Personality Types and Ransomware Victimisation

YAGIZ YILMAZ, Sabancı University, Turkey
ORCUN CETIN, Sabancı University, Turkey
CLAUDIA GRIGORE, University of Kent, United Kingdom
BUDI ARIEF, University of Kent, United Kingdom
JULIO HERNANDEZ-CASTRO, University of Kent, United Kingdom

Ransomware remains one of the most prevalent cyberthreats to individuals and businesses alike. Psychological techniques are often employed by attackers when infecting victims' devices with ransomware, in an attempt to increase the likelihood of the victims paying the ransom demand. At the same time, cybersecurity researchers are continually putting in effort to find new ways to prevent ransomware infections and victimisation from happening. Since employees and contractors are often considered to be the most frequent and well-known attack vectors, it makes sense to focus on them. Identifying factors to predict the most vulnerable population to cyberattacks can be useful in preventing or mitigating the impact of ransomware attacks. Additionally, understanding victims' psychological traits can help us devise better solutions to recover from the attack more effectively, while at the same time, encouraging victims not to pay the ransom demand to cybercriminals. In this paper, we investigated the relationship between personality types and ransomware victimisation, in order to understand whether people with certain personality types would be more prone to becoming a ransomware victim or not. We also studied the behavioural and psychological effects of becoming a ransomware victim, in an attempt to see whether such an experience can be used to reinforce positive cybersecurity behaviours in the future. We carried out a survey involving 880 participants, recruited through the Prolific online survey platform. First, these participants were asked to answer a set of standard questions to determine their personality type, using the Big-Five personality trait indicators. They were then asked to answer several follow-up questions regarding victimisation, as well as their feelings and views post-victimisation. We found that 9.55% (n=84) of the participants had been a victim of ransomware. Out of these, 2.38% (n=2) were found to have paid the ransom. We found no compelling evidence to suggest that personality traits would influence ransomware victimisation. In other words, there are no discernible differences regarding potential ransomware victimisation based on people's personality types alone. Therefore, we should not blame victims for falling prey – in particular, we should not apportion the blame to their personality type. These findings can be used to improve positive cybersecurity behaviours, for example, by encouraging victims to invest more in cybersecurity products and tools. Additionally, our results showed that the aftermath of a ransomware attack could be quite devastating and hard to deal with for many victims. Finally, our research shows that properly dealing with ransomware is a complex socio-technical challenge that requires both technical and psychological support.

CCS Concepts: • **Security and privacy** → **Social aspects of security and privacy**; *Malware and its mitigation*; • **Social and professional topics** → *User characteristics.*

Additional Key Words and Phrases: ransomware, personality types, big-five, victimisation, socio-technical security, user study, cybercrime, cybersecurity behaviours

Authors' addresses: Yagiz Yilmaz, yagizyilmaz@sabanciuniv.edu, Sabancı University, Turkey; Orcun Cetin, orcun.cetin@sabanciuniv.edu, Sabancı University, Turkey; Claudia Grigore, claudia.dan@gmail.com, University of Kent, United Kingdom; Budi Arief, b.arief@kent.ac.uk, University of Kent, United Kingdom; Julio Hernandez-Castro, jch27@kent.ac.uk, University of Kent, United Kingdom.

Manuscript submitted to ACM

ACM Reference Format:

Yagiz Yilmaz, Orcun Cetin, Claudia Grigore, Budi Arief, and Julio Hernandez-Castro. 2022. Personality Types and Ransomware Victimisation. *Digit. Threat. Res. Pract.* 1, 1, Article 1 (October 2022), 29 pages. https://doi.org/10.1145/3568994

1 INTRODUCTION

Ransomware continues to be a major and growing threat in the cybersecurity domain, especially because our lives are getting more and more dependant on the digital systems we rely on and use day after day. Ransomware could be considered a risk to both individuals and organisations. Whilst ransomware could be released in the wild without any specific target (such as in the case of the WannaCry ransomware incident [22]), it could also be utilised as a weapon against a specific individual or organisation, as seen in the case of the Kaseya ransomware attack [26].

Reports published by various cybersecurity companies provide a good overview of the current state of ransomware. According to the Global Threat Landscape Report by Fortinet published in August 2021, the prevalence of ransomware among organisations has shown a growth of 1,070% from July 2020 to June 2021 [17]. Furthermore, high profile incidents – such as the Colonial Pipeline hack, which resulted in a ransom payment of US$4.4 million [3], and the ransomware attack on JBS, who paid US$11 million in ransom [19] – caused the US Department of Justice to increase the level of security concern of ransomware, which is now similar to that of terrorist attacks [2]. Moreover, 85% of the business leaders and cybersecurity professionals surveyed by Fortinet in 2021 denoted that ransomware is a bigger risk compared to other cyberthreats [8].

However, according to Sophos' survey of IT decision-makers, the chance of getting hit by ransomware showed a decreasing trend (54%, 51%, and 37% for years 2017, 2020 and 2021, respectively). Yet, the cost of ransomware remediation has increased considerably. For example, the average remediation cost per incident for 2020 was estimated at US$761,106 while the estimate for 2021 had increased to US$1.85 million [35].

Ransomware is a type of malware that blackmails its victim into paying a ransom in return for gaining access back to their data or device, or for preventing the victim's embarrassing or compromising data from being revealed to the world [13]. The first incident of ransomware occurred in 1989 when the *AIDS Trojan* (also known as the *PC Cyborg*) was distributed to the participants of the World Health Organization's AIDS conference in floppy discs [34]. The distributed discs were labelled "AIDS Information – Introductory Diskettes", thus deceiving the recipients into inserting these discs into their systems, causing the infection of the malware. After the infection, the malware counted the number of boots in the system, and when the number reached 90, it encrypted the files and hid directories within the system. In order to get the access back, victims were asked to pay $189 to PC Cyborg Corporation in Panama [39]. Following this initial attempt, a 1996 seminal paper by Young and Yung [44] demonstrated the feasibility of cryptography being used for malicious purposes, such as extortion, in this case. Since then, various ransomware strains have been created [7, 23, 31], and many ransomware actors have conducted extortion campaigns – to varying degrees of success – including through the "Ransomware-as-a-Service" *modus operandi* [21].

Ransomware often relies on social engineering techniques to spread. It is commonly seen that ransomware gets delivered by downloading malicious files (e.g. malicious PDF files) from websites or phishing emails [13]. The most visible element of ransomware is its *ransom notes*, and psychological techniques have been incorporated into these in an attempt to increase the chances of the victim paying the ransom [43]. As highlighted by Hadlington, psychological theories could be applied to understand the effectiveness of ransomware splash screens, and the current literature needs to be expanded with empirical studies [11]. In addition to Hadlington's recommendations, ransomware victimisation should also be investigated from the victims' perspective. From this point of view, looking for patterns in the personality traits of victims could help ransomware mitigation.

There have been numerous studies aiming to develop a taxonomy for personality traits. A well-accepted model for personality trait descriptors named the "Big-Five"; was first accidentally discovered by Donald Fiske in 1949, as cited in [10], who analysed a set of selected variables presented by Cattell [4] and observed patterns among samples for five of these variables, indicating those variables being replicable. Table A1 provides an overview and definition of these five personality traits: Extraversion, Agreeableness, Conscientiousness, Neuroticism, and Openness to Experience.

In this paper, we present the first empirical study aiming to establish a link –if any– between Big-Five personality traits and ransomware victimisation. This is a key part of our effort to gain a better understanding of the psychological and behavioural impact of ransomware victimisation. More specifically, we investigated and contributed novel insights into the following: (i) the influence of the Big-Five personality types on the likelihood of someone becoming a ransomware victim; (ii) the changes in victim's attitude regarding cybersecurity following a ransomware attack; and finally, (iii) the psychological effects of becoming a ransomware victim.

The rest of the paper is organised as follows. Section 2 provides an overview of related work in the general area of ransomware research (in particular, socio-technical papers exploring ways for countering it), as well as relevant research investigating the effect of personality traits on cybercrime. Section 3 presents our approach and methodology, including the way we collected our data. Section 4 provides the key results of our work, covering the quantitative data and its analysis. Section 5 discusses the implications and limitations of our research, as well as some avenues for future work. Finally, Section 6 concludes our paper and reiterates the key contribution of our study.

2 RELATED WORK

The growing number of ransomware attacks and victims over the years made ransomware a point of interest amongst researchers. When we consider the impact of ransomware, it is clear that the scope extends beyond cybersecurity due to its economic and psychological implications. Moreover, it is also important to emphasise that the success of ransomware attacks depends not solely on system security; but also on human factors since social engineering is a typical component of attack vectors used to spread ransomware. Therefore, alongside the technical point of view, which focuses on detection, prevention and remediation; there are other perspectives of ransomware research concerning other disciplines.

Various studies have investigated the psychological and societal impacts of ransomware attacks upon its victims. Ransomware typically displays a splash screen that explains how victims should make payments to recover their data. In a recent study, Yilmaz et al. evaluated the impact of the most commonly seen splash screen types on the victims' decision-making process [43]. For that purpose, they conducted an online study where participants were randomly assigned to one of three ransomware infection scenarios that feature Text-based, Graphical User Interface (GUI) and GUI+Timer ransomware splash screen designs. Ultimately, they found no relationship between participants' willingness to pay and ransomware UI components. Additionally, in a comparable work, Arief et al. reached similar conclusions. Also, they discovered that some ransomware UI components and characteristics might actually discourage victims from making a payment [1]. These features are reported as the presence of typos, the use of an authoritarian tone in the content of the splash screen, and the complexity of the instructions given. In a purely descriptive study, Hadlington explored various ransomware UI components and the psychology behind them [11]. The study identified and categorised ransomware UI elements designed to intimidate victims. Results showed that ransomware splash screens have significant similarities in terms of psychological techniques employed to demand payment from the victims.

Moreover, Connolly and Wall conducted interviews with ransomware victims and investigators to find ways to prevent ransomware attacks [6]. Based on the interviews, the authors developed a taxonomy against ransomware attacks. Their results confirmed that there is no simple technological solution against ransomware. They emphasised the importance of a multi-layered cybersecurity approach which includes socio-technical measures.

Furthermore, Filiz et al. investigated the effectiveness of the data recovery process and data decrypting tools in infected machines [7]. The study outcome clearly demonstrated that nearly half of the decryption tools failed to recover any of the compromised data. Moreover, the study also confirms that finding the ransomware family is a tricky issue, and even major platforms fail to point victims to the right decryptor.

From the more technical side of things, many researchers have proposed anti-ransomware detection and prevention solutions. McIntosh et al. studied various published literature on anti-ransomware proposals and identified inadequacies in current ransomware research [20]. Their study outcome showed that the vast majority of anti-ransomware proposals preferred a programmatic, data-centric, or user-centric approach to detect ransomware. Additionally, the authors pointed out that as ransomware binaries become more obfuscated, detection algorithms will become less and less accurate.

In addition, Pont et al. explored existing anti-ransomware tools in terms of both accuracy and their fit into the landscape, in order to provide future directions for ransomware research [29]. The authors highlighted that accuracy comparison of anti-ransomware tools could not be performed that easily, mainly because many in the literature cannot be accessed at all.

From a cybersecurity point of view, Big-Five personality traits have been tested to determine whether they could be used as psychological predictors for various cybersecurity cases, such as phishing email susceptibility [16, 18], generic cybercrime victimisation [41], and privacy-related concerns while using online apps [42].

Jones et al. investigated psychological predictors of fraud email susceptibility [16]. Participants were asked to examine legitimate and phishing emails and complete cognitive tasks. In the study, factors such as Big-Five personality traits and time pressure while judging emails were considered. They reported no evidence of a systematic contribution of personality traits to email fraud susceptibility.

Moreover, in order to understand neuroticism's role in individuals' susceptibility to phishing victimisation, López-Aguilar and Solanas conducted a comprehensive literature review on the matter [18]. They included 38 papers out of the initially extracted 1076 papers in the study and reviewed those 38 within three contexts: literature survey, prevention frameworks and personality traits. According to the studies they considered, no consensus on neuroticism's role in phishing susceptibility was established.

When personality traits' effects on victimisation are considered, Van de Weijer and Leukfeldt investigated how the Big-Five personality traits affect traditional crime victimisation, and cybervictimisation [41]. They found that people who scored higher on emotional stability were less likely to become a cybercrime victim compared to traditional crimes. They also indicated that a higher score in openness to experience yielded a higher probability of becoming a victim of cyber-enabled crimes (such as online intimidation or consumer fraud, theft from a bank account), in contrast to cyber-dependent crimes (such as virus infection and hacking).

Finally, a 2020 paper by Van der Schyff et al. evaluated personality traits' impact on attitudes regarding privacy settings, social norms and information privacy concerns (IPCs) while using Facebook apps [42]. Their findings showed that individuals who scored higher on extraversion are particularly vulnerable to privacy violations. Furthermore, they discovered that the combination of high scores of extraversion and conscientiousness results in the most considerable negative effect on attitude regarding privacy settings.

3 METHODOLOGY

Our approach followed a quantitative research method based on a retrospective and cross-sectional study. We designed a questionnaire containing multiple questions to measure the personality traits of each participant, followed by questions about their experience with regard to cybercrime victimisation, paying further attention to ransomware victimisation in particular.

3.1 Study design

Our study consists of questions to measure the Big-Five personality traits, participants' victimisation status, their feelings and behaviours after a ransomware attack and lastly, demographics (see Appendix I).

3.1.1 Measuring personality traits. To measure participants' personality traits, we used the 50-item International Personality Item Pool (IPIP) representation of the Big-Five lexical factor markers, developed by Goldberg [9, 14] (see Appendix D). In this representation, each of the Big-Five personality traits is measured with ten items rated on a 5-point Likert scale (e.g., regarding extraversion: "I start conversations.", "I talk to a lot of different people at parties."; regarding agreeableness: "I am interested in people.", "I sympathise with others' feelings."; regarding conscientiousness: "I like order.", "I get chores done right away."; regarding neuroticism: "I get stressed out easily.", "I seldom feel blue."; regarding openness to experience: "I spend time reflecting on things.", "I am full of ideas.").

3.1.2 Measuring victims' psychology and behaviour. Following the measurement of personality traits, participants were evaluated in terms of ransomware victimisation. The ones who had been victimised by ransomware were directed towards an additional set of questions (of length 46) about pre- and post-victimisation behaviour as well as regarding their post-victimisation psychological state (see Appendices E, F, G, J). More specifically, they were asked about the approximate time of the incident; whether they had paid the ransom, had reported the incident or sought help from other parties, been able to recover their infected system/data; ratings of several feelings following the attack (e.g. anger, anxiety, sadness, fear, lack of confidence). These were followed by questions regarding pre- and post-victimisation backup frequencies; use of various security solutions (e.g. antivirus, firewall), and change in habits (e.g. online banking, shopping; downloading/installing software from unknown sources) following the attack. In a latter part of the questionnaire, participants were asked whether they had been victims of other types of cybercrime (see Appendix H).

3.2 Data collection

A considerable number of behavioural studies rely on crowd-sourcing platforms as a data collection medium, because they can provide a good representation of the general population when compared to limited participant pools (e.g. institutional pools). Amazon Mechanical Turk (MTurk) [40] and Prolific [32] are widely used and quite popular. MTurk is a more general-purpose platform, whereas Prolific specialises in surveying its participants. In this study, we decided to publish our survey on Prolific since they were able to provide comprehensive pre-screening options and a diverse participant pool alongside comparable data quality to MTurk [24, 27, 28].

We conducted this study with a representative sample of the United Kingdom in terms of sex, age and ethnicity factors gathered from simplified Great Britain Census data, as claimed by Prolific [38]. Prior to data collection, we piloted our questionnaire with ninety participants in November 2019. Actual data collection was made in December

2019. The average duration for the pilot was 6 minutes and 26 seconds, and for the actual data collection, it was 6 minutes and 11 seconds. The payment made for each participant was £1.05, which was within Prolific's recommended compensation rate.

All the questions in our questionnaire were optional to answer to avoid making any of the participants feel unease. However, in the final set evaluated for the study, we discarded incomplete series of responses. Prior to the questionnaire, participants were informed about it, and their consent was gathered before letting them start. To assure data quality, we included three attention-check questions (ACQs) as suggested by Newman et al. [24] (see Appendix J). Responses collected from participants who failed any one of them were excluded from the final data set. The total number of responses we collected was 1001, and after eliminating invalid responses (due to wrong answers in ACQs and incompleteness), we had a total of 880 valid responses.

3.3 Ethical considerations

Using crowd-sourcing platforms as a data collection tool for human subject studies brings out two prominent ethical concerns: anonymity and compensation. Regarding anonymity, no personally identifiable information (PII) was collected during the study. Moreover, participants were paid appropriately. Prior to the questionnaire, participants were informed about the study and asked for their consent. This study has been evaluated and approved by the Ethics Committee at the University of Kent.

Table 1. Demographic background of the participants.

Measure	Item	Count	Percentage (%)
Gender	Female	462	52.50
	Male	417	47.39
	Other	1	0.11
Age	18-24	140	15.91
	25-34	272	30.91
	35-44	184	20.91
	45-54	125	14.20
	55-64	116	13.18
	65 or over	43	4.89
Education	GCSE or equivalent	129	14.66
	A-levels or equivalent	210	23.86
	Professional qualification	85	9.66
	Undergraduate degree	300	34.09
	Postgraduate degree	140	15.91
	Other	16	1.82
Employment	Employed full-time	393	44.66
	Employed part-time	135	15.34
	Student	90	10.23
	Unemployed	87	9.89
	Self-employed	78	8.86
	Retired	59	6.70
	Other	38	4.32

4 RESULTS

4.1 Participants' profile

Data collected from the participants included information on their demographics and whether they have been a victim of any ransomware attack or other types of cybercrime (e.g. online fraud, data hack, online extortion, cyberstalking or harassment). Table 1 shows summary statistics of responses collected from the participants regarding their demographics. Only one participant identified themselves as non-binary, while more than half of the participants were female, and less than half were male. Almost one-third of the participants' age was in the range 25-34, followed by 35-44, 18-24, 45-54, 55-64 and lastly, 65 or over. In terms of educational background, exactly half of the participants stated they have an undergraduate or a postgraduate degree, and approximately one-quarter of them had A-levels or equivalent, followed by GCSE or equivalent, professional qualification and others. A large portion of the participants was employed full-time, while the rest were employed part-time, students, unemployed, self-employed, retired, or had a different employment status.

Regarding cybervictimisation, 84 participants (9.55%) stated that they had been a victim of a ransomware attack. However, when other types of cybercrime (e.g. online fraud, cyberstalking or online harassment, data hack, and online extortion) were being considered, victimisation rates were considerably higher: 213 of the participants (25.36%) reported that they had been victimised. Interestingly, a small portion of the participants (1.82%, n=16) had suffered from both ransomware and other types of cybercrime, as depicted in Figure 1. For the rest of the paper, when we talk about the characteristics and figures related to ransomware victimisation, we base it on the data obtained from the 84 participants who explicitly stated that they had experienced this type of victimisation.

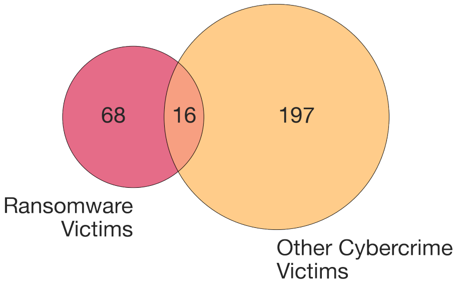

Fig. 1. Ransomware and other cybercrime victimisation among participants.

When the demographic composition of the ransomware victims was examined, it was observed that the majority of them identified as males, whereas most of our participants were female. However, the distribution by age groups, education level and employment status did not severely differ compared to all participants combined. Table 2 provides statistics regarding demographics of ransomware victims.

4.2 Personality traits

Participants were measured in terms of the Big-Five personality traits. The internal consistency values for each trait were either good or excellent (αs = 0.91, 0.87, 0.83, 0.91, 0.82 for extraversion, agreeableness, conscientiousness, neuroticism, and openness to experience, respectively). An overwhelming majority of the participants scored in the higher half of the scale for agreeableness, conscientiousness and openness traits resulting in a left-skewed distribution. Extraversion

Table 2. Demographic background of the ransomware victims (N=84).

Measure	Item	Count	Percentage (%)
Gender	Female	31	36.90
	Male	52	61.90
	Other	1	1.19
Age	18-24	17	20.24
	25-34	24	28.57
	35-44	21	25.00
	45-54	10	11.90
	55-64	8	9.52
	65 or over	4	4.76
Education	GCSE or equivalent	11	13.10
	A-levels or equivalent	25	29.76
	Professional qualification	4	4.76
	Undergraduate degree	29	34.52
	Postgraduate degree	14	16.67
	Other	1	1.19
Employment	Employed full-time	38	45.24
	Employed part-time	11	13.10
	Student	7	8.33
	Unemployed	14	16.67
	Self-employed	9	10.71
	Retired	2	2.38
	Other	3	3.57

and neuroticism scores were more evenly distributed and closer to being symmetrical. Figure 2 depicts the distribution of the participants in more detail.

In our study, the observed range for the extraversion trait was from 1.0 to 5.0. The mode for extraversion was 2.7 and 25th, 50th, 75th percentiles were 2.1, 2.7 and 3.4. The agreeableness trait ranged from 1.2 to 5.0. The mode for agreeableness was 4.2 and 25th, 50th, 75th percentiles were 3.4, 4.0 and 4.4. The conscientiousness trait ranged from 1.5 to 5.0. The mode for conscientiousness was 3.7 and 25th, 50th, 75th percentiles were 3.1, 3.6 and 4.1. The neuroticism trait ranged from 1.1 to 5.0. The mode for neuroticism was 2.6 and 25th, 50th, 75th percentiles were 2.2, 2.9 and 3.7. And lastly, the openness trait ranged from 1.8 to 5.0. The mode for openness was 3.9 and 25th, 50th, 75th percentiles were 3.3, 3.7 and 4.1. Table 3 depicts summary statistics for personality traits of our participants, which are consistent with another study conducted in Great Britain (except for extraversion, it seems like our sample consists of more "introverted" people, for comparison, see Figure 3) [30, 33].

When solely ransomware victims were considered, the distributions of personality trait scores were rather similar. Again, an overwhelming majority for agreeableness, conscientiousness and openness traits were scored higher than the middle point. These traits were closer to being left-skewed, whereas extraversion and neuroticism yielded a more symmetrical distribution. In Figure 4, the distribution of personality traits for ransomware victims is shown.

Among the ransomware victims, the observed range for extraversion was from 1.0 to 5.0. The mode values for extraversion were 2.7 and 3.2. And 25th, 50th, 75th percentiles were 1.85, 2.7 and 3.325. The agreeableness trait ranged from 1.6 to 5.0. The mode for agreeableness was 3.4 and 25th, 50th, 75th percentiles were 3.4, 3.9 and 4.2. Conscientiousness

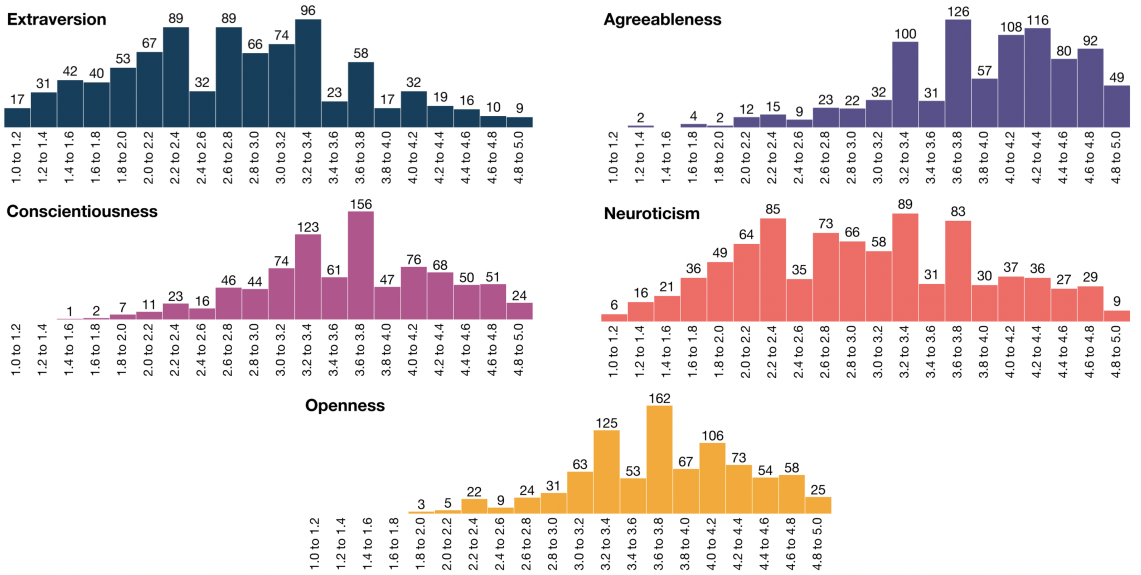

Fig. 2. Big-Five personality distribution of the participants.

Table 3. Descriptive statistics of the Big-Five personality traits among all participants.

	N	Mean	SD	α
Extraversion	880	2.73	0.88	0.91
Agreeableness	880	3.87	0.69	0.87
Conscientiousness	880	3.59	0.68	0.83
Neuroticism	880	2.96	0.91	0.91
Openness	880	3.71	0.62	0.82

ranged between 2.2 and 5.0. The mode values for conscientiousness were 3.1 and 3.5. Moreover, 25th, 50th, 75th percentiles were 3.075, 3.5 and 4.025. Neuroticism had a minimum score of 1.2, whereas the maximum value was 4.8. The mode for neuroticism was 2.0 and 25th, 50th, 75th percentiles were 2.1, 2.75 and 3.5. Lastly, openness was in the range of 1.8 and 5.0. The mode for openness was 4.1 and 25th, 50th, 75th percentiles were 3.4, 3.9 and 4.2.

When we compared the different personality traits, we observed that ransomware victims seem to be less "agreeable". For other personality traits, no significant differences were observed between ransomware victims and non-victims. However, due to the family-wise error rate ($FWER = (1 - (1 - 0.05)^5) = 0.226$, for $\alpha = 0.05$) and to improve the reproducibility of the findings [5], we needed to apply the Bonferroni correction[1], resulting in an α value of $0.0452 \sim \frac{FWER}{number\_of\_traits}$. Therefore the p-values observed in this study indicate no strong evidence (at the 0.01 level at least) to reject the null hypotheses for any single trait, meaning there is no significant sole effect of personality traits on ransomware victimisation. Table 4 provides descriptive statistics for different personality traits in various subgroups regarding ransomware victimisation.

[1] The Bonferroni correction, which is the simplest and most popular approach, should be used in cases like this, in which we prefer to be conservative in our conclusions, and specifically to minimise type I errors.

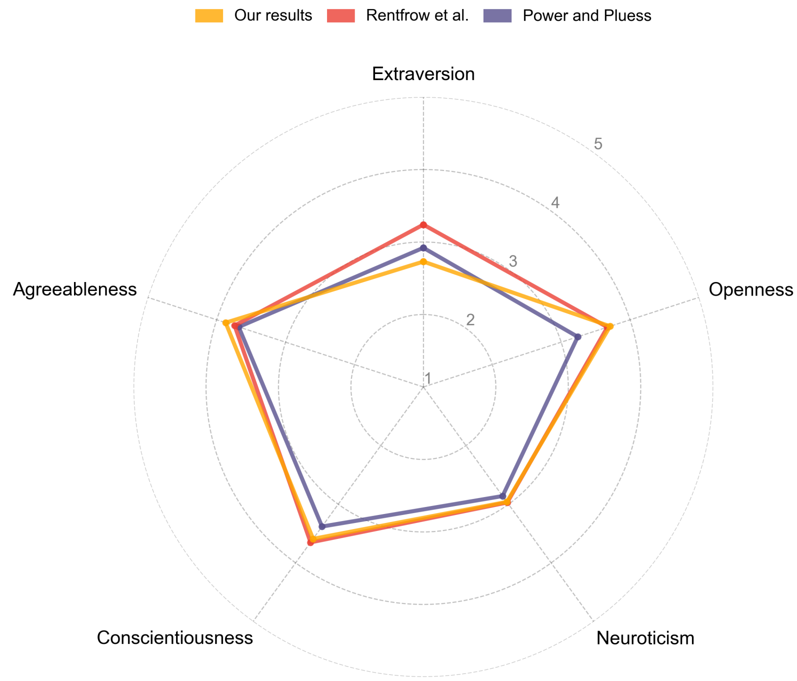

Fig. 3. The composition of the Big-Five traits in our study, compared with those from other studies [30, 33].

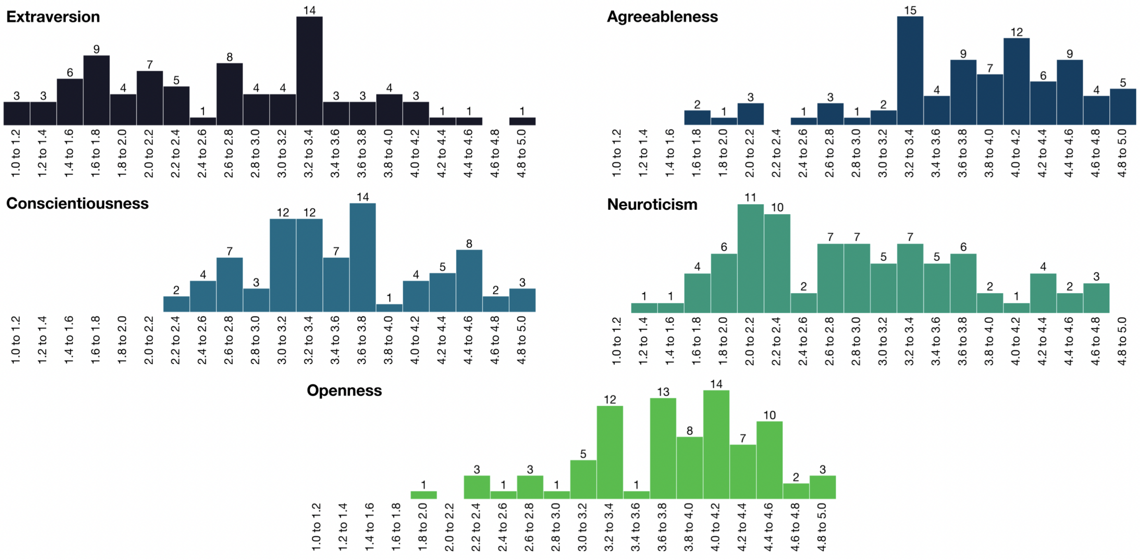

Fig. 4. Big-Five personality distribution of the ransomware victims (N=84).

Table 4. Statistics of the Big-Five personality traits comparing victims and non-victims of ransomware.

	Victim (n = 84)		Non-victim (n = 796)		t	p-value
	Mean	SD	Mean	SD		
Extraversion	2.63	0.93	2.75	0.88	-1.076	.142
Agreeableness	3.72	0.76	3.88	0.68	-1.842	.034
Conscientiousness	3.52	0.67	3.60	0.68	-1.062	.145
Neuroticism	2.85	0.88	2.98	0.91	-1.233	.11
Openness	3.76	0.64	3.71	0.62	0.657	.256

4.3 Ransomware victimisation

Before delving into post-victimisation feelings and behaviour changes, we asked when the most recent attack occurred, and the overwhelming majority (n=59, 70.24%) indicated that the attack had occurred more than one year ago, followed by 10-12 months ago (n=11, 13.1%), within the past three months (n=7, 8.33%), 4-6 months ago (n=6, 7.14%) and 7-9 months ago (n=1, 1.19%).

To better understand the post-ransomware infection state of victims, we asked them several questions regarding their behaviour and feelings. We then analysed their responses regarding their personality traits, feelings and behaviour. Our findings are presented in the following sections.

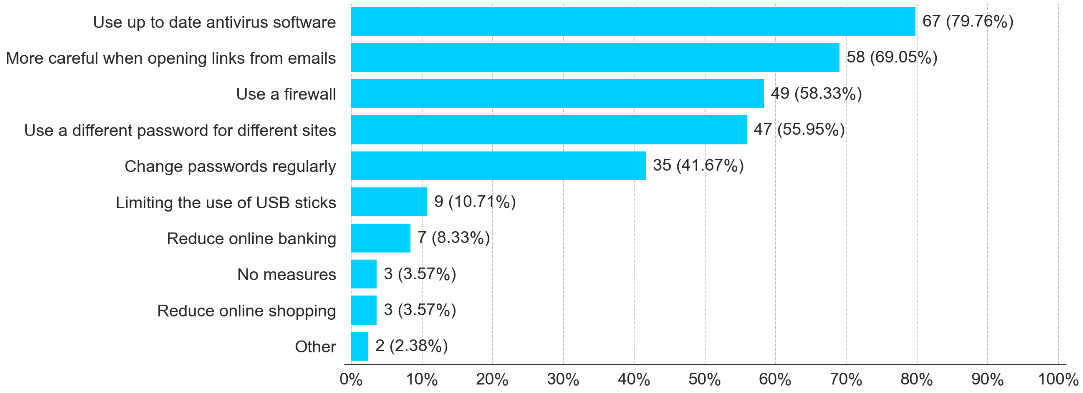

Fig. 5. Measures taken by victims after ransomware attack (N=84).

4.3.1 Post-victimisation behaviour. Two participants among the ransomware victims reported they paid the ransom, and the majority of the victims claimed to have had a successful recovery from the ransomware attack. When they were asked whether they had reported the incident or talked to anyone about it, exactly three-fourths affirmed they had. Of those who responded positively, the majority preferred talking to a friend or family member, followed by reporting to an action fraud helpline, getting in touch with other parties, and lastly, filing a police report. An overwhelming majority of the victims took at least one additional measure after ransomware infection. Only three of them reported they took no new countermeasures at all. When we investigated what measures were taken by the participants after the incident, prevalent responses were as follows: using up-to-date antivirus software, being more careful when opening links from emails, using a firewall, using different passwords for different websites and changing passwords regularly. Figure 5 provides more detailed information regarding such measures.

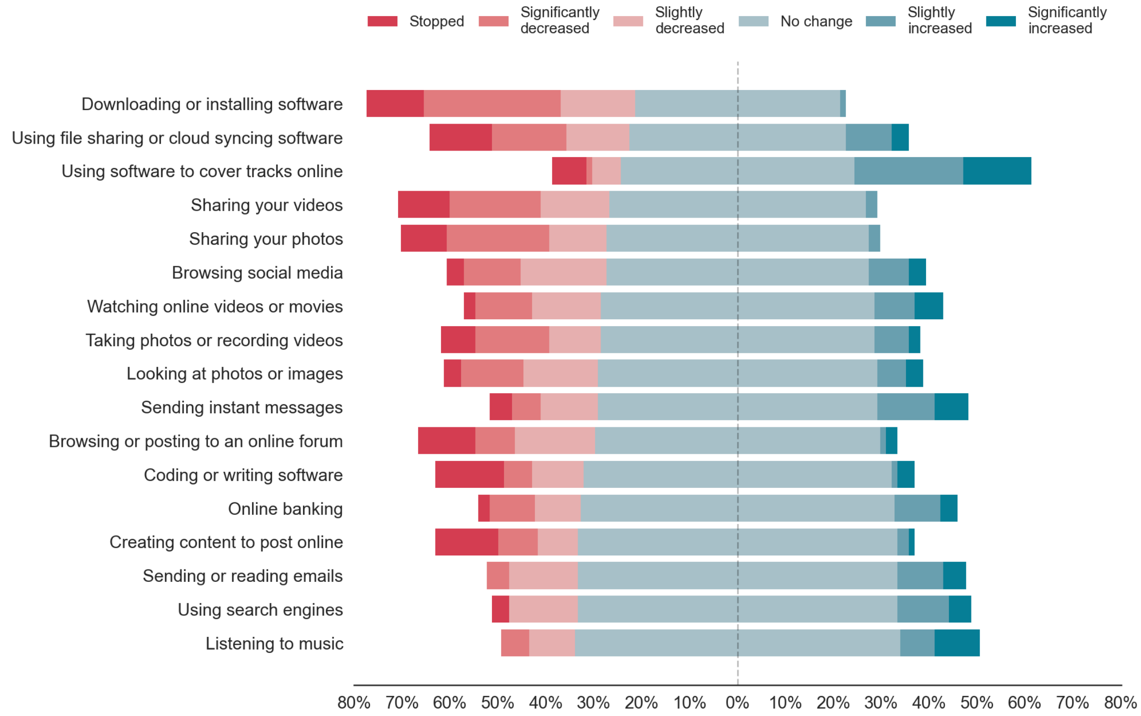

Fig. 6. Post-victimisation behavioural changes (N=84).

When victims' daily computer usage habits were investigated, we mainly observed no change after the attacks. However, their tendency to download and install software from online sources showed a decreasing trend, which might indicate that they became more cautious. The data also indicate an increasing trend in the use of software to cover tracks online (i.e. privacy-enhancing features such as browsing in incognito mode or using Tor), which is also a good sign of adopting a more careful browsing habit. In Figure 6, trends in the post-victimisation behavioural changes are depicted. Moreover, raw figures are provided in Appendix B2.

Having regular backups of crucial information has a significant role in ransomware recovery, especially if decryption is not possible since it then becomes the only viable option. Thus, we investigated whether being a ransomware victim affects backup frequency. We observed that more than two-thirds of the ransomware victims who had never backed up their data started using backups. Figure 7 shows before and after backup frequency distributions and the flow between them.

4.3.2 Post-victimisation feelings. To evaluate how ransomware victims felt following the attack, we wanted them to rate their feelings on a 5-point Likert Scale (1-Not present, 2-Low, 3-Moderate, 4-High, 5-Very High). Descriptive statistics for feelings after victimisation are shown in Table 5, whereas the distributions of ratings for feelings are provided in Figure 8. Additionally, raw figures are provided in Appendix B1. On average, anger was the highest-rated feeling, while

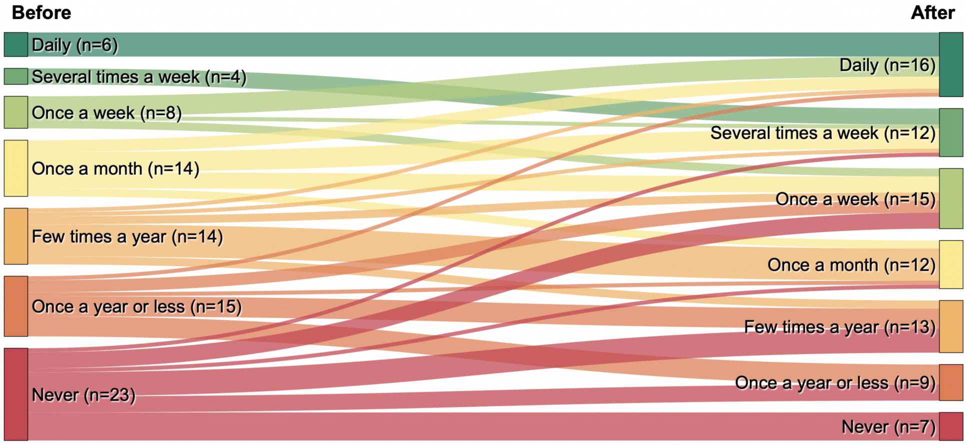

Fig. 7. Backup frequencies before and after ransomware victimisation (N=84).

Table 5. Descriptive statistics of victims' feelings post-ransomware attack.

	Mean	SD	Mode	Median
Anger	4.00	1.22	5	4
Anxiety	3.37	1.28	4	4
Distress	3.15	1.32	4	3
Vulnerability	3.06	1.30	4	3
Fear	3.02	1.32	2, 3, 4	3
Sadness	2.92	1.33	4	3
Paranoia	2.89	1.28	4	3
Nervousness	2.86	1.42	1	3
Regret	2.73	1.39	1	2.5
Embarrassment	2.57	1.32	1	3
Shame	2.26	1.25	1	2
Lacking in confidence	2.13	1.12	1	2
Depression	2.01	1.13	1	2
Sleeplessness	1.92	1.16	1	1
Isolation	1.70	1.01	1	1

isolation was the lowest. The second highest-rated feeling was anxiety, and this was followed by distress. The results also revealed that a small percentage of the victims also felt sleeplessness, depression and a lack of confidence.

5 DISCUSSION

The results of our study reveal several interesting and potentially useful insights, as outlined in the previous section. In this section, we look a bit further and discuss the implications of these findings. We also point out several limitations of our study, as well as some ideas for future research.

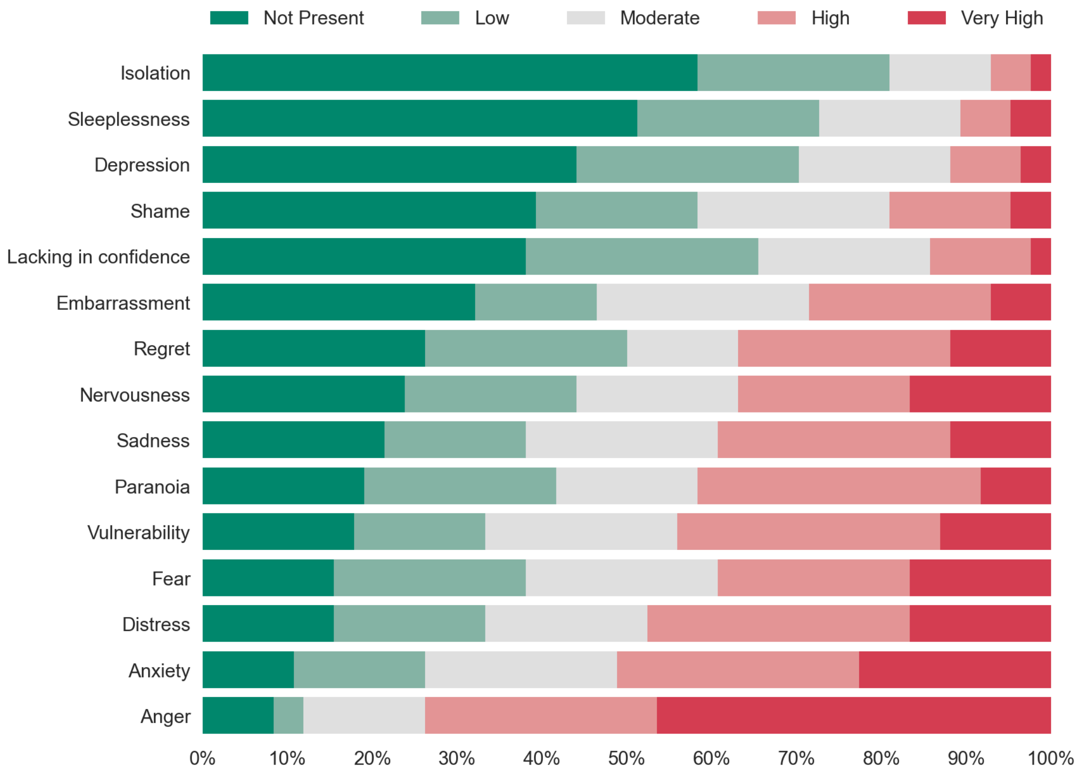

Fig. 8. Distribution of post-victimisation feelings (N=84).

5.1 Implications

The growing threat of ransomware and increasing prevalence of cyberinsurance illustrate the need for a better understanding of factors behind ransomware victimisation, for example, to assist future victims. Once vulnerable populations are identified, more proactive strategies can be deployed to decrease their likelihood of ransomware victimisation. For that purpose, we study the influence of personality traits on the probability of becoming a ransomware victim. One of our most sobering results is that ransomware victimisation seems not to be influenced directly by using any of the five broad personality traits. Our results show that no distinct personality traits account for explaining the majority of the victimisation. Future research could complement our work by adding features on top of the five broad personality traits to establish more explicit links between personality types and victimisation. This could further improve our understanding of the factors behind ransomware victimisation.

As observed in this study, some ransomware victims tend to change digital device usage habits, including the ones related to the security of their systems. This empirically confirms earlier findings on a study that recommends showing the impact of ransomware attacks during ransomware awareness campaigns to increase the adoption of good cybersecurity practices [43]. These results show that becoming a victim of ransomware or watching a ransomware demonstration can provide the necessary motivation to adopt good (or better) security behaviour. This might be because after seeing or experiencing the devastating effect that ransomware can cause, the concept of ransomware changes from being a non-threatening abstract one into a genuine threat that anyone can become a victim of.

A hotline focusing on ransomware remediation might be helpful. We have seen that the overwhelming majority of ransomware victims had sought help from other parties or had reported the incident to law enforcement authorities. On top of that, many victims would go through a period of negative feelings following victimisation. This kind of hotline might provide psychological support alongside technical aid, such as pointing towards ransomware decryptors and recovery methods. Moreover, preventive measures can also be introduced to mitigate future victimisation.

5.2 Limitations

Here we present the limitations that may influence the findings from our study in its current form. Firstly, our participants were selected from a UK-based research platform called Prolific. This means there is a limitation regarding the generalisation of our findings from the population's perspective. Moreover, the representative sample of the UK which we gathered data from was provided by Prolific, resulting in a non-transparent sampling process. Nonetheless, we believe the current results yield some valuable insights already, and they can provide indications for future research. Secondly, some researchers suggest that self-reported personality traits might change over time due to reasons such as significant life events (e.g. marriage, having children, death of a family member), maturational changes, and even desires of individuals [12, 36, 37]. In our study, we assume that personality traits did not change over time. Therefore, the reproducibility of our results is a matter for further research. Additionally, due to the sample size, it was not possible to investigate ransomware victims' changes in behaviour and emotions pre- and post-attack by personality traits. Lastly, in this research, we were not able to examine the personality traits of the ransomware victims who actually paid up due to the insufficient number of samples.

5.3 Future work

In this study, we investigated whether the Big-Five personality traits can be used in isolation to identify potential victims. Our results demonstrated that there is no clear link between the Big-Five personality traits and ransomware victimisation. Based on these results, we recommend two specific areas of further study: first, researchers can investigate whether the Big-Five personality traits can be used to identify cybercrime victimisation in general; and secondly, researchers can expand this work to take into account technical characteristics (e.g. the operating system used, whether any protection software was used, or the cyber proficiency levels of victims) and combining these with personality traits to obtain a more balanced perspective on victimisation. Furthermore, we suggest investigating the relationship between personality traits and changes in pre- and post-victimisation feelings and behaviour with a larger sample for future research.

Additionally, we discovered that ransomware victims require both technical and psychological support when they are dealing with ransomware. Our results showed that victims could face various negative emotions such as isolation, sleeplessness and depression. In the future, the research community can focus on developing practical solutions that may deliver both psychological and technical support for ransomware victims.

Finally, in order to improve the generalisability of the findings, two strands of future work can be pursued: (i) collecting data from more participants and (ii) increasing the internationalisation of the study by involving participants from more countries.

6 CONCLUSION

In this paper, we investigated the potential link between the Big-Five personality traits and the psychological effects of being a ransomware victim, as well as potential changes in cybersecurity behaviour following ransomware victimisation.

We carried out an online survey using the Prolific platform. Out of the 880 anonymous online participants, 84 of them (under 10%) reported that they had been a victim of ransomware in the past. We also found that only a small portion of the victims (2.38%, n=2) paid the ransom demand. The payment rate we observed in this study is consistent with another online study that investigates ransomware victimisation [25]. Interestingly, our study found no evidence that the Big-Five personality traits can convincingly be used to identify potential ransomware victimisation. In particular, we could not identify any specific group of personality traits that would indicate a high susceptibility to becoming a victim of ransomware, or paying the ransom demand. This might be due to the "spray-and-pray" strategy commonly used in ransomware infection, which would involve launching a large number of attacks indiscriminately (i.e. there would be no controlled experiment specifically dedicated to investigating each personality type in isolation), in the hope that someone would be infected and then pay the demand.

Furthermore, we found that only a small percentage of ransomware victims would not change their attitudes towards better cybersecurity practices after ransomware infection. The majority of them claimed that they would use cybersecurity tools and be more careful regarding weblinks post-victimisation. In addition, we observed that after experiencing a ransomware attack, victims were more likely to increase their backup frequency (or they would plan to start doing backup if they did not use backup before victimisation). Some victims also changed their passwords and limited the usage of USB sticks, online banking and online shopping. These results show that a large number of victims were encouraged to improve their cybersecurity practices after the attack. However, limiting the usage of online banking and online shopping indicate that some of the changes in cybersecurity-related behaviour were a consequence of a severely reduced trust that some victims would place on the online services.

Lastly, we explored how the participants of our study might have felt after becoming a victim of ransomware. Our results indicate that the majority of victims felt anger. This was followed by anxiety, distress and fear. Also, a few victims felt paranoia, depression, isolation and sleeplessness. These show that some victims would require additional psychological support as well as technical support post-victimisation. Thus, ransomware recovery should not be considered solely as a technical process. Psychological support and better socio-technical preventive measures must also be provided to lessen the unpleasant psychological effects of ransomware victimisation, while minimising the threat of future victimisation.

REFERENCES

[1] Budi Arief, Andy Periam, Orcun Cetin, and Julio C Hernandez-Castro. 2020. Using Eyetracker to Find Ways to Mitigate Ransomware. In *6th Int'l Conf. on Information Systems Security and Privacy (ICISSP 2020)*. 448–456.

[2] Christopher Bing. 2021 [Online]. Exclusive: U.S. to give ransomware hacks similar priority as terrorism. *Reuters* (June 04, 2021 [Online]). https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/

[3] Jacob Bogage. 2021 [Online]. Colonial Pipeline CEO says paying $4.4 million ransom was 'the right thing to do for the country'. *The Washington Post* (May 19, 2021 [Online]). https://www.washingtonpost.com/business/2021/05/19/colonial-pipeline-ransom-joseph-blunt/

[4] Raymond B Cattell. 1947. Confirmation and clarification of primary personality factors. *Psychometrika* 12, 3 (1947), 197–220.

[5] Open Science Collaboration. 2015. Estimating the reproducibility of psychological science. *Science* 349, 6251 (2015), aac4716.

[6] Lena Y Connolly and David S Wall. 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security* 87 (2019), 101568.

[7] Burak Filiz, Budi Arief, Orcun Cetin, and Julio Hernandez-Castro. 2021. On the Effectiveness of Ransomware Decryption Tools. *Computers & Security* 111 (2021), 102469.

[8] Fortinet. 2021. The 2021 Ransomware Survey Report. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-ransomware-survery.pdf

[9] Lewis R Goldberg. 1992. The development of markers for the Big-Five factor structure. *Psychological assessment* 4, 1 (1992), 26.

[10] Lewis R Goldberg. 1993. The structure of phenotypic personality traits. *American psychologist* 48, 1 (1993), 26.

[11] LJ Hadlington. 2017. *Exploring the psychological mechanisms used in ransomware splash screens.* Technical Report.

[12] Nathan W Hudson and R Chris Fraley. 2015. Volitional personality trait change: Can people choose to change their personality traits? *Journal of personality and social psychology* 109, 3 (2015), 490.

[13] Gavin Hull, Henna John, and Budi Arief. 2019. Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science* 8, 1 (2019), 1–22.

[14] IPIP. [n. d.]. Administering IPIP Measures, with a 50-item Sample Questionnaire. https://ipip.ori.org/New_IPIP-50-item-scale.htm

[15] Oliver P John, Laura P Naumann, and Christopher J Soto. 2008. Paradigm shift to the integrative Big Five trait taxonomy: History, measurement, and conceptual issues. In *Handbook of personality: Theory and research* (3 ed.), Oliver P. John, Richard W. Robins, and Lawrence A. Pervin (Eds.). The Guilford Press, New York, NY, 114–158.

[16] Helen S Jones, John N Towse, Nicholas Race, and Timothy Harrison. 2019. Email fraud: The search for psychological predictors of susceptibility. *PloS one* 14, 1 (2019), e0209684.

[17] Fortinet Labs. 2021. Global Threat Landscape Report. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/report-threat-landscape-2021.pdf

[18] Pablo López-Aguilar and Agusti Solanas. 2021. Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism. In *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 1363–1368.

[19] Kalyeena Makortoff. 2021 [Online]. World's biggest meat producer JBS pays $11m cybercrime ransom. *The Guardian* (June 10, 2021 [Online]). https://www.theguardian.com/business/2021/jun/10/worlds-biggest-meat-producer-jbs-pays-11m-cybercrime-ransom

[20] Timothy McIntosh, ASM Kayes, Yi-Ping Phoebe Chen, Alex Ng, and Paul Watters. 2021. Ransomware Mitigation in the Modern Era: A Comprehensive Review, Research Challenges, and Future Directions. *ACM Computing Surveys (CSUR)* 54, 9 (2021), 1–36.

[21] Per Håkon Meland, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 2020. The Ransomware-as-a-Service economy within the darknet. *Computers & Security* 92 (2020), 101762.

[22] Amyas Morse. 2018. Investigation: WannaCry cyber attack and the NHS. *Report by the National Audit Office* 1 (2018). https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/

[23] New Jersey Cybersecurity & Communications Integration Cell (NJCCIC). [n. d.]. Ransomware. https://www.cyber.nj.gov/threat-center/threat-profiles/ransomware-variants

[24] Alexander Newman, Yuen Lam Bavik, Matthew Mount, and Bo Shao. 2021. Data collection via online platforms: Challenges and recommendations for future research. *Applied Psychology* 70, 3 (2021), 1380–1402.

[25] Anna-Marie Ortloff, Maike Vossen, and Christian Tiefenau. 2021. Replicating a Study of Ransomware in Germany. In *European Symposium on Usable Security 2021*. 151–164.

[26] Charlie Osborne. 2021 [Online]. Updated Kaseya ransomware attack FAQ: What we know now. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

[27] Stefan Palan and Christian Schitter. 2018. Prolific.ac — A subject pool for online experiments. *Journal of Behavioral and Experimental Finance* 17 (2018), 22–27.

[28] Eyal Peer, Laura Brandimarte, Sonam Samat, and Alessandro Acquisti. 2017. Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology* 70 (2017), 153–163.

[29] Jamie Pont, Osama Abu Oun, Calvin Brierley, Budi Arief, and Julio Hernandez-Castro. 2019. A roadmap for improving the impact of anti-ransomware research. In *Nordic Conference on Secure IT Systems*. Springer, 137–154.

[30] Robert A Power and Michael Pluess. 2015. Heritability estimates of the Big Five personality traits based on common genetic variants. *Translational psychiatry* 5, 7 (2015), e604–e604.

[31] The No More Ransom Project. 2016. Decryption tools. https://www.nomoreransom.org/en/decryption-tools.html

[32] Prolific. 2014. Prolific. https://www.prolific.co/

[33] Peter J Rentfrow, Markus Jokela, and Michael E Lamb. 2015. Regional personality differences in Great Britain. *PloS one* 10, 3 (2015), e0122245.

[34] Ronny Richardson and Max M North. 2017. Ransomware: Evolution, mitigation and prevention. *International Management Review* 13, 1 (2017), 10.

[35] Sophos. 2021. The State of Ransomware 2021. https://secure2.sophos.com/en-us/content/state-of-ransomware.aspx

[36] Jule Specht, Boris Egloff, and Stefan C Schmukle. 2011. Stability and change of personality across the life course: the impact of age and major life events on mean-level and rank-order stability of the Big Five. *Journal of personality and social psychology* 101, 4 (2011), 862.

[37] Sanjay Srivastava, Oliver P John, Samuel D Gosling, and Jeff Potter. 2003. Development of personality in early and middle adulthood: Set like plaster or persistent change? *Journal of personality and social psychology* 84, 5 (2003), 1041.

[38] Prolific Team. [n. d.]. Representative samples FAQ. https://researcher-help.prolific.co/hc/en-gb/articles/360019238413-Representative-samples-FAQ

[39] Jason Thomas and Gordon Galligher. 2018. Improving backup system evaluations in information security risk assessments to combat ransomware. *Computer and Information Science* 11, 1 (2018).

[40] Amazon Mechanical Turk. 2005. Amazon Mechanical Turk. https://www.mturk.com/

[41] Steve GA Van de Weijer and E Rutger Leukfeldt. 2017. Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking* 20, 7 (2017), 407–412.

[42] Karl van der Schyff, Stephen Flowerday, and Paul Benjamin Lowry. 2020. Information privacy behavior in the use of Facebook apps: A personality-based vulnerability assessment. *Heliyon* 6, 8 (2020), e04714.

[43] Yagiz Yilmaz, Orcun Cetin, Budi Arief, and Julio Hernandez-Castro. 2021. Investigating the impact of ransomware splash screens. *Journal of Information Security and Applications* 61 (2021), 102934.

[44] Adam Young and Moti Yung. 1996. Cryptovirology: Extortion-based security threats and countermeasures. In *Proceedings 1996 IEEE Symposium on Security and Privacy*. IEEE, 129–140.

A BIG-FIVE PERSONALITY TRAITS

Definitions of Big-Five personality traits are provided in Table A1.

Table A1. Definitions of the Big-Five personality traits.

Trait	Conceptual definition
Extraversion	This trait indicates an energetic approach towards the social and material world. Key characteristics associated with this trait include sociability, activity, assertiveness, and positive emotionality.
Agreeableness	Agreeableness pits a pro-social and communal orientation towards others with antagonism. Key characteristics associated with this trait include altruism, tender-mindedness, trust, and modesty.
Conscientiousness	It describes socially-prescribed impulse control that facilitates task- and goal-directed behaviour. Key characteristics associated with this trait include thinking before acting, delaying gratification, following norms and rules, as well as planning, organising and prioritising tasks.
Neuroticism	This trait contrasts emotional stability and even-temperedness with negative emotionality (such as feeling anxious, nervous, sad, and tense). Key characteristics associated with this trait include mood swings, irritability, depression, and impulsiveness.
Openness to Experience	It describes the breadth, depth, originality, and complexity of an individual's mental and experiential life. Key characteristics associated with this trait include imagination, curiosity, and open-mindedness.

Note. Table adopted from John et al. [15].

B ADDITIONAL STATISTICS

Here we present additional statistics from our data. Table B1 provides descriptive statistics for victims' feelings after ransomware attack, and Table B2 shows descriptive statistics for behaviour changes post-ransomware victimisation.

Table B1. Victims' feelings post-ransomware attack.

Item	Not present	Low	Moderate	High	Very High
Anxiety	9 (10.71%)	13 (15.48%)	19 (22.62%)	24 (28.57%)	19 (22.62%)
Sadness	18 (21.43%)	14 (16.67%)	19 (22.62%)	23 (27.38%)	10 (11.90%)
Fear	13 (15.48%)	19 (22.62%)	19 (22.62%)	19 (22.62%)	14 (16.67%)
Anger	7 (8.33%)	3 (3.57%)	12 (14.29%)	23 (27.38%)	39 (46.43%)
Embarrassment	27 (32.14%)	12 (14.29%)	21 (25.00%)	18 (21.43%)	6 (7.14%)
Shame	33 (39.29%)	16 (19.05%)	19 (22.62%)	12 (14.29%)	4 (4.76%)
Paranoia	16 (19.05%)	19 (22.62%)	14 (16.67%)	28 (33.33%)	7 (8.33%)
Regret	22 (26.19%)	20 (23.81%)	11 (13.10%)	21 (25.00%)	10 (11.90%)
Depression	37 (44.05%)	22 (26.19%)	15 (17.86%)	7 (8.33%)	3 (3.57%)
Sleeplessness	43 (51.19%)	18 (21.43%)	14 (16.67%)	5 (5.95%)	4 (4.76%)
Vulnerability	15 (17.86%)	13 (15.48%)	19 (22.62%)	26 (30.95%)	11 (13.10%)
Distress	13 (15.48%)	15 (17.86%)	16 (19.05%)	26 (30.95%)	14 (16.67%)
Nervousness	20 (23.81%)	17 (20.24%)	16 (19.05%)	17 (20.24%)	14 (16.67%)
Isolation	49 (58.33%)	19 (22.62%)	10 (11.90%)	4 (4.76%)	2 (2.38%)
Lacking in confidence	32 (38.10%)	23 (27.38%)	17 (20.24%)	10 (11.90%)	2 (2.38%)

Table B2. Victims' behavioural changes post-ransomware attack.

Item	Stopped	Significantly decreased	Slightly decreased	No change	Slightly increased	Significantly increased
Using search engines	3 (3.57%)	0 (0.00%)	12 (14.29%)	56 (66.67%)	9 (10.71%)	4 (4.76%)
Sending or reading emails	0 (0.00%)	4 (4.76%)	12 (14.29%)	56 (66.67%)	8 (9.52%)	4 (4.76%)
Sending instant messages	4 (4.76%)	5 (5.95%)	10 (11.90%)	49 (58.33%)	10 (11.90%)	6 (7.14%)
Browsing social media	3 (3.57%)	10 (11.90%)	15 (17.86%)	46 (54.76%)	7 (8.33%)	3 (3.57%)
Watching online videos or movies	2 (2.38%)	10 (11.90%)	12 (14.29%)	48 (57.14%)	7 (8.33%)	5 (5.95%)
Looking at photos or images	3 (3.57%)	11 (13.10%)	13 (15.48%)	49 (58.33%)	5 (5.95%)	3 (3.57%)
Taking photos or recording videos	6 (7.14%)	13 (15.48%)	9 (10.71%)	48 (57.14%)	6 (7.14%)	2 (2.38%)
Sharing your photos	8 (9.52%)	18 (21.43%)	10 (11.90%)	46 (54.76%)	2 (2.38%)	0 (0.00%)
Sharing your videos	9 (10.71%)	16 (19.05%)	12 (14.29%)	45 (53.57%)	2 (2.38%)	0 (0.00%)
Listening to music	0 (0.00%)	5 (5.95%)	8 (9.52%)	57 (67.86%)	6 (7.14%)	8 (9.52%)
Browsing or posting to an online forum	10 (11.90%)	7 (8.33%)	14 (16.67%)	50 (59.52%)	1 (1.19%)	2 (2.38%)
Online banking	2 (2.38%)	8 (9.52%)	8 (9.52%)	55 (65.48%)	8 (9.52%)	3 (3.57%)
Creating content to post online	11 (13.10%)	7 (8.33%)	7 (8.33%)	56 (66.67%)	2 (2.38%)	1 (1.19%)
Using file sharing or cloud syncing software	11 (13.10%)	13 (15.48%)	11 (13.10%)	38 (45.24%)	8 (9.52%)	3 (3.57%)
Coding or writing software	12 (14.29%)	5 (5.95%)	9 (10.71%)	54 (64.29%)	1 (1.19%)	3 (3.57%)
Using software to cover tracks online	6 (7.14%)	1 (1.19%)	5 (5.95%)	41 (48.81%)	19 (22.62%)	12 (14.29%)
Downloading or installing software	10 (11.90%)	24 (28.57%)	13 (15.48%)	36 (42.86%)	1 (1.19%)	0 (0.00%)

C CONSENT FORM

Please read the information below, and if you agree, please tick the box to indicate that you understand and consent.

1. I confirm I have read and understand the information sheet for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

2. I understand that my participation is voluntary and that I am free to withdraw at any time before completing the study without giving any reason.

3. I understand that this study is run as an anonymous survey, where no personally identifiable information is sought by the investigators. I give permission for members of the research team, identified on the information sheet, to have access to my responses. Please also note that for free text responses, we may include direct quotes in any publications or reports arising from this research.

4. I agree to take part in the above research project.
○ I agree to the 4 points mentioned above, and consent to participate in this study.
○ I do not consent. I do not want to participate in this study.

D QUESTIONS RELATED TO PERSONALITY TRAITS

Note: All the questions within this subset have the same five options for their answer:

○ 1 ○ 2 ○ 3 ○ 4 ○ 5

The purpose of these 50 questions was to collect Likert scale data that can be used to determine the participants' personality type. These are standard questions, adapted from IPIP [14].

1. Am the life of the party.

2. Feel little concern for others.

3. Am always prepared.

4. Get stressed out easily.

5. Have a rich vocabulary.

6. Don't talk a lot.

7. Am interested in people.

8. Leave my belongings around.

9. Am relaxed most of the time.

10. Have difficulty understanding abstract ideas.

11. Feel comfortable around people.

12. Insult people.

13. Pay attention to details.

14. Worry about things.

15. Have a vivid imagination.

16. Keep in the background.

17. Sympathize with others' feelings.

18. Make a mess of things.

19. Seldom feel blue.

20. Am not interested in abstract ideas.

21. Start conversations.

22. Am not interested in other people's problems.

23. Get chores done right away.

24. Am easily disturbed.

25. Have excellent ideas.

26. Have little to say.

27. Have a soft heart.

28. Often forget to put things back in their proper place.

29. Get upset easily.

30. Do not have a good imagination.

31. Talk to a lot of different people at parties.

32. Am not really interested in others.

33. Like order.

34. Change my mood a lot.

35. Am quick to understand things.

36. Don't like to draw attention to myself.

37. Take time out for others.

38. Shirk my duties.

39. Have frequent mood swings.

40. Use difficult words.

41. Don't mind being the center of attention.

42. Feel others' emotions.

43. Follow a schedule.

44. Get irritated easily.

45. Spend time reflecting on things.

46. Am quiet around strangers.

47. Make people feel at ease.

48. Am exacting in my work.

49. Often feel blue.

50. Am full of ideas.

E QUESTIONS RELATED TO THE EXPERIENCE OF BEING A RANSOMWARE VICTIM

Note: Questions 53-56 within this subset were only asked to ransomware victims.

52. Have you ever been a victim of a ransomware attack? Ransomware is a type of malicious software, or malware, that denies access to a computer system or data until a ransom is paid.

○ Yes ○ No

53. When did the (most recent) attack take place?

○ Within the past 3 months
○ 4-6 months ago
○ 7-9 months ago
○ 10-12 months ago
○ More than a year ago

54. Did you pay the ransom?

○ Yes ○ No

55. Did you recover your files?

○ Yes ○ No

56. Did you report or talked about the attack to anyone? (Please tick all that apply)

□ Friend or family member
□ No-one
□ Action Fraud helpline
□ Police
□ Other

F QUESTIONS RELATED TO THE FEELING AFTER RANSOMWARE VICTIMISATION

Note: All the questions within this subset have the same five options for their answer:

○ 1 - not present
○ 2
○ 3 - moderate
○ 4
○ 5 - very high level

The purpose of these questions was to collect Likert scale data regarding the range of feelings that the participants experienced after becoming victim of a ransomware attack.

57. Anxiety

58. Sadness

59. Fear

60. Anger

61. Embarrassment

62. Shame

63. Paranoia

64. Regret

65. Depression

66. Sleeplessness

67. Vulnerability

68. Distress

69. Nervousness

70. Isolation

71. Lacking in confidence

G QUESTIONS RELATED TO CHANGES IN SECURITY BEHAVIOUR AFTER VICTIMISATION

Note: Questions 76–92 within this subset have the same five options for their answer:

○ 1 - stopped
○ 2
○ 3
○ 4
○ 5
○ 6 - increased

The purpose of these questions was to collect Likert scale data regarding any changes in cybersecurity-related online activities, ranging from "completely stopped" to "increased", after ransomware victimisation.

73. After the ransomware attack, on average, how often do you back up your important data?

○ Daily
○ Several times a week
○ About once a week
○ About once a month
○ A few times a year
○ About once a year or less frequently
○ Never

74. How often did you back up your important data before the ransomware attack occurred?

○ Daily
○ Several times a week
○ About once a week
○ About once a month
○ A few times a year
○ About once a year or less frequently
○ Never

75. After the ransomware attack occurred, what measures have you taken to improve your online security? (Please tick all that apply)

□ Use up to date anti-virus software
□ More careful when opening links from emails

□ Use a firewall
□ Use a different password for different sites
□ Change passwords regularly
□ Limiting the use of USB sticks
□ Reduce online banking
□ Reduce online shopping
□ No measures
□ Other

76. Searching for information using search engines (Google, Wikipedia, etc.)

77. Sending/reading emails.

78. Sending instant messages (SMS, iMessage, Facebook messenger, WhatsApp etc.)

79. Browsing social media (Facebook, Instagram, Twitter, etc.)

80. Watching online videos or movies *(outside of your social media feeds)*

81. Looking at photos or images *(outside of your social media feeds)*

82. Using the camera on any of your devices to take photos or record videos.

83. Sharing your photos (including posting to social media or sending via messaging apps).

84. Sharing your videos (including posting to social media, sending via messaging apps or video-calling).

85. Listening to music (including Spotify, Apple Music or MP3s that you downloaded).

86. Browsing or posting to an online forum.

87. Online banking.

88. Working on your own website or creating your own content to post online *(outside of social media).*

89. Using file sharing or cloud syncing software (e.g. Dropbox, OneDrive, BitTorrent etc.)

90. Coding or writing software.

91. Using software to cover your tracks online (i.e. used privacy enhancing features such as incognito mode, using Tor or a webcam cover).

92. Downloading/installing software or other files from an online source.

94. After the attack, to what extent do you feel at risk from cybercrime?
○ I don't feel at risk, it won't happen to me.
○ I don't feel at risk, I didn't think about it.
○ I don't feel at risk, but it could happen to me.
○ I feel at risk, I'm careful online.
○ I feel at risk, I'm very careful online.
○ I feel the risk is unbearably high.

95. To what extent did you feel at risk from cybercrime before the attack?
○ I didn't feel at risk, I thought it won't happen to me.
○ I didn't feel at risk, I didn't think about it.
○ I didn't feel at risk, but I thought it could happen to me.
○ I felt at risk, I was careful online.
○ I felt at risk, I was very careful online.
○ I felt the risk was unbearably high.

96. Have you received any training on computer security (either through work, school, or other venues)?
○ Yes ○ No

97. Did you receive the training on computer security before the ransomware attack?
○ Yes ○ No

H QUESTIONS ABOUT EXPERIENCE WITH OTHER CYBERCRIME VICTIMISATION

Note: Question 99 within this subset were only asked to who had responded positively to question 98.

98. Have you ever been the victim of any other types of online crime?
○ Yes ○ No

99. Please give details about the type(s) of online crime you were a victim of. Tick all that apply:
□ ONLINE FRAUD: Had any of your online accounts accessed by someone (without your consent).
□ ONLINE FRAUD: You have noticed unauthorised online transactions on any of your bank accounts.
□ ONLINE FRAUD: You were tricked into buying goods, software or services online that turned out to be fake or counterfeit.
□ ONLINE FRAUD: You have been tricked into sending money to someone you met online.
□ ONLINE FRAUD: You have been tricked into sending goods or services to someone online without adequate compensation.

□ CYBERSTALKING OR ONLINE HARASSMENT: Someone said something to you privately online in order to make you feel bad or scared.

□ CYBERSTALKING OR ONLINE HARASSMENT: Someone posted something about you publicly online in order to make you feel bad or scared.

□ CYBERSTALKING OR ONLINE HARASSMENT: Someone revealed sexual images, videos or details of you online without your consent.

□ DATA HACK: Someone intentionally locked you out of any of your devices or disabled access to your data remotely.

□ DATA HACK: Your files have been copied, modified or deleted without your permission.

□ ONLINE EXTORTION (OR ATTEMPTED): You have been asked to provide a payment in order to prevent sexual images, videos or details being posted online (or used against you in some other way).

□ ONLINE EXTORTION (OR ATTEMPTED): You have been asked to provide a payment in order to prevent other stolen data or files being posted online (or used against you in some other way).

□ Other

I DEMOGRAPHICS QUESTIONS

100. Please select your age group:

○ 18-24 years old
○ 25-34 years old
○ 35-44 years old
○ 45-54 years old
○ 55-64 years old
○ 65 or older

101. Please select your gender:

○ Female
○ Male
○ Other

102. Please select your employment status:

○ Employed part time (up to 34 hours per week)
○ Employed full time (35 or more hours per week)
○ Student
○ Unemployed
○ Self-employed
○ Retired
○ Other

103. Please select the highest degree you have completed:

○ GCSE or equivalent

○ A-levels or equivalent
○ Undergraduate degree
○ Postgraduate degree
○ Professional qualification
○ Other

104. Please select your region:

○ Greater London
○ South East
○ North West
○ South West
○ Scotland
○ West Midlands
○ Yorkshire and the Humber
○ East of England
○ East Midlands
○ Wales
○ North East
○ Northern Ireland
○ Other

105. Please select the type of settlement you live in:

○ Suburban community
○ City or urban community
○ Rural community
○ Other

J ATTENTION CHECK QUESTIONS

Note: These three questions were scattered within the questionnaire – the number in front of each question indicates the position of that question within the questionnaire. These questions served as a validation tool to ensure that the participants paid attention to the questions being asked while filling in the questionnaire online. Any failure in correctly completing *all* of these "attention check questions" would result in the corresponding participant's data being excluded from the dataset.

51. It is important that you pay attention to this study. Please tick "disagree".

○ 1 - disagree
○ 2
○ 3 - neutral
○ 4

○ 5 - agree

72. It is important that you pay attention to this study. Please tick “very high level”.

○ 1 - not present
○ 2
○ 3 - moderate
○ 4
○ 5 - very high level

93. Parity check. For the parity check please select option 1, “completely stopped”.

○ 1 - stopped
○ 2
○ 3
○ 4
○ 5
○ 6 - increased