"I was told to buy a software or lose my computer. I ignored it": A study of ransomware

Camelia Simoiu
Stanford University

Christopher Gates
Symantec

Joseph Bonneau
New York University

Sharad Goel
Stanford University

Abstract

Ransomware has received considerable news coverage in recent years, in part due to several attacks against high-profile corporate targets. Little is known, however, about the prevalence and characteristics of ransomware attacks on the general population, what proportion of users pay, or how users perceive risks and respond to attacks. Using a detailed survey of a representative sample of 1,180 American adults, we estimate that 2%–3% of respondents were affected over a 1-year period between 2016 and 2017. The average payment amount demanded was $530 and only a small fraction of affected users (about 4% of those affected) reported paying. Perhaps surprisingly, cryptocurrencies were typically only one of several payment options, suggesting that they may not be a primary driver of ransomware attacks. We conclude our analysis by developing a simple proof-of-concept method for risk-assessment based on self-reported security habits.

1 Introduction

Ransomware is a particularly pernicious form of malware that restricts an individual's access to their computer (e.g., by encrypting their data) and demands payment to restore functionality. While the first documented ransomware attack dates back to 1989, ransomware remained relatively uncommon until the mid 2000s [26]. Since then, the attack has been automated and professionalized. It is believed to be highly lucrative, with previous damages estimated at hundreds of millions of dollars per year. For example, the damages caused by a single ransomware variant, CryptoWall3, were estimated to be over $320 million in 2015 alone [1].

Consumers are thought to be the most common victims of ransomware [5, 7]. While most attacks are thought to be untargeted, consumers are often less likely to have robust security in place, increasing the likelihood of falling victim to an attack [7]. Despite the harm ransomware can inflict, relatively little is known about the prevalence and characteristics of such attacks in the general population. Reliable estimates of the prevalence of ransomware are necessary both for understanding the nature of today's threat landscape, as well as for longer-term comparison and analysis.

Various government, industry organizations, and researchers have attempted to document the phenomenon, but results have been often inconsistent. This is in large part due to the non-representative data they are based on. Industry reports are typically published by security firms and are based on users of their software products. Such samples are thus inevitably biased towards a set of consumers who have sufficient security awareness and the financial resources to purchase such products. Their experiences may thus not reflect those of the general population. In contrast, government agencies typically report rates based on voluntary victim reports. These estimates are thought to grossly underestimate the true rate [33]. For example, the U.S. Department of Justice estimates that only 15 percent of the nation's fraud victims report their crimes to law enforcement [2], however it is unclear what the true rate of reporting is in the general population.

Apart from the difficulty in characterizing the extent of the problem, little is known about the factors and behavioral patterns that place individuals at risk of such attacks. Devising accurate risk assessment methods to identify the vulnerable population is particularly relevant for ransomware attacks, as infection may impose an especially high cost to consumers. There is often little recourse for victims who need to recover their data other than to pay the ransom. Once identified, information about the vulnerable population can be used to establish proactive strategies to mitigate the effects of ransomware attacks for those individuals that are most at-risk.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

For example, the vulnerable population may be influenced through several means, including personalized educational resources and training, or discounted offers for services to mitigate the effects of infection (e.g., cloud-based data backup services). Consumers, if made aware they are at risk of infection, may be better motivated to adopt preemptive measures to mitigate the effects of a potential attack.

We make two key contributions. First, we report the results of a representative online survey of 1,180 U.S. adults that queried respondents' experiences with ransomware attacks. Our results allow us to estimate the prevalence of ransomware in the general U.S. population and responses to such attacks. Second, we develop a simple, proof-of-concept risk assessment for ransomware victimization based on self-reported security habits, which offers an approach for computer users to self-assess their risk of an attack.

2 Related work

2.1 Estimates of ransomware victimization

The FBI's Internet Crime Complaint Center received 2,673 reports about ransomware in 2016, corresponding to an estimated $2.4 million in losses [4]. The numbers were slightly lower in 2017, with 1,783 ransomware reports received and an estimated $2.3 million in losses [8]. Government estimates, however, are known to underestimate the true rate, as they rely on voluntary self-reports.

Another source of data comes from industry reports that publish experiences of users of their antivirus products. These reports typically use blocked detections as a proxy for actual infections. For example, Symantec reports 405,000 consumer ransomware infections blocked between June 2016 and June 2017 [7]. While analyses by security vendors have the advantage of not relying on self-reports, they suffer from other biases. Industry reports only have visibility into the experiences of the subsection of the population who self-selected to purchase their security product. This sample is likely not representative of the general online population, as it is comprised of individuals who may have a heightened security awareness of online threats, value the product, and have the financial resources to purchase protection. Moreover, blocked detections are imperfect metrics of infection. Traditional, signature-based methods can only detect and block known threats likely missing newer attacks, while more modern machine learning methods suffer from false positives.

More recently, researchers have leveraged public Bitcoin transactions to estimate ransomware infections. For example, Huang et al. [23] provide a lower-bound estimate of 19,750 potential victims globally who made ransom payments using Bitcoins. They do so by (1) scraping reports of ransomware infections in public forums and lists of seed ransom addresses from proprietary sources that maintain a record of ransomware victims and the associated ransom addresses, and (2) extracting ransom addresses by executing several ransomware binaries in a controlled environment. Although the measurement framework presented allows for large-scale measurement of victim rates, it is only able to provide insights into one payment method, namely Bitcoin payments. As we will show, our findings suggest that only focusing on this payment method may provide an incomplete picture of total infections.

2.2 Susceptibility to ransomware

The classical paradigm to defend against malware attacks has traditionally been victim-agnostic and reactive, with defenses focusing on identifying the attacks or attackers (e.g., phishing emails, malicious websites, and files) [22]. For example, several studies propose technical, automated solutions to prevent ransomware attacks [16, 25, 26, 35, 39].

More relevant to our work are user studies that identify the vulnerable population and the behaviors that predispose users to malware infections. These cover a wide range of contexts and sub-segments of the population and are typically administered to small, non-representative sample sizes. As a result, it has been difficult to draw conclusions with respect to the general importance of demographic, situational, and behavioral factors on risk of victimization. Ngo et al. [31] apply the general theory of crime and routine activities [17] to assess the effects of individual and situational factors on seven types of cybercrime victimization—among them, a computer virus. They administer an online survey of self-reported cybercrime victimization to 295 students in the U.S., and find that non-white students and younger students had significantly higher odds of obtaining a computer virus. Perhaps counter-intuitively, they also find that individuals who frequently opened any unfamiliar attachments or clicked on web-links in the emails that they received, opened any file or attachment on their instant messengers, and frequently clicked on a pop-up message that interested them, had lesser odds (by about 35%) of obtaining a computer virus.

Bossler et al. [15] conducted a survey of 788 college students to study the risk factors of data loss caused by malware infection. The factors studied include "deviant" behavior (e.g., pirated media downloads, visiting adult websites), routine behaviors (e.g., social media use, programming, shopping), guardianship measures (e.g., having AV software, sharing passwords), and computer skills. The authors find that being employed and being female increased the odds of malware victimization. Engaging in deviant behavior was generally not a strong predictor of malware infection—only pirating media increased the risk of malware infection. Guardianship played small roles in explaining infections, and strong computer skills and careful password management did not reduce estimated threat of malware victimization. Milne et al. [30] conduct a national online survey of 449 US online shoppers. They find that gender, age and number of hours spent online,

excluding email, have a significant impact on users' likelihood to adopt risky online behaviors, concluding that male, younger users, and users who spend many hours online were more at risk.

More recently, researchers have turned to large-scale, data-driven approaches to predict user risk of various cyber threats. Maier et al. [29] examine whether the risk of generating malicious traffic is correlated with security hygiene using DSL data logs of anonymized network traces. They find that having good security hygiene (e.g., applying operating system software updates) has little correlation with being at risk, while accessing blacklisted URLs more than doubles risk.

Levesque et al. [27, 28] observe malware exposure of 50 subjects over a four month period using instrumented computers from the clinical trial of an antivirus product. They find that malware victimization is correlated with a high self-reported level of computer expertise, increased file downloads and application installations, and high browsing volume. The authors find mixed results with respect to the age of the user and the content categories of websites.

Using Symantec telemetry for a subset of 1.6 million users over an 8-month period, Ovelgonne et al. [32] study the relationship between the number of attempted malware attacks detected and user profiles. The authors classify users into 4 categories (gamers, professionals, software developers, others), and find that software developers are more at risk of engaging in risky cyber-behaviors and that there is a sub-population of gamers with especially risky behavioral patterns.

Yen et al. [38] and Bilge et al. [14] study individual user-level malware encounters in an enterprise setting. Yen et al. draw on web proxy logs, user demographics, and VPN logs from a large, multi-national enterprise. The authors investigate features related to categories of web sites visited, aggregate volumes of web traffic, and connections to blocked or low-reputation sites. Using a logistic regression model for inferring the risk of hosts encountering malware, they find that among the three feature categories, user demographics is the strongest indicator of risk, followed by VPN behavior. Counterintuitively, web activity contributed marginally to the overall model and the authors reasoned that this is due to the fact that only 3% of the hosts encountered malware from the web.

3 Survey Methodology

3.1 Sample selection

We administered a survey on ransomware experiences to a sample of 1,180 U.S. adults. Participants were recruited between June 20, 2017 and September 6, 2017 by YouGov, an online global market research firm, and reimbursed for their participation[1]. YouGov employs a panel of 2 million opt-in participants in the U.S and actively recruits hard-to-reach respondents, such as younger people and those from ethnic minorities, via a network of partners with access to a wide range of online sources that cater to these groups. [2]

In order to derive nationally representative estimates of the U.S. population, YouGov draws stratified samples that approximate the characteristics of random samples of the U.S. population. The sampling frame was designed to match the population in the full 2010 American Community Survey (ACS) conducted by the US Census, and was augmented with voter and consumer databases using the November 2010 Current Population Survey. Summary statistics detailing the demographics of respondents are provided in Table 1, and a more extensive exposition of demographics and socioeconomic characteristics is given in A2 in the Appendix.

3.2 Adjustment weights

When constructing a representative sample, non-response and self-selection bias are two common problems that occur, resulting in some population groups being over- or under-represented in the final sample [20, 33]. We use sample weights to address these issues, a standard technique to correct for sample bias. At a high-level, each sample member is assigned a weight such that respondents in under-represented groups receive a weight larger than 1, and those in over-represented groups receive a weight smaller than 1.

YouGov provided adjustment weights for our full sample of 1,180 respondents, which we use throughout our analysis to weight responses.[3] The weights were created by matching to the sampling frame using propensity scores. The matched cases and the frame were combined and a logistic regression was estimated for inclusion in the frame. The propensity score function included age, gender, race/ethnicity, and years of education; propensity scores were then grouped into deciles of the estimated propensity score in the frame and post-stratified according to these deciles.

3.3 Defining a ransomware attack

We define ransomware as the class of malware that attempts to defraud users by restricting access to the user's computer or data, typically by locking the computer or encrypting data. There are thousands of different ransomware strains in existence today, varying in design and sophistication [13]. Some ransomware strains can be easily circumvented, while others employ a variety of advanced tactics. For example, they may utilize payload persistence, ensuring the ransomware persists after a restart; use strong encryption methods that are nearly

[1] Participants accumulate points on YouGov for each survey they complete, which an later be redeemed for cash rewards or gift cards at a number of retailers (e.g., Amazon, Best Buy, Target etc.).

[2] The sources include search engine optimization (SEO), affiliate networks, niche websites, and growth hacking techniques such as panelist refer-a-friend campaigns and social networks [6].

[3] Weighted rates were typically quite close to the raw proportions. Omitting the weights did not change the results qualitatively.

	Raw prop.	Weighted prop.
Female	55%	54%
Male	45%	46%
White	81%	75%
Black or African American	8%	11%
Hispanic or Latino	5%	8%
Asian	2%	2%
Native American	1%	1%
Other	4%	3%
Age (19 – 30)	11%	16%
Age (31– 45)	19%	25%
Age (45 – 60)	28%	27%
Age (over 60)	42%	32%
Some high school	1%	2%
High school	20%	31%
Some college	22%	22%
College	39%	33%
Post-graduate	17%	12%

Table 1: *Demographic information and highest level of education achieved (n=1,180 respondents). The raw proportion represents the fraction of respondents and the weighted proportion represents the post-stratified proportion.*

impossible to reverse; or disable system restore functionality (e.g., delete Windows shadow copies) in order to prevent encrypted data from being restored to an older, unencrypted version [19].

Yet another class of ransomware, sometimes referred to as "fake ransomware", informs infected users that their data has been encrypted or their computer locked, however does not actually do these things. These types of attacks are less sophisticated from a technical perspective, are usually relatively easy to circumvent, and rely on scare tactics to coerce the user into paying the ransom amount. We ask respondents to report all types of ransomware, and distinguish between different types, post-response.

3.4 Establishing victimization status

Respondents were asked to report any ransomware attack that they had experienced in the past. In order to ensure the accuracy of self-reported ransomware attacks, respondents progressed through a series of ten question and information pages describing typical ransomware attacks and their characteristics. Respondents were initially shown the following definition of ransomware: *"Ransomware is a type of malware that will either lock your computer screen or encrypt your files. If you've been infected with ransomware, you will see screens like the examples below, informing you that you must pay a ransom to re-gain access to your computer and/or files, providing instructions on how to do so."*

Three screenshots of ransomware variants were shown as examples: a strain impersonating the FBI and two encryption ransomware variants, with and without a timer (Figure 1). In

Figure 1: Respondents were shown these three sample screenshots of ransomware: a strain impersonating the FBI and two encryption ransomware variants, with and without a timer.

order to distinguish ransomware attacks from malware with similar characteristics, respondents were shown a page explaining how ransomware is different from technical support scams. [4]

A series of additional questions were then used to confirm respondents' self-reported victimization status. Three multiple choice questions asked whether they experienced various characteristics commonly found in ransomware attacks, namely: (1) whether they had seen similar images notifying them that their computer was locked or files/data encrypted; (2) whether their files were encrypted and they saw files with names such as "DECRYPT INSTRUCTIONS.HTML" or with unusual extensions such as ".locky"; and (3) if they saw a timer counting down and messages indicating that if payment is not completed before the time expires, the ransom amount will increase or the encryption key will be deleted. The ransomware definition above was then repeated and respondents were asked whether they had experienced a ransomware attack, and could answer *Yes*, *No*, or *I am not sure*. If respondents indicated that they were not sure or if their initial response was inconsistent with their answers to the three questions on ransomware characteristics (e.g., they checked off at least one of the three characteristics, but concluded that they did not have ransomware), they progressed through a series of further clarification questions and information pages, which ultimately culminated with the same question (as above) asking them to confirm whether or not they had been infected with ransomware.

Respondents indicating they had experienced a ransomware attack either in the first or second prompt progressed to a series of questions soliciting information about the attack. They

[4] Technical support scams are misleading application that alert the user to a fictitious security issue or vulnerability on their computer, and then prompt them to call a tech support number or to download or purchase anti-virus software in order to resolve the issue.

were asked to describe the ransomware attack in their own words, with prompts to include the contents of the message or instructions, the appearance of the screen, and if any functionality of their computer was disabled. They were also asked a series of questions detailing: the month and year of the attack, the name of the ransomware variant, how much ransom (money) was demanded, the method of payment, whether they paid the ransom and why (or why not), whether access was restored after payment (if applicable), which strategies, if any, they attempted to remove the ransomware and restore access to their computer, whether they sought help in removing the ransomware, whether they were able to remove the ransomware without losing data, how the ransomware was eventually removed, and whether they notified the authorities.

These questions served a dual purpose: apart from allowing us to distinguish between strains with differing attributes (e.g. encryption, screen lock, impersonation of law enforcement), they provided an additional means of validating that the reported incident was indeed a ransomware attack. If respondents had experienced more than one ransomware attack, they were instructed to respond to all questions based on the last attack.

3.5 Ethical considerations

All aspects of our study were approved in advance by the university's Institutional Review Board (IRB protocol number 40466). Participants had to reside in the United States and be over 18 years of age to participate. The average completion time was 9.1 minutes (sd=6.8min). Respondents had the option to withdraw at any point during the survey without providing any reason. We informed them that in such a case, none of their data would be used in the analysis. No participant withdrew. Prior to running the study, the survey tool was piloted on Amazon's Mechanical Turk. Five pilot tests with 100 participants each were run. The average completion time ranged from 5min - 8min and each participant was reimbursed the equivalent of $10/hr for completing the survey. Following each pilot, the tool was updated based on preliminary results and feedback from respondents.

3.6 Limitations

By design, our survey instrument was intended to mirror the general U.S. population along demographic and socioeconomic dimensions. Nevertheless, it may be still be biased along dimensions other than those that we have explicitly accounted for. For example, YouGov respondents may have technological expertise and privacy and security preferences that differ from those of the broader population.

Additionally, as is the case with nearly all surveys, our results are subject to limitations as they are based on self-reported infection rates rather than upon actual detections of malware. Despite our efforts to ensure that respondents understood what a ransomware attack is, we cannot be certain that ransomware attacks or their attributes were correctly identified. For example, if respondents did not remove the ransomware themselves or did not try relevant troubleshooting strategies (e.g., changing the extensions of files back to the original in order to test whether the encryption was real or not), we cannot know with certainty whether strong encryption was used. Some participants may have confused locked or encrypted files with other problems such as corruption, deletion, or other access issues. Additionally self-reported responses could reflect inaccurate recall and social desirability bias. For example, participants may have been embarrassed to report paying a ransom to restore their data despite their answers being anonymous.

We made several attempts to mitigate these issues. First, the survey tool was piloted on Amazon's Mechanical Turk prior to running the study. The pilots included options to select "I am not sure" or "other" on each question, allowing us to identify which questions were creating confusion as well as any missing options in our multiple choice questions. A follow-up free-text question was displayed to participants that selected "I don't know" to understand the source of confusion, allowing us to further refine our survey tool on each iteration. Second, all self-reports of ransomware victimization for the study on YouGov respondents were independently reviewed by two independent researchers and re-classified when necessary (details provided in Section 4.1).

One limitation to piloting on Mechanical Turk is that the population there differs from that used for the final study. Mechanical Turkers, for example, have been found to be a relatively tech-savvy group [33] and YouGov respondents may not have interpreted questions in the same way due to lower technical expertise. To mitigate these issues, future work could pilot the survey tool on the same population as the target population. The use of focus group with members of the public would also allow researchers to ask follow-up questions on the survey and discuss any ambiguities with respondents. While our results may be impacted by these limitations, we believe that our study is still a step forward in understanding ransomware experiences for the general online population.

4 Results

4.1 Re-classifying victimization status

All responses from self-reported ransomware victims were independently reviewed by two independent researchers, and all conflicting classifications were reviewed and resolved. Each response was classified under two regimes: a *conservative* regime and an *inclusive* regime. [5] Both regimes exclude cases where the respondent described a different type of malware

[5] Cohen's kappa measuring inter-rater agreement prior to reaching consensus was 0.53 and 0.66 for the conservative and inclusive regimes, respectively.

attack (e.g., scareware, pop-up announcing that they were the winner of a contest, or tech support scam), or admitted that they did not remember the details of the attack. The difference between the two regimes is relevant for ambiguous cases. The conservative regime includes only cases where the description of the attack provides sufficient information to confirm beyond reasonable doubt, that it was ransomware. The inclusive regime includes, in addition to the above, cases where the description was ambiguous or no description was provided. We include both regimes as both require an assumption on the part of the coders, namely either that the respondent understood what a ransomware attack was and simply did not choose to provide lengthy description (inclusive regime), or did not understand what a ransomware attack was (conservative regime). Fortunately, estimated prevalence was similar under both the inclusive and conservative classification schemes. For this reason, with the exception of the ransomware rate, all results are reported for victims classified under the *inclusive* regime for ease of exposition. Sample responses and their classification under the two regimes are listed in Table 2.

Prevalence is estimated by the following:

$$r = \frac{\sum_i I_i(\text{victim}) w_i}{\sum_i w_i} \tag{1}$$

where $I_i(\text{victim})$ is an indicator function representing whether the respondent reported experiencing ransomware or not, and w_i is the weight.

4.2 Rate of ransomware victimization

Originally, 153 respondents (14%) reported that they had experienced a ransomware attack at some time in the past (Table 3). Following re-classification, we estimate that the overall proportion of the U.S. population reporting a ransomware infection at any time in the past ranges between 6% (se=1%, n=63) under the conservative regime, and 9% (se=1%, n=96) under the inclusive regime[6] We similarly estimate that between 2% (se=0.4%, n=19) and 3% (se=0.5%, n=33) of the U.S. population were affected over the one-year period between June 2016 to June 2017 under the conservative, and inclusive regimes, respectively.

Given that there are approximately 200 million U.S. adults who have a computer with internet access [10, 12, 34], our results suggest that several million Americans were victims of ransomware in the 1-year period we studied. We note, however, that multiple people may share the same computer. As such, the number of *victims* of ransomware attacks may be substantially larger than the number of *households* that experienced an attack or the number of infected *computers*.

It is difficult to directly compare our estimates to those from previous studies, but our results appear to be broadly consistent with past evidence. For example, Symantec reported 405,000 consumer ransomware infections were blocked between June 2016 and June 2017 [7]. Given that approximately 25 million U.S. consumers use Symantec AV [11], that suggests an infection rate of 1.6%.[7] Our estimate also appears to be approximately consistent with evidence provided by Huang et al. [23], though we must make several assumptions to compare their reported numbers to our own. Specifically, Huang et al. identify approximately 20,000 bitcoin payments for ransomware globally over a 22-month period, or roughly 10,000 over 12-months. This number, though, likely substantially undercounts the true number of payments because only a fraction of all such bitcoin transactions could be identified, as described in Section 2. In our survey, only 1% of ransomware victims made a bitcoin payment—the vast majority did not pay at all. If that number is representative, the 10,000 bitcoin payments globally translates to approximately 10,000 / 1% = 1 million global ransomware incidents. We caution that one cannot directly compare this estimate to our own: we consider only U.S. victims, not global victims; and the number of bitcoin payments identified by Huang et al. is an underestimate of the actual number of payments. Nonetheless, despite being based on quite different methodologies, the two approaches yield estimates of the same order of magnitude.

4.3 Ransomware attributes

We now turn our focus to examining the characteristics of ransomware attacks experienced by respondents. Overall, ransomware strains that lock the computer appear to be more common than those that employ encryption — 74% of victims reported experiencing computer locks, while only 35% reported that their files were encrypted. Our finding is in line with a recent report by Kaspersky Lab, which finds that 40% of users are attacked with encryption ransomware as a proportion of users attacked with any kind of ransomware in the U.S. between 2015 and 2016 [3]. Figure 2 shows the distribution of attributes experienced by ransomware victims. Two observations stand out. First, a large proportion of victims reported experiencing strains that impersonate law enforcement agencies, typically the FBI (46%). These strains typically display a message claiming that the user's computer was locked because they engaged in illegal activities (e.g., browsed illegal pornographic websites), and a fine must be paid to regain access. Second, encryption does not appear to be commonly used in conjunction with law enforcement impersonation. Only 22% of victims reporting law enforcement strains also reported that their files were encrypted, whereas 43% of victims that did not experience law enforcement strains experienced encryption.

[6] Standard errors (se) are given in parenthesis.

[7] To estimate the number of U.S. Symantec users, we scaled the reported number of global Symantec users (50 million) by the reported share of revenue generated by U.S. users (52%).

Respondent's description	Screen lock	Encryption	Law enforcement	Timer	Inclusive	Conservative
"Illegal files detected. FBI has locked your computer. purchase a prepaid VISA and pay fine online . (included a fake web cam window)	•		•		Ransomware	Ransomware
"FBI - YOU HAVE BEEN WATCHING PORN OR GAMBLING OR BOTH, YOU MUST PAY $200 TO MONEYGRAM"	•	•	•		Ransomware	Ransomware
"The screen looked like one you previously displayed. It encrypted just about all my files except *.exe files and a few others. I lost everything on my PC and external hard drive. I ended up reformatting and starting from scratch. I could run programs, but could not access any of my saved working files. A screen would display telling me to call a number, pay the ransom and they would decrypt my files. They wanted $500."		•			Ransomware	Ransomware
"i don't remember what the message said it just prevented me from getting to any of the stuff on my computer and then i started it in safe mode and got rid of it"	•				Ransomware	False Positive
" It wasn't a specific ransom note but it was inferred that unless I bought the software my files wouldn't be at my disposal. They were."		•		•	Ransomware	False Positive
"It popped up and stated that I had to pay to gain access back to my computer and I was unable to do anything."	•				Ransomware	False Positive
"the screen was flashing call this number immediately to get your computer repaired. I was gullible and scared so I called. the guy got a hold of my computer and then told me I had to pay $300 for him to fix it. I told him I didn't have that kind of money and he hung up on me. I then went and changed all my passwords and prayed he didn't get any important info from me."		•			False positive	False positive
"I don't recall exactly, However when I called to find out what was going on, I was told that I would have to pay to get what ever was holding up my computer off, I said, You put it on, just take it off. My computer was older, I just went and bought another computer, I decided not to be an ATM for criminals."					False positive	False positive
"Was told to send $1000.00 dollars to clean up computer."					False positive	False positive

Table 2: *Sample descriptions and reported characteristics of the attack, and their corresponding classification under the conservative and inclusive classification regimes. Responses classified as false positives under the conservative regime, but not the inclusive regime, are typically classified as such due to unclear or ambiguous descriptions. Responses classified as false positives under both regimes are typically classified as such because the descriptions provided typically describe other scams (technical support scams, scareware, etc.) and they include few ransomware characteristics (if any).*

4.4 Ransom payment

A histogram of reported ransomware amounts demanded is shown in Figure 3. The median and average reported ransom is $250 and $530 (standard error $125), respectively, while the maximum amount reported reached $8,000. This finding is approximately in line with Industry reports. For example, Symantec reports the average ransom 2016 to be $1,077 in 2016 and $522 in 2017 [7, 9].

The most common payment methods reported were wire transfers and payment voucher systems (e.g., Paysafecard, MoneyPak, CashU, MoneXy, prepaid Visa)[8], which together accounted for 56% of all reports. In contrast, only 12% of

[8]Respondents were presented with a multiple choice question and asked what payment method they were asked to pay the ransom in. As respondents could not select multiple payment methods, we are able to estimate a lower bound on the distribution of payment methods. Only respondents that were able to recall the ransom amount are included (n=66).

	All victims	Last 12 months
Self-reported	14%	5%
Re-classified (inclusive)	9%	3%
Re-classified (conservative)	6%	2%

Table 3: *Proportions of ransomware victimization for the U.S. population under the conservative and inclusive classification schemes. The "all victims" column includes respondents who reported experiencing a ransomware attack at any time in the past; the "last 12 months" column includes respondents who reported attacks within one year of the survey date.*

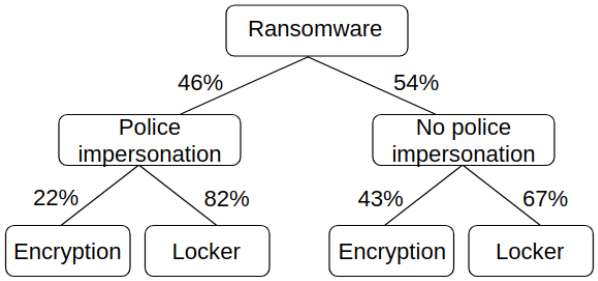

Figure 2: *Distribution of ransomware attributes (impersonation of law enforcement, locker, encryption). Categories are not mutually exclusive. Strains employing police impersonation tactics are widespread (46%) and tend to favor locking mechanism as opposed to encryption.*

respondents reported being asked to pay only via cryptocurrency. Table 4 shows the distribution of payment method for respondents reporting a ransomware attack[9].

Our results are primarily driven by the predominance of locker ransomware in our sample (recall that 74% of victims reported experiencing locker ransomware). This is consistent with characteristics of ransomware samples observed in the wild. Since ransomware strains that rely on locking techniques (as opposed to encryption) effectively restrict functionality to the computer, they must rely on pre-paid cash vouchers or wire transfers for payment. Encryption ransomware strains typically do not restrict functionality and tend to favour cryptocurrency payment schemes [13].

While recent work has focused on tracking Bitcoin payments as a means to estimate ransomware infections and quantify financial losses [23], this finding suggests that focusing solely on cryptocurrencies may underestimate losses as it focuses on only one of many types of ransomware families. Secondly, it casts doubt on the hypothesis that increased adoption of cryptocurrencies is a main driving force of the recent ransomware trend.

[9]Results are qualitatively similar for victims reporting experiencing a ransomware infection within the last 12 months: 62% reported wire transfers or payment voucher systems whereas only 2% reported cryptocurrencies.

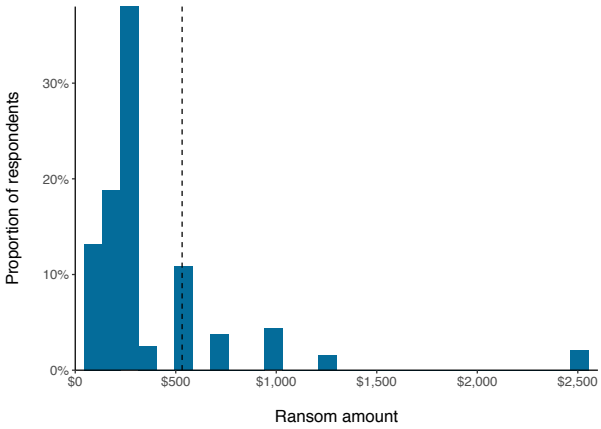

Figure 3: *Histogram of reported ransom amounts for respondents recalling an amount (n=66). The median and mean reported ransom is $250, and $530 (se. $125), respectively. The dashed line represents the mean. The maximum amount reported, $8,000 is omitted from the plot.*

Method of payment	Proportion
Pre-paid cash voucher	42%
Wire transfer	14%
Cryptocurrency	12%
Premium-rate text message	7%
Not displayed	15%
Do not remember	10%

Table 4: *Distribution of payment methods. Wire transfers and pre-paid cash vouchers predominate, whereas cryptocurrencies account for 12% of reported payment methods. The"not displayed" category includes cases where the payment method was not directly displayed (e.g., respondents would have had to follow a link to find out, and did not do so).*

4.5 Means of dealing with the attack

Respondents reported a wide range of methods for dealing with the ransomware infection, depending on the severity of the strain. As detailed in Table 5, the majority of victims either found a tool online to remove the ransomware and/or decrypt their files, restored their computers from backups, or re-started their computers (e.g., in safe mode). 13% of victims obtained help in removing the ransomware, either paying for repairs at a computer shop or asking friends or family for help.

Few victims paid the ransom (n=6, 4%) or reported the attack to authorities (n=7, 9%). Access was restored for all victims that did pay. The self-reported reasons for paying the ransom focused on feelings of distress, aversion to losing files, as well as lack of computer knowledge. Respondents' original reasons are given below:

Method	Proportion
Restarted computer	30%
Online tool	18%
Restored computer from backup	22%
Removed by someone else	13%
Reformatted computer	5%
Removed using AV software	5%
Paid ransom	4%
Other means	3%

Table 5: *Self-reported means of dealing with the attack.*

1. *"I am computer illiterate. A little smarter now."*
2. *"We were very distressed and felt it was a legitimate request."*
3. *"Did not want to lose any files or programs on my system."*
4. *"I'm so scared"*
5. *"I was a full time caregiver for my critically ill husband. He used the computer a great deal to maintain contact with friends and family. I did not want to take the computer somewhere to have the problem corrected at what likely would have been a more expensive cost.*
6. *"The price was not that high."*

To note is that financial losses associated with paying the ransom only capture one dimension of the total costs imposed on victims. These include psychological costs associated with losing valuable data (e.g., family photos) and time costs of dealing with the aftermath of the attack. As one respondent details, *"It was a mess for a while [...] and very troubling, my husband worked on it for a whole day."* In addition, victims may incur additional financial costs to deal with the attack such as paying technicians to remove the ransomware or investing in protection tools such as anti-virus products to prevent future infections.

4.6 Behavioral changes post-attack

Victims were asked to indicate whether they changed any of their habits following the attack, if any. We find that 56% of respondents reported changing two or more habits. The top three changes reported were more careful browsing (65%), purchasing an antivirus software (44%), and updating their existing antivirus product (31%) (Table 6).

Few respondents reported changing their operating system (OS), although we find that victimization varies significantly with OS. We find that 10% of Windows users were victims, whereas only 5% of non-Windows users were victims. This difference is statistically significant using a two-proportion Z-test at the 5% significance level. The majority of respondents used Windows as their OS (82%)[10]. Only 26% of respondents began to backup their data or backed up their data more frequently following the attack.

Habit	Proportion
More careful browsing	65%
Purchased AV product	44%
Updated AV product	31%
Started to backup data	26%
Enable automatic updates	24%
Backup data more regularly	22%
Changed OS configurations	20%
Changed OS	10%
Changed default browser	12%
Encrypted hard drive	0%

Table 6: *Behavioral changes following the attack for ransomware victims. Multiple answers were permitted. The top three changes reported were more careful browsing, and purchasing or updating an antivirus product. "Enable automatic updates" refers to updates to the OS, browser, antivirus, and other programs. Examples of configuration changes are disabling Windows Script Host, restricting login access, enabling the "show file extension" feature in Windows.)*

Whether or not participants truly changed their habits following the attack, or if this is a form of social desirability bias, is difficult to know for sure. Nevertheless, two observations stand out. First, this result suggests that the majority of victims attribute the cause of the attack, at least in part, to their own behaviors. At the very least, they display the intention to change their behaviors in order to minimize their risk. Secondly, data backup habits are arguably the single most effective way to mitigate the effects of ransomware attacks, yet few respondents adopt this behavior even after experiencing an attack. This suggests that more awareness is needed around the importance of this habit.

4.7 Perceptions of risk and responses

Along with precautionary security habits and online behaviors, risk perception — or the awareness of one's susceptibility to adverse security outcomes — is thought to play an important role in making better security decisions [37]. We investigate how experiencing a ransomware infection affects perception of risk via two questions: (1) "How likely do you think you are to experience a ransomware attack in the future?" and (2) "Suppose you were to experience a ransomware attack today and the only way of restoring access to the data on your computer was to pay the ransom (say $300). How likely is it that you'd pay the ransom?". Participants were prompted to enter a number between 0 and 100, where 100 means: "I'm

[10] 12% used a Mac, 4% used Chrome, while the remaining 2% used another OS.

definitely (100% likely) going to [experience a ransomware attack in the future / pay the ransom]." and 0 means: "There is no way (0% chance) I will [experience a ransomware attack in the future / pay the ransom]".

Whereas victims reported a mean of 47 (sd=34) for the likelihood of experiencing a future ransomware attack, non-victims reported a mean of 30 (sd=25). This difference was significant based on an independent-samples t-test, t (104) = -4.97, 95% CI of the difference (10.78, 25.07) Similarly, victims reported a mean=2.9 (sd=11) for the likelihood of paying the ransom, versus a mean of 8.4 (sd=20) for non-victims. The difference was significant: t (158)=4.26, 95% CI of the difference (2.93, 8.00). These results suggest that victims believe they are more at risk of a future attack, and less likely to pay a ransom. This may be due to victims feeling better prepared to deal with a future attack due to a change in habits or improved mitigation strategies, or feeling less uncertainty about the consequences of an attack after having experienced one. Further research, however, is needed to understand the exact reasons for these differences and carefully mitigate any response biases that may exist here.

5 Predicting ransomware infection

Given the potentially high cost of a ransomware infection, a natural follow-up question is whether it is possible to identify the set of at-risk users. Once identified, the hope is that we can mitigate the effects of an infection for those individuals that are most likely to experience an attack. In the same vein, employers could offer personalized educational resources and training; antivirus companies could fine-tune and re-prioritize defense mechanisms to offer additional protection layers, set different default settings, or partner with vendors to provide discounted offers for services to mitigate the effects of infection (e.g., online backup services). Finally, consumers—if made aware they are "at risk"—may be better motivated to improve their security posture and adopt better security habits. For example, in several health domains, Strecher et al. [36] found that perceived susceptibility—the belief that one is at risk for the issue at hand—was a necessary factor to achieve behavior change.

5.1 Traditional, machine-learned models

To estimate risk of infection, we start by training traditional statistical models on our survey data. We consider the complete set of responses (n=1,180) and define positive examples to be those that have experienced ransomware at any time in the past (9%, n=96). Given each respondent's answers, we construct a model to predict infection status using two standard machine learning models: lasso (a linear model), and gradient boosted trees (GBM, a non-linear model). To do so, we draw on several features extracted from the survey: demographics, socioeconomic status, the software used, level of computer knowledge[11], and general security habits. Table A1 in the Appendix includes a comprehensive record of features extracted from the survey questions, several of which have been inspired by previous work [15, 18, 29–31].

Features	Lasso	GBM
Dem + SES	65	63
Dem, SES, Tech, Computer	61	65
Habits	66	67
Habits + Scam	75	74
All features	76	76

Table 7: *Average AUC across K=10 folds for lasso and gradient boosting tree (GBM) models using demographics ("Dem"), socioeconomic covariates ("SES"), the technology used ("Tech"), computer knowledge ("Computer"), security habits ("Habits"), and an indicator of previously experienced an online scam ("Scam"). Models based solely on self-reported security habits and previous experience with online scams performed on par with the saturated models using all covariates.*

We believe these features are appropriate to illustrate the general predictive power of such information. But we suggest that future work along these lines make use of scales that have been expressly designed and validated to measure the relevant information. Doing so can lead to a more accurate measurement of underlying behaviors, and may ultimately lead to improved predictive performance.

We evaluate our predictive models with stratified K-fold cross-validation, where K=10, [12] and report performance in terms of average AUC score across the folds, in Table 7. We find that models using only demographic and socioeconomic features achieve a maximum average AUC of 65%. Slightly higher performance is achieved using only features related to security habits (67% average AUC). Previously experiencing an online scam also proves to be highly predictive of ransomware infection, and the model including both security habits and past experience with an online scam achieves performance on par with the saturated model that includes all features (an average AUC of 75%).

5.2 A simpler approach to risk assessment

Given the results above, we now present and discuss a proof-of-concept approach to risk assessment to estimate future ransomware infection that is based only on self-reported security habits and past exposure to online scams. The method demonstrates that assessments can, in theory, be made with

[11] We assess the level of computer knowledge using an 8-question test developed by the authors.

[12] The data is randomly partitioned into K=10 equal sized subsamples with the proportion of positive examples equal to that in the full data set. A single subsample is retained as the validation data for testing the model, and the remaining K - 1 subsamples are used as training data.

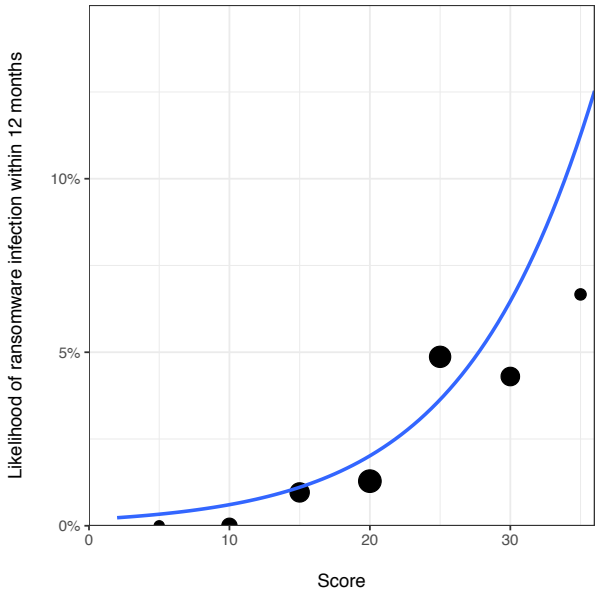

Figure 4: *Calibration plot for our simple approach to risk assessment, showing the calculated score versus the empirical proportion of ransomware infections within 12 months, and the fitted logistic regression line. Scores are grouped into buckets of 5, with each bucket containing between 3 to 13 infections. Higher scores correspond to an increased likelihood of infection.*

relatively little information, enabling consumers to estimate their own risk. We stress from the outset, however, that we merely intend to illustrate the general approach; in particular, the strategy we present would need to undergo more rigorous evaluation before it could be responsibly used for risk assessment in the broader population.

Following Jung et al. [24], we use the "select-regress-and-round" method to create a weighted risk-assessment rubric, which we find performs on par with the traditional machine learning algorithms described above. The rubric is constructed using the output from the tuned lasso model presented in Section 5.1, where we re-scale and round the resulting model coefficients to yield integer weights from 1 to 10 [24].[13]

The final risk assessment rubric is based on six factors: use of two-factor authentication, data backup habits, encryption of hard drive, frequency of using torrent services, password protection for login, and previous experience with online scams. The complete list of questions used to assess risk of ransomware, and their corresponding scores, are included in Table 8. Higher scores correspond to a higher likelihood of infection. We find that this simple approach to risk assessment performs on par with more complex models, achieving average cross-validated AUC of 78% across $K = 10$ folds.

[13]The coefficients are normalized to integers on a scale of 1-10, where the scaled coefficients are equal to $c_{\text{scaled}} = \text{round}(c_{\text{original}} * 10/c_{\max})$ and $c_{\max}$ is the maximum coefficient produced by the original model. Questions with re-scaled coefficients that round to zero are dropped from the rubric. For each remaining question, the re-scaled coefficient is multiplied by each possible answer to obtain the points in Table 8.

Question	Points
How frequently do you download files from online torrent sites such as the Pirate Bay, ExtraTorrent, or TorrentZ2?	
• I frequently download files from torrent sites.	15
• I occasionally download files from torrent sites.	10
• I rarely download files from torrent sites.	5
• I never download files from torrent sites.	0
Do you backup your personal files to an external hard drive or a cloud-based storage service?	
• I do not have any of my files backed up.	8
• I backup my files once a year.	6
• I backup my files every couple of months.	4
• I backup my files every couple of weeks.	2
• I backup my files every day.	0
Is your hard drive encrypted?	
• Yes, my hard drive is encrypted.	0
• No, my hard drive is not encrypted.	1
Have you ever downloaded—or been asked to download—an application that you suspect was malicious, like fake anti-virus software?	
• Yes, I have.	10
• No, I haven't.	0
Do you use two-step authentication for at least one of your online personal accounts (i.e., not for a work-related account)?	
• Yes, I use two-step authentication.	0
• No, I don't use two-step authentication.	1
Is your computer password-protected for login?	
• Yes, my computer has a password.	0
• No, my computer doesn't have a password.	8

Table 8: *Questions included in our simple risk assessment rubric based on self-reported security habits and previous experience with online scams.*

To aid interpretation, we convert risk scores to probability of infection as follows: we first calculate the risk score for each respondent using the derived weights in Table 8, and then predict ransomware status within 12 months via logistic regression using the calculated risk score as the sole feature. In Figure 4, we show the resulting calibration plot for the risk scores. For example, a risk score of 15 corresponds to 1% likelihood of infection.

It bears emphasis that the risk assessment method we present is only *predictive*, in the sense that the factors we identify are *correlated* with the risk of infection; the features we use are not necessarily *causally* related to future infection. For example, not backing up your data is correlated with infection, although opting to regularly back up your data will

not cause the likelihood of infection to decrease. Further, the relationship between the predictive factors we identify and ransomware infection will likely change over time. For example, as it becomes easier and less expensive to backup data, doing so may be less indicative of technical savviness and, accordingly, may be less predictive of ransomware infection. Finally, we have carried out our analysis on a relatively small dataset of users.

6 Conclusions and future work

Our survey results shed new light on the scale of ransomware in the general population and the actions users took in response. Our estimated victimization rate of 2–3% of the population per year suggests millions of ransomware cases per year. An important future research question is whether these figures are growing (and at what rate), which will require longitudinal follow-up studies.

Conventional wisdom has held that cryptocurrencies would fuel growth in ransomware, but our results suggest most cases in 2016–2017 were not reliant solely on cryptocurrency for payment. Another open question for future research is if payment rates will increase or decrease as more individuals affected have either been previously victimized themselves or have heard more about ransomware from affected friends and family. Follow-up work might study what factors affect payment rates in more detail, how users perceive their susceptibility to attack, what affects their risk perceptions, whether they are well-calibrated, and how previous infections affects their perceptions.

Finally, the simple approach to risk assessment that we present suggests that vulnerability can, in theory, be estimated from self-reported security habits and previous exposure to online scams. Our model is relatively straightforward and transparent, enabling consumers to estimate their own risk of infection. While prior research suggests these qualities make risk-assessments more acceptable to users [21], future research is required to gauge user reaction.

Acknowledgments

We thank Ansh Shukla, Leyla Bilge, Petros Efstathopoulos, Dan Boneh, and Darren Shou for helpful comments and feedback.

References

[1] Lucrative ransomware attacks: Analysis of the cryptowall version 3 threat. Technical report, Cyber Threat Alliance, 2015 (accessed August 24, 2018). https://www.cyberthreatalliance.org/resources/lucrative-ransomware-attacks-analysis-cryptowall-version-3-threat/.

[2] Financial crime fraud victims. Technical report, The United States Attorney's Office, Western District of Washington; United States Department of Justice, 2015 (accessed October 12, 2018). https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud.

[3] KSN report: Ransomware in 2014-2016, kaspersky lab. Technical report, Kaspersky Lab, 2016. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

[4] 2016 internet crime report. Technical report, Internet Crime Complaint Center, Federal Bureau of Investigation, 2016 (accessed August 7, 2018). https://pdf.ic3.gov/2016_IC3Report.pdf.

[5] KSN report: Ransomware in 2014-2016. Technical report, Kaspersky Lab, 2016 (accessed January 12, 2019). https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190822/KSN_Report_Ransomware_2014-2016_final_ENG.pdf.

[6] The YouGov online panel. Technical report, YouGov, 2017 (accessed August 19, 2018). https://d25d2506sfb94s.cloudfront.net/r/93/YouGov_-Online_Panel_Book2017.pdf.

[7] 2017 internet security threat report, symantec, vol. 22. Technical report, Symantec, 2017 (accessed August 6, 2018). https://www.symantec.com/content/dam/symantec/-docs/reports/istr-22-2017-en.pdf.

[8] 2017 internet crime report. Technical report, Internet Crime Complaint Center, Federal Bureau of Investigation, 2017 (accessed January 12, 2019). https://pdf.ic3.gov/2017_IC3Report.pdf.

[9] 2018 internet security threat report, symantec, vol. 23. Technical report, Symantec, 2018 (accessed August 6, 2018). https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf.

[10] Internet/broadband fact sheet. Technical report, Pew Research Center, 2018 (accessed January 19, 2019). https://www.pewinternet.org/fact-sheet/internet-broadband/.

[11] Corporate fact sheet. Technical report, Symantec Corporation, 2018 (accessed March 3, 2019). https://www.symantec.com/content/dam/symantec/docs/other-resources/symantec-corporate-fact-sheet-060517-en.pdf.

[12] Annual estimates of the resident population by sex, age, race, and hispanic origin for the united states and states: April 1, 2010 to july 1, 2017. Technical report, U.S. Census Bureau, Population Division, Release Date: June 2018 (accessed August 24, 2018). https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=bkmk.

[13] Pranshu Bajpai, Aditya K Sood, and Richard Enbody. A key-management-based taxonomy for ransomware. In *2018 APWG Symposium on Electronic Crime Research (eCrime)*, pages 1–12. IEEE, 2018.

[14] Leyla Bilge, Yufei Han, and Matteo Dell'Amico. Riskteller: Predicting the risk of cyber incidents. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1299–1311. ACM, 2017.

[15] Adam M Bossler and Thomas J Holt. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1), 2009.

[16] Krzysztof Cabaj and Wojciech Mazurczyk. Using software-defined networking for ransomware mitigation: the case of cryptowall. *IEEE Network*, 30(6):14–20, 2016.

[17] Kyung-shick Choi. Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 2008.

[18] Serge Egelman and Eyal Peer. Scaling the security wall: Developing a security behavior intentions scale (sebis). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 2873–2882. ACM, 2015.

[19] Alexandre Gazet. Comparative analysis of various ransomware virii. *Journal in computer virology*, 6(1):77–90, 2010.

[20] Andrew Gelman, Sharad Goel, Douglas Rivers, David Rothschild, et al. The mythical swing voter. *Quarterly Journal of Political Science*, 11(1):103–130, 2016.

[21] G. Gigerenzer, R. Hertwig, and T. Pachur. *Heuristics: The Foundations of Adaptive Behavior*. OUP USA, 2011.

[22] Hassan Halawa, Konstantin Beznosov, Yazan Boshmaf, Baris Coskun, Matei Ripeanu, and Elizeu Santos-Neto. Harvesting the low-hanging fruits: defending against automated large-scale cyber-intrusions by focusing on the vulnerable population. In *Proceedings of the 2016 New Security Paradigms Workshop*, pages 11–22. ACM, 2016.

[23] Danny Yuxing Huang, Damon McCoy, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, and Alex C Snoeren. Tracking ransomware end-to-end. In *Tracking Ransomware End-to-end*, page 0. IEEE.

[24] Jongbin Jung, Connor Concannon, Ravi Shroff, Sharad Goel, and Daniel G Goldstein. Simple rules for complex decisions. 2017.

[25] Amin Kharraz, Sajjad Arshad, Collin Mulliner, William K Robertson, and Engin Kirda. Unveil: A large-scale, automated approach to detecting ransomware. In *USENIX Security Symposium*, pages 757–772, 2016.

[26] Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda. Cutting the gordian knot: A look under the hood of ransomware attacks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 3–24. Springer, 2015.

[27] Fanny Lalonde Levesque, Jude Nsiempba, José M Fernandez, Sonia Chiasson, and Anil Somayaji. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 97–108. ACM, 2013.

[28] Fanny Lalonde Lévesque, José M Fernandez, and Anil Somayaji. Risk prediction of malware victimization based on user behavior. In *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*, pages 128–134. IEEE, 2014.

[29] Gregor Maier, Anja Feldmann, Vern Paxson, Robin Sommer, and Matthias Vallentin. An assessment of overt malicious activity manifest in residential networks. In *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, pages 144–163. Springer, 2011.

[30] George R Milne, Lauren I Labrecque, and Cory Cromer. Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 43(3):449–473, 2009.

[31] Fawn T Ngo and Raymond Paternoster. Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1), 2011.

[32] Michael Ovelgönne, Tudor Dumitraş, B Aditya Prakash, VS Subrahmanian, and Benjamin Wang. Understanding the relationship between human behavior and susceptibility to cyber attacks: a data-driven approach. *ACM*

Transactions on Intelligent Systems and Technology (TIST), 8(4):51, 2017.

[33] Elissa M Redmiles, Sean Kross, Alisha Pradhan, and Michelle L Mazurek. How well do my results generalize? comparing security and privacy survey results from mturk and web panels to the us. Technical report, 2017.

[34] Camille Ryan. Computer and Internet Use in the United States: 2016.

[35] Nolen Scaife, Henry Carter, Patrick Traynor, and Kevin RB Butler. Cryptolock (and drop it): stopping ransomware attacks on user data. In *Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on*, pages 303–312. IEEE, 2016.

[36] Victor J Strecher and Irwin M Rosenstock. The health belief model. *Cambridge handbook of psychology, health and medicine*, pages 113–117, 1997.

[37] Paul Van Schaik, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, 2017.

[38] Ting-Fang Yen, Victor Heorhiadi, Alina Oprea, Michael K Reiter, and Ari Juels. An epidemiological study of malware encounters in a large enterprise. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 1117–1130. ACM, 2014.

[39] Pavol Zavarsky, Dale Lindskog, et al. Experimental analysis of ransomware on windows and android platforms: Evolution and characterization. *Procedia Computer Science*, 94:465–472, 2016.

A Survey questions

A.1 Demographics and device details

1. What is your age? [*free text*]
2. What is your gender?
   - Male
   - Female
3. What is the highest level of education you have completed?
   - Some high school
   - High school graduate
   - Vocational training
   - Some college
   - College graduate
   - Some post-graduate work
   - Post graduate degree
4. What is your current employment status?
   - Employed full time
   - Employed part time
   - Unemployed looking for work
   - Unemployed not looking for work
   - Retired
   - Student
   - Disabled
5. What is your race or ethnicity?
   - White
   - Black or African American
   - American Indian or Alaska Native
   - Asian
   - Native Hawaiian or Pacific Islander
   - Other
6. What is your annual household income?
   - Less than $10,000
   - $10,000 - $19,999
   - $20,000 - $29,999
   - $30,000 - $39,999
   - $40,000 - $49,999
   - $50,000 - $59,999
   - $60,000 - $69,999
   - $70,000 - $79,999
   - $80,000 - $89,999
   - $90,000 - $99,999
   - $100,000 - $149,999
   - More than $150,000
7. What is your 5-digit zip code? [*free text*]
8. What is your field of work or study? [*drop down menu*]. Available choices included: Architecture, Engineering, and Math; Arts and Design; Building and Grounds Cleaning; Business and Financial; Community and Social Service; Computer and Information Technology; Construction and Extraction; Education, Training, and Library; Entertainment and Sports; Farming, Fishing, and Forestry; Food Preparation and Serving; Healthcare; Installation, Maintenance, and Repair; Legal; Life, Physical, and Social Science; Management; Media and Communication; Military and Protective Service; Office and Administrative Support; Personal Care and Service; Production; Sales; Transportation and Material Moving;
9. Are you currently using your personal computer (i.e., not one owned by an employer) to fill out this survey?
   - Yes
   - No
10. What operating system do you have installed on your personal computer?
    - Windows

- Mac OS
- Linux
- Chrome OS
- Other

11. What web browser do you typically use on your personal computer?

    - Google Chrome
    - Microsoft Internet Explorer
    - Firefox
    - Microsoft Edge
    - Safari
    - Opera
    - Other

A.2 Establishing whether a ransomware attack occurred

1. There are many malware attacks that attempt to extort (obtain) money from users. They can be broadly classified into two categories:

   (a) Misleading applications (e.g., fake antivirus scams, spyware removal tools, or PC cleaning apps)

   (b) Ransomware

   Please answer the following questions to help us understand whether you've experienced either of these online scams on your personal computer.

2. Misleading applications usually alert the user to a security issue or vulnerability on their computer, and prompt them to act (e.g., call a tech support number, download or purchase anti-virus software) in order to resolve the issue. Have you ever experienced any of the following scenarios that you suspect were scams? Please select all statements that apply.

    - A security alert or warning popped-up, prompting you to call a tech support number.
    - A security alert or warning popped-up, prompting you to purchase or download software.
    - I have experienced both the above scenarios.
    - I have not experienced any of the above scenarios.
    - I am not sure.

3. [*Screenshot shown to respondents here (Figure 1)*] Ransomware is another type of malware that will either lock your computer screen or encrypt your files. If you've been infected with ransomware, you will see screens like the the examples below, informing you that you must pay a ransom to re-gain access to your computer and/or files, providing instructions on how to do so.

4. Have you ever seen a screen similar to the examples above that lock your computer or encrypt your data and ask for money to restore it to normal? Note: These screens are typical of ransomware attacks and will explicitly inform you that your computer has been locked or the files on your computer have been encrypted. It will not tell you to download anti-virus software.

    - Yes, I have seen a screen notifying me that my computer is locked or my data encrypted.
    - No, I have never seen a screen notifying me that my computer is locked or my data encrypted.

5. Some ransomware includes a time limit (typically in the form of a timer counting down), indicating that if you don't pay before the specified time limit expires, then the decryption key will be deleted and your files will be lost forever, or the ransom amount will increase. Have you ever been told that you must pay within some time limit or seen such a timer counting down?

    - Yes, I've seen messages with time limits or timers counting down, telling me I must pay before they expire.
    - No, I've never seen messages with time limits or timers counting down.

6. Some variants of ransomware will encrypt your files so that you can no longer access them. In this case, you might see: (1) Files in all directories with names such as HOW_TO_DECRYPT_FILES.TXT or DECRYPT_INSTRUCTIONS.HTML. (2) Files in all directories with strange extensions such as ".locky". Have you ever had your files encrypted such that you couldn't access them?

    - Yes, I've experienced (1) or (2), or a similar message informing me that my files are encrypted.
    - No, I have never had my files encrypted such that I couldn't access them.

7. **Please read and answer this question carefully!** Have you ever experienced a ransomware attack that informed you your computer was locked or your data encrypted, and asked for money to re-gain access to your computer or files?

    - No, I have not experienced a ransomware attack on my personal computer.
    - Yes, I have experienced a ransomware attack on my personal computer.
    - I am not sure.

8. [*logic: shown if "I am not sure" selected in Q7*]. Please help us understand why you have selected "I am not sure". Below are some clarifications about ransomware. Ransomware is a type of malware that will either lock your computer, or encrypt your data. Ransomware will inform users that their computers are locked or their data is encrypted, typically with a large pop-up screen that is difficult to close A common trick is to impersonate law-enforcement agencies and claim that the user has broken the law by downloading copyrighted materials such as pirated music or software, or by viewing other illegal digital materials such as pornography Ransomware will demand money to re-gain access to your computer and/or files, and provide instructions on how to pay Ransomware does not tell users to download software (e.g. antivirus software) to fix the issue.

9. [*logic: shown if "Yes" selected in Q4, Q5, or Q6, and "No" in Q7*]. You have reported that you have not experienced a ransomware attack, but have experienced at least one scenario that is typical of ransomware attacks. Why

do you think your experience(s) were not ransomware attacks? Below are some clarifications about ransomware. Ransomware is a type of malware that will either lock your computer, or encrypt your data. Ransomware will inform users that their computers are locked or their data is encrypted, typically with a large pop-up screen that is difficult to close. A common trick is to impersonate law-enforcement agencies and claim that the user has broken the law by downloading copyrighted materials such as pirated music or software, or by viewing other illegal digital materials such as pornography. Ransomware will demand money to re-gain access to your computer and/or files, and provide instructions on how to pay. Ransomware does not tell users to download software (e.g. antivirus software) to fix the issue.

10. [*logic: shown if "I am not sure" selected in Q7*]. Please confirm whether or not you've ever experienced a ransomware attack. That is – did you ever see a message informing you that your computer is locked or your data is encrypted which was difficult to close, and which demanded money in order to restore access to your computer or files? Please select "yes" if you've experienced a ransomware attack, regardless of whether or not you paid.
    - No, I have not experienced a ransomware attack on my personal computer.
    - Yes, I have experienced a ransomware attack on my personal computer.
    - I am still not sure.
11. [*logic: shown if "Yes" selected in Q7 or Q10*]. [*free text*]. Please describe the ransomware attack you experienced. Do you remember what the message / instructions said? What did the screen look like? Was any functionality of your computer disabled? Please give as many details as possible.

A.3 Ransomware attack details

The following questions were shown to respondents who reported experiencing a ransomware attack (i.e., selected "Yes" in Q7 or Q10 in the previous section).

1. The following questions refer to the ransomware attack you experienced. If you have experienced more than one ransomware attack, please give details about the most frecent attack.
2. When did the ransomware attack occur? If you don't remember exactly, please give an approximate date (ideally your best guess of the month and year). [*free text*]
3. [*free text*] Do you remember the name of the ransomware? If so, please enter it below. Some examples are: "CryptoLocker", "CryptoWall", "Locky", "TeslaCrypt".
4. How were you asked to pay the ransom (i.e., what was the method of payment used in the attack)?
    - Cryptocurrency (e.g., Bitcoin, Litecoin, Zcash)
    - Payment voucher system (e.g., Paysafecard, MoneyPak, UKash, CashU, MoneXy)
    - Wire transfer
    - Send premium-rate text message to attacker's number
    - Credit card
    - Other
    - I don't remember
5. How much ransom (money) was requested? [*free text*]
6. In the question above, in which currency did you enter the ransom amount?
    - U.S. dollars
    - Cryptocurrency (e.g., Bitcoin, Litecoin, Zcash)
    - Other currency
7. Did the ransomware attack you experience include any of the following characteristics? Please select all that apply.
    - I saw a screen or large pop-up telling me that my computer was locked.
    - I saw a screen or large pop-up telling me that my data or files were encrypted.
    - I was told that unless I paid money, I would not be able to access my files, data, or computer.
    - I saw a timer counting down and was told I must pay money before it expired.
    - I saw a notification page, supposedly from a law enforcement agency (e.g., FBI, Department of Justice, etc.), informing me that I was caught doing an illegal or malicious activity online.
    - I did not experience any of the above.
8. How much time were you initially given to pay the ransom (before the timer expired)? For example, 24 hours, 5 days, 7 days, etc.[*free text*]
9. Did you pay the ransom amount requested ?
    (a) Yes, I paid the ransom amount.
    (b) No, I did not pay the ransom amount.
10. Why did you decide to pay or not pay the ransom? Briefly describe the motivating factors that led to your decision. [*free text*]
11. [*logic: shown if "yes" selected in Q9*] Was access to your data / computer restored after you paid the ransom?
    - Yes, access was restored.
    - No, access was not restored.
    - I am not sure.
12. Did you notify the authorities of the ransomware attack?
    - Yes, I notified the authorities.
    - No, I did not notify the authorities.
13. Did you try any of the following strategies to remove the ransomware and restore access to your computer or files? Please select all that apply.
    - I re-started my computer.

- I tried to change the extension of files back to their original format and open them.
- I restored my computer from a backup.
- I found and ran a tool to remove the ransomware.
- I found and ran a tool to decrypt my files.
- I used some other strategy.
- I don't remember.

14. Were you able to remove the ransomware?
    - Yes, I was able to remove the ransomware without losing any of my data or files.
    - Yes, I was able to remove the ransomware, but lost my data and/or files.
    - No, I was not able to remove the ransomware. I still can't access my computer and/or files.
15. How did you remove the ransomware?
    - I paid the ransom amount.
    - I re-started my computer.
    - I restored my computer from a backup.
    - I found and ran a tool to remove the ransomware or decrpyt my files.
    - I used some other method to remove the ransomware.
    - I am not sure, I did not remove the ransomware myself.
    - I was not able to remove the ransomware or re-gain access to my computer or files.
16. Did you seek help from anyone else to remove the ransomware? Please select all that apply.
    - I sought help / advice from family and or friends.
    - I sought help from co-workers and/or acquaintances.
    - I sought help from a computer store, repair shop, or other paid IT professional etc.
    - I did not seek help from anyone.
17. What other resources did you use to inform yourself of ransomware, figure out how to remove the ransomware, or to help you decide whether or not to pay the ransom? [*free text*]
18. How do you think you were infected with ransomware? [*free text*]
19. Do you think any of the following actions led you to be infected with ransomware? Please select all that apply.
    - I clicked on a malicious link in an email.
    - I downloaded a malicious program.
    - I clicked on a warning or notification that popped up (either by accident, or purposefully, for example, to close it).
    - I clicked on an advertisement while browsing the internet or on social media (either purposefully, or by accident).
    - I was browsing the internet and did not click on anything.
    - Other
20. Did you change any of your online browsing and/or security behavior following the ransomware attack? Please select all that apply.
    - I changed my operating system.
    - I started backing up my data to an external hard drive or remote file storage server.
    - I bought an antivirus / firewall product.
    - I changed configurations on my computer (e.g., enabled "show file extension" feature, disabled Windows Script Host, restricted login access, etc.)
    - I enabled automatic updates to my operating system, browser, antivirus, and other programs (wherever possible).
    - I changed my default browser.
    - I back up my data more regularly to an external hard drive or remote file storage server.
    - I changed or updated my antivirus / firewall product.
    - I am more careful about which web sites I visit, what I download, and what attachments I open.
    - I update my operating system, browser, antivirus, and other programs more often than before.
    - I encrypted my hard drive.
    - How likely do you think you are to experience a ransomware attack in the future? Please enter a number between 0 and 100, where 100 means: "I'm definitely (100% likely) going to experience a ransomware attack in the future." and 0 means: "There is no way (0% chance) I will experience a ransomware attack in the future."
    - Suppose you were to experience a ransomware attack today and the only way of restoring access to the data on your computer was to pay the ransom (say $300). How likely is it that you'd pay the ransom? Please enter a number between 0 and 100, where 100 means: "I would definitely pay the ransom to restore access to my personal computer and files." 0 means: "No way I would pay the ransom, I would prefer to lose all of my data and files."

A.4 Security habits

Participants were shown the following prompt at the beginning of this section: "Please answer a few questions about your online habits **right before** the ransomware attack occurred."

1. Approximately how much time did you spend on the internet on your personal computer each day, at the time of the ransomware attack?
    - Less than 1 hour
    - Between 1 - 2 hours
    - Between 3 - 5 hours
    - Between 5 - 10 hours
    - More than 10 hours

2. Approximately how many emails did you open per day on **your personal computer**, at the time of the ransomware attack?
    - Less than 5 emails
    - Between 6 - 10 emails
    - Between 11 - 20 emails
    - Between 21 - 50 emails
    - More than 50 emails
3. How frequently did you download files from online torrent sites such as The Pirate Bay, Extratorrent, TorrentZ2, etc., at the time of the ransomware attack?
    - I frequently downloaded files from torrent sites.
    - I occasionally downloaded files from torrent sites.
    - I rarely downloaded files from torrent sites.
    - I never downloaded files from torrent sites.
4. How did you store information on your computer that you didn't want anyone to see, at the time of the ransomware attack? Please select all that apply.
    - My computer was protected with a password.
    - All sensitive data was stored in a password-protected folder.
    - All sensitive data was stored in an obscure folder that is difficult to find.
    - I only hid data if I expected another person to use my computer temporarily.
    - I immediately deleted all data I don't want anyone to see.
    - I had no sensitive data on my computer.
5. Were you in the habit of backing up your personal files to an external hard drive or a cloud-based storage service, at the time of the ransomware attack? Which of the following statements most accurately describes your behaviour at the time?
    - I did not have any of my files backed up at the time of the ransomware attack.
    - I had been backing up my files approximately once a year.
    - I had been backing up my files approximately every couple of months.
    - I had been backing up my files approximately every couple of weeks.
    - I had been backing up my files approximately every day.
6. Was the hard drive on your personal computer encrypted at the time of the ransomware attack?
    - Yes, my hard drive was encrypted.
    - No, my hard drive was not encrypted.
7. Suppose you have entered your login and password on a website site that you use occasionally (e.g. every two weeks). The browser offers you the option to save your credentials so that they can be used for automatic form completion in the future. At the time of the ransomware attack, what would you generally do?
    - I generally would have saved my credentials.
    - I generally would not have saved my credentials.
8. Suppose Flash Player, Adobe reader, or Flash notified you about updates that need to be downloaded and installed. What wold you generally do at the time of the ransomware attack?
    - I would select "Install updates now".
    - I would select "Remind me later".
    - I rarely see any notifications from such software.
    - I never see notifications from such software.
9. Suppose you are creating a new account on a website that you intend to use occasionally (e.g., airline frequent flyer account). How would you have created a password, at the time of the ransomware attack?
    - I had one password for all my accounts.
    - I had several passwords that I rotated when creating new accounts.
    - I had a password template that I would modify for each account.
    - I'd make up an entirely new one, ensuring that it's strong.
10. Did you own a blog or website at the time of the ransomware attack?
    - Yes, I owned a blog or website.
    - No, I did not own a blog or website.
11. Two-step authentication is an extra layer of security involving two steps to log in to an online account: You'll enter your user name and password. A code will be sent to your phone via text, voice call, or a mobile app. Did you use two-step authentication for at least one of your online personal accounts (i.e., not for a work-related account), at the time of the ransomware attack?
    - Yes, I had two-step authentication on at least one of my personal accounts.
    - No, I didn't have two-step authentication on any of my personal accounts.
12. Did you use a desktop or laptop computer at work at the time of the ransomware attack?
    - Yes, I use a computer at work.
    - No, I do not use a computer at work.
    - Not applicable.
13. [*logic: shown if "yes" selected in Q12*] What task(s) did you use a computer at work for? Please select all that apply.
    - Internet or email
    - Word processing or desktop publishing
    - Spreadsheets or databases
    - Calendar or scheduling
    - Graphics or design
    - Programming
    - Other

Category	Features
Demographics	Gender, race, age
Socioeconomic (SES)	Highest level of education completed, household income, employment status, marital status, field of work or study, child under 18 in household
Computer knowledge	8 question multiple choice test (developed by the authors)
Security habits	Time spent on the computer each day, number of emails opened per day, frequency of downloading files from online torrent sites, data backup habits (on external hard drive or cloud-based storage device), storage strategy for sensitive information on personal computer (e.g., use of password-protected computer or folder), has encrypted hard drive, credential saving habits in browser, software updating habits (e.g., postpone, install immediately, etc.), own a blog or website, use two-factor authentication (if yes, for which services), password creation habits (e.g., use the same password for all sites), use of computer at work (if yes, for which tasks)
Software used	Operating system (name and version), most commonly used browser (name and version), list of plugins installed

Table A1: *Survey features. Software used were collected passively, and the name of operating system and browser currently used was also asked as a survey question.*

A.5 Computer knowledge quiz

1. Select the bigger amount of data
   (a) One kilobyte
   (b) One megabyte
2. "Net neutrality" refers to:
   (a) The posting of non-partisan content on websites.
   (b) The manner in which Wikipedia editors are instructed to handle new entries on their site.
   (c) Equal treatment of digital content by internet service providers.
   (d) A promise by users of certain websites that they will not contribute non-partisan comments or work.
3. What does the acronym RAM stands for?
   (a) Random access monitoring
   (b) Running access mount
   (c) Random access memory
   (d) Random access mount
4. Which of the following is an example of an I/O device?
   (a) CPU
   (b) Keyboard
   (c) Power supply
   (d) USB port
5. You are authorizing on a banking website (let's say "Money Bank"). Which web address looks safest to you?
   (a) http://MoneyBank.com
   (b) https://Moneybamk.com
   (c) https://MoneyBank.com
   (d) https://MoneyBank.net.com
6. What is a Trojan horse virus?
   (a) Software that replicates itself to spread to other computers.
   (b) Software that records every keystroke made by a computer user.
   (c) Software that is often disguised as legitimate software.
   (d) Software that encodes itself in a different way (using different algorithms and encryption keys) every time it infects a system.
7. 1 byte consists of ...
   (a) 4 bits
   (b) 8 bits
   (c) 16 bits
   (d) 32 bits
8. Data is permanently stored in:
   (a) RAM
   (b) Hard disk
   (c) CPU
   (d) Cache memory

Category	Raw proportion	Weighted proportion
Female	55%	54%
Male	45%	46%
White	81%	75%
Black or African American	8%	11%
Hispanic or Latino	5%	8%
Asian	2%	2%
Mixed	3%	2%
Other	2%	2%
Age (19 – 30)	11%	16%
Age (31– 45)	19%	24%
Age (45 – 60)	28%	27%
Age (over 60)	42%	32%
No High school	1%	2%
High school	20%	32%
Some college	22%	22%
College	39%	33%
Post-graduate	17%	12%
Full-time	38%	40 %
Retired	28%	22%
Part-time	11%	10%
Permanently disabled	9%	8%
Student	4%	7%
Unemployed	3%	5%
Homemaker	5%	5%
Temporarily laid off	1%	1%
Other	1%	1%
Married	51%	49%
Never married	26%	31%
Divorced	13%	11%
Widowed	6%	6%
Domestic / civil partnership	3%	2%
Separated	1%	0%
Child under 18 in household - yes	19%	25%
Child under 18 in household - no	81%	75%
Less than $10,000	3%	4%
$10,000 - $29,999	8%	8%
$20,000 - $29,999	10%	10%
$30,000 - $39,999	11%	12%
$40,000 - $49,999	9%	9%
$50,000 - $59,999	10%	11%
$60,000 - $69,999	7%	6%
$70,000 - $79,999	8%	7%
$80,000 - $99,999	9%	8%
$100,000 - $119,999	6%	6%
$120,000 - $149,999	5%	5%
$150,000 - $199,999	4%	4%
$200,000 - $249,999	2%	1%
$250,000 - $349,999	1%	1%
Prefer not to say	8%	9%

Table A2: *Demographics and socioeconomic status of respondents, n=1,180. The raw proportion represents the fraction of respondents out of n=1,180 having a particular characteristic, and the weighted proportion represents the post-stratified proportion.*