *IEEE*, 311-314. Doi: 10.1109/WI-IATW.2007.79

Securelist. (2013). Spam in March 2013. Retrieved from http://www.securelist.com/en/analysis/204792289/Spam_in_March_2013

Shannon, L., & Bennett, J. (2011). A case study: Applying critical thinking skills to computer science and technology. *Information Systems Educators Conference*, 28.

The Spamhaus Project. (2012). The definition of spam. Retrieved from http://www.spamhaus.org/consumer/definition/

Trustwave. (2013). Spam statistics. Retrieved from https://www.trustwave.com/support/labs/spam_statistics.asp

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Phishing Susceptibility: an investigation into the processing of a targeted spear phishing email. *Professional Communication, IEEE Transactions*, 99. Doi: 10.1109/TPC.2012.2208392

Windstream. (2012). Internet Threats. Retrieved from https://windstream.custhelp.com/app/answers/detail/a_id/212/~/types-of-internet-threats

APPENDICES

Appendix A: Tables

Table 1 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 2 Frequency of e-mail usage, awareness of e-mail scam, ability to identify e-mail scam, and awareness of common practices to identify e-mail scam

		Frequency	Valid Percent
E-mail usage	Hourly	77	47.2
	Daily	80	49.1
	Weekly	6	3.7
	Total	163	100.0
Aware of e-mail scams	Yes	155	95.1
	No	8	4.9
	Total	163	100.0
Ability to identify e-mail scam	Yes	96	59.3
	No	6	3.7
	Maybe/Unsure	60	37.0
	Total	162	100.0
Awareness of common practices to identify e-mail scam	Yes	86	68.8
	No	36	28.8
	Unsure	3	2.4
	Total	125	100.0

Table 3 Frequency of receipt of scam e-mail, and e-mail scam victimization

		Frequency	Valid Percent
Ever received scam e-mail	Yes	141	88.7
	No	16	10.1
	Unsure	2	1.3
	Total	159	100.0
E-mail scam victimization	Yes	15	9.5
	No	143	90.5
	Total	158	100.0

Table 4 Frequency of actions taken after receiving a scam e-mail

	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 5 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

Table 6 Frequency of respondent's score in identifying e-mail scam, and respondent's scam identification results

	Number of identified e-mails	Frequency	Valid Percent
Scam identification score	4	2	1.7
	3	76	62.8
	2	30	24.8
	1	12	9.9
	0	1	0.8
	Total	121	100.0
Scam identification results	Pass	78	64.5
	Fail	43	35.5
	Total	121	100.0

Table 7 Identification of e-mails as scam or legitimate e-mail by respondents claiming to be able to identify scam e-mails

		Frequency	Valid Percent
E-mail 1	Correct Identification	87	100.0
	Total	87	100.0
E-mail 2	Correct Identification	6	7.4
	Incorrect Identification	67	82.7
	Unsure	8	9.9
	Total	81	100.0
E-mail 3	Correct Identification	61	73.5
	Incorrect Identification	15	18.1
	Unsure	7	8.4
	Total	83	100.0
E-mail 4	Correct Identification	64	81.0
	Incorrect Identification	5	6.3
	Unsure	10	12.7
	Total	96	100.0

Appendix B: Pearson 2-Tailed Correlation table

	Age	Gender	Email Frequency	Aware of Email Scam	Can ID Email Scam	Aware of Common Practices	Received Email Scam	Actions Taken	Been Scam Victim	Other Scam Media Awareness
Age	1	.109	-.160	-.070	-.002	-.050	-.107	**.223**	-.093	-.020
Gender	109	1	-.083	.090	-.052	-.110	-.140	.051	.146	-.183
Email Frequency	-.160	-.083	1	.175	**.231**	**.289**	.028	-.041	-.063	.086
Aware of Email Scam	-.070	.090	.175	1	**.208**	**.214**	.156	-.118	-.024	**.327**
Can ID Email Scam	-.002	-.052	.231	.208	1	**.373**	.116	-.067	.011	.189
Aware of Common Practices	-.050	-.110	.289	.214	.373	1	.055	-.167	.002	**.399**
Received Email Scam	-.107	-.140	.028	.156	.116	.055	1	-.127	.108	.084
Actions Taken	.223	.051	-.041	-.118	-.067	-.167	-.127	1	.030	**-.243**
Been Scam Victim	-.093	.146	-.063	-.024	.011	.002	.108	.030	1	-.027
Other Scam Media Awareness	-.020	-.183	.086	.327	.189	.399	.084	-.243	-.027	1

Appendix C: Survey

Email and Scams

This is a voluntary and anonymous survey that aims at understanding the awareness of email scams. No personal information will be asked if you decide to participate in the study. The information gathered in this survey will be kept confidential. If any of the questions make you uncomfortable, you may skip them or withdraw from the survey. You may withdraw from taking the survey at any point in time without any consequences.

The team would like to thank you in advance for participating in this study.

Survey Questionnaire

1. Please specify you age (Please circle the option that applies)
    a. 18-30
    b. 31-45
    c. 46-65
    d. 65 and above
2. Please specify you gender (Please circle the option that applies)
    a. Male
    b. Female
3. How often do you use emails? (Please circle the option that applies)
        a. Hourly
        b. Daily
        c. Weekly
        d. Biweekly
        e. Never
4. Are you aware that emails can be a potential scamming medium? (Please circle the option that applies)
    a. Yes
    b. No
5. If you receive an email scam, can you identify it? (Please circle the option that applies)
    a. Yes
    b. Maybe
    c. No
6. Are you aware of common practices to identify scams? If yes, please specify. (Please ask for extra paper if you need more space)
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
7. Have you ever received a scam email? (Please circle the option that applies)
    a. Yes
    b. No

8. If you receive an email that looks like a scam, what are the likely actions you would take? (Circle all that apply)
    a. Research online if the mail is a scam
    b. Delete it/ Ignore it
    c. Report it to authorities
    d. Click on the links in the email
    e. None of the above
9. Have you ever been a victim of an email scam? If yes please specify the actions that were taken. (Please circle the option that applies)
    a. Yes
    b. No
    Specify:
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
10. If you ever fall for a financial email scam or clicked on a malicious link contained within the email, what actions will you take? If unsure, please state so. (Please ask for extra paper if you need more space)
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
    ____
11. Are you aware of other types of online scam medium other than email? If so, please specify. (Please ask for extra paper if you need more space)
    ____
    ____
    ____
    ____
    ____
    ____
    ____

____
____
____
____

12. Below are four sample emails. Please read through them and identify if it is a scam or not. Please explain the indicators that lead you to this conclusion.

____
____
____
____
____
____
____
____
____
____

Email # 1

Lagos, Nigeria. Attention: The President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce And Industry, I have the privilege to request your assistance to transfer the sum of $47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank.

We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

(a) your banker's name, telephone, account and fax numbers.

(b) your private telephone and fax numbers —for confidentiality and easy communication.

(c) your letter-headed paper stamped and signed.

Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

Best regards

Howgul Abul Arhu

Please write your response here (Please ask for extra paper if you need more space):

____

____

____

____

____

____

Email # 2

Dear VONAGE Customer,

Thank you for choosing Vonage, the award winning Internet phone company. This email is to notify you that we have successfully processed the billing transaction for your Vonage account in the amount listed below.

Date Processed: 10/01/2009

Amount: $16.80

A detailed online invoice is available through your Vonage Online Account. Vonage provides you with an online account available to you anytime, anywhere. Get the most of your Vonage service by logging on to https://secure.vonage.com /webaccount/ . Check real-time call activity; review your billing information and access an extensive set of Vonage features such as: Call Forwarding, SimulRing, Network Availability and Voicemail Plus. You can also print your invoice or edit your payment information.

We are looking out for you! For your protection checking and credit card information should not be submitted through email. You can easily update your payment information through your Vonage Online Account. Get there fast, click here: https://secure.vonage.com/webaccount/.

For a complete explanation on how to read your online invoice, please visit: http://vonage.com/help.php?article=1250&category=65&nav=6.

Vonage FEATURE FOCUS...

Vonage Voicemail Plus Did you know that you can access your voicemail in 3 easy ways - Phone, Web or Email, all at no extra charge? For quick access simply dial *123 from your Vonage phone. Or login to your Online Account. You can also receive your voicemail as email attachments. We'll get you through the basics and a lot more. Simply click here: http://vonage.com/help.php?keyword=VoicemailPlusBasics.

This email was sent from a mailbox that does not accept replies. To send us an email, please visit our Contact Us page.

If you have any questions, Ask Vonage is here to assist you! Ask Vonage is your Virtual Customer Service Agent available 24 hours a day, 7 days a week. You can ask any questions you have about Vonage. Just click on the link below and type in your question.

http://www.vonage.com/help.php?keyword=AskVonage&forum=1&

refer_id=WEBPO070501003W1

Thanks again for choosing Vonage!

Sincerely,

Vonage Customer Care

Please write your response here (Please ask for extra paper if you need more space):

____

____

____

____

____

____

____

Email # 3

Account Alert: Statement Available

Dear Kevin Beair,

As requested, we're writing to let you know that your most recent Orchard Bank Credit Card statement is now available online at orchardbank.com.

Log in to Online Account Access to conveniently:

View or print your Paperless Statement
Make a secure payment
Update email Account Alerts
Contact us with questions

Sincerely,
Orchard Bank Credit Card Customer Care

Monitor and maximize your personal credit score.
Get your report now

Email Security Information
Email intended for: Kevin Beair
For your account ending in: 0992

To ensure delivery to your inbox, add **orchardbank@ebusiness.orchardbank.com** to your address book.

ABOUT THIS MESSAGE
This email was sent to MBEAIR@GMAIL.COM
for Account number ending in 0992.

You are receiving this recurring email alert because you registered online at orchardbank.com and elected to receive email alerts about your Orchard Bank Credit Card Account.

If you do not wish to receive future email alerts about your Orchard Bank Credit Card Account, please log in and update your email preferences at orchardbank.com.

We maintain strict security standards and procedures to prevent unauthorized access to information about you. HSBC Bank Nevada, N.A. will never contact you by email or otherwise to ask you to validate personal information such as your Login ID, password or account numbers. If you receive such a request please notify us or call the number listed on the back of your card.

Orchard Bank Credit Card Correspondence

1441 Schilling Place
Salinas, CA 93912

Copyright. HSBC Card Services 2011. All rights reserved.

Privacy and Security | Terms of Use | Link Policy

Please write your response here (Please ask for extra paper if you need more space):

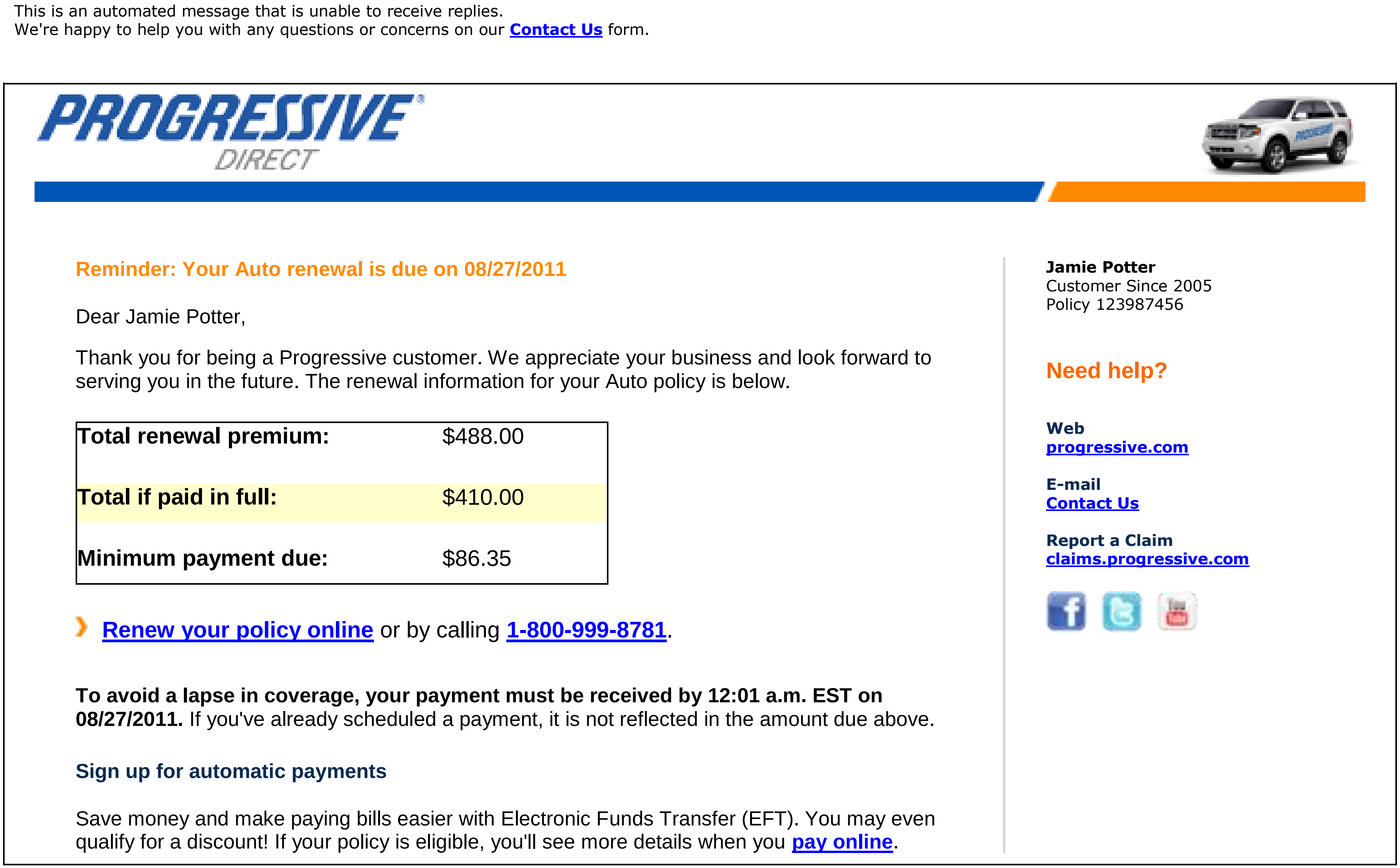
____

____

____

____

Email # 4



This is an automated message that is unable to receive replies.
We're happy to help you with any questions or concerns on our **Contact Us** form.

Reminder: Your Auto renewal is due on 08/27/2011

Dear Jamie Potter,

Thank you for being a Progressive customer. We appreciate your business and look forward to serving you in the future. The renewal information for your Auto policy is below.

Total renewal premium:	$488.00
Total if paid in full:	$410.00
Minimum payment due:	$86.35

› Renew your policy online or by calling 1-800-999-8781.

To avoid a lapse in coverage, your payment must be received by 12:01 a.m. EST on 08/27/2011. If you've already scheduled a payment, it is not reflected in the amount due above.

Sign up for automatic payments

Save money and make paying bills easier with Electronic Funds Transfer (EFT). You may even qualify for a discount! If your policy is eligible, you'll see more details when you pay online.

Jamie Potter
Customer Since 2005
Policy 123987456

Need help?

Web
progressive.com

E-mail
Contact Us

Report a Claim
claims.progressive.com

View Your Policy / **Make a Payment** / **Update Your Preferences** / **Privacy Policy**

Policy underwritten by Progressive Paloverde Insurance Co

Progressive Direct Insurance Company
6300 Wilson Mills Rd, Mayfield Village, Ohio 44143

Billing_Renewal_7.2

Please write your response here (Please ask for extra paper if you need more space):

____

____

____

____