Investigating the Impact of Ransomware Splash Screens

Yagiz Yilmaz[a], Orcun Cetin[a,*], Budi Arief[b], Julio Hernandez-Castro[b]

[a] *Sabancı University, Turkey*
[b] *University of Kent, United Kingdom*

Abstract

Ransomware is a type of malicious software that locks out its victim from accessing functionality or data on their device, typically by encrypting files. To regain access, victims would typically need to make a ransom payment. Victims get notified that their device has been infected through a ransom note (splash screen) displayed on their device. Ransomware splash screens can be presented in many ways; the most common ones are via a text file or a graphical user interface (GUI). Splash screens may also include additional features, such as a countdown timer, as part of the ransomware operator's ploy to encourage their victims to pay. The main aim of this study was to gain valuable insights into how ransomware splash screens might affect victims' responses. Moreover, the study also investigated whether exposure to different splash screens would encourage participants to adopt good security behaviours. A controlled experiment was conducted by randomly assigning 538 participants into one of the three ransomware infection scenarios based on the splash screen type (Text-based, GUI or GUI + Timer). After watching a demonstration of a ransomware scenario, each participant was asked to complete a survey regarding their post-infection behaviour and their cybersecurity habits. The study concluded that ransomware's user interface elements do not have a notable effect on how victims would react, in terms of their willingness to pay or their reporting rates. Additionally findings included that, even though 60% of the participants would

*Corresponding author
Email address: orcun.cetin@sabanciuniv.edu (Orcun Cetin)

like to report a ransomware incident, they were not sure how to do this. This illustrates the lack of public awareness about cybercrime reporting. Lack of trust was the main reason why participants did not want to click on links offering cybersecurity advice after the exposure. This shows that more effective methods for encouraging cybersecurity behaviour are still needed.
Keywords: cybersecurity, ransomware, ransom notes, splash screens, user interface, behavioural experiment

---

1. Introduction

Ransomware poses a serious threat to the security of computer systems and the Internet. In its most common form, this type of malicious software (malware) abuses encryption algorithms to lock victims out of their data and demands payment in exchange for their safe decryption [1, 2]. Ransomware is often delivered through phishing emails or by exploiting vulnerabilities in software and networks. Other infection methods are also possible, including drive-by downloads, in which victims would visit a website and inadvertently download the ransomware [3]. Victims could be individuals or organisations. Moreover, besides the "spray and pray" campaigns, ransomware could be deployed in a very targeted manner, such as in the case of the BitPaymer ransomware attack on a Spanish consultancy firm called Everis, in which the encrypted files were given a specific extension name of `.3v3r1s` [4].

It could be argued that the first ransomware incident happened in 1989, during the international AIDS conference organised by the World Health Organization [5]. Attendees were given floppy disks containing a malicious program that counted the number of boots on their MS-DOS systems. When this figure reached 90, the malware hid directories and encrypted filenames, making the affected systems unusable. Victims then encountered a ransom note demanding a payment which should be sent to a post office box in Panama. However, this incident is not considered a part of modern ransomware: the attack itself and the payment method were not sophisticated enough to make it practical or

profitable.

After many hiccups and lots of trial and error on the part of cybercriminals, ransomware evolved into its current form. Modern ransomware is capable of encrypting all types of drives within reach, including cloud backup solutions and shared network drives. This means that infection through a single entry point could easily spread and affect multiple devices [6]. The first instances of modern ransomware can be traced back to 2005 [6]. Although they had a more sophisticated structure when compared to prior ransomware, they commonly had errors in their cryptographic components. Accordingly, they were rarely profitable and easily remedied by antivirus vendors.

There are two main classes of modern ransomware: *lockers* and *crypto-ransomware* [7]. Lockers stop victims from accessing their systems and data, typically with a password set by their authors. Crypto-ransomware, however, encrypts victims' data and without the decryption key the data becomes unusable. In other words, crypto-ransomware directly tampers with the data, while lockers leaves the data intact, but prevent access to it. As such, it is possible for sophisticated users to recover the data affected by lockers, for example by using a clean bootable device (i.e. uncompromised operating system) to access the data directly. Regardless of which class ransomware belongs to, a payment from its victims is requested for the return of their data or access.

The evolution of payment methods plays an important role in the increased prevalence of ransomware attacks. Moving on from primitive methods such as the physical transfer of money or mailing cash to a PO-Box, ransomware authors use nowadays more sophisticated approaches to make it harder to track them. These involve SMS to premium-rate numbers, gift vouchers, payment services (e.g. YandexMoney, Qiwi), prepaid services (e.g. Ukash, Paysafecard), and lastly, cryptocurrencies [8]. With the introduction of cryptocurrencies (e.g. Bitcoin, Ethereum, Monero, Zcash), it has been much harder – yet not impossible – to track down ransomware operators because cryptocurrencies offer a certain degree of anonymity [9].

The impact of ransomware attacks can be felt directly in our society. For

example, in 2020 alone ransomware attacks caused a US natural gas facility to shut down, and in Europe one of the largest energy operators faced extortion, as criminals demanded 10 million euros in exchange for 10 terabytes of sensitive data [10]. After the WannaCry incident in 2017 [11], it is obvious that the healthcare industry faces real threats from ransomware attacks. Cybercriminals continued targeting the healthcare industry even during the global pandemic, as exemplified by an attack on a COVID-19 testing laboratory in Europe, as well as another attack on a hospital in Colorado, which prevented staff from using their patient information system [10]. One of the reasons why the healthcare industry is at high risk is because – in comparison to other industries – healthcare institutions often use unpatched legacy systems that are easier to exploit [12].

1.1. Motivation

Ransomware is a significant threat to both individuals and organisations. Understanding victims' behaviour could help to implement more effective countermeasures against it. An important issue is that remarkably little is known about whether – and how – a ransomware's user interface (UI) features would affect its victims' reaction. To address this shortcoming, an experiment involving a large number of participants was carried out. Each participant was shown a ransomware scenario, and their reactions (with regard to their willingness to pay the ransom demand and whether they would report the incident) were recorded.

1.2. Research objectives and research questions

There were three objectives of this research:

O1: To better understand the triggers behind victim's response, so that we can forecast – and hinder – future attempts by cybercriminals to evolve ransomware into more profitable variants.

O2: To find out whether there are circumstances that can discourage victims from making ransom payment, hence reducing their profitability for the cybercriminals.

O3: To determine whether exposure to a mock-up security incident in the form of a ransomware attack can have a positive impact in the adoption of better cybersecurity practices.

These objectives were formulated as part of our effort to answer the following research questions:

Q1: To what extent can the design of ransomware splash screens affect the way its victims perceive it?

Q2: To what extent does exposure to a ransomware infection scenario influence the participants' later adoption of good cybersecurity behaviour?

1.3. Contributions

The key contributions of this work are as follows:

- In relation to Q1, the results show that there is no statistically significant difference – in terms of payment rate, reporting rate, and adoption of good cybersecurity behaviour – among treatment groups that were shown different ransomware splash screens.
- In relation to Q2, the findings show that a significant proportion of the participants (nearly 75%) did not click on the security advice links provided. In particular, 32% of those who did not click on the links (i.e. 24% of all participants) explicitly raised trust issues. Additionally, a considerable number of them took note of the links to investigate them later.
- The reporting rates of participants in a ransomware scenario were also reviewed, and the findings showed that only around 60% stated they would report the incident. However, the vast majority was not aware of how to report or to whom they should report to.

2. Related Work

Ransomware has become a relatively common threat in the modern world. As a result of its growing popularity, it has drawn interest from researchers from multiple disciplines. Studies on ransomware have involved a variety of perspectives, from detection to prevention, as well as the analysis of its psychological or economic context, to name a few.

2.1. Human aspects

There have been previous works aiming to understand the psychological aspects of ransomware, especially on the victim's part. A study conducted by Arief et al. [13] investigated how ransomware UI components would affect victims' willingness to pay ransoms. Twenty-five participants were shown ransomware samples with differing types of splash screens ("Text", "Time-Sensitive Counter", and "Other") and were asked to answer a set of questions afterwards. Also, during the experiment, the participants' eye movements were tracked in order to understand if any of the UI components were more attention-catching. The study also found that some of the ransomware characteristics might actually discourage victims from making a payment, such as the use of an authoritarian tone in the ransom message, the presence of typos, and the complexity of instructions. Lastly, no inherent impact of ransomware splash screens was observed on payment rates.

While the study conducted by Arief et al. purely focused on ransomware UI components' impact on the willingness to pay ransom demands ("payment rates"), the work presented here was focused on reporting rates and adoption of good security behaviours, on top of the payment rates.

Another study conducted by Hadlington [14] was focused on the psychology behind ransomware splash screens. In particular, that study looked into the UI elements to identify mechanisms that can be used to intimidate victims. The key finding was that even though ransomware splash screens are constructed in widely varying ways, they also have significant similarities in terms of structure

and some other key aspects (e.g. social engineering techniques are often used to make ransom messages more convincing, and many of the splash screens specify a deadline to make a payment; otherwise the compromised files would be deleted). Hadlington's study was purely descriptive regarding the ransomware splash screens' visual appearance. As such, he did not measure the effectiveness of ransomware UI components in terms of payment rates. In comparison, our study focused on empirically measuring the impact of ransomware splash screens with varying UI components in terms of cybercrime reporting, ransom payment and good security behaviour adoption rates.

A recent study conducted by Simoiu et al. [15] was aimed at understanding ransomware prevalence and characteristics through a survey on US citizens. It was estimated that 2-3% of the population get victimised per year, and ransoms are estimated to be $530 on average. Moreover, Simoiu et al. reported that only 4% of the participants paid the ransom. A similar payment rate was found in the current study in all ransomware scenarios tested (see Section 4.2.1).

Research on ransomware prevention has so far been mostly focused on ransomware detection. However, Ferreira [16] emphasised that existing solutions are not effective; instead, studying human factors in ransomware mitigation would be more productive. We agree with this; as such, our work has been focused on how to conduct more effective ransomware information campaigns in order to prevent ransomware infection while, at the same time, looking at ways to improve the mitigation and recovery methods.

2.2. Detection & prevention

Human aspects are not the only areas of interest in ransomware related studies. A multitude of works previously investigated how ransomware can be detected. Tang et al. introduced Ransomspector [17], with an aim to detect ransomware based on an introspection approach, which consists of monitoring virtual machines at the hypervisor layer. Ransomspector provides an additional layer to virtualisation: between the hypervisor and guest operating system, the tool monitors filesystem and network activity to spot ransomware infection.

The Unveil system – developed by Kharaz et al. [18] – is another tool that can be used for detection. Unveil has two main components. The first aims at detecting lockers, and it creates an artificial environment based on user data and monitors filesystem activities around it for any modifications. The second component aims to detect screen lockers; it compares screenshots of the desktop before and after the execution of malware through image analysis methods.

In a study conducted by Huang et al. [19], ransomware payments were tracked end-to-end, and cryptocurrency transactions worth a total of 16 million USD were traced, coming from almost 20 thousand victims. Considering that the number of ransomware complaints reported to the Internet Crime Complaint Center in 2019 was only 2,047 [20] – while at the same time the estimated loss was 8.9 million USD – the study conducted by Huang et al. shows that many – if not most of – ransomware attacks remain unreported and therefore not properly included in any statistics.

3. Methodology

The first research question of our study (Q1 as shown in Section 1.2) was whether the design of a ransomware splash screen would influence the way its victim perceives the ransomware, especially with regard to the likelihood of them paying the ransom or reporting the incident. To answer this question, an experiment was designed based on presenting ransomware infection scenarios with differing types of splash screens to our study's participants. This would then be followed by a survey (discussed in Section 3.2) asking each participant how they reacted to the scenario.

While designing the scenarios, one of the goals was to make them as realistic as possible. To achieve that, existing ransomware variants were investigated, and their characteristics analysed. As a starting point, three main types of ransomware splash screens – as proposed by Arief et al. [13] – were considered:

- "Text": whereby the splash screen is presented in an entirely textual format,

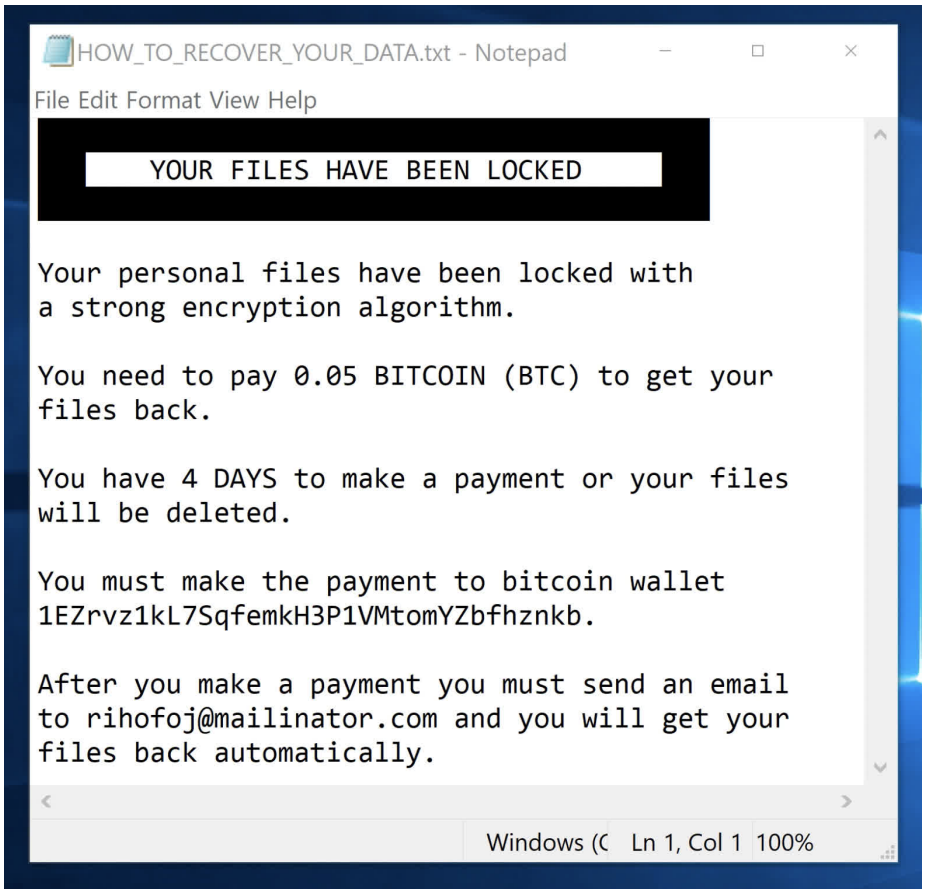

Figure 1: Text-based version of the splash screen

- "Time-Sensitive Counter": in which an active countdown timer is used as a way of applying extra pressure on the victim, and
- "Other": covering those types that do not belong to the first two types.

This classification was adopted in our study. As such, three similar types were used in our study, namely "Text-based", "GUI", and "GUI + Timer".

In the study, ransomware splash screen types were designed to be shown in the scenario accordingly: the focus was on the main differing characteristics of *textual* versus *GUI* versus *timer* features. To minimise the risk of bias, the

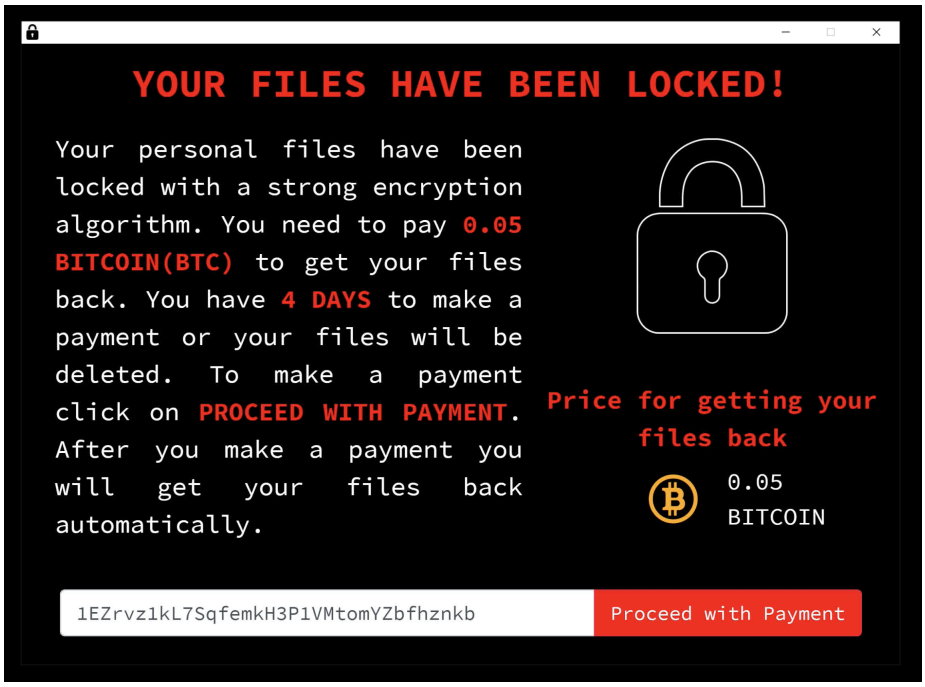

Figure 2: GUI version of the splash screen

three types of splash screens were simplified and standardised into mock-ups, as shown in Figures 1, 2 and 3, respectively.

First, the extracted features from existing ransomware splash screens were introduced, which were then implemented into mock-ups for the study. This was followed by a detailed explanation of the setup for the experiment, as well as the data collection process through an online user study.

3.1. Extracting ransomware features

To better understand how various ransomware splash screen types affect victims' reactions, splash screens with similar contents – but with different ways of displaying the ransom message – were designed for the study. Fifty ransomware splash screen samples from the list on the New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) website [21] were systematically

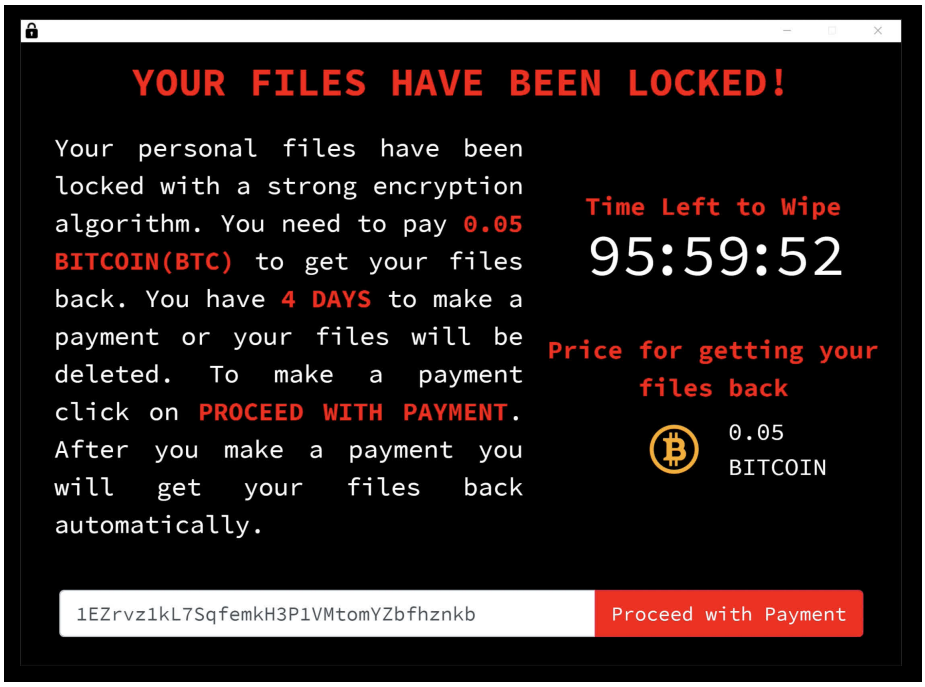

Figure 3: GUI + Timer version of the splash screen

selected for extracting common features for the experiment. We used samples from the NJCCIC because it is a trustworthy US government site that provides a regularly updated overview of the most frequently observed ransomware variants.

The features related to payment methods, the time given to pay the ransom and the means to contact the ransomware operators (if any) were reviewed. The following subsections explain the key features that would later be incorporated into the mock-ups, which would then be used in the study.

3.1.1. Payment methods

First, the payment methods most commonly used by ransomware operators were explored. It was observed that 46 (92%) of the ransom notes explicitly stated the payment method(s). The rest of the ransom messages might contain

email addresses or would ask the victim to contact the ransomware operator to find out how to make a payment. Payment via cryptocurrency was the most prevalent method among the collected data, with a total of 44 (88%) of the ransomware strains observed using this method. Other payment methods were also found, including gift cards (such as Amazon's) and payment services such as Yandex Money (also known as YooMoney[1]) and Qiwi[2].

3.1.2. Time-based elements

A feature of interest was whether ransomware authors used any techniques that might scare victims, such as a countdown timer, to further push victims into making a payment. Out of 50 samples, 31 (62%) of them specified a deadline for the payment. The rest of the samples (38%) did not include any deadline.

Payment deadlines varied between 10 minutes and 31 days. Deadlines to pay were either mentioned with a countdown timer or written in the ransom note. Of these 31 samples, 18 (58%) included a countdown timer, while the rest only mentioned the deadline in the ransom note. To clarify, the difference between the absence and presence of timer as a UI element is illustrated in Figures 2 and 3, respectively.

3.1.3. Contact methods

The analysis also looked into the means to contact ransomware operators. The contact methods were mostly related to the post-payment phase: victims might need to inform ransomware operators after they paid the ransom to get their access or files restored. The most common methods to contact the ransomware operators were via email (24 samples, 48%) or through a payment site (22 samples, 44%). Other methods identified were via Bitmessage, Discord or through a dedicated ransomware GUI. Figure 4 shows the payment website of the Sigma ransomware, which contains instructions on how to make a payment or contact the ransomware operators.

[1] `https://yookassa.ru/docs/support`
[2] `https://qiwi.com/`

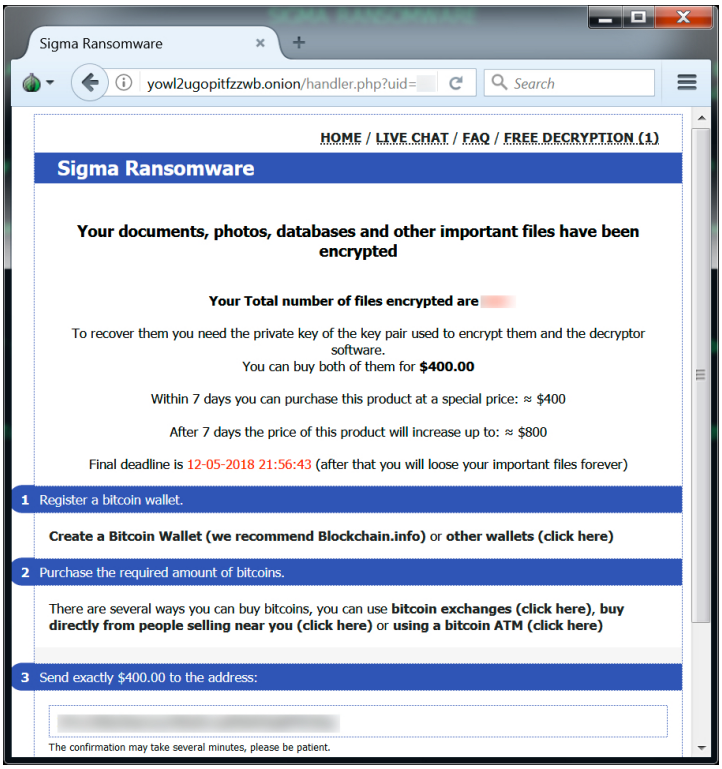

Figure 4: A payment website for the Sigma ransomware [22]

3.2. Experiment design

To better understand the impact of the ransomware splash screen types on victims' behaviour, a randomised controlled experiment was designed with varying splash screen types: "Text-based", "GUI", and "GUI + Timer", as introduced earlier.

The Text-based version consisted of a ransom note in a plain-text file. The GUI version contained an almost identical ransom note with two additional images and a button to further incentivise victims to pay. Lastly, the GUI + Timer version was a GUI variant with a countdown timer added, which indicated the time remaining before the encrypted files get deleted.

The participants were randomly assigned into one of these three groups, so that the numbers assigned to each group were kept reasonably balanced. The

control group contained participants who would see the scenario involving the Text-based version, while two treatment groups were composed of participants who would see the GUI or the GUI + Timer splash screen types.

The three different splash screens types represented the independent variable. The designs of these were based on the data, as explained in the previous section. It was decided to show Bitcoin as the payment method in all of the scenarios since Bitcoin is the most frequently used payment method observed. The given time to make a payment was set to four days – again, because this is the most common value in the samples. The ransom messages were kept consistent across all types of the splash screen, as can be seen in Figures 1, 2 and 3. The amount of 0.05 BTC was chosen because it was the amount found in several of the splash screen samples we analysed, such as Bad Rabbit [23], JNEC.a [24], and WannaRen [25]. The study did not look into the effect of varying the amount of the ransom demand, so it was only necessary to keep the amount consistent.

To collect data for the experiment, a survey was designed, which consisted of three parts (a link to view or download the full questionnaire can be found in Appendix A):

- The first part contained questions about the participant's demographics and security practices (such as backup frequency, whether the participant had any training on cybersecurity and the methods they used to protect their systems).

- In the second part, a ransomware infection scenario was presented through a YouTube video. The same scenario was depicted through Text-based, GUI, or GUI + Timer splash screen types. The assignments of splash screen types were made randomly for each participant. The first question in the second part was used as an attention check question (ACQ) in order to discern whether the participants understood the scenario or not (in case of the latter, the participant's data would be removed from the final data set). Participants were expected to answer ten questions after seeing the

scenario. Those questions were aimed to gather information on what each participant would do in such a situation, including whether they would pay the ransom or not, and if they would consider reporting the incident.

- The third part aimed to find out whether the participants were more likely to take extra precautions post-incident – in other words, whether they would develop good security behaviours or not after being shown the scenario. In this part, useful links to some security solutions and informative links about ransomware were presented to the participants, who were then asked if they clicked on the links to read the useful information or not. Participants were also asked whether they performed backups of their data and whether they used any Multi-factor Authentication (MFA) solutions. If they responded "no" to either of those questions, they were then asked if they would consider using them. A rough estimate was made on the effectiveness of ransomware splash screen demonstrations by comparing the rates of the participants who would consider using backup or MFA solutions for each splash screen type.

Figure 5 shows a graphical representation of the methodology. It can be seen that all participants were asked the same questions regarding their demographics (Part 1), and they were presented with the same scenario debriefing and advice on cybersecurity awareness and good practices (Part 3). However, in Part 2, the participants were shown slightly different scenarios (in terms of splash screen design, but not the content) and asked to complete the same set of questions.

3.3. Data collection

Crowdsourcing platforms are frequently used to collect data in behavioural studies, since they can provide a better representation of the population than what limited participant pools – such as within the confine of the authors' institutions – may offer [26]. In this study, the Amazon Mechanical Turk (MTurk) platform [27] was used to reach out to an extensive pool of participants. It is

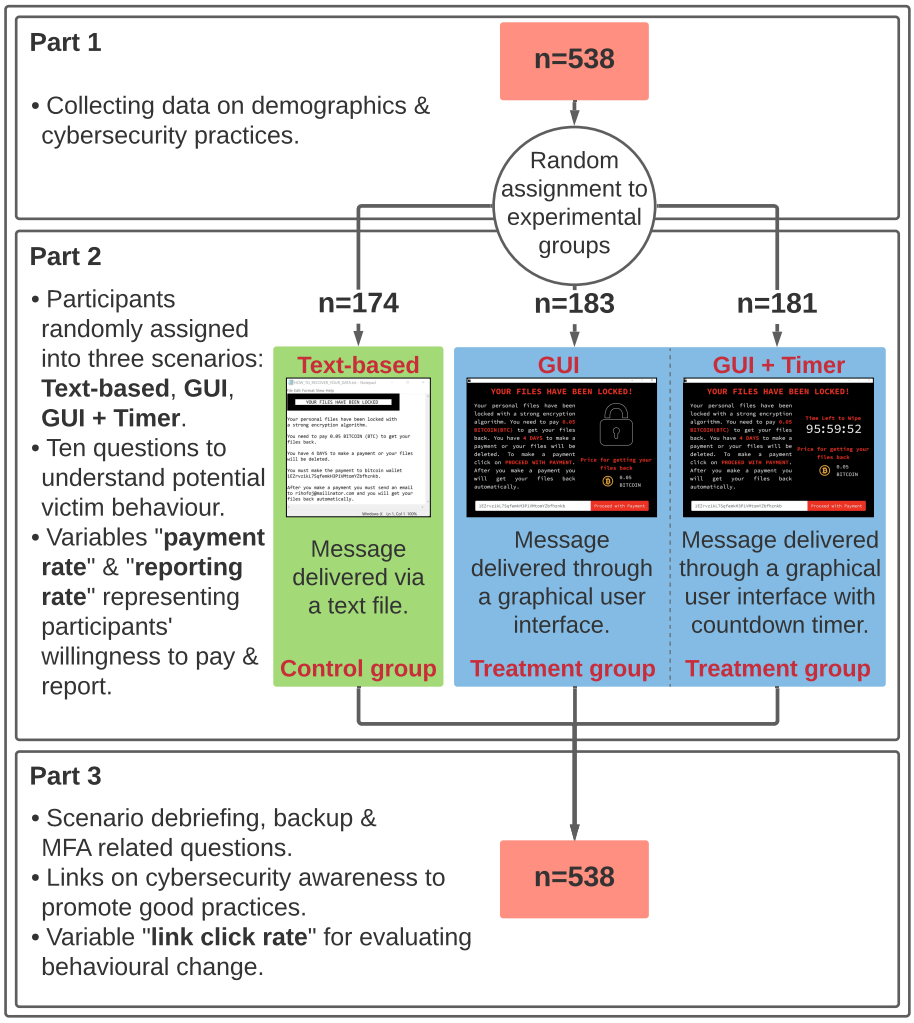

Figure 5: A graphical representation of the research model

estimated that MTurk has more than 100K registered workers, with at least 2K of them being active at any given time [28].

To fine-tune the experiment, several pilots were released on MTurk. To ensure data quality, a decision was made on using the following MTurk qualification filters: each participant must have at least 1,000 approved assignments and a 95% approval rate. These filters are important, as recommended by other

MTurk studies, such as that by Peer et al. [29]. To avoid language barrier issues, location criteria were applied: accepted participants must be from countries considered native English-speaking by the United Kingdom Government's immigration website [30]. These countries include Antigua and Barbuda, Australia, The Bahamas, Barbados, Belize, Canada, Dominica, Grenada, Guyana, Jamaica, New Zealand, Ireland, St Kitts and Nevis, St Lucia, St Vincent and the Grenadines, Trinidad and Tobago, United Kingdom and the United States of America (USA) [30]. Of these countries, the USA has the most number of workers on the MTurk platform.

In the pilots, the average time needed to complete the study was 6 minutes and 24 seconds, and the median was 6 minutes 11 seconds. During the data collection period between June and August 2020, a total of 538 valid responses were received. The average duration for the participants to complete the survey was 8 minutes and 1 second. On average, Parts 1, 2 and 3 took 1 minute 26 seconds, 3 minutes 58 seconds and 2 minutes 37 seconds, respectively.

As stated in Section 3.2, the study involved two treatment groups (GUI and GUI + Timer), on top of the control group (Text-based). Each participant was randomly assigned to one of these three groups. The distribution of the participants with valid responses was as follows:

- Text-based (control group): 174 participants (32.34%)
- GUI (treatment group): 183 participants (34.02%)
- GUI + Timer (treatment group): 181 participants (33.64%)

3.4. Ethical considerations

Two of the most common ethical concerns when using MTurk as a research medium are *compensation* and *anonymity* [31]. Since it was expected that most of the participants would be residents of the USA [28][3], the study's compensation rate was set based on the USA's minimum hourly wage, which was USD

[3]It turned out that 91.45% of the participants were US residents.

Table 1: Participants' demographics and educational background

Demographic information	The number (and percentage) of participants
Female	302 (56.13%)
Male	230 (42.75%)
Other	1 (0.19%)
Prefer not to answer	5 (0.93%)
Age (18-25)	61 (11.34%)
Age (26-30)	75 (13.94%)
Age (31-40)	191 (35.5%)
Age (41-50)	95 (17.66%)
Age (over 50)	116 (21.56%)
Primary/grade school	4 (0.74%)
High school	110 (20.45%)
Associate degree	82 (15.24%)
Bachelor's degree	238 (44.24%)
Master's degree	85 (15.8%)
Doctorate degree	16 (2.97%)
Other	3 (0.56%)

7.25 [32]. Furthermore, no personally identifiable information (PII) that could reveal the participants' identity was collected in the study.

Most importantly, due to ethical and legal concerns, simulating a real ransomware incident – whereby the participants were presented with a surprising and stressful scenario of their files being encrypted in front of their eyes – would not be possible. This is one of the limitations of the study; further discussion on this matter can be found in Section 5.3.

Before letting participants start the survey, their consents were obtained. Prior to releasing the experiment on MTurk, the study was evaluated and approved by the Sabancı University's Research Ethics Council.

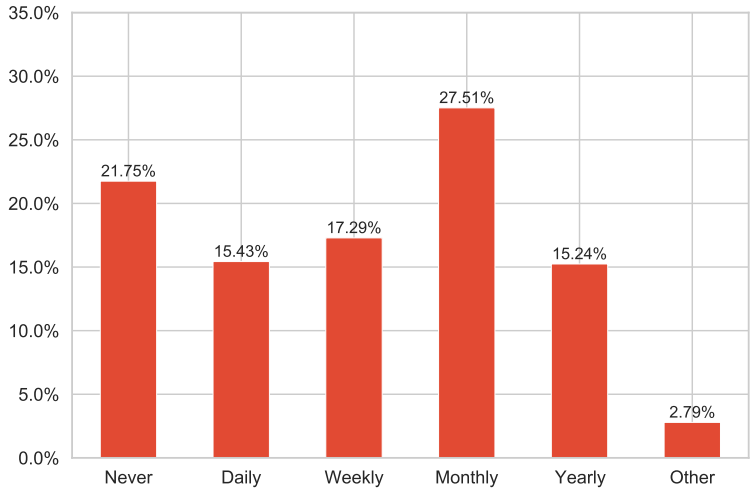

Figure 6: Participants' backup habits

4. Results

4.1. Participants' profile

The first part of the study aimed at knowing the participants' backgrounds, and as such, it consisted of demographics and basic security-related questions. Table 1 shows the statistics regarding participants' demographics. The gender distribution of the participants was as follows: 56.13% was female, 42.75% was male, 0.19% was non-binary, and the rest (0.93%) preferred not to answer. The majority's age was between 31 and 40 (35.5%), followed by 50 and over (21.56%), 41-50 (17.66%), 26-30 (13.94%) and lastly 18-25 (11.34%). The vast majority of the participants were residents of the United States of America (91.45%), 5.39% of them resided in Canada, 1.86% was from the United Kingdom, and the rest were from Australia, Ireland and Saint Vincent and the Grenadines. Almost two-thirds of the participants had a Bachelor's degree or higher.

On top of basic demographic questions, several additional questions were asked to understand participants' technical background. The most common operating system among participants was Windows 10 (68.59%), followed by MacOS (19.33%), Chrome OS (11.75%), older version of Windows (8.18%), and

Table 2: Protection methods used by the participants

Protection method	# unique users
Firewall	313 (58.18%)
Antivirus (regularly updated)	311 (57.81%)
Strong passwords	302 (56.13%)
Keeping software up-to-date	208 (38.66%)
Password manager tool	105 (19.52%)
Virtual private network (VPN)	101 (18.77%)
Antivirus software (not regularly updated)	100 (18.59%)
Encryption product	26 (4.83%)
Other	7 (1.3%)
I do not know	33 (6.13%)

Linux (4.83%). Nearly 45% of the participants stated that they had received some form of security training – either through work, school or other venues. Approximately one-fifth never used backups, and the majority of them backed up their data once a month. Figure 6 shows the participants' backup habits.

The most common security mechanisms used by the participants were antivirus software (76.4%), firewalls (58.18%), and strong passwords (56.13%). One-quarter of antivirus users were not sure whether their software was up-to-date or not. Less than half of the participants kept their software (other than antivirus) up-to-date. Table 2 presents the statistics about the participants' security mechanisms in more detail.

4.2. Behavioural analysis of potential victims

To get a better sense of potential victim's behaviour after a successful ransomware infection, the answers that participants gave in the second part of the experiment were quantitatively analysed. In particular, the effects of the three ransomware splash screen types on the payment and reporting rates were evaluated, as shown in Table 3.

Table 3: Participants' responses after being shown a particular ransomware scenario

	Combined	Text-based	GUI	GUI + Timer
I would pay the ransom	27 (5.02%)	6 (3.45%)	8 (4.37%)	13 (7.18%)
I would report	328 (60.97%)	108 (62.07%)	111 (60.66%)	109 (60.22%)
Seen a similar screen before	158 (29.37%)	47 (27.01%)	47 (25.68%)	64 (35.36%)
Experienced a similar incident	61 (11.34%)	25 (14.37%)	15 (8.2%)	21 (11.6%)

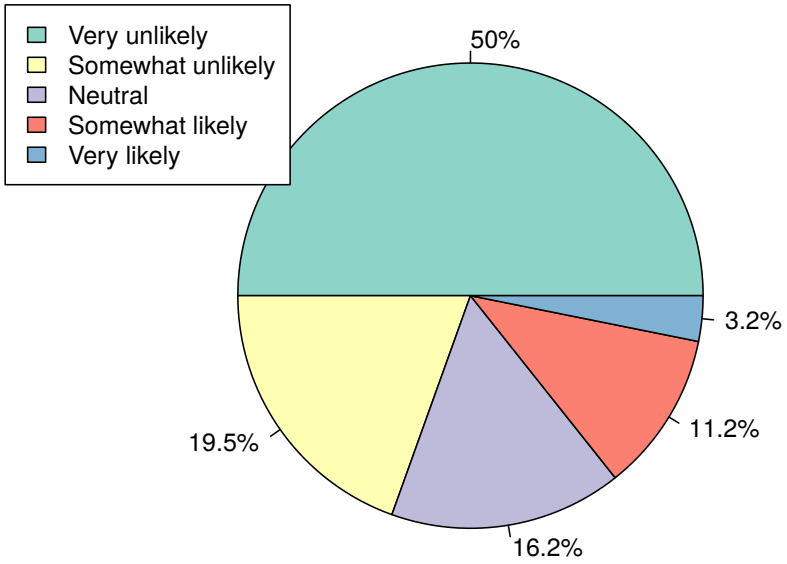

Figure 7: Perceived likelihood of ransomware removal after paying the ransom

The participants were asked whether they had seen or experienced a similar incident before. Almost one-third (across the three different experimental groups) claimed to have seen a similar incident on the Internet news and blogs or other media platforms. Furthermore, 11.34% of them stated that they experienced a similar incident before.

In another question, an evaluation was made on the participants' trust to-

wards getting their files back in the case of paying the ransom demand. Figure 7 shows the responses regarding the participants' perceived likelihood of getting the problem solved by making a payment. Half of the participants thought they would not regain their access or get their files back by making a ransom payment. However, around fourteen per cent believed that there would be a chance of getting their data or access back. This shows that while the majority of the participants did not believe that they would get their files back even if they paid the ransom, there was still quite a significant proportion who would pay.

This is an interesting observation, especially in relation to a published report by CyberEdge [33], which shows that 62.4% of the organisations that participated in their survey had suffered a ransomware infection in 2020, and 57.5% of these chose to pay the ransom demand. The report suggested that 66.9% of the organisations that paid the ransom had a chance to recover their files after payment. The report also indicated that out of the 42.5% who did not pay, 84.5% of them managed to recover their data. This could be because these organisations had good security practices (including regular backups), which would make it easier for them to recover their data without paying the cybercriminals. However, due to the size and nature of the data used in that report – their survey only collected data from 1200 medium to large organisations from 17 countries – it would be prudent not to generalise the findings.

When the participants were asked about their thoughts on the effectiveness of several protection methods against ransomware, it was observed that the overwhelming majority believed that antivirus software was the most useful, followed by firewalls. Approximately half of the participants thought that having backups would be a good precaution. Table 4 shows the perceived effectiveness of common security solutions according to the participants. People who selected the "Other" option stated that having common sense, avoiding clicking suspicious links and not installing untrusted software could also help.

Table 4: Perceived effectiveness of solutions according to participants' responses

Protection method	# unique users
Antivirus	422 (78.44%)
Firewall	313 (58.18%)
Backups	265 (49.26%)
Strong passwords	229 (42.57%)
Keeping software up-to-date	213 (39.59%)
Security awareness training	211 (39.22%)
Virtual private network (VPN)	162 (30.11%)
Encryption product	144 (26.77%)
Password manager tool	97 (18.03%)
Other	15 (2.79%)

4.2.1. Payment rates

Investigating the victims' likelihood with regard to paying the ransom demand could be a useful indicator on the ransomware's success. As shown in Table 3, the findings of the study show that overall, approximately 5% of the participants would pay the ransom in case of infection. Moreover, when the payment rates for each group were analysed, there is an increase from Text-based to GUI, as well as from GUI to GUI + Timer. However, the statistical analysis shows that there is no significant difference between Text-based and GUI + Timer experimental groups (Pearson's Chi-squared test: $\chi^2 = 2.4$, $p = 0.118$). The relatively small sample size could have unavoidable and undesirable effects on the results. However, in this case (n = 27), Pearson's Chi-squared test is a good tool since a minimum of 10 samples is required for a test containing two classes.

A null hypothesis states that there is no significant difference among experimental groups in terms of the victims' payment rates. The findings of this study cannot reject the null hypothesis.

A large majority of the participants indicated that they would not pay the

ransom demanded by the ransomware operators in exchange for a safe turn of their data/access. The study further explored the reasons as to why most of the participants preferred not to pay:

- They thought it was a scam and they would not get their files back
- They thought they could recover through another way
- In order to avoid further extortion, they thought it would be wise not to reward/encourage criminals
- They could not afford to pay the ransom

4.2.2. Reporting rates

Table 3 also shows the reporting rates for each of the groups in the experiment, as well as the combined rate. Approximately 60% of the participants replied that they would report this incident. However, when it was asked which authority they would report this to, responses such as police and other generic law enforcement agencies were observed. Only a small portion of them (around 2%) pointed out the specific authorities to report, such as Internet Crime Complaint Center (IC3), Cybersecurity and Infrastructure Security Agency (CISA), and The Australian Cyber Security Centre (ACSC). The rest (approximately 40%) declared that they would report nothing. The common reasons for not reporting was because they did not know where to report to, or they had a lack of trust in the authorities with regard to tracking the criminals, or they could not be bothered with reporting. Some of the participants also stated that they would feel ashamed to admit being a victim of ransomware infection, and some were scared of possible "retribution" from cybercriminals.

4.2.3. Post-infection actions

To understand post-infection victim behaviour, the study's participants were asked what they would do if they experienced a ransomware attack. About 40% of the participants would rely on their antivirus software to remove the ransomware infection. Getting help from someone else was suggested by 28.44%

Table 5: Action taken after the appearance of a ransomware splash screen

	Combined	Text-based	GUI	GUI + Timer
Remove with an antivirus program	219 (40.71%)	80 (45.98%)	64 (34.97%)	75 (41.44%)
Take it to someone else	153 (28.44%)	53 (30.46%)	51 (27.87%)	49 (27.07%)
Search online	148 (27.51%)	48 (27.59%)	55 (30.05%)	45 (24.86%)
Format the entire PC	136 (25.28%)	34 (19.54%)	52 (28.42%)	50 (27.62%)
Other	34 (6.32%)	10 (5.75%)	11 (6.01%)	13 (7.18%)

of the participants. The most common places the participants would go for help were either a computer repair shop or the place where they bought their computer from. Just under 28% of the participants stated that they would search online to find a solution. Some of the most common search terms were the ransom message itself, the given bitcoin address, and open questions such as "How do I get rid of ransomware?". One-quarter of the participants mentioned that they would format and reinitialise their systems without bothering to deal with the encrypted files. Table 5 provides a detailed breakdown of the post-infection actions across all groups.

4.3. Promoting good security behaviour

In the final part of the study, the participants were presented with some useful security information and advice regarding ransomware infection, recovery and prevention methods. The importance of backups and multi-factor authentication (MFA) against cyber threats was emphasised. Moreover, questions on whether the participants were currently using backups or MFA solutions were

Table 6: The rates of participants' backup and MFA usages, as well as the likelihood of the participants clicking the security advice links

	Combined		Text-based		GUI		GUI + Timer	
	#	usage	#	usage	#	usage	#	usage
I am backing up my data	538	390 (72.49%)	174	130 (74.71%)	183	125 (68.31%)	181	135 (74.59%)
I am using MFA	538	384 (71.38%)	174	123 (70.69%)	183	129 (70.49%)	181	132 (72.93%)
I clicked on at least one link	538	132 (24.54%)	174	39 (22.41%)	183	47 (25.68%)	181	46 (25.41%)
I would consider backing up my data	148	124 (83.78%)	44	38 (86.36%)	58	47 (81.03%)	46	39 (84.78%)
I would consider using MFA	154	118 (76.62%)	51	40 (78.43%)	54	42 (77.78%)	49	36 (73.47%)

asked. If they were not using these two security mechanisms, they were asked whether they would consider using backup or MFA solutions after participating in this study.

First, the popularity of backup and MFA solutions among the participants was calculated. Table 6 presents the backup and MFA solutions usage rates among the control and treatment groups in the experiment. It was found that 72.49% of the participants were already backing up their data, and 71.38% were using MFA solutions in at least one of their online accounts.

As a reminder, the second research question of the study aimed to investigate whether taking part in this study would encourage participants to adopt backup and MFA solutions. Table 6 shows that participants who did not use these protection mechanisms prior to the study had a certain willingness to use backup and MFA solutions after being presented with the ransomware attack scenario. Adoption rates, however, were similar among both treatment groups. Therefore, it is concluded that presenting GUI or GUI + Timer splash screens – instead of Text-based splash screen – would not increase the MFA or backup adoption

Table 7: Detailed analysis of link clicks

	Combined	Text-based	GUI	GUI + Timer
Informative	88 (39.82%)	22 (37.29%)	34 (43.59%)	32 (38.10%)
Backup-related	52 (23.53%)	15 (25.42%)	14 (17.95%)	23 (27.38%)
MFA-related	81 (36.65%)	22 (37.29%)	30 (38.46%)	29 (34.52%)
Total	221 (100%)	59 (100%)	78 (100%)	84 (100%)

rates significantly.

Finally, useful security links were also presented to the participants. These links could be classified into three categories: informative, backup-related and MFA-related. The informative category consisted of links to webpages that offer information about ransomware decryptors, authorities to report cybercrime and detailed information on best cybersecurity practices. Backup-related and MFA-related categories provided links to various backup and MFA solutions. Approximately one-quarter of all participants (24.54%) clicked on at least one of the links provided (see Table 6). Clicking rates among experiment groups were close to each other, which resulted in no significant difference in terms of the impact of ransomware splash screens.

Table 7 shows the detailed statistics regarding the clicking rates of the three categories of links. In total, 221 link clicks were recorded throughout the experiment, and it was observed that the click rates for informative and MFA-related links were higher compared to backup-related ones. Furthermore, it was found that participants from the treatment groups were more willing to click on the links in order to investigate the useful resources further. However, these differences were not statistically significant (Pearson's Chi-squared test: $\chi^2 = 0.62871$, $p = 0.7303$). Approximately two-thirds of the participants who

Table 8: Distribution of link clicks

	Combined	Text-based	GUI	GUI + Timer
Clicked one link	89 (67.42%)	28 (71.80%)	30 (63.83%)	31 (67.39%)
Clicked two links	25 (18.94%)	5 (12.82%)	14 (29.79%)	6 (13.04%)
Clicked 3 or more links	18 (13.64%)	6 (15.38%)	3 (6.38%)	9 (19.57%)
Total	132 (100%)	39 (100%)	47 (100%)	46 (100%)

Table 9: A summary of reasons why users did not click on the information security links

Category	# unique users
Trust issues	130 (32.01%)
Claims to have the resources and/or awareness	93 (22.90%)
Claims to deal with it in the future	86 (21.18%)
Not worried or interested	61 (15.02%)
Do not have time	45 (11.08%)
Irrelevant & Unclear	14 (3.44%)
Other	19 (4.67%)

clicked on the links only clicked one of the thirteen links provided (see Table 8). One-third of the participants spent additional time viewing more than one resource.

4.3.1. Reasons for ignoring security advice links

In total, 406 participants did not click on any of the security advice links. To gain more insights into the reason behind this decision, a qualitative analysis of the explanations given by the participants who did not click on any security advice links was performed.

Table 9 presents the number of unique participants and the percentage of participants who did not click on the links, with the reasons they provided. The reasons can be grouped into seven main categories: (*i*) trust issues; (*ii*) do not have time; (*iii*) claims to already have the resources and/or awareness; (*iv*) not worried or interested; (*v*) claims to deal with it in the future; (*vi*) irrelevant and unclear and; (*vii*) other.

Trust issues. Around 32% of the participants did not want to click on any security advice links due to trust issues. They were worried that this could be a phishing attack or another type of scam to install ransomware or steal personal information. Some participants specifically stated that they thought these links were a test placed by the study designers to see how many participants could be tricked by the study to click on (assumed) malicious links. Furthermore, many stated that they did not know the domains presented in the study; thus, they preferred not to take a look at them. This shows the importance of being able to convey useful information that would allow non-experts to reliably distinguish security advice links from phishing and malware download links. This information can be useful to extend the effectiveness of cybersecurity information campaigns or security notifications.

Claims to have the resources and/or awareness. Almost 23% of the participants stated that they had the necessary resources and awareness to deal with cyber threats. Some of these participants also mentioned the protection mechanisms and procedures that they used. In contrast, others claimed to be aware of all the links and ways to protect themselves against cyberattacks. A few participants also mentioned that they work in cybersecurity or a related field, professionally. Lastly, one participant indicated that they did not need any further information because they were a former hacker, and they designed and implemented malicious software to steal passwords.

Claims to deal with it in the future. Interestingly, a high number of participants (n = 86, or 21.18%) stated that they would take a look at the links later. Some

also mentioned that they took a screenshot of the pages, while others indicated that they copied the links into their computers to take a look after the survey. This shows that the study had a good potential to provide an indirect effect of promoting security advice, if this were to be believed. This also indicates that counting link clicks would only include information on immediate action taken by the participants. Therefore, the study's effectiveness in promoting security advice might have been underestimated.

Not worried or interested. About 15% of the participants claimed that they were not worried about cyberattacks nor interested in the links mentioned in the study. Some of these participants stated that they did not have anything worth stealing or ransoming.

Do not have time. Around 11% of the participants reported that they did not have time to click on the links to conduct further research on the topic. Some of these participants stated that they would prefer finishing this MTurk job and picking up another one quickly to earn more money rather than spending time to gain insights on cybersecurity. This is a common behaviour in crowdsourcing platforms. Perhaps a different incentive mechanism or demonstration can be used to increase user engagement in the future. On a similar note, cybersecurity information campaign designers should also consider issues such as this while designing their campaign websites and posters.

Irrelevant & Unclear. Around 3.4% of the participants did not understand the question correctly and provided irrelevant answers. Their responses were not discarded because their answers to other questions were logical, and they did not fail the attention check question. They mainly stated that they did not click on the links but did not state the reason behind their decision.

Other. A few participants (n = 19 or 4.67%) provided other explanations, such as not finding materials presented in the study useful. The ones who did not find the links useful did not add any reason behind their answer. Their responses were short and lacked details.

5. Discussion

This section provides an evaluation of the main results and discusses directions for future research, as well as the limitations of the study.

5.1. Effectiveness of Timer component

The security community knows surprisingly little about the influence of ransomware splash screens on the victims. It is a common belief that timers on ransomware splash screens push users to ignore rational security decisions and pressure them into paying the ransom in order to prevent data loss. Surprisingly, in this study, no evidence was found to suggest that having a timer on a ransomware splash screen would increase the likelihood of the victim to pay the ransom demand, as compared with ransomware splash screens without a timer.

On the other hand, the experiment setup in this study might not accurately reproduce the stress and emotional trauma caused by ransomware attacks and splash screen timers. This is one of the study's limitations, which are discussed further in Section 5.3. Nevertheless, it could be argued that infecting participants' real assets in order to replicate a real ransomware infection is unethical.

Additionally, in real-life cases of ransomware infection, victims would likely be forced to look at the ransomware splash screen for a long time. This could also play a role in the payment and reporting process.

The scenarios demonstrated in this study only concern individuals using their own personal computers. Businesses and organisations might react very differently due to the large sums of money involved. In business cases, victims might also try to negotiate with the attackers in order to reduce the ransom amount. Even with these limitations, this study reveals similar payment rates and victim reactions compared to other studies [13, 15]. This indicates that in the majority of cases, the timer element would have a very limited impact on the victims' choices.

Ransomware authors seem to be trying different combinations of splash screen schemes to increase their profits. However, judging by the results of

this study, none of the analysed strategies seemed to work significantly better than others. So thankfully, ransomware authors have not found yet a way to increase their profitability in this way – and we would like to keep it that way. As they will no doubt keep exploring new ways to put extra pressure on victims to pay, it would be useful to repeat this study periodically to detect as soon as possible whether they have come up with a new and more successful strategy, so it would be possible to react to this new threat accordingly and effectively.

5.2. Direct and indirect impact of promoting security advice

Promoting security advice is a common problem in cybersecurity. Typically, users are not willing to invest time and resources into securing their online assets. Even when they are notified about an infection, Internet users are less interested in learning more about security tips to remediate or visit security advice links to prevent future abuse [34]. This situation is similar when users are notified to patch a vulnerability or misconfiguration [35]. As a result of this, users remain vulnerable to various cyberattacks.

The study presented in this paper first introduced a successful ransomware attack scenario and then asked participants to describe what they would do in this situation. It was expected that having this experience would incentivise them to invest more time in prevention and recovery methods such as backup and other generic cybersecurity tips. The results showed that almost a quarter of the participants clicked on the security advice links. These were the ones that decided to take immediate action. Additionally, insights gained from the ones that did not click the security advice links provide evidence that around 16% of all participants also benefited from the links after the survey. When both immediate and potential indirect actions are combined, around 40% of the participants were estimated to benefit from these security advice links. This is quite a high figure compared to the number of visits in abuse and vulnerability notifications studies [34, 35, 36]. This might be because, in this study, the security advice contents and ransomware attack scenario were presented as a part of the questionnaire, compared to security email notifications, which could

be easily discarded or removed by the users.

Of course, it is also possible that some participants might not get the maximum benefit, and they did not follow the advised security solutions for various reasons. However, visiting these links also shows initial willingness towards improving their cybersecurity knowledge or adopting security products.

The study also shows that one of the main reasons why participants did not take immediate action is due to a lack of trust in the displayed links or the study designers – even when the links were hosted at trusted sites such as the UK National Cyber Security Centre. Security-conscious users might consider all links as security threats. This is indeed a good practice for avoiding malicious links. However, this could also prevent users from gaining valuable cybersecurity-related information. All of these put a premium on finding a way to increase the credibility and trustworthiness of the security advice. One way forward could be increasing the popularity of the government and security initiative links through advertisements, TV shows and social media.

5.3. Limitations

There are three main limitations associated with this study. First, the results and the data are tied to the MTurk participant pool, which is mainly from the United States [37]. Therefore, there is an over-representation of US citizens.

The second limitation is that the data were collected only from residents of native English-speaking countries due to the experiment design choices. The reason behind this was to make sure that the participants understood the content of the questionnaire and they would know how to answer the questions easily and consistently. Therefore, the generalisability of this work is a matter of replicating studies in other crowdsourcing platforms and qualitative lab studies.

Finally, the third limitation is on the ecological validity of replicating or simulating the real impact of a ransomware infection. The true nature of this kind of cyberattack is very stressful. For ethical reasons, it was not possible to reproduce the stressful context of risk, urgency, loss and guilt in which many

of the victims, unfortunately, would find themselves in when presented with a real ransomware splash screen. It may be the case that, under these conditions, the different splash screens analysed in this work might lead to very different outcomes. This is an inherent limitation of this work – or any other research that operates within a reasonable ethical framework – and it is suggested that any reader remain acutely aware of this limitation before reading too much into our conclusions. In the future, addressing this limitation will be attempted by devising alternative ways to study such phenomena, most likely based on post-incident interviews that come with their own methodological limitations.

6. Implications

The growing and persistent threats of ransomware attacks show the need for impactful research in this area. The current state of the literature in ransomware research indicates that there are many areas for improvement. These include the increasing need to not overlook the human aspects when considering the prevention methods, for example, as highlighted by Ferreira [16]. This is one of the shortcomings that the work presented in this paper is addressing. Increasing awareness among Internet users could have an important role in fighting ransomware, and to do so, behaviours and perceptions of Internet users should be better understood.

The results also indicate that demonstrating a ransomware scenario can be very useful at promoting security training materials. However, trust issues towards clicking security links decrease the potential benefits gained by the demonstration. This is a problematic issue to address since clicking on any links on the Internet could easily set off all kinds of security red flags for conscious Internet users. Moreover, attackers could also leverage information campaigns to distribute their malicious links. One way to move forward could be to host up-to-date security advice materials in trusted and secure sites such as CERTs or governmental websites. Moreover, the use of mainstream channels such as TV and newspapers could help in raising awareness of these websites. Another

approach could be to provide security training materials without external links. Future work will determine which one(s) of these alternatives will have a more observable impact on promoting security training materials.

Another implication is that the majority of the participants would like to report ransomware incidents. However, the findings from the study show that an overwhelming majority cannot identify the right authority to file a complaint to. This observation highlights the need for better and more effective cybersecurity awareness campaigns, which would allow potential victims to know how to recognise a security threat, how to report them, how to find potential remediation steps and where to get further help from. Concerning cybercrime reporting, an additional observation from this study was that a small – yet not insignificant – proportion of the participants who chose not to report (14.76%) had a lack of trust in the authorities's ability for tracking and remediating cybercrime. Authorities might consider developing more transparent policies such that victims could query the status of their case after filing a report. Another possible solution could be through improving the usability and accessibility of cybercrime reporting tools and interfaces.

Finally, despite the ransomware authors' evolving scare tactics to pressure victims into paying the ransom, no evidence has been found that these techniques – as delivered through the ransomware splash screen – would affect the victims' willingness to pay. This is a positive and encouraging finding. Nonetheless, it is fair to assume that ransomware authors will continue to conceive and develop new schemes to try and increase their profit. Therefore, it is imperative to keep abreast of the new tactics used by ransomware authors and operators in order to assess their effectiveness. This would allow security researchers to devise more appropriate countermeasures against these new threats.

7. Conclusions

In this paper, an empirical study to measure the impact of different ransomware splash screens was carried out, testing variants such as text file, a

GUI, or a GUI with a countdown timer. The evaluation is based on the likelihood of victims paying the ransom demand or reporting the incident. The results show that there is no evidence that ransomware splash screens influence victims' behaviour as gathered through their responses.

A key finding of the study is that only 5% of the participants would pay the ransom demand after being presented with a ransomware scenario. This result is consistent with other studies, such as the work by Simoiu et al. [15].

A large number of participants – 328 out of 538 participants – stated that they would report such an incident. However, they were not sure regarding whom to report to. Generic authorities, made-up authority names and police departments were suggested in the participants' responses, even though most of the police departments do not have a cybersecurity division.

The investigation into which security mechanisms were being used by the study's participants reveals that there were high rates of backup and MFA solutions (around 70% in both cases). Moreover, over 75% of the participants who had not employed those solutions prior to the study stated that they would consider using them after taking part in the study. This shows that demonstrating cyberattacks could be a good method for raising awareness and promoting better security practices.

The analysis of the security advice click rates reveals that approximately one-quarter of the participants clicked on at least one of the links provided. This shows that ransomware demonstrations can be a useful tool to promote responsible security behaviour. On the other hand, the same mechanism can be used by attackers to disseminate their malware or even for launching phishing attacks. Thus, future work will have to determine ways to avoid and prevent malicious cybersecurity awareness campaigns. Additionally, an effort was made to better understand why most of the participants did not click on these links. A majority stated that they did not trust the links or the study designers, even when links were hosted in trusted third party domains. Other reasons mentioned by the participants were that they believed they already had enough awareness or access to resources, or that they did not have time to follow up on the links,

or that they were not interested or worried about the topic. Surprisingly, some users claimed to have saved the links to read the advice later.

Moving forward, two areas of study to build on this work are suggested. First, it is important to conduct further investigations into how the effectiveness of cybercrime reporting can be increased. Second, it is imperative to deal with the double-edged sword of disseminating cybersecurity advice. This is a very complex challenge, but it could be addressed, for example, through an initiative involving national CERTs and other government agencies. The aim here is to create more credible and trustworthy channels for providing actionable advice to Internet users.

8. Acknowledgement

Part of the work presented in this paper was funded by the UK Engineering and Physical Sciences Research Council (EPSRC) project EP/P011772/1 on the EconoMical, PsycHologicAl and Societal Impact of RanSomware (EMPHASIS).

References

[1] A. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, E. Kirda, Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks, in: Intl Conf on Detection of Intrusions and Malware, and Vulnerability Assessment, Springer, 2015, pp. 3–24.

[2] E. Kolodenker, W. Koch, G. Stringhini, M. Egele, PayBreak: Defense Against Cryptographic Ransomware, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 2017, pp. 599–611.

[3] G. Hull, H. John, B. Arief, Ransomware deployment methods and analysis: views from a predictive model and human responses, Crime Science 8 (1) (2019) 2.

[4] J. M. Esparza, Blueliv, Spanish consultancy everis suffers bitpaymer ransomware attack: a brief analysis (November 2019).
URL https://tinyurl.com/rm5lf6m

[5] A. L. Young, M. Yung, Cryptovirology: The birth, neglect, and explosion of ransomware, Communications of the ACM 60 (7) (2017) 24–26.

[6] K. Cabaj, W. Mazurczyk, Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall, IEEE Network 30 (6) (2016) 14–20. doi:10.1109/mnet.2016.1600110nm.

[7] K. Savage, P. Coogan, H. Lau, The Evolution of Ransomware (2015).
URL https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

[8] P. O'Kane, S. Sezer, D. Carlin, Evolution of ransomware, IET Networks 7 (5) (2018) 321–327. doi:10.1049/iet-net.2017.0207.

[9] J. Hernandez-Castro, E. Cartwright, A. Stepanova, Economic Analysis of Ransomware, Available at SSRN 2937641.
URL http://arxiv.org/abs/1703.06660

[10] Kaspersky, Ransomware 2018-2020.
URL https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2020/05/12075747/KSN-article_Ransomware-in-2018-2020-1.pdf

[11] Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) Report (Jul 2020).
URL https://tinyurl.com/y9fk5x6o

[12] J. Gomez, C. Konschak, Cyber-security in healthcare (2015).
URL https://www.divurgent.com/wp-content/uploads/2015/03/Cyber-Security-Healthcarepdf.pdf

[13] B. Arief, A. Periam, O. Cetin, J. C. Hernandez-Castro, Using eyetracker to find ways to mitigate ransomware, in: 6th Int'l Conf. on Information Systems Security and Privacy (ICISSP 2020), 2020, pp. 448–456.

[14] L. Hadlington, Exploring the psychological mechanisms used in ransomware splash screens, Tech. rep. (2017).

[15] C. Simoiu, J. Bonneau, C. Gates, S. Goel, "I was told to buy a software or lose my computer. I ignored it": A study of ransomware, in: Fifteenth Symposium on Usable Privacy and Security ({SOUPS} 2019), 2019.

[16] A. Ferreira, Why ransomware needs a human touch, in: 2018 Int'l Carnahan Conf. on Security Technology (ICCST), IEEE, 2018, pp. 1–5.

[17] F. Tang, B. Ma, J. Li, F. Zhang, J. Su, J. Ma, Ransomspector: An introspection-based approach to detect crypto ransomware, Computers & Security (2020) 101997.

[18] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, E. Kirda, {UNVEIL}: A large-scale, automated approach to detecting ransomware, in: 25th {USENIX} Security Symposium, 2016, pp. 757–772.

[19] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, J. Levin, K. Levchenko, A. C. Snoeren, D. McCoy, Tracking ransomware end-to-end, in: 2018 IEEE Symposium on Security and Privacy (SP), IEEE, 2018, pp. 618–631.

[20] Federal Bureau of Investigation, 2019 Internet Crime Report.
URL `https://pdf.ic3.gov/2019_IC3Report.pdf`

[21] New Jersey Cybersecurity & Communications Integration Cell (NJCCIC), Ransomware.
URL `https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants`

[22] SANS Internet Storm Center, Malspam pushing sigma ransomware.
URL https://isc.sans.edu/forums/diary/MalspampushingSigmaransomware/23443/

[23] O. Mamedov, F. Sinitsyn, A. Ivanov, Bad rabbit ransomware (Oct 2017).
URL https://securelist.com/bad-rabbit-ransomware/82851/

[24] I. Ilascu, JNEC.a Ransomware Spread by WinRAR Ace Exploit (Mar 2019).
URL https://www.bleepingcomputer.com/news/security/jneca-ransomware-spread-by-winrar-ace-exploit/

[25] C. Cimpanu, WannaRen ransomware author contacts security firm to share decryption key (Aug 2020).
URL https://tinyurl.com/s8khx6n7

[26] T. S. Behrend, D. J. Sharek, A. W. Meade, E. N. Wiebe, The viability of crowdsourcing for survey research, Behavior research methods 43 (3) (2011) 800.

[27] Amazon Mechanical Turk.
URL https://www.mturk.com/

[28] D. Difallah, E. Filatova, P. Ipeirotis, Demographics and dynamics of mechanical Turk workers, in: Proceedings of the eleventh ACM international conference on web search and data mining, 2018, pp. 135–143.

[29] E. Peer, J. Vosgerau, A. Acquisti, Reputation as a sufficient condition for data quality on Amazon Mechanical Turk, Behavior research methods 46 (4) (2014) 1023–1031.

[30] GOV.UK, Prove your knowledge of English for citizenship and settling (Dec 2014).
URL https://www.gov.uk/english-language/exemptions

[31] J. Chandler, D. Shapiro, Conducting clinical research using crowdsourced convenience samples, Annual Review of Clinical Psychology 12 (1) (2016) 53–81. doi:10.1146/annurev-clinpsy-021815-093623.

[32] U.S. Department of Labor, Minimum wage.
URL https://www.dol.gov/general/topic/wages/minimumwage

[33] CyberEdge, 2020 Cyberthreat Defense Report.
URL https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf

[34] O. Cetin, M. Hanif Jhaveri, C. Gañán, M. van Eeten, T. Moore, Understanding the role of sender reputation in abuse reporting and cleanup, Journal of Cybersecurity 2 (1) (2016) 83–98.

[35] O. Cetin, C. Ganan, M. Korczynski, M. van Eeten, Make notifications great again: learning how to notify in the age of large-scale vulnerability scanning, in: Workshop on the Economy of Information Security, 2017.

[36] B. Stock, G. Pellegrino, F. Li, M. Backes, C. Rossow, Didn't you hear me?—towards more successful web vulnerability notifications.

[37] N. Stewart, C. Ungemach, A. J. Harris, D. M. Bartels, B. R. Newell, G. Paolacci, J. Chandler, et al., The average laboratory samples a population of 7,300 amazon mechanical turk workers, Judgment and Decision making 10 (5) (2015) 479–491.

Appendix A. Questionnaire

The questionnaire described and used in this paper can be downloaded from: https://drive.google.com/file/d/18TrMgd-6Y1yoHwg5Yi_K1CQxNhQfL80y