University of California Berkeley
Master of Information and Cybersecurity (MICS)

“What Would You Do If You Received a Ransomware Email?”

A Ransomware Email Case Study

W215 Usability and Privacy
Fall 2020 Final Project
December 10th, 2020

Authors:
Alanna Franklin
Atefeh Namvaryshad
Nestor Catano

Abstract

Ransomware is a type of malware or in this case an email that threatens to publish the victim's data or perpetually block access to it by encrypting their data and demands a ransom is paid to avoid the victim’s private and/or sensitive data from being exposed.

We conducted a survey to identify the vulnerable population that are victims of Ransomware email and to understand their level of concern, level of anxiety, if they reported it, and details about the ransom requested (paid or not, type of currency, amount).

This research is based on a real life scenario, in which a real Ransomware email was received by one of the researchers in this study back in April 2020. However, we removed the actual email address of the receiver to preserve confidentiality. In the very beginning of the survey, we provide the participant’s with the Ransomware email example, as shown in Figure 1.
Please refer to the “Reference section”, for a link to all survey questions in this study.

Introduction

Motivation

Our purpose and motivation of this research is to determine the behavior of a victim or a potential victim if they received a threatening email that contains their “actual email password” in an attempt to blackmail them by requesting a ransom payment in exchange for not sharing a non-consensual intimate (“doing nasty things”) video of them while visiting an adult-only website to their contacts, similar to the example email provided in Figure 1.

Figure 1: Ransomware definition and example email included in the survey.
Ransomware is a type of email or malware that threatens to publish the victim's data or perpetually block access to it, unless a ransom is paid.

Please carefully read the Ransomware email example provided below, which will be helpful in answering the questions in this survey.

Sent: Thursday, April 9, 2020 11:05 AM
To: al_frank@hotmail.com <al_frank@hotmail.com>
Subject: al_frank: ILOVEYOU2020

I know, ILOVEYOU2020, is your password. You don't know me and you're thinking why you received this e mail, right?

I made a split-screen video, recorded a video of what you were viewing, and there was malware on the porn website and guess what, you visited this web site to have fun. While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account. taste haha), and next part recorded your webcam (Yep! It's you doing nasty things!).

Well, I believe, $1900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

Important:

You have 24 hours in order to make the payment. (I have an unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immidiately. If you want evidence, reply with "Yes!" and I will send your video recording to your 5 friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

Goal

Our goal is to identify a correlation between the participant's Technical/Computer and IT Security/Cybersecurity expertise, primary email provider, that possibly influences being vulnerable to receiving a Ransomware email and reaction to the threat.

To reach this goal we asked a series of survey questions that measure how each participant responded if they received a Ransomware email. If the participant did not receive a Ransomware email in the last year, we still thought it was valuable data to know what participants "would do" after receiving a Ransomware email.

Research Hypotheses

Our research will prove or disprove the following hypotheses:

- The participants that received Ransomware emails and # received in the last year are dependent on the user's primary email provider.
- Technical/Computer and IT Security/Cybersecurity that self-reported themselves as "experts" are less concerned about the Ransomware email threat, than the "non-experts".
- The level of concern and Technical/Computer and IT Security/Cybersecurity expertise influences the decision to pay the ransom or not.

Research Questions

The goal of our research are to answer the questions:

- Would the majority of user's believe the threat in the Ransomware email?
- What would be the major concerns for the majority of users?
- What percentage of users would report and/or attempt to remediate the threat?
- Based on the "self-reported" level of Technical/Computer and IT Security/Cybersecurity expertise, are there any noticeable trends based on the answers provided to the survey questions?

Methodology

The researchers created the survey questions using Qualtrics and then used an anonymous survey link to allow the participants to feel comfortable to answer the questions truthfully, especially questions related to visiting adult-only (e.g. porn) websites.

Preliminary Survey

A preliminary survey was created and feedback was collected from personal interviews with friends, neighbors, and also UC MIC instructors and students. This was very helpful to identify a trend that most of our non-technical peers were not aware of the definition of "Ransomware" and how it differs from Phishing or SPAM emails. With that said, we included the definition of

Ransomware and an example in the very beginning of the survey to be used as a reference for the survey questions, as seen in Figure 1.

In addition, we received notable feedback that it was difficult for the participant to remember if they ever received a Ransomware email in the last 5 years. To avoid memory falsifications, we reduced the time period for the number of Ransomware Email(s) received to only the last year vs. 5 years, like we had before.

Trial Survey

In the 1st round of conducting the survey, we recruited 10 participants, paying each $2 each using Amazon MTurk. The objective was to verify the survey was working as expected for any worker located in the United States with a MTurk 90% HIT rate.

However, the results were not as expected, the ratio of men and women was not evenly distributed, only 2 women and 8 men participated in the survey. This helped to identify the necessary sample size needed to achieve an increased distributed amount of men and women in this study. In the final survey we increased the sample size by 3 times to 30 participants. However only 29 participant's results were collected by Qualtrics, see details in the "Final Survey" section below.

In addition, many survey questions were not answered possibly because some questions contained logical errors, since AND is the default value in Qualtrics vs. OR when distinguishing those participants that received 1 to 5 or more vs. those that answered, "Not sure" or "None".

Another possibility for unanswered questions, is that the participants simply refused to answer the question and were able to transverse through the survey without answering every question, see more details in the "Final Survey" section below.

Final Survey

After many rounds of edits and changes to the survey questions wording, logic, and ordering based on our previous survey results and individual feedback from our peers (instructors, friends, classmates) in the Trial Survey, a new finalized survey was released on Amazon MTurk for 30 participants, known as workers. Each worker was paid $2 with the condition that they are located in the United States, with a MTurk 90% HIT rate.

Unfortunately, only 29 out of 30 participants' results were collected from Qualtrics. We suspect that one person did not select the final "arrow" to complete the survey to allow their final results to be included in this study.

This time all survey questions had the "Forced Response" feature enabled, so that the participants were not able to skip questions in the survey, as seen in the Trial Survey.

Results

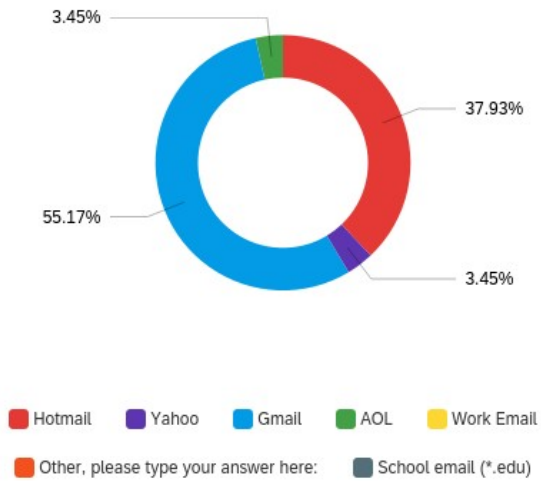
This section analyzes the results obtained through the conducted survey. Not only do we discuss the research hypotheses stated in Section *"Research Hypotheses*" but we also discuss other observations.

General Observations

A total of 27% (8 out of 29) of the participants reported being victims of at least 1 Ransomware email or more. The results show 10% received 1 Ransomware email, 17% reported 2 to 4 emails, and 0% reported receiving 5 or more. There were approximately 65% (19 out of 29) participants that reported "None", when asked how many Ransomware emails they have received in the last year.There were 7% (2 pout of 29) participants that reported "Not Sure",

There were a total of 65% (19 out of 29) participants that reported that they have NOT received a Ransomware email in the last year. Since there were 27% (8 out of 29) participants that have received Ransomware email(s), we can conclude that those that have NOT received a Ransomware email (19 out of 29) participants are more than double than those that have received Ransomware email.

Figure 2: Participants' Primary Email Providers



As shown in Figure 2 above, the survey results show that a majority of our participants 55% use Gmail as their primary email provider. Coming in second place was Hotmail with approximately 38% users and coincidentally the same amount 3.45% for both Yahoo and AOL, as their primary email provider.

Ransomware Emails Received vs. Primary Email Provider

Our first research hypothesis states,"The participants that received Ransomware emails and # received in the last year are dependent on the user's primary email provider".

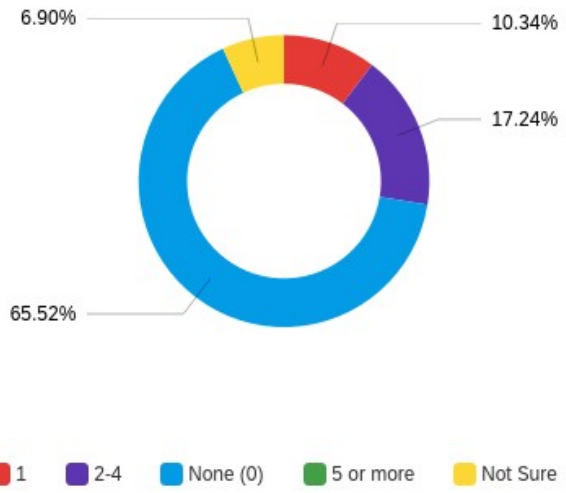
The evaluation of this hypothesis mainly depends on these 2 questions:

1. What is your primary email provider?
2. How many Ransomware email(s) have you received during the last year that threatened to publish your data or block access to it unless a ransom is paid?

If taken independently, results of Question #1 above shows that 11/29 = 38% of the participants use Hotmail as a primary email provider.

The results of Question #2 above, show 1/29 = 3.4% use Yahoo, 16/29 = 55.2% use Gmail, and 1/29 = 3.4% use AOL.

Figure 3: Ransomware Emails Received In The Last Year



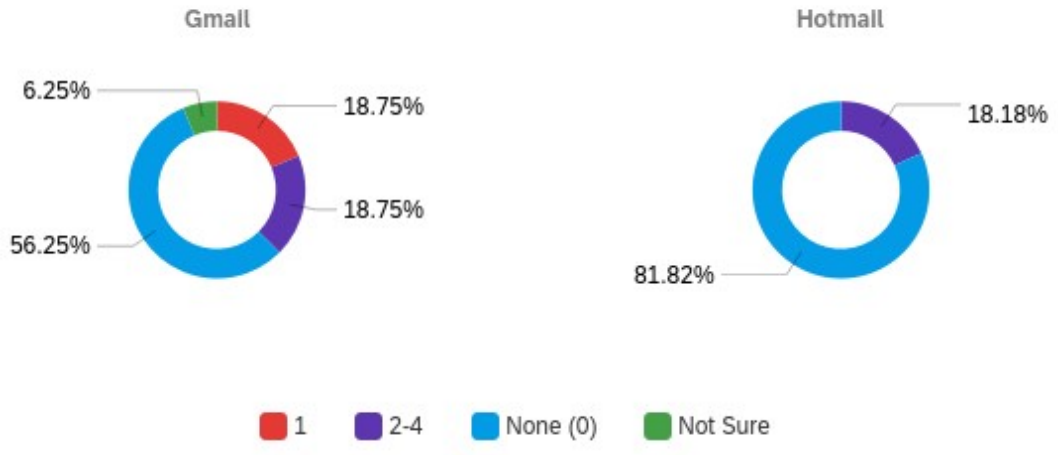
As seen in Figure 3 above, we combined the results of all the participants in the two previous questions to get more interesting results and an astounding 65% of the total participants regardless of the email provider, have never been victims of receiving a Ransomware email in the last year reporting "None", as shown in pie chart above in Figure 3.

Hotmail vs. Gmail

There were 8 participants that received Ransomware email(s), and 25% (2 out of 8) Hotmail users versus 75% (6 out of 8) Gmail users. However, the survey results show that 55% (16 out of 29) total participants use Gmail, possibly receiving more Ransomware emails due to the fact more Gmail users took the survey vs. other primary email providers (Hotmail, AOL, Yahoo).

Out of the 65% total participants that responded “None” for receiving Ransomware emails.For Gmail specifically, there were 37% (18.75% + 18.75%) of participants that reported that they received 1 or more Ransomware email(s) in the last year, see left graph in Figure 4 below. However, for Hotmail there were 18% users that reported receiving Ransomware emails in the last year.

Figure 4: Ransomware Emails vs Primary Email Provider (Gmail vs Hotmail)



Now we compare the number of Ransomware emails received by Gmail users versus Hotmail users, see Figure 4. As reported in the survey results, the number of Ransomware emails received (1 or 2-4) for the top 2 primary email providers were Gmail and Hotmail, For both Gmail and Hotmail, the majority 85% (19 out of 29) of participants answered that they have not received (None) any Ransomware emails in the last year. There were a total of 2 participants that answered, “Not Sure”

Comparing the number of Ransomware emails received by participants based on the top 2 email providers, there Gmail users were approximately 21% (6 out of 29) participants versus Hotmail users were 7% (2 out of 29) participants.

However, we cannot generalize that Gmail user’s are more likely to receive Ransomware emails, when we observe the whole population of Gmail and Hotmail users in the survey for the following reasons:

1. There were 55% of Gmail users in the survey, however a very high percentage 81% of those participants have not received a Ransomware email, as reported in the survey.
2. The very high number of 65% (19 out of 29) participants, regardless of the email provider answered “None” for # of Ransomware emails received.
3. The dataset for the survey shows that approximately 55% (16 out of 29) participants used Gmail, thus receiving more Ransomware emails. This can be due to the fact more Gmail users took the survey.

4. The majority 65% (19 out of 29) of all survey participants reported they did not receive a Ransomware email, 55% of Gmail users vs. 86% of Hotmail users.

Technical Experts vs. Non-Experts

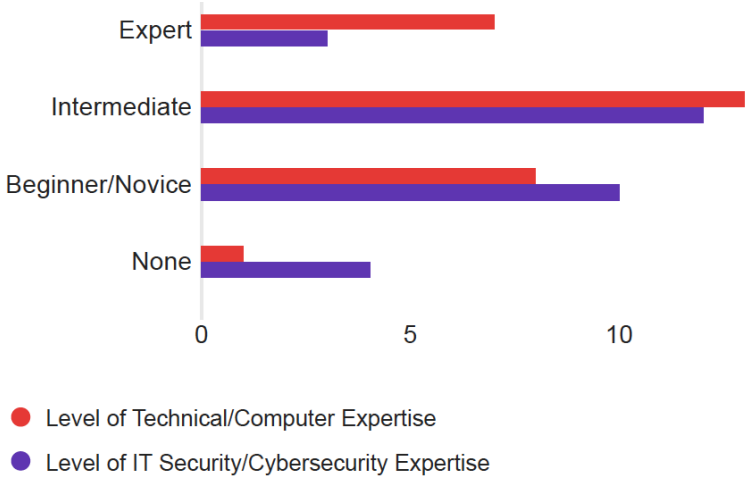
Our second research hypothesis,"Technical/Computer and IT Security/Cybersecurity that self-reported themselves as "experts" are less concerned about the Ransomware email threat, than the "non-experts" is true, but only if you don't include "Intermediate" level of expertise.

The participants' self-reported level of expertise is shown below. The survey responses suggest that 43% of participants report a similar level of expertise for 2 separate fields:

- Technical/Computer
- IT Security/Cybersecurity
-

As seen in Figure 5 below, an interesting observation is that only half of those that self-reported "expert" levels of Technical/Computer expertise considered themselves as an IT security/Cybersecurity "expert" as well.

Figure 5: Technical Experts vs. Non Experts



Ransomware Emails Received vs. Not Received

There are 2 distinct groups for the results reported in Figures 6-9 below:

Group 1: Participants that received a Ransomware email in the last year

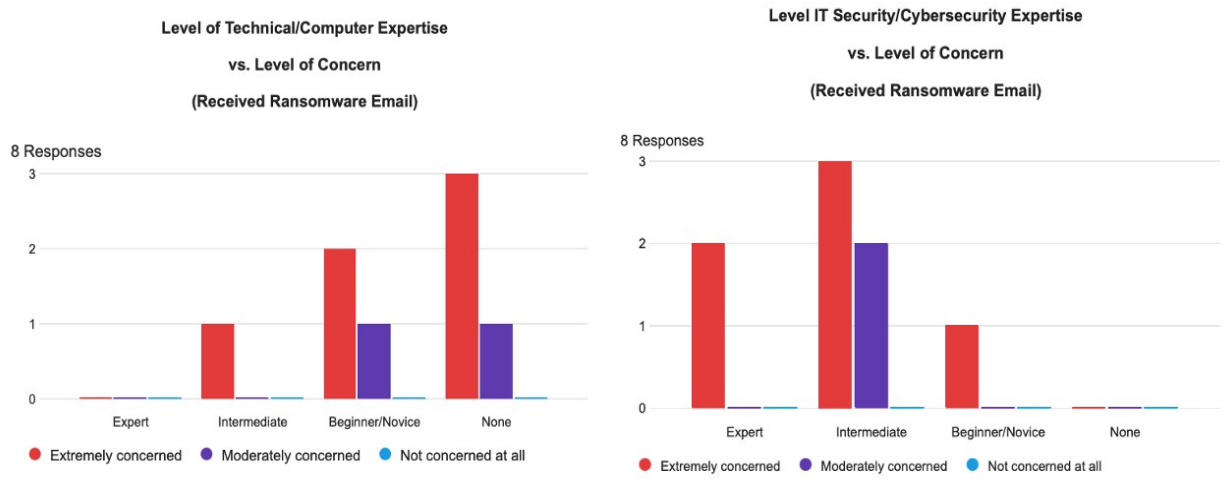
Group 2: Participants that did NOT receive a Ransomware email in the last year

In order to understand the influence of the self-reported level of expertise with the level of concern caused by receiving a Ransomware email, we compared the survey responses of participants who reported receiving 1 or more Ransomware Email(s) (the graph on left) with those who never received any or were not sure (the graph on right).

The left graph in Figure 6 below shows shows that 8 participants reported that they received 1 or more Ransomware emails and that self-reported their Technical/Computer Expertise as higher levels (Expert/Intermediate) are less concerned about Ransomware Email(s) then those that are non-experts (Beginner/None).

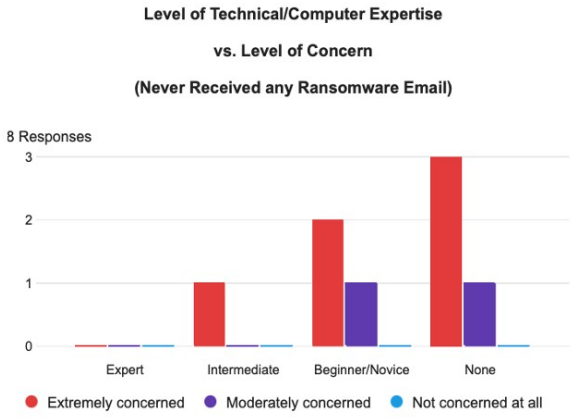
The right graph in Figure 6 below, shows those that self-reported Intermediate or Expert levels of IT Security/Cybersecurity expertise, expressed higher levels (Extremely/Moderately) of concern vs. those that are non-experts (Beginner/None).

Figure 6: Technical Expertise vs. Level of Concern (Group 1 Received)



To identify the correlation between the concern level and level of expertise in Technical/Computer and IT Security/Cybersecurity and how these factors influence victims to make the ransom payment(s) we compared the latter two variables. In total 75% of victims confirmed that they have paid the ransom and also self-reported a higher level of Technical/Computer and IT Security/Cybersecurity expertise (Expert or Intermediate level).

Figure 7: Technical Expertise vs. Level of Concern (Group 2 Not Received)

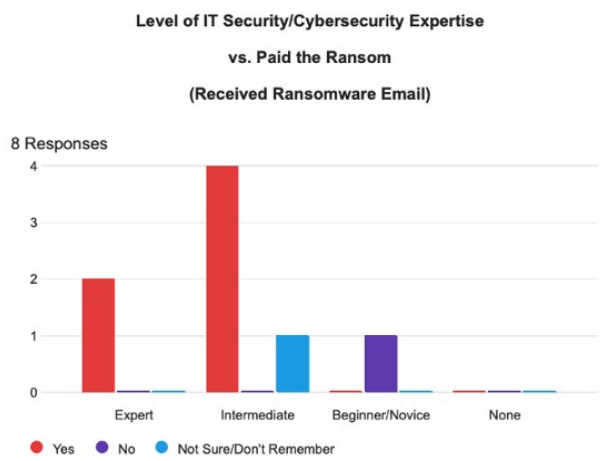


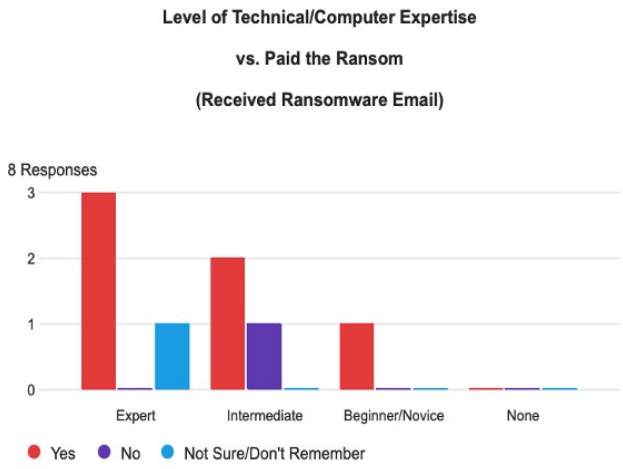
Technical Expertise vs. Paid the Ransom

We also observed a direct influence of the self-reported Security/Cybersecurity expertise levels with the increased level of concern, which potentially may have led the victim to pay the ransom.

Comparing the results of both graphs below, we can clearly notice the direct influence of the level of expertise in Technical/Computer and IT Security/Cybersecurity in causing concerns and ultimately leading the potential victim to pay the ransom.

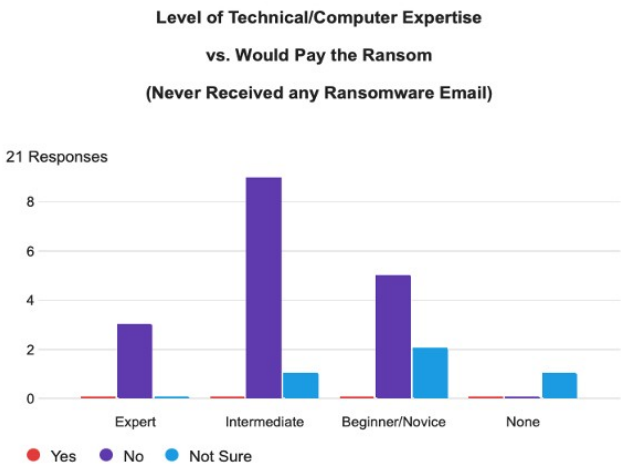
Figure 8: Technical Expertise vs. Paid Ransom (Group 1 Received)





A notable observation of the results shown in Figure 6 above, is that participants who have never been victim of a Ransomware Email consider themselves less expert in both Technical/Computer Expertise and Security/Cybersecurity. We may be able to conclude that this is the reason why they would NOT pay the ransom if they were ever received one.

Figure 9: Technical Expertise vs. Would Pay Ransom (Group 2 NOT Received)



Discussion

Limitations

Our survey was intended to reflect the general U.S. population with diverse socio-economic backgrounds. Nevertheless, it may still be biased along other dimensions than those that we have explicitly accounted for in this research.

For example, Amazon MTurk has reportedly shown poor quality of responses, participants are found to be more tech savvy, and since it is an unregulated platform the participants are left unmonitored, leading to poor quality data. A platform like YouGov might be a better option specially for studying the U.S. population, with an increased sample size of +400 participants.

We also discovered after the survey was already conducted, that there are different interpretations of “Not Sure” listed below:

a. Not sure about receiving Ransomware (ie. SPAM mailbox, etc..)
b. Not sure about how many Ransomware emails

In addition, there are other confounding factors, which included conducting a survey during the Covid era, which may have impacted the prevalence of receiving Ransomware emails when Cyber crime is at an all time high and most US citizens are working from home, that’s if they are non-essential workers. We are looking forward to 2020 reports of Cybersecurity types for crime, including but not excluding Ransomware emails.

Further Research

Apart from characterizing the technical aspect of the Ransomware email attacks and how they reach their targets, we would like to conduct further research to know more about the victims perception of the Ransomware email threat, their defensive actions, and other factors that may lead them to take such actions. Cultural factors for participants such as embarrassment and shame, can coerce victims into paying the ransom.

We would like to conduct further research to help identify a correlation between trends. (i.e. employment status, marital status, gender classification….) that possibly influences being vulnerable to receiving a Ransomware email and reaction to the threat.

Further Research Hypothesis

The following proposed hypothesis are very interesting but were removed in this research because they would require further research and due to time constraints and resources, we could not prove or disprove these hypothesis:

- The participants that visit adult-only (e.g. porn) websites are more likely to experience increased anxiety levels when they receive a Ransomware email.
- Men and women may select different responses and actions based on if they visit adult-only (e.g. porn) websites. Women may be less likely to visit porn sites, thus less concerned if they received an email similar to the Ransomware email provided."

Future Research Questions

The goal of future research would answer the question:

- Do participants that visit adult-only (e.g. porn) websites more likely to experience increased anxiety levels when they receive a Ransomware email?
- Does the gender of a participant determine their behavior and response to the survey questions?
- Are men and women less or more likely to visit adult-only websites and does this correlate to their level of concern?
-

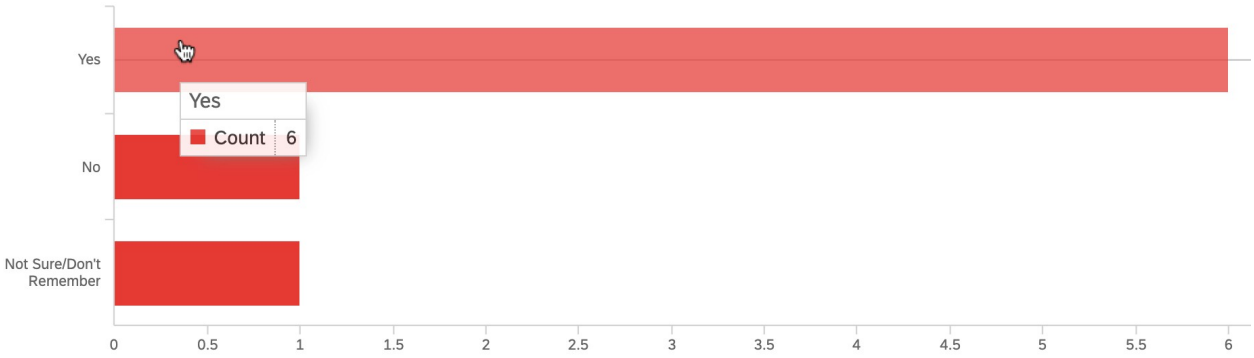
Other Observations

It is also interesting to discuss the percentage of people that paid for a ransom based on employment status, depends on these 2 questions:

1. Did you pay the ransom (e.g. bitcoin, money, ...)?
2. What is your employment status?

Figure 10 below depicts the results of Question #1 above. It shows that 6/8 = 75% of the participants that were victims of a Ransomware email ended up paying for it, a very high percentage of participants. Based on our results, we can possibly conclude that most people are likely to pay for ransom if they received a Ransomware email, in general. However, we would need to conduct further research with a larger sample size to make a definite conclusion.

Figure 10: Participates that Paid Ransom



In some of our group meetings, the question arose whether “employment status” influences the decision of a victim of (not) paying for a ransom. Hence, we here filter the previous results to Question #1 above by employment status as given by Question #2 above.

Figure 11: Employment status for those Received Ransomware Email and Paid Ransom

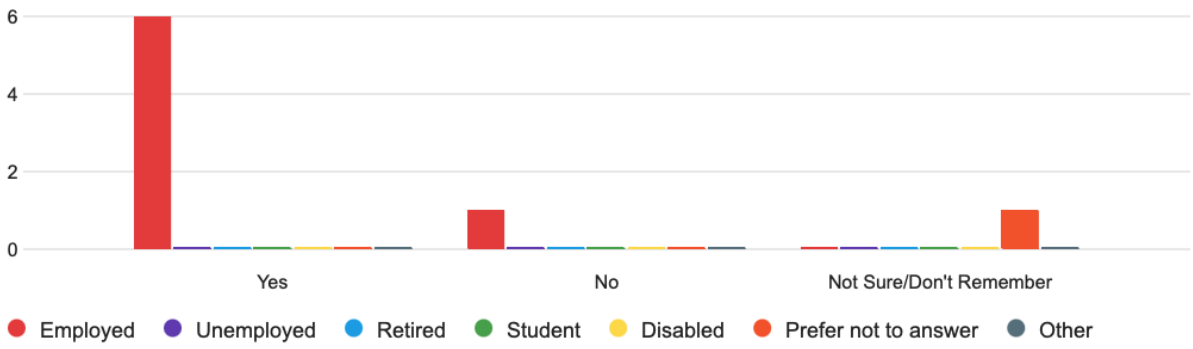


Figure11 groups the answer to Question #1 above by those participants who answered “Employed” to Question #2 above.. In short, 6 of 7 participants (86%) that paid the ransom were employed at the time, and 1/7 = 14% were not. Although 86% is a large percentage of participants, we cannot infer that if they were not be employed, they would not have paid for the ransom; we needed to have asked that directly in the survey as a “dependent” (conditional) question.

Related Work

In a detailed survey of Ransomware, they found that 2% to 3% of the survey participants were affected over 1 year. They also found that about 4% of the affected ended up paying the ransom. In our survey, we have (at least) two questions that relate to these two findings of theirs. In one of the questions of our survey, we discretize the number of Ransomware emails received for the last year (1, 2 or more, and so on) to compare our work to theirs. Regarding their second finding, our work attempts to go beyond by trying to infer if paying a ransom depends on the participants’ Technical/Computer level or employment status (Goel,C. Simoiou *et al.,*2019).

In another case study, the authors give an account of one-click frauds that have occurred in Japanese society. Authors found out that Japanese people are often ashamed of the possible consequences of ransom threats of exposing their private information and/or activities to the public, which often influence them to pay ransoms. In the early versions of our survey, we discussed as a group the implications of having a few questions regarding the effects that would have for the participants of our survey to have visited adult-only websites and the effects of this on paying for a ransom (Kamataki, 2010). However, we did not conduct a full analysis of this particular issue in our research.

One particular study demonstrated that Ransomware emails are automated and not targeted to a particular population, e.g., men vs. women (Goel, 2019). Our survey did not attempt to characterize the incidence of sex/gender in relations to the susceptibility of a Ransomware email, however see Further Research section below.

Over the past decade, Ransomware emails have been customized and automated to reach more victims. Multiple studies have found that the impact of Ransomware email is more than just financial, often victims experienced psychological complications such as stress, anxiety, embarrassment, fear, anger, and isolation. (Button et al., 2020).

One way attackers inflict concerns and fear among their targeted victims is through Ransomware email, in which the malicious attacker threatens to expose the victim's private multimedia data, such as unconsented video recordings of the victim after visiting a porn website in exchange for paying the ransom. Ordinary users are found to be the most common victims of Ransomware emails.(Bada & Nurse, 2020)

There are a few resources accessible for victims to identify a fake Ransomware email threat from a real one. There's a list of different types of "Malware Ransom Threats" located on the https://answers.microsoft.com/ website. (Microsoft Forum, 2019).

In addition there is an article that discusses a new email scam that specifically describes the type of Ransomware email in this study; "People are being victimized by a terrifying new email scam were attackers claim they stole your password and hacked your webcam while you were watching porn — here's how to protect yourself". (Business Insider, 2018).

Conclusion

Our goal was to identify a vulnerable population of participants that were victims of receiving a Ransomware Email, the # received, measure their level of concern, and then we use statistical methods to find correlations among these factors based on their primary email provider, or Technical/Computer and IT Security/Cybersecurity expertise.

Using a multi-step and self-reporting survey, we identified a vulnerable population for receiving a Ransomware email(s) that threatened to send a non-consensual recording of them while visiting an adult-only website to their contacts, as shown in Figure 1.

Our results provide two types of data: first, the latest estimate on the prevalence of Ransomware Emails received by U.S. users, measure their level of concern, and then we use statistical methods to find correlations among these factors based on their Technical/Computer and IT Security/Cybersecurity expertise.

Research Hypotheses Findings

Hypothesis 1

The participants that received Ransomware emails and # received in the last year are dependent on the user's primary email provider.

Results were inclusive. The survey results show that 55%(16 out of 29) participants use Gmail and 75% (6 out of 8) also received more Ransomware emails versus 25% (2 out of 8) of Hotmail users . However, this can be due to the fact more Gmail users took the survey vs. other primary email providers (Hotmail, AOL, Yahoo).

In addition, as reported since there were 55% of Gmail users that took the survey but a very high percentage (81%) of those participants did not receive a Ransomware email in the last year. Since there were more Gmail participants approximately 55% (16 out of 29) participants in the survey versus Hotmail participants 38% (11 out of 29) participants, thus there is not a fair comparison between those that did not receive a Ransomware email vs. those that did not.

Hypothesis 2

Technical/Computer and IT Security/Cybersecurity that self reported themselves as "Experts" are less concerned about the Ransomware email threat, than the Non-Experts.

T**his hypothesis is false,** since results show that those with higher Technical/Computer and IT Security/Cybersecurity expertise have a higher level of concern.

Hypothesis 3

The level of concern and Technical/Computer and IT Security/Cybersecurity expertise influences the decision to pay the ransom or not.

Results show that this hypothesis is true, since Technical/Computer and IT Security/Cybersecurity expertise have a higher level of concern as stated in Hypothesis 2, thus impacting their decision to pay the ransom. Surprisingly even though 27%(8 out of 29) participants received a Ransomware email in the last year, a higher than expected 75% (6 out of 8) participants reported that they paid the ransom.

We also observed that those that have not "actually" received a Ransomware email are less likely to pay the ransom if it happened to them, regardless of their Technical/Computer and IT Security/Cybersecurity level of expertise.

University of California Berkeley
Master of Information and Cybersecurity (MICS)

References

Version 6 Mturk30: Usability and Privacy: Ransomware Email Survey
https://drive.google.com/drive/u/0/folders/1BQgyRXNvblQwDgmnsaq8Sj3L9TaOx51b

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities, 73–92. https://doi.org/10.1016/b978-0-12-816203-3.00004-6

Button, M., Suguira, L., Blackbourn, D., Kapend, R., Shepherd, D., & Wang, V. (2020, April). Victims of Computer Misuse Main Findings. University of Portsmouth.

Goel, C. S. (2019). “I was told to buy a software or lose my computer. I ignored it": A study of ransomware. USENIX Association. Santa Clara, USA.

Kamataki, N. C. (2010). Dissecting one click frauds. Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS). ACM.

Ponnurangam Kumaraguru, S. S. (2003). Teaching Johnny Not to Fall for Phish. CMU-CyLab.

Camelia Simoiu, Christopher Gates, Joseph Bonneau, and Sharad Goel. 2019. "I was told to buy a software or lose my computer. i ignored it": a study of ransomware. In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security(SOUPS'19). USENIX Association, USA, 155–174.

Leswing, K. (2018, July 28). People are being victimized by a terrifying new email scam where attackers claim they stole your password and hacked your webcam while you were watching porn - here's how to protect yourself. Retrieved December 09, 2020, from https://www.businessinsider.com/new-email-scam-uses-old-password-fake-porn-threats-webcam-video-bitcoin-2018-7

Malware Ransom Threat. (n.d.). Retrieved December 09, 2020, from https://answers.microsoft.com/en-us/protect/forum/all/malware-ransom-threat/f8d7891d-1e7d-453d-8372-9cc01b82de25

Acknowledgements

We would like to thank our course instructors for very detailed feedback in the earlier and later versions of our Ransomware email survey and also for their dedication to our success and support along the way.