Phishing During and After Disaster: Hurricane Harvey

Rakesh Verma
Department of Computer Science
University of Houston
Houston, Texas 77204–3015
Email: rverma@uh.edu

Devin Crane
Department of Computer Science
University of Houston
Houston, Texas 77204–3015
Email: devin.crane@gmail.com

Omprakash Gnawali
Department of Computer Science
University of Houston
Houston, Texas 77204–3015
Email: gnawali@cs.uh.edu

Abstract— **Hurricane Harvey was a major disaster that struck Texas in August 2017. We wondered whether such disasters are being exploited by phishers, as phishing is one of the most popular attacks. In October 2017, we surveyed the University of Houston population to study their experiences and behavior during/after the storm. Over 300 responses were received. This paper discusses our study design and the results from that survey. Results show that the storm did cause about 6.3% of the participants *to change their behavior*, i.e., they clicked on links or downloaded attachments they normally would NOT have. An analysis using the symmetric Jensen-Shannon divergence shows that the increased email volume and the timing of arrival or non-arrival of hurricane-related spam had the biggest impacts.**

Index Terms— **Phishing, disaster, hurricane, Harvey, survey, user study, statistical analysis, Cronbach alpha, Jensen-Shannon divergence, association analysis**

I. Introduction

Hurricane Harvey was a major storm ("100 or 500 year event") that stalled over Texas during Fall 2017. In a few days, it dumped rainfall amounting to the annual precipitation for Greater Houston. Schools, colleges, government agencies (except emergency departments and workers), and most businesses were closed during the storm. There were reports of electrical outages ranging from a few days to couple of weeks. Such an unprecedented disaster can lead to more criminal behavior. For example, this was reported after Katrina hit New Orleans. Some of it was just people looking for food and shelter, but some looting did take place after the storm. We found some Katrina related scams at https://www.scambusters.org/hurricanekatrinascams.html. One example is in the Appendix.

With the US now an Internet-based economy, and with phishing being a major bane, we wondered whether cyber crime, more specifically phishing attacks, increased during this stressful period.[1,2] In addition to the change in phishing attacks during and immediately after the storm, we also wanted to find out whether people responded differently to attacks, e.g., under stress. A final goal was to find whether there were any new types of phishing attacks.

With these goals, we decided to conduct a within-subjects study of University of Houston (UH) employees and students. An application was submitted to the UH IRB committee, which was approved in October 2017. An email, containing a link to the survey, was sent via official channels to the entire UH population with university or other registered email addresses. We discuss some related work in Section II. We discuss the design of the survey in Section I and the results in Sections IV and VI. In Section V we provide a statistical analysis of our survey and results. Section VII concludes the paper. A brief Appendix provides context and some examples.

We had also contacted the IT departments of several universities and colleges in the hurricane-affected area, to determine the change in phishing attacks from their perspective, but only two responded to our requests. The two that responded did not have either the time or the resources to help with our study.

II. Related Work

Phishing is a well-studied problem with at least one book [5] and over 760[3] research papers on various aspects including its taxonomy, detection methods, user education and studies. In this paper, we point the reader to the following sources, and the references cited therein, for understanding phishing. For a taxonomy of phishing, see [1], for phishing detection on emails, see [17], [15], [13], [4], [11], for phishing website detection, see [9], [10], and for phishing website detection through URL analysis, see [14], [12], [8]. Since phishing is a part of the cyber security field, one should keep in mind the unique needs of this domain [16]. Phishing may also be considered a form of email masquerade attack, on which the reader should consult [2].

However, despite the above research on phishing, to our knowledge, this study is the first of its kind. In May 2018, a search of DBLP with queries: scam disaster, scam hurricane, phish disaster, phish hurricane, spam hurricane and spam disaster, yielded just one relevant result [7], which analyzed Twitter spam. On 20 July 2018, these queries were repeated and new queries were added: earthquake scam, earthquake spam, earthquake phish, tsunami scam, tsunami spam, tsunami phish, flood spam, flood scan and flood phish. Two additional

[1] We did find a few reports, e.g., https://blog.appriver.com/2017/08/first-harvey-scam-email-appears/

[2] https://www.buzzfeed.com/mbvd/false-information-about-texas-storm?utm_term=.uwxwdxR0#.ow5NZ4pM

[3] DBLP query 'phish' on 12 July 2018

results were obtained: one on “flooding attacks and spam over IP telephony” and another by Jason Flood on comparing malware and phishing attacks. The queries were repeated on Google Scholar in May 2018 and 20 July 2018 with *allintitle* option and no other relevant papers were found. There were quite a few papers and patents on detection and stopping spam flood(s) and one on a spam tsunami wiping out a website.

III. The Survey Design in Detail

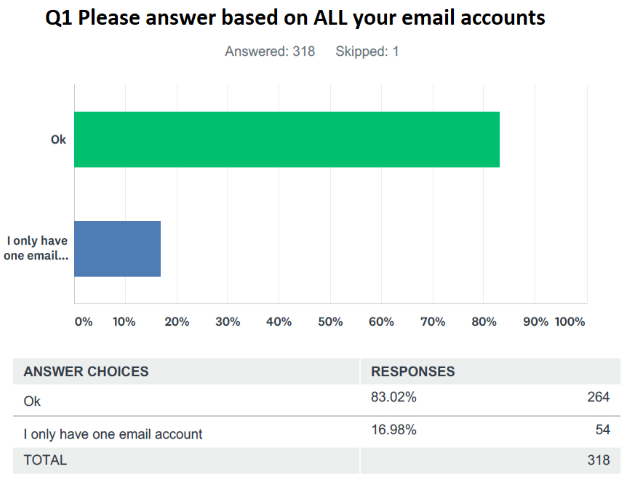
The first page of the survey gave information about the survey and asked for informed consent. There were 10 questions/requests for information, in a somewhat random order, on the following pages. They are listed in Table I. Note that spam was used as a proxy for both spam and phishing attacks on this survey, although technically they are different attacks. No money, nor any other incentives, were offered for taking the survey. Questions 1, 3 and 7 had two choices each. The remaining questions, Questions 2, 4-6, 8-9 had three to five responses each, with each of them having an “Other” option. For this option, a text field was provided that asked for more information (“please specify”). For question 10, we provided an email address for participants to forward us the attack emails relating to Hurricane Harvey. Question 7 is linked to the change in behavior goal, Questions 2 and 5 are linked to the change in environment and disruption, Questions 6, 8 and 9 try to quantify the change in attacks and new types of attacks. Question 4 considers timing of attacks. Question 3 checks whether participants had access.

TABLE I
The Hurricane Harvey Spam Survey

No.	Question/Request
1.	Please answer based on ALL your email accounts
2.	How badly were you affected by Harvey?
3.	Did you have Internet or some other access to your email during the hurricane?
4.	When did you get any spam regarding the hurricane (select all that apply)?
5.	Did your environment change in which you normally access your email (select all that apply)?
6.	Did the amount of email you received change?
7.	Did you click on any emails/links or download any attachments that you normally would not have?
8.	What kinds of attacks did you notice more or less of, i.e. donations, encouragement to click on links, or provide financial information, etc. (select all that apply)?
9.	Were there new examples of attacks that you haven’t seen before?
10.	If you have any emails - from ANY email account - regarding Hurricane Harvey, please send them to x@y.com, with the full header if possible. Find instructions here. Also be sure to remove/black out your email address before sending.

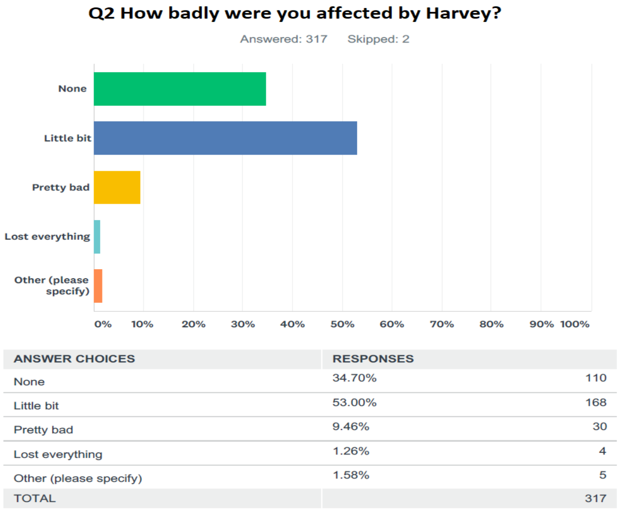
IV. Results from the Survey

A total of 319 people took the survey over Nov-Dec 2017. Figure 1 shows results for Question 1. Only one person skipped this question. We see that 17% of the respondents had only one email account and the rest agreed to provide answers based on ALL their email accounts. Note that the percentages on each question are out of the participants who did not skip the question.



ANSWER CHOICES	RESPONSES	
Ok	83.02%	264
I only have one email account	16.98%	54
TOTAL		318

Fig. 1. Responses for Question 1



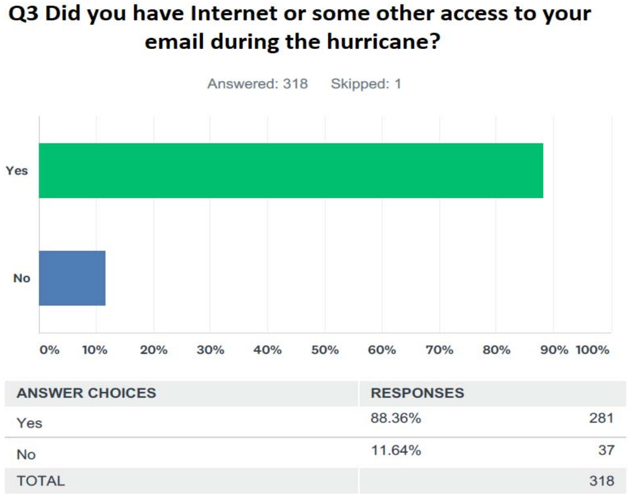
ANSWER CHOICES	RESPONSES	
None	34.70%	110
Little bit	53.00%	168
Pretty bad	9.46%	30
Lost everything	1.26%	4
Other (please specify)	1.58%	5
TOTAL		317

Fig. 2. Responses for Question 2

Question 2 had five possible responses, including an “Other (please specify)” option. Figure 2 shows that only five respondents (1.6%) took this option. Of the remaining participants four (1.3%) lost everything, 30 (9.5%) were pretty badly affected, 168 (53%) were affected a little and 110 (34.7%) were unaffected. The question was skipped by two people. We elaborate on the responses for the Other option in Section **??**. Most participants (87.7%) were not severely affected, which is consistent with a report by Greater Houston Partnership (“approximately 7% of housing Units were impacted”) [6].

Consistent with responses for Question 2, Figure 3 shows that 281 participants (88.4%) had access to email during the hurricane and 37 (11.6%) people did not have email access, with one participant skipping the question.

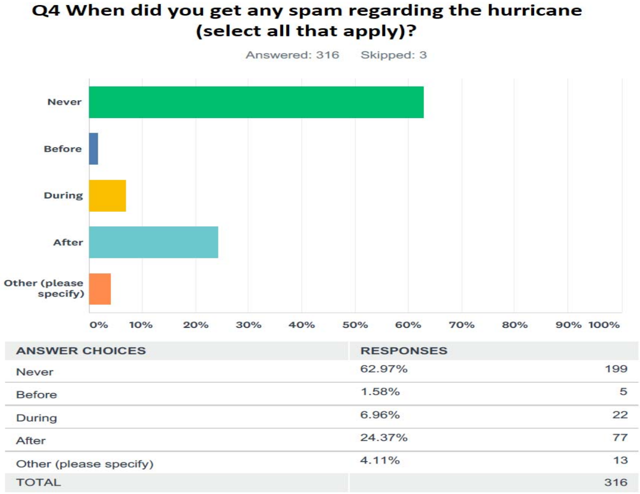
Question 4 again had an Other (please specify) option. This time 13 (4.1%) participants chose this option and three skipped


Q3 Did you have Internet or some other access to your email during the hurricane?

Answered: 318 Skipped: 1

ANSWER CHOICES	RESPONSES	
Yes	88.36%	281
No	11.64%	37
TOTAL		318

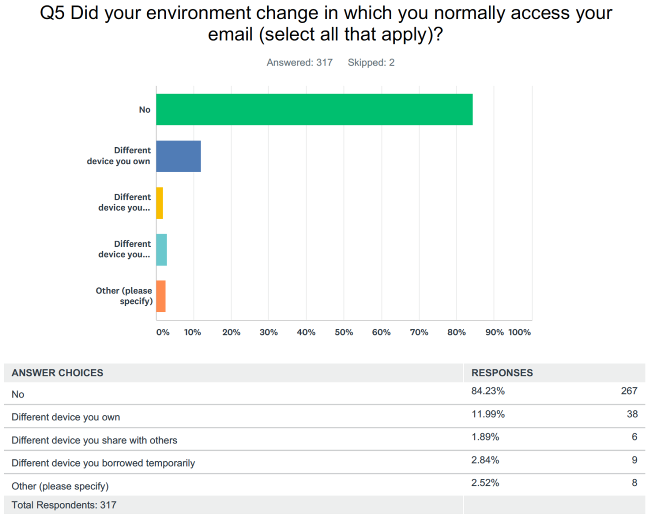
Fig. 3. Responses for Question 3


Q4 When did you get any spam regarding the hurricane (select all that apply)?

Answered: 316 Skipped: 3

ANSWER CHOICES	RESPONSES	
Never	62.97%	199
Before	1.58%	5
During	6.96%	22
After	24.37%	77
Other (please specify)	4.11%	13
TOTAL		316

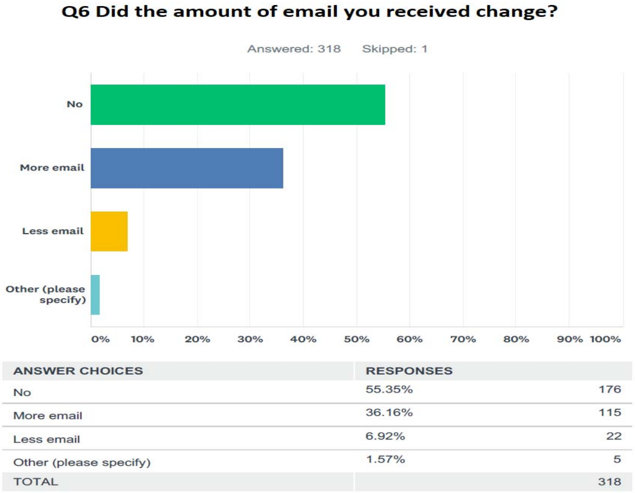
Fig. 4. Responses for Question 4


Q5 Did your environment change in which you normally access your email (select all that apply)?

Answered: 317 Skipped: 2

ANSWER CHOICES	RESPONSES	
No	84.23%	267
Different device you own	11.99%	38
Different device you share with others	1.89%	6
Different device you borrowed temporarily	2.84%	9
Other (please specify)	2.52%	8
Total Respondents: 317		

Fig. 5. Responses for Question 5


Q6 Did the amount of email you received change?

Answered: 318 Skipped: 1

ANSWER CHOICES	RESPONSES	
No	55.35%	176
More email	36.16%	115
Less email	6.92%	22
Other (please specify)	1.57%	5
TOTAL		318

Fig. 6. Responses for Question 6

the question. The majority of the participants, 199 or 63.0%, did not get any spam regarding the hurricane. Of the remaining participants who answered the question, five (1.6%) reported getting hurricane-related spam *before* the survey, 22 (7.00%) during the hurricane and 77 (24.4%) after the hurricane. Thus we see a trend towards exploitation after the event.

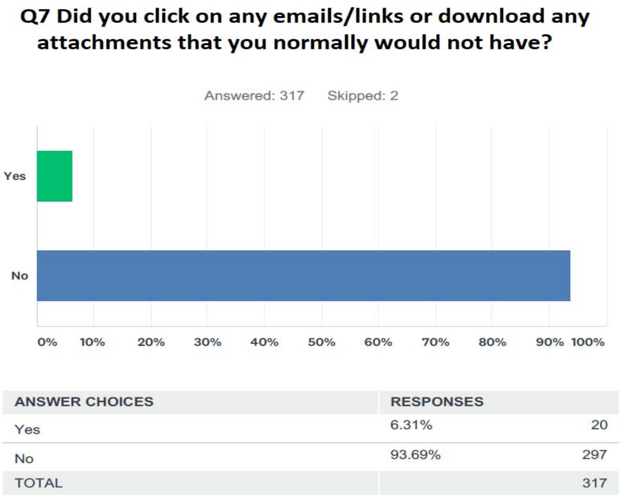
Question 5 looks at the change in the way participants accessed their email. This was a “Select all that apply” question so numbers may not add up to 319.[4] It also include an “Other (please specify)” option. Two people skipped this question. Of the remaining 317 respondents, the overwhelming majority, 267 or 84.2% of participants incurred no change in how they accessed their email. Of the people who incurred some disruption in their normal email access, we find that most people, 38 or 12.0%, switched to a different device they own, six switched to different device they shared with others, and nine switched to a borrowed device. Again, we see that most of the participants did not face significant disruptions.

Question 6 examined the change in the amount of email received. Here a narrower majority, 176 or 55.4%, did not report any change in the amount of email received. More email was reported by 115 or 36.2%, less email was reported by 22 or 6.9% and the Other option was chosen by 5 or 1.6%. One person skipped this question.

Question 7 looked at change in behavior of the participants. Interestingly, 20 (6.3%) out of the 317 participants, who answered this question, admitted to either clicking on links or downloading attachments, which they would not have done ordinarily. Only 2 participants skipped this question. This percentage becomes even more significant, when we recall that most of our participants were not “significantly affected” by the storm, nor did they face any significant disruptions.

Question 8 asked participants about the kinds of attacks that

[4] This time we omit the question to make the figure larger, since it is wordy.

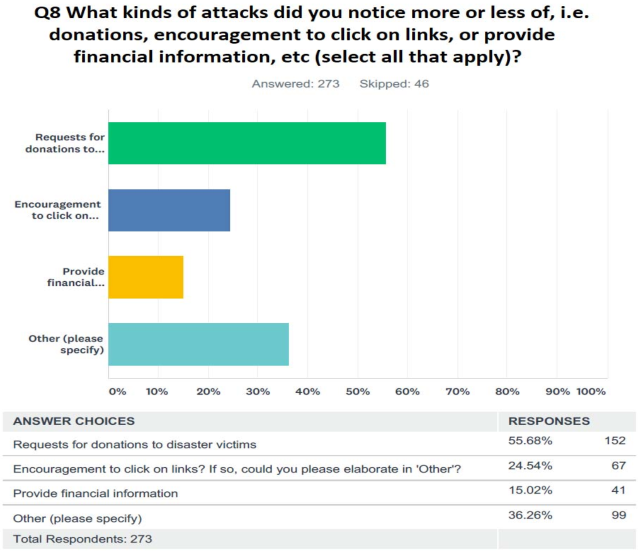


Q7 Did you click on any emails/links or download any attachments that you normally would not have?

Answered: 317 Skipped: 2

ANSWER CHOICES	RESPONSES	
Yes	6.31%	20
No	93.69%	297
TOTAL		317

Fig. 7. Responses for Question 7



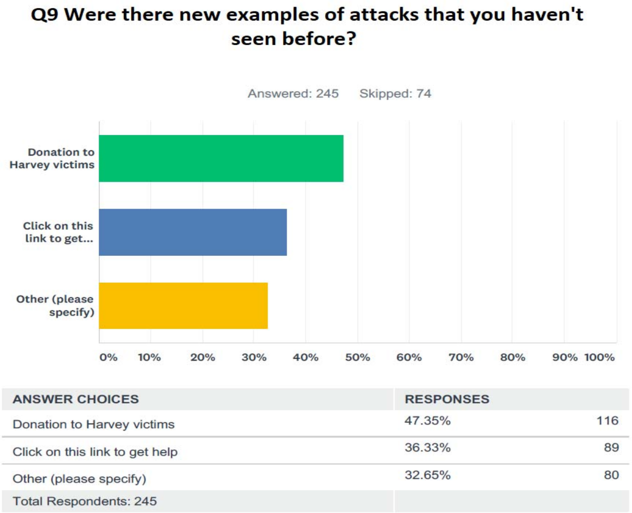
Q8 What kinds of attacks did you notice more or less of, i.e. donations, encouragement to click on links, or provide financial information, etc (select all that apply)?

Answered: 273 Skipped: 46

ANSWER CHOICES	RESPONSES	
Requests for donations to disaster victims	55.68%	152
Encouragement to click on links? If so, could you please elaborate in 'Other'?	24.54%	67
Provide financial information	15.02%	41
Other (please specify)	36.26%	99
Total Respondents: 273		

Fig. 8. Responses for Question 8

participants observed more of during/after the hurricane. This was also a "Select ALL that apply" question. Quite a few participants, 46, skipped this question. A majority of participants (152 or 55.6%) reported receiving requests for donations. A significant minority (67 or 24.5%) reported receiving some kind of incentive to click on a link. Participants were asked to elaborate further under the second ("Encouragement to ...") and Other choices. We examine detailed answers below.



Q9 Were there new examples of attacks that you haven't seen before?

Answered: 245 Skipped: 74

ANSWER CHOICES	RESPONSES	
Donation to Harvey victims	47.35%	116
Click on this link to get help	36.33%	89
Other (please specify)	32.65%	80
Total Respondents: 245		

Fig. 9. Responses for Question 9

Question 9 asked about the new types of attacks seen by the participants. Here also 74 participants skipped the question. At first glance, this question may seem to overlap with the previous question, Question 8. On closer inspection, readers will find that they are actually different questions, since one talks about what the participants noticed more of, which could be old kinds of phishing attacks for example, and the other asks specifically about the new types of attacks seen. In fact, we see that 15% of the participants did choose "Provide financial information," on Question 8, which could be considered as classic phishing attacks. We notice that the top two categories (Donations and Click on the link to get help) dominate the responses. Here again participants could choose more than one answer.

Question 10 asked participants to share attacks they received. But it seems that the procedure to obscure their email addresses may have been a discouraging factor for the participants. We will examine the responses in the next section.

V. Statistical Analysis

We dichotomized the responses to Questions 2 through 7 and calculated the Cronbach alpha whose range is 0 to 1. We got an alpha value of 0.5,[5] which is to be expected considering the smaller number of questions and the variation in the information each question is seeking. Questions 8 and 9 had Other as a response, which was selected by 99 and 80 participants respectively. Hence, it was much harder to dichotomize the responses for these two questions.

We check how many of the respondents, who answered Never or Before the Question 4 (When did you get any spam regarding the hurricane?), answered Yes to Question 7. The answer is 10. So even though 204 participants either never received hurricane-related spam, or got hurricane related spam before the hurricane, 10 of them (4.9%) clicked on a link or downloading an attachment, they would not have normally. This suggests that 10 respondents fell for non-hurricane related spam/phishing attacks. We list their responses to the other questions in Table II.

We check how many of the respondents, who answered During or After on Question 4 (When did you get any spam regarding the hurricane?), answered Yes to Question 7. The answer is again 10. So even though 99 participants

[5] https://www.wessa.net/rwasp_cronbach.wasp

TABLE II
RESPONSES TO OTHER QUESTIONS OF THE 10 PARTICIPANTS WHO CLICKED ON NON-HURRICANE RELATED SPAM/PHISHING ATTACKS THAT THEY OTHERWISE WOULD NOT HAVE. LB - LITTLE BIT, LE - LOST EVERYTHING, OTH. - OTHER, RV - REQUEST FOR DONATIONS TO DISASTER VICTIMS, CLGH - CLICK ON LINK TO GET HELP, DHV - DONATE TO HARVEY VICTIMS.

2	3	4	5	6	8	9
None	Y	Never	No	More	RV/Oth.	No
LB	Y	Never	No	More	PFI	CLGH
LB	No	Never	No	No	RV	CLGH
None	Y	Never	No	More	RV	DHV
None	Y	Never	No	No	RV	CLGH
LB	Y	Never	No	More	RV	CLGH
None	Y	Never	No	More	RV	DHV
LE	Y	Never	Y	No		
None	Y	Never	No	No	RV	DHV
None	Y	Before	Y	No	RV	DHV

received hurricane-related spam during or after Harvey, 10 of them (10.1%) admitted clicking on a link or downloading an attachment, they would not have normally. This shows a significant rise in the probability from the Never/Before group (4.9%) to the During/After group (10.1%). For a one-tailed test, we get $p < 0.044$. We now list the responses of the During/After group to the other questions in Table III.

TABLE III
RESPONSES TO OTHER QUESTIONS OF THE 10 PARTICIPANTS WHO CLICKED ON HURRICANE RELATED SPAM/PHISHING ATTACKS THAT THEY OTHERWISE WOULD NOT HAVE. LE - LOST EVERYTHING, PB - PRETTY BAD, PFI - PROVIDE FINANCIAL INFORMATION, ECL - ENCOURAGEMENT TO CLICK ON A LINK, LB, RV, DHV AND CLGH ARE GIVEN ABOVE IN TABLE II

2	3	4	5	6	8	9
LE	Y	After	Y	More	RV/PFI	DHV/CLGH
None	Y	After	No*	More	RV	DHV/CLGH
LB	Y	During	No	More	ECL	CLGH
PB	Y	After	No	No	RV/ECL/PFI	DHV
LB	No	After	Yes	No	RV/ECL/PFI	DHV
LB	Y	After	No	More	RV	DHV/CLGH
PB	Y	During	No	More	RV	DHV/CLGH
LB	No	During	Y	More	RV	DHV
LB	No	After	No	No	RV	DHV
PB	No	After	Y	No	ECL	CLGH

We now compare the probability distributions on Questions 2, 4, 5 and 6 of the 20 participants who answered Yes to Question 7 with the distributions on the same four questions for the 297 participants who answered No on Question 7. For Question 2, the symmetric version of the Jensen-Shannon (SJS) divergence [3] between the distributions is 0.0564. For Question 6, the SJS divergence is 0.0661 and for Question 4 it is 0.0606. For Question 5, the SJS value is the smallest, 0.0250. Question 6 is about how the volume of email changed, so we see that this had the biggest impact on the participants, and the next biggest impact was of the timing of arrival or non-arrival of hurricane-related spam.

For association analysis, we identified four pairs of questions as worth examining further. They are (Q2, Q7), (Q4, Q7), (Q5, Q7) and (Q6, Q7). Weak associations between 0.1 and 0.35 were observed using contingency tables after suitably dichotomizing the responses.

VI. DETAILED RESPONSES

The "Other (please specify)" option on Question 2 was chosen by five participants. One of them mentioned that his laboratory at UH was badly damaged, one "got sick from wading through the water," one was displaced for several weeks, one was "unable to go anywhere," and one had a death in the family, which was very hard and upsetting.

The same option on Question 4 was chosen by 13 participants. Two of them did not recall any Harvey spam. Three were not sure if the amount of spam changed, one explained that "I delete or filter spam regularly so did not differentiate between hurricane spam from other spam." One wrote, "before, during and after." Four of them had some after ("Only a little after," "Maybe some after - but I ignore spam ...," "After the hurricane, but not specifically about it," and "Not specifically regarding hurricane, but seemed to get more in general right after"). Two wrote that they did not recall. One wrote that spam received was not directly related to storm situation, just the usual occasional emails. One chose "All of the above," which could mean the same as "before, during and after," but since none was also a choice, it is hard to be sure.

Eight respondents chose the "Other (please specify)" option on Question 5. One lost Internet access during storm, one "lost wireless access at home due to flooding; still could access email on my phone and at night when I was in a hotel." One lost a laptop, and one lost a personal computer but still had a work (university) laptop. One relied on a smart phone, one on a different service provider, and one changed location and used a friend's Internet service. One had email access only at work (UH), which was closed for more than a week, "so I did not have access to email during that time."

Of the five respondents who chose the "Other" option on Question 6, three received more junk email or spam, and two wrote that they could not tell.

Ninety nine respondents chose the "Other" option on Question 8 and 39 wrote some variant of "none/no attacks/none that I recall/." Nine wrote "n/a." Five had some variant of "don't remember/can't remember." One wrote that "I receive more spam post Harvey," but did not elaborate. One wrote "phishing and spam emails," one wrote "General spam," one wrote "advertisement," one said "Usual spam mail," one said "General spam/phishing messages that also mentioned disaster recovery, and one wrote "phishing." One "didn't keep tabs" and one does "not open spam to see what they are about." Three responses were garbled and unusable. Two respondents gave detailed responses (one had an email body), which are in the Appendix. Remaining responses are summarized below.

Responses from Question 9 that give additional information beyond the above table are: Three computers on our network in my area had malware and viruses, lots of cell phone spam, and "**Your bank was compromised (by the hurricane)**." One participant mentioned a whaling attempt unrelated to Harvey.

TABLE IV
DETAILED RESPONSES ON QUESTION 8 (31 PARTICIPANTS). N - NUMBER OF RESPONDENTS, POTENTIAL NEW/SPEAR PHISH IN BOLDFACE FONT

N	Response
1	Notices from FEMA
1	**Email scam supposedly from FEMA received by friend**
1	Certain seedy looking emails asking for donations
2	Job spam, “Easy” jobs to make “good” money
1	“More donation requests **on Facebook** than on email”
1	Guides on how to navigate relief efforts, clean up homes, volunteer opportunities/donations, etc.
1	Blank email from someone in my contacts with only a link, emails asking for me to update my password
3	Grant offer or Free gift cards or giveaway emails/links
1	Links to update information
1	**Survey that asked for address information for cash from govt.**
1	Password expiry unless account is updated
2	Fake UH IT team link to reinitialize email account/give up credentials
1	Mostly sales related spam e-mails
1	Click a link to go to a place to input login info
1	**Click on links to volunteer or receive support**
1	Click a link to donate, Click a link to file your claim
1	Emails from insurance company about filing claims and how that isn’t required before 9/1
1	View pictures of victims; read stories of “faith,” Your Bank was compromised, click here to protect your account
1	request to volunteer
2	Click link to reset email account/enter email credentials
1	A lot more e-mail in what I think is Chinese
1	**Apply link with FEMA**
1	Spam about other things
1	More news articles, etc.
1	**Harvey “relief” related spam**
1	**Click here to see affected areas, click here to view qualifications for relief**, click here to donate

One participant mentioned receiving “non-English (Chinese?) emails.”

VII. CONCLUSION

We conducted a first-of-its-kind study of UH population after Hurricane Harvey and found some evidence for change in behavior and also some noteworthy items, e.g., some new attacks, cell phone spam, Facebook, for further investigation. Our analysis showed that the increase in volume of email did have an impact on the participants inclination to click on a link or download an attachment that they would not have.

There are several avenues for future research. Our survey was intentionally brief to ensure higher probability of participation. We were worried that participants after a disaster would be so traumatized and involved in recovery that they would not have the time, nor the inclination, to participate in our survey.[6] We recommend that future surveys include at least a question on contact information for participants, who want to help with follow-up questions to established cause and effect and perhaps a detailed factor analysis. Perhaps a few more “conditional” questions can also be added to probe deeper into some of the answers.

ACKNOWLEDGMENTS

We thank the IEEE Resilience Week reviewers for their constructive criticisms, Wenyaw Chan for useful suggestions on statistical analysis, and Puneet Goyal for a careful reading of the paper and discussion. This research was supported in part by NSF grants CNS 1319212, DGE 1433817, DUE 1241772, and DUE 1356705. This material is also based upon work supported in part by the U. S. Army Research Office under contract/grant number W911NF-16-1-0422.

REFERENCES

[1] Ahmed AlEroud and Lina Zhou. Phishing environments, techniques, and countermeasures: A survey. *Computers & Security*, 68:160–196, 2017.

[2] Shahryar Baki, Rakesh Verma, Arjun Mukherjee, and Omprakash Gnawali. Scaling and effectiveness of email masquerade attacks: Exploiting natural language generation. In *Proc. 12th ACM ASIACCS, 2017, April, 2017, Abu Dhabi, UAE*, 2017.

[3] Ido Dagan, Lillian Lee, and Fernando Pereira. Similarity-based methods for word sense disambiguation. In *Proceedings of the Eighth Conference on European Chapter of the Association for Computational Linguistics*, EACL ’97, pages 56–63, 1997.

[4] Ayman El Aassal, Luis Moraes, Shahryar Baki, Avisha Das, and Rakesh Verma. Anti-phishing pilot at ACM IWSPA 2018: Evaluating performance with metrics for unbalanced datasets. In *Proceedings of the 1st Anti-Phishing Shared Task Pilot at 4th ACM IWSPA*, volume 2124, 2018.

[5] Markus Jakobsson and Steven Myers. *Phishing and countermeasures: understanding the increasing problem of electronic identity theft.* John Wiley & Sons, 2006.

[6] Greater Houston Partnership. Houston and Hurricane Harvey: What You Need to know. http://www.houston.org/pdf/comm/Hurricane-Harvey-Statistics.pdf, March 2018. Accessed May 3, 2018.

[7] Meet Rajdev and Kyumin Le. Fake and spam messages: Detecting misinformation during natural disasters on social media. In *IEEE/WIC/ACM Int’l Conf. on Web Intelligence and Intelligent Agent Technology, WI-IAT 2015, Singapore, Dec. 6-9, 2015 - Volume I*, pages 17–20, 2015.

[8] Doyen Sahoo, Chenghao Liu, and Steven C. H. Hoi. Malicious URL detection using machine learning: A survey. *CoRR*, abs/1701.07179, 2017.

[9] Tanmay Thakur and Rakesh M. Verma. Catching classical and hijack-based phishing attacks. In *Information Systems Security - 10th International Conference, ICISS 2014, Hyderabad, India, December 16-20, 2014, Proceedings*, pages 318–337, 2014.

[10] Gaurav Varshney, Manoj Misra, and Pradeep K. Atrey. A survey and classification of web phishing detection schemes. *Security and Communication Networks*, 9(18):6266–6284, 2016.

[11] Rakesh M. Verma and Ayman El Aassal. Comprehensive method for detecting phishing emailsusing correlation-based analysis and user participation. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, CODASPY 2017, Scottsdale, AZ, USA, March 22-24, 2017*, pages 155–157, 2017.

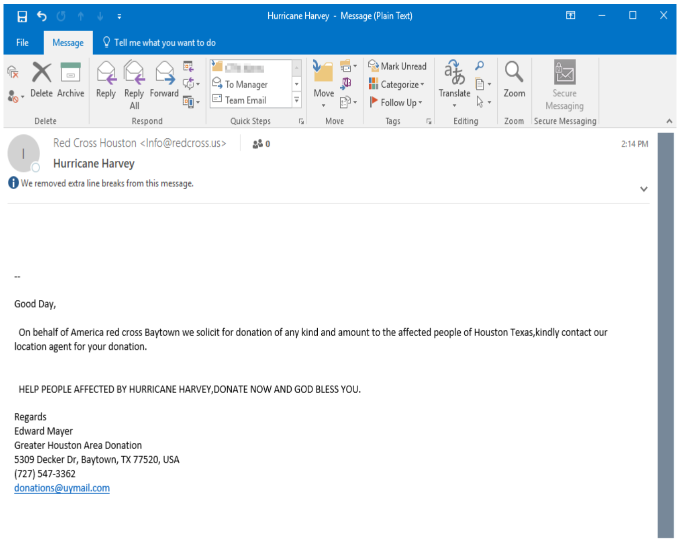
[12] Rakesh M. Verma and Avisha Das. What’s in a URL: fast feature extraction and malicious URL detection. In *Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics, IWSPA@CODASPY 2017, Scottsdale, Arizona, USA, March 24, 2017*, pages 55–63, 2017.

[13] Rakesh M. Verma and Avisha Das, editors. *Proceedings of the 1st Anti-Phishing Shared Task Pilot at 4th ACM IWSPA*, volume 2124, 2018. http://ceur-ws.org/Vol-2124/.

[14] Rakesh M. Verma and Keith Dyer. On the character of phishing URLs: Accurate and robust statistical learning classifiers. In *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy, CODASPY 2015, San Antonio, TX, USA, March 2-4, 2015*, pages 111–122, 2015.

[15] Rakesh M. Verma and Nabil Hossain. Semantic feature selection for text with application to phishing email detection. In *Information Security and Cryptology - ICISC 2013 - 16th International Conference, Seoul, Korea, November 27-29, 2013, Revised Selected Papers*, pages 455–468, 2013.

[6] For example, one participant, who lost everything, skipped questions 8 and 9.



Red Cross Houston <Info@redcross.us> 0 2:14 PM

Hurricane Harvey

We removed extra line breaks from this message.

--

Good Day,

On behalf of America red cross Baytown we solicit for donation of any kind and amount to the affected people of Houston Texas,kindly contact our location agent for your donation.

HELP PEOPLE AFFECTED BY HURRICANE HARVEY,DONATE NOW AND GOD BLESS YOU.

Regards
Edward Mayer
Greater Houston Area Donation
5309 Decker Dr, Baytown, TX 77520, USA
(727) 547-3362
donations@uymail.com

Fig. 10. An Example of a Harvey Scam Email

[16] Rakesh M. Verma, Murat Kantarcioglu, David J. Marchette, Ernst L. Leiss, and Thamar Solorio. Security analytics: Essential data analytics knowledge for cybersecurity professionals and students. *IEEE Security & Privacy*, 13(6):60–65, 2015.

[17] Rakesh M. Verma, Narasimha Shashidhar, and Nabil Hossain. Detecting phishing emails the natural language way. In *Computer Security - ESORICS 2012 - 17th European Symposium on Research in Computer Security, Pisa, Italy, September 10-12, 2012. Proceedings*, pages 824–841, 2012.

VIII. Appendix

Two respondents gave detailed answers for Question 8. One gave the body of a phishing attack as below.

> FW: HELP DESK, Final Warning: upgrade your University of Houston mail box quota limit for better performance and more storage space, CLICK HERE . SIGN IN to complete the process. Failure to follow this instruction immediately will lead to permanent deactivation of your mail box in the next 9 hours. Regards UH MAIL ADMIN

One respondent wrote that: “I was encouraged to click on links, but the emails didn’t have anything to do with Harvey. They were the usual ‘your package didn’t deliver’ or ‘read this!’ type of phishing scam emails. None of them were ever specific to Harvey that I can recall. **All I noticed was that the volume of these types of emails dramatically increased, and I’m not sure why.**”

We give an example of a Harvey scam email in Figure 10 from the website: https://blog.appriver.com/2017/08/first-harvey-scam-email-appears/

Katrina-related phishing email attack[7] **is below**:

Please donate to Hurricane Relief Efforts. We have seen the horrible destruction this past week that was caused by natural causes. Our hearts and prayers go out to those affected by Hurricane Katrina. If youd like to help we encourage you to make a generous donation to the American Red Cross. Thank You for your compassion.

⟨“Bogus but legitimate sounding domain name is omitted.”⟩

[7] https://www.scambusters.org/hurricanekatrinascams.html