A Large-Scale Measurement of Cybercrime Against Individuals

Casey F. Breen
caseybreen@berkeley.edu
University of California, Berkeley
Berkeley, CA, USA

Cormac Herley
cormac@microsoft.com
Microsoft Research
Redmond, WA, USA

Elissa M. Redmiles
eredmiles@mpi-sws.org
Max Planck Institute
for Software Systems
Saarbrucken, Germany

ABSTRACT

We know surprisingly little about the prevalence and severity of cybercrime in the U.S. Yet, in order to prioritize the development and distribution of advice and technology to protect end users, we require empirical evidence regarding cybercrime. Measuring crime, including cybercrime, is a challenging problem that relies on a combination of direct crime reports to the government – which have known issues of under-reporting – and assessment via carefully-designed self-report surveys. We report on the first large-scale, nationally representative academic survey (n=11,953) of consumer cybercrime experiences in the U.S. Our analysis answers four research questions: (1) What is the prevalence and (2) the monetary impact of these cybercrimes we measure in the U.S.?, (3) Do inequities exist in victimization?, and (4) Can we improve cybercrime measurement by leveraging social-reporting techniques used to measure physical crime? Our analysis also offers insight toward improving future measurement of cybercrime and protecting users.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; *User studies*; • **Security and privacy** → **Economics of security and privacy**.

KEYWORDS

cybercrime, network scale-up, digitial inequity

ACM Reference Format:
Casey F. Breen, Cormac Herley, and Elissa M. Redmiles. 2022. A Large-Scale Measurement of Cybercrime Against Individuals. In *CHI Conference on Human Factors in Computing Systems (CHI '22), April 29-May 5, 2022, New Orleans, LA, USA.* ACM, New York, NY, USA, 41 pages. https://doi.org/10.1145/3491102.3517613

1 INTRODUCTION

While cybercrime protection is an area of significant focus in human-computer interaction (HCI) research [10], relatively little is known about the prevalence and severity of the cybercrimes we aim to prevent. Most efforts to quantify the size and cost of crime still focus solely on physical crimes (e.g., robbery, assault), ignoring the reality of digital victimization [5, 6].

CHI '22, April 29-May 5, 2022, New Orleans, LA, USA

ACM ISBN 978-1-4503-9157-3/22/04.
https://doi.org/10.1145/3491102.3517613

Yet, in an empirical science of HCI, "measurements create certain possibilities for action and exclude other possibilities" [59]. That is, data – or a lack of it – guides system design. In the presence of data on people's digital experiences of crime (i.e., cybercrime incidence), for example, HCI researchers and security technologists may prioritize the design of certain cybercrime protections over others. In the absence of such data, researchers may instead privilege the goals of technology companies or state entities that fund their research [59] or turn to computational transformations – "solve[ing] a computationally tractable transformation of a problem rather than the problem itself" [7] – to prioritize design and intervention. As such, recent research in HCI [10] and in cybersecurity [66] calls for measurement of cybercrime to provide appropriate context for the data-driven design of interventions, with the former noting that: "it is critical that we examine and make explicit the impact of crime...to inform safer, intelligent and just digital and non-digital spaces for all."

No prior academic work has focused on survey-based measurements of cybercrime incidence in the U.S., nor has prior academic work, within or outside of the U.S., investigated potential inequities in the prevalence of these crimes (see Figure 1). The latter investigation is critical to ensure that we address these crimes equitably across user groups. In this study, we take a first step toward filling this measurement gap by conducting a probabilistic, nationally-representative survey of 11,953 Americans to measure the prevalence of six exemplar cybercrimes against individuals in the U.S.: bank account or credit card compromise, non-delivery, non-payment, overpayment, advanced fee scams[1], and digital blackmail / extortion.[2]

Perceived monetary losses are a significant driver of research agendas. For example, research efforts to get users to choose strong passwords or adopt two-factor authentication generally assume that these measures would significantly reduce losses [29]. Work appearing in CHI that addresses efficacy of phishing countermeasures and training [21, 51, 79] routinely cites the Gartner estimates of phishing monetary losses as a justification for research on phishing prevention [1]. As monetary loss is not only a common justification for the prioritization of cybercrime interventions but also the metric used in existing government statistics that are leveraged to decide the funding awarded for cybercrime research, we focus on cybercrimes – computer- or internet-enabled crimes – where a victim suffers a monetary loss.

Our work addresses four primary research questions, the first three of which are:

RQ1 What is the prevalence of six representative cybercrimes in the U.S.?

[1]Best known as "Nigerian Prince" or 419 scams [25].
[2]For more detail regarding our selection criteria see Section 3.1.

RQ2 What is the direct monetary impact of these six cybercrimes?
RQ3 Do sociodemographic and/or digital skill-based inequities exist in victimization?

The *way* in which we produce data informs the actions taken from it. As such, we must critically examine how we produce data in addition to drawing implications from the data itself [59]. Correspondingly, this work seeks to critically examine methods of cybercrime measurement. One reason cybercrime is challenging to study is that it is often underreported. The FBI IC3, the most authoritative source of cybercrime statistics in the U.S., estimates that only 10-12% of cybercrimes are reported to them [24]. There is a critical need to understand the source of underreporting about cybercrime in order to inform how best to measure it. One primary hypothesis for underreporting is stigma [19]. While stigma can strongly deter reporting of incidents to government agencies, it can also lead to underreporting on self report surveys [68]. Prior work in the social sciences leverages *network scale-up techniques* to mitigate underreporting about crime victimization or criminal behavior (e.g., intravenous drug use) [27, 48, 68]. A network scale-up approach to measurement requires asking respondents to report on the experiences of their friends and social circle and then applying statistical estimation techniques to these data to estimate the prevalence of a certain behavior or experience in the overall population. To apply a network scale-up approach effectively, it is necessary that (a) the friends or social circle of the victim know about their experience so that they can report on it and (b) we be able to estimate the size of respondents' personal networks. As prior work shows that listening to others' stories of cybercrime victimization is a primary mechanism through which people learn security behaviors [62], we hypothesize that criterion (a) is viable: respondents may be able to report on the experiences of those in their personal network.[3] We use existing network estimation techniques to satisfy criteria (b), as described in Section 3.3. Thus, we conduct a multi-method survey in which respondents are asked to report on their own cybercrime victimization and the cybercrime victimization of others in their social network in order to answer:

RQ4 Do social-reporting techniques used to generate estimates of physical crime prevalence generalize to measurements of cybercrime?

We find that (RQ1) the six cybercrimes we study – estimated by FBI reports to cover nearly 30% of cybercrime in the U.S. – are rare, with only two crimes having an annual prevalence above 1%, and none having a prevalence above 3.5%. Further, (RQ2) the typical monetary harm sustained is quite low. The median loss across all cybercrimes was $100. We (RQ3) find that older Americans and Black Americans are significantly more likely to be the victims of cybercrimes, with the exceptions of scams that involve the victim selling goods on the internet, where they are significantly less likely to be victims.Our network scale-up approach (RQ4) produces results that are lower than our direct estimates, suggesting uniquely low visibility in a cybercrime settings as compared to studies of physical crime. Finally, we place our results in context, by synthesizing key academic and governmental measurements of cybercrime – both in the U.S. and internationally – to examine the consistency of these measurements across methods and geography. Our results broadly agree with past measurements of cybercrime, and can be used as reliable baseline metrics for future studies.

Our findings offer implications for the design of security technologies and for future measurement of cybercrime incidence, the current academic conversation around digital inequity specifically related to digital security, and our understanding of cybercrime incidence rates. Additionally, we introduce a novel approach for studying cybercrime, the network scale-up method, and highlight the situations where we would expect the network scale-up method to outperform direct estimation.

[3]See Section 3.3 for further detail about how awareness of incidents is accounted for by our estimation approach.

2 BACKGROUND AND RELATED WORK

Here, we provide background on the techniques used to measure cybercrime and prior work doing so. We additionally review prior work investigating inequities in digital security, as no prior work to our knowledge has conducted such investigation specific to cybercrime.

2.1 Measuring Cybercrime

Measuring cybercrime is challenging. The landscape of digital victimization changes rapidly, and the relatively limited body of work to date on cybercrime has yet to agree on universal definitions for cybercrimes, nor is there a clear consensus on how best to measure it. Most importantly, estimates of cybercrime from different sources are difficult to reconcile. The Federal Bureau of Investigation (FBI) Internet Complaint Center (IC3) shows fewer than 0.15% of Americans have been the victim of a cybercrime, while Norton – a vendor of internet security software – released a 2019 report stating that over 30% of Americans were the victims of cybercrime in 2019.

There are several prominent methods for measuring the size and cost of cybercrime. One approach to measuring cybercrime is direct observations of attack trends. That is, for banks, email providers, and social networking companies to count and report the number of cybercrime incidents. In practice, this is quite challenging; many incident types are cross-platform, so that no one company has a beginning-to-end view of the scam. As a result, while a scam may begin with one company, the user may ultimately be harmed on a different platform. For example, a cybercriminal may initiate a scam on a social media platform, such as Facebook, but receive payment on a different platform, such as Western Union. As a result, Facebook will not have the ability to know whether the potential victim actually made a payment to the attacker. The difficulty of tracking such exploits end-to-end is described by Huang *et al.* [40]. Even for single-platform account compromise, email providers and social networking sites seldom have out-of-band trustworthy channels to contact their users and verify that compromise has taken place [61]. This is partly a consequence of the scale at which they operate. At many providers, there is no source of ground truth; estimates of crime must be inferred indirectly by observing anomalous behavior and may not reflect actual victimization. Additionally, translating counts of direct observed attack trends into a concrete incidence rate requires a number of hard-to-verify assumptions.

Due to these difficulties, measuring cybercrime thus relies on (1) collecting and aggregating complaints or report filed to police

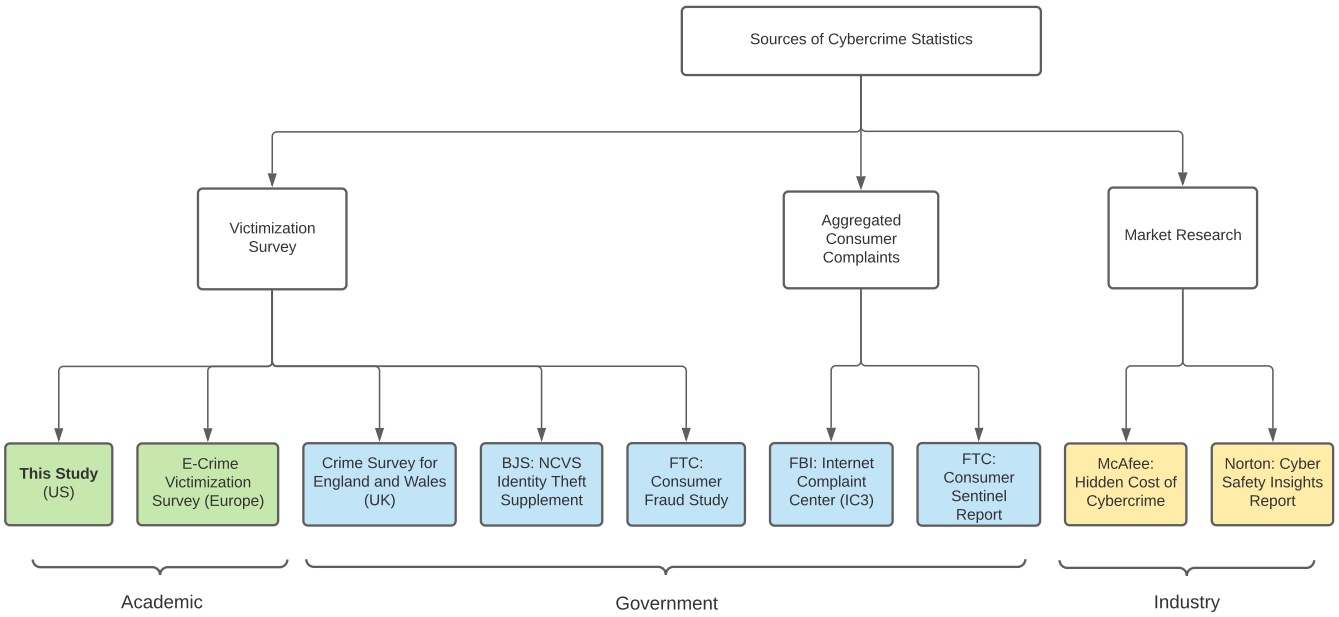


Figure 1: Large-Scale efforts to measure cybercrime prevalence.

departments or other government bodies and (2) survey-based measurements. The former is the approach taken by the FBI. Their IC3 database provides a "mechanism for reporting information concerning suspected internet-facilitated criminal activity" [42]. These reports are collected and compiled into an annual report. Similarly, the FTC compiles consumer complaints from individuals and other organizations into an online database, the Consumer Sentinel [17]. These databases are important sources of cybercrime metrics, but they have a key limitation: they only capture cybercrimes that victims chose to report. For example, the FBI IC3 estimates that only 10-12% of all cybercrime victims actually filed complaints. Therefore, using such databases to calculate cybercrime incidents rates will severely underestimate the true incidence rate.

Thus, the most promising approach for estimating incidence rates, and the approach used in this study, is to measure cybercrime with a crime victimization survey. Crime victimization surveys ask respondents directly whether they have been the victim of a crime over a defined period of time, such as the last 12 months. A growing number of crime victimization surveys, which traditionally focus only on physical crime, have begun including supplements on cybercrime. The U.S. Bureau of Justice Statistics (BJS) fields the National Crime Victimization Survey (NCVS), the primary source of physical crime statistics in the U.S. Beginning in 2008, an Identity Theft Supplement was included approximately every-other year to collect data on "the attempted or successful misuse of an open account, misuse of personal information, or misuse of personal information for any other fraudulent activity." This identity theft supplement provides estimates of the incidence rate of banking and credit card fraud in the U.S., but does not estimate the prevalence of any other cybercrimes included in this study.

In Europe, the E-Crime Victimization Study collected nationally representative data on "consumer-facing" cybercrime using a tailored instrument, producing nationally representative estimates for six different European countries [67]. The E-Crime study surveyed a total of 6,934 respondents over the age of 18 who used the internet for personal purposes, asking respondents about seven different cybercrimes related to ecommerce, payment, and fraud. The E-Crime study did not collect data on how many times a respondent was the victim of a cybercrime, and instead used a binary yes/no measure for whether a respondent had been the victim of a cybercrime in the past five years. The Crime Survey for England and Wales (CSEW) is a "face-to-face victimisation survey, which asks people resident in households in England and Wales about their experiences of a selected range of offences in the 12 months prior to the interview" [75]. The CSEW interviews approximately 35,000 households, allowing for precise estimates of fraud and computer misuse rates. As the CSEW module focused on cybercrime is not publicly released, it is not possible to identify which specific cybercrimes are included in the fraud and computer misuse estimates.

The most relevant source of recent statistics for our work is the FTC "Mass-Market Consumer Fraud in the United States" random-digit dial survey of 3,717 consumers conducted in 2017 [4]. This survey provides an update of nationally-representative FTC studies in 2003, 2007, and 2012 to quantify the prevalence of consumer experiences of fraudulent transactions in the United States, focusing on specific fraudulent transactions, such as those involving weight-loss products, buyers' club memberships, unauthorized cell phone billing, etc. Only two of the six categories that we survey are also covered by the FTC 2017 report (non-delivery of goods and advance-fee fraud).

Other estimates of cybercrime prevalence come from corporate white papers that have have poor methodology, lack transparency and/or have clear conflict of interest: e.g., they are conducted by the vendors of security software. A common shortcoming of survey estimates (such as the 2007 Gartner Phishing estimate [1] and the 2007 Federal Trade Commission Identity Theft survey [26]) is use of unverified self-reported numbers: a single respondent who misunderstands the question, exaggerates, or even lies, exerts enormous bias [30] which, since losses are never negative, is always upward and cannot be cancelled. Many reports – for example, Norton's 2019 report stating that a third of Americans were the victims of cybercrime in 2019 – describe a frequency of cybercrime that is hard to reconcile with non-vendor sources of cybercrime statistics. The coding that we perform (see Section 3.5) sanitizes the data and greatly reduces this effect. The McAfee Corp. has since 2014 sponsored estimates produced by the Center for Strategic and International Studies (CSIS). Their methodology is simply to assume [14] "that the cost of cybercrime is a constant share of national income, adjusted for levels of development." Thus, their estimates reflect assumed percentages of GDP rather than any observed, reported or surveyed cybercrime activity. The 2020 report [15] "The Hidden Costs of Cybercrime" released by the Center for Strategic and International Studies estimated cybercrime costs the world over 1 trillion dollars, more than 1% of global GDP.

Another stream of research focuses on bank and payment fraud, with an emphasis on how victimization rates and payment cultures vary across time and place. Kemp et al. [46] uses a time series analysis to show that COVID-19 and its associated lockdown led people in the UK to spend less time in physical outdoor spaces and more time connected to the internet, causing an increase in cybercrime and a decline in traditional crimes. Other research has highlighed the large cultural differences in payment cultures. Respondents from China and the U.S. were more comfortable with credential sharing, while German participants were less willing to credential share and more willing to adopt cryptocurrencies [12]. There is also substantial variation by country in rates of understanding bank terms and conditions, with only 35% of customers on average fully understand their bank's terms and conditions [9]. Broadly, this research underscores the importance of examining variance in cybercrime experiences, for example along the lines of demographics – as we do in RQ3 – or culture.

In Figure 1 we summarize existing large-scale approaches to measuring cybercrime prevalence.

2.2 Inequities in Digital Security

A large body of prior work has investigated inequities in digital security behavior, advice sources, attitudes, and concerns [23, 49, 62, 66, 70, 76, 80]. Most relevant to our work, a limited body of prior work in digital security has examined inequities in people's self-reports of negative experiences online. These experiences include a mix of cybercrimes, such as having been the victim of an online scam, and having had important personal information stolen, such as Social Security Number, credit card, or bank account information as well as broader incidents such as experiencing relationship or job trouble due to something the respondent posted on social media [53, 63]. This work finds overall that less educated users are less likely to report having had any of these negative experiences [63]. Looking just at the experiences most relevant to the crimes we study: having personal information stolen and being the victim of an online scam, prior work finds that higher income, more educated, and white Americans are more likely to have had personal information stolen [53]. Those who earn less than $20,000 per year are significantly more likely to have been a victim of an online scam, however prior work finds no other inequities in victimization [53]. Our work builds upon these prior findings to investigate inequities specifically in cybercrime victimization. The 2017 FTC Consumer Fraud survey [4] also presents demographic analysis of bi-variate relationships, that is, without controlling for the confounding effects of intersectional marginalization. We compare our regression-based findings with these bivariate findings in Section 4.2. Our analysis builds on these prior works – on general security incidents and on fraudulent transactions, specifically – to more broadly investigate inequities in victimization across six representative cybercrimes.

3 METHODS

In July 2020, we conducted a nationally representative, probabilistic surveys of a total of 11,953 American internet users to estimate the frequency of six types of cybercrimes (Table 1) among Americans. Our work was approved by our institution's ethics review board.

3.1 Cybercrime Selection

As aforementioned, we sought to study cybercrimes that (1) directly impact users (consumer-facing), rather than businesses or other institutions and (2) result in monetary loss. Further, given the low incidence of crime victimization, we prioritized measurement of the most common cybercrimes. We used the only dataset of cybercrime incidence rates in the US, the FBI IC3 database to assess scam incidence rates [42] and select the most common cybercrimes that could be clearly and unambiguously defined in the context of an online survey and understood by non-security-expert internet users. The chosen number of cybercrimes is in line with prior work, with prior cybercrime surveys asking about a median of 5.5 crimes.

A full list of cybercrime incidents and the definitions used in this study is given in Table 1.

3.2 Survey Samples

We collected two survey samples: a general ($N = 1,002$) and rare-incident ($N = 10,951$) sample. The general sample was given the full survey questionnaire. The rare-incident sample was shown, at the beginning of the survey, a check-list of the six cybercrime incidents and asked whether they had experienced any of these incidents. If they reported experiencing one of the four rare incidents (advanced fee, non-payment, extortion, overpayment), they were shown the subset of the full survey questionnaire pertaining to those incidents. This method was necessary to make our approach financially feasible (the total survey costs for this measurement still exceeded $40,000) due to the extremely low ($< 1\%$) incidence of these cybercrimes, which are still amongst the most commonly reported to the FBI.

Our survey was administered through the National Opinion Research Center's (NORC) Amerispeak Panel. The Amerispeak Panel,

Cybercrime Incident	Description
Non-Delivery	Non-delivery scams occur when a scammer requires the victim to use an unexpected payment mechanism (e.g., Western Union, gift cards, Bitcoin). After being paid, the scammer never delivers the product or service.
Non-Payment	Non-Payment scams occur when a victim sells a product or service, but never receives payment from the scammer buying the goods.
Extortion	Extortion scams occur when a scammer either: (1) threatens to release a victim's confidential information (e.g. passwords, photographs, browsing history) to friends, family, or the public or (2) holds a victim's computer, account, or confidential information hostage. The scammer then asks for money in exchange for either not releasing the victim's information or returning the computer/account/information to the victim.
Overpayment	Overpayment scams occur when a scammer overpays for something a victim is selling online. The scammer then asks for the excess amount to be refunded. Once the excess amount is refunded, it is discovered that the original payment method is invalid (credit card stolen, check bounced, etc.)
Advanced Fee	Advanced fee scams occur when a scammer asks the victim for fees before providing a promised prize or reward (e.g., $1,000, a TV, a cruise). After the victim pays the fees, the scammer never actually sends the prize or reward that they promised.
CC/Banking	Banking scams occur when a scammer makes fraudulent charges on the victim's credit or debit account or directly steals money by accessing their bank account.

Table 1: Cybercrimes of interest

operated by NORC at the University of Chicago, is a probability-based panel designed to be representative of the population. Households are randomly selected using area probability and address-based sampling with a known, non-zero probability of inclusion. The selected households are then recruited by mail, telephone, and in-person field interviewers, and the resulting panel provides sample coverage of approximately 97% of the household population. We follow the guidelines of the American Association for Public Opinion Research and use probability-based sampling in our survey, which ensures that all persons in a population (in our case the US) have a non-zero chance of being sampled to take the survey [43]. The survey was fielded from July 21st, 2020 to September 8th, 2020. The study was conducted online and was offered in English only. A general population sample of adults age 18 and older were selected from NORC's Amerispeak panel. Statistical weights were constructed to adjust for panel design, differential non-response across subpopulations, and limits of the sampling frame. Separate sets of statistical weights were constructed for the general sample and total sample. For technical details on the Amerispeak panel and weighting procedure, see the Amerispeak Technical Overview [20]. Unweighted sample demographics are provided in Table 2 and weighted demographics are provided in the Appendix.

3.3 Network Scale-Up Techniques

To answer RQ4 – in which we sought to investigate whether social-reporting methods could improve cybercrime survey estimates and provide insight into the relevance of stigma in cybercrime reporting – we compare estimates of cybercrime prevalence based on network scale-up estimation. This allows us to generate estimates of cybercrime based on respondents' reports regarding the experiences of people in their personal networks and compare them to direct estimates generated from respondents' reports about their own experiences. Here, we provide background on network scale-up techniques – which are commonly used in the social sciences, but less commonly in HCI – and on the specific statistical methodology used to generate network-based estimates of cybercrime prevalence in this study.

Survey respondents frequently avoid reporting behavior that is illegal or stigmatized [48, 68]. Thus, survey-based estimates can underestimate the size of heavily-stigmatized groups such as crime victims or drug users. Indirect methods, such as the network scale-up method, aim to produce more accurate estimates for these hard-to-count ("hidden") populations as they do not require survey respondents to report about themselves, but rather only about others in their personal network. Network scale-up methods have been used to estimate the prevalence of rape, homelessness, and human immunodeficiency virus (HIV) seropositivity in the U.S. [48]. They have also been used to measure key groups most at risk of HIV, such as men who have sex with men, female sex workers, and illicit drug users [68]. Table 3 shows a select set of completed network scale-up studies.

The most basic form of network scale-up estimation requires estimating two quantities: how many people a respondent knows and how many people a respondent knows in the population of interest (e.g., crime victims). To estimate the first quantity, a typical network scale-up survey asks respondents a set of questions about how many people they know in groups of known size (e.g., "How many people do you know named Rose?"). The answers to these questions, known as *aggregate relational data* (ARD), allows us to estimate the size of a respondent's personal network. To estimate the second quantity, the survey asks questions about how many people they know in the hidden population (e.g., "How many people do you know who were the victim of a scam on the internet?").

The intuition behind network scale-up estimation is to estimate the size of a hard-to-count population – or incidence of an event experienced by that population – by dividing the number of crime victims the respondent knows by the number of people they know estimated from the ARD. Expressed mathematically, and considering more than one respondent, computing a *basic network scale-up*

	General Sample		Rare-Incident Sample		Total	
	No.	%	No.	%	No.	%
Gender						
Male	470	46.9	4512	41.2	4982	41.7
Female	532	53.1	6439	58.8	6971	58.3
Age						
18-29	150	15.0	837	7.6	987	8.3
30-44	288	28.7	2378	21.7	2666	22.3
45-59	208	20.8	2726	24.9	2934	24.5
60+	356	35.5	5010	45.7	5366	44.9
Education						
<HS Equivalent	39	3.9	283	2.6	322	2.7
HS Equivalent	170	17.0	1418	12.9	1588	13.3
Some college	444	44.3	3893	35.5	4337	36.3
Bachelors	203	20.3	2961	27.0	3164	26.5
Advanced degree	146	14.6	2396	21.9	2542	21.3
Race/Ethnicity						
White, non-Hispanic	675	67.4	8355	76.3	9030	75.5
Black, non-Hispanic	110	11.0	931	8.5	1041	8.7
Other, non-Hispanic	18	1.8	162	1.5	180	1.5
Hispanic	154	15.4	863	7.9	1017	8.5
2+, non-Hispanic	25	2.5	325	3.0	350	2.9
Asian, non-Hispanic	20	2.0	315	2.9	335	2.8
Income						
<$29,999	202	20.2	2050	18.7	2252	18.8
$30,000 to $74,999	404	40.3	4265	38.9	4669	39.1
$75,000 to $124,999	268	26.7	2862	26.1	3130	26.2
>$125,000+	128	12.8	1774	16.2	1902	15.9
Metro						
Non-Metro Area	130	13.0	1870	17.1	2000	16.7
Metro Area	872	87.0	9081	82.9	9953	83.3
Marital Status						
Married	526	52.5	6077	55.5	6603	55.2
Widowed	27	2.7	531	4.8	558	4.7
Divorced	108	10.8	1329	12.1	1437	12.0
Separated	52	5.2	564	5.2	616	5.2
Never married	223	22.3	1849	16.9	2072	17.3
Living with partner	66	6.6	601	5.5	667	5.6
Total	1002	100	10951	100	11953	100

Table 2: Sample descriptive statistics (unweighted). Sample is subsequently weighted to account for any under-sampling relative to the U.S. demographics. See Appendix Table 11 for weighted sample statistics. Sample collected from NORC's Amerispeak panel.

Study Citation	Population/Variable of Interest	Location
Killworth et al., 1998	HIV prevalence, homelessness, and rape	United States
Kadushin et al., 2006	Heroin users	14 Cities
Salganik et al., 2011	Heavy drug users	Curitiba, Brazil
Wang et al., 2015	Men who have sex with men	Shanghai, China
Feehan et al., 2016	Groups most at risk for HIV/AIDS	Rwanda
Sully et al., 2020	Abortion incidence	Ethiopia and Uganda

Table 3: Select set of network scale-up studies.

estimator involves using the ARD to estimate the proportion of the general population in the hidden population $\hat{N}_H$:

$$\hat{P}_H = \frac{\sum_{i \in s_F} y_{i,H}}{\sum_{i \in s_F} \hat{d}_{i,U}} \tag{1}$$

where $\hat{d}_{i,U}$ is the total degree (size of personal network), $y_{i,H}$ is the total number of connections to hidden population, s_F is the sampling frame, and $\hat{P}_H$ is the estimated proportion of the population who are in the hidden population. For example, if we estimated that members of our sample had 3,000 connections to people who had been the victim of a cybercrime (hidden population), and 100,000 connections in total, we would combine these pieces of information to estimate that 3% of the population had been the victim of a cybercrime.

While the basic scale-up method has been applied widely to measure the size of hidden populations, it makes a few modeling assumptions that may be problematic. Specifically, it makes three main assumptions that are often violated in practice, that: (1) social ties are formed at random (barrier effects); (2) respondents have perfect awareness about the relevant traits of the people they are connected to (transmission error); and (3) respondents are able to provide accurate answers to survey questions about their personal network (recall error). In sum, the basic scale-up estimator will only give an unbiased estimate if all these assumptions are met. In this work, we expect the assumption of perfect awareness, that everyone knows exactly how many people in their social network were the victims of a given scam on the internet, will be violated.

To address this issue, we use the *generalized* rather than *basic* scale-up estimator, which adjusts for a few of the biases of the basic network scale-up estimator by computing (1) a degree ratio which corrects for the difference in average network size between hidden population and the general population and (2) a visibility ratio which corrects for respondents not having perfect knowledge of whether people in their personal network are in the hidden population (i.e., cybercrime victims). To compute these adjustment factors, we need to collect data from cybercrime victims to estimate their personal network size and how many people on average in their social network know they were the victim of a cybercrime [27]. We can then multiply the basic scale-up estimate by these two adjustment factors to achieve the more accurate generalized scale-up estimate. Expressed mathematically, we compute:

$$\widehat{P}_H = \underbrace{\left(\frac{y_{F,H}}{\bar{d}_{U,F}}\right)}_{\text{Basic Scale-Up}} \times \underbrace{\frac{1}{\bar{d}_{H,F}/\bar{d}_{F,F}}}_{\text{degree ratio}} \times \underbrace{\frac{1}{\bar{v}_{H,F}/\bar{d}_{H,F}}}_{\text{visibility ratio}} \tag{2}$$

where $y_{F,H}$ is total number of connections between general and hidden population, $\bar{d}_{U,F}$ is the average degree, $\bar{d}_{H,F}$ is the average degree of the hidden population, $\bar{d}_{F,F}$ is the average degree of the general population, and $\bar{v}_{H,F}$ is the number of connections from the hidden population to the general population.

3.4 Survey Instrument

Our survey proceeded as follows. First, we asked respondents whether they have been the victim of six different cybercrimes. We defined being a victim as the respondent having lost money. For banking/credit card fraud, we additionally asked respondents to report experiences that did not involve monetary loss, since we found in pretests that this was very common. The response to these questions were used to generate the direct estimates of cybercrime incidence rates for each of the six cybercrimes.

As described in Section 3.2, all respondents in the general survey, regardless of whether they experienced a cybercrime, answered all of the survey questions except where explicitly noted. In the rare incident sample, only respondents who had experienced an incident were asked the following questions.

Second, respondents completed a validated measure of internet skills from the literature [36].

Third, we asked the respondent to report how many people they knew (defined as people over 18 who live in the U.S., who they know by sight and name and who also know them by sight and name, and with whom they had some contact – in person, over the phone, or over the computer – in the past 2 years) with 12 different names. This information was used to compute their personal network size for the network-scale-up estimation (see Section 3.6 below for more detail).

Fourth, for each crime the respondent reported having been a victim of in the first question, if any, we asked them to report how much money they had lost and to qualitatively describe what happened.

Fifth, respondents who reported (in the first question) having been a victim of a crime were asked whether any of the target people in their network was aware of this fact. We asked this for each crime they reported (or none if they reported none). The target people in their network were those with any of the 12 chosen names that we had asked about at the beginning of the survey. Following best practice, these data were used to construct correction factors for low visibility (transmission bias).[4]

Sixth and finally, we asked all respondents, including in the general survey, those who had not been the victims of any cybercrimes, to report whether anyone they knew had been a victim of that crime, and if so, asked them to report how many people they knew that had been victims and to describe their experiences. These data were used to compute our scale-up estimates of cybercrime incidence. Our full survey instrument can be found in the supplementary appendix.

3.5 Questionnaire Validity

Self-report biases common to all survey studies may be especially acute in studies of crime experiences [13, 34, 44]. Such biases plague both self-report surveys of crime and official crime reports to the police [38]. Prior work in survey methodology and criminology has sought to reduce biases in the measurement of crime prevalence using surveys in various ways. First, in addition to multiple-choice options (e.g., attesting that they were or were not a victim) respondents are asked open answer validation questions, which are then hand-coded by experts to validate responses. Further, extensive

[4]In designing our survey instrument, we followed standard best practices outlined in the network scale-up literature [27, 68, 72]. Specifically, we surveyed a general, nationally-representative sample and asked respondents about the number of connections they had to cybercrime victims. These data were used to produce our *basic* scale-up estimates. We additionally collected data from victims of cybercrimes to calculate correction factors to produce the *generalized* network scale-up estimates presented in this paper.

survey testing is done to reduce errors that might be caused by the survey instrument (e.g., questions that are confusing or subject to multiple interpretations). Finally, probabilistic surveys are performed online instead of by telephone, as – while there is an inherent tradeoff between survey modes – social desirability bias is known to be lower in online surveys [16, 34, 58]. We followed all of these practices.

Regarding our testing, we first conducted six cognitive interviews, in which survey respondents think aloud as they answer a survey and the interviewer probes their understanding of various terms, to validate that respondents understood our questions as is typical for survey methodology best practice [8]. Following these cognitive interviews, we ran three pretests to further validate and refine our survey instrument and reduce respondent error. Respondents for all of these pretests were recruited from Amazon's Mechanical Turk (MTurk) pool of survey takers. MTurk populations are certainly not nationally representative; they tend to be younger and more technologically adept [41]. However, research shows that MTurk respondents are relatively representative of the security-related experiences of those in the U.S. who have some college education and are under 50 [64]. Hence, we consider MTurk sufficient for our pretests, but use a high-quality probabilistic survey sample for our final measurement. For more details on our pretests, see Appendix Section 6.

Qualitative response coding. Given the low incident rate of many of these cybercrimes, there is a risk of false-positive reports upwardly biasing estimates [30]. To reduce the likelihood of false reports, whenever respondents reported being a victim of a cybercrime, we asked them to report their experience in open-text; whenever respondents reported knowing someone who had been the victim of a cybercrime, we also asked them to report the scam(s) that these people experienced. Three researchers, two of whom have postdoctoral training in computer security, independently coded the open-answer responses to ensure their legitimacy. As all three researchers reviewed each decision, we did not calculate an inter-rater reliability (IRR) [55]. We removed a report from the positives list when it did not clearly match the cybercrime category definition. In certain cases, a respondent answered that they had been victim of one type of cybercrime when the described experience clearly matched a different category. For example, one respondent reported the following as non-payment: "I purchased some items on eBay, but never received the goods. I had to contact eBay to resolve the issue." This appears to be a clear case of non-delivery. In cases such as this, we moved the response to the appropriate category (if it was one of our surveyed cybercrime categories) and counted it there. As aforementioned, pretest #1 revealed the need for an additional answer option for the banking and credit card scam question. In cases where respondents selected that they were a victim of a banking/credit card scam and lost money, but reported $0 lost, we changed their answer to the third answer option: that they were a victim of the scam but did not lose money. In cases where the respondent did not describe their experience, their description was insufficient, or their description was of a crime not covered by our survey, we discounted the answer (i.e., counted as not-a-victim). For example, if a respondent put "internet scam" or "online hackers" as their description of the incident, we did not count it.

We then conducted a second round of coding on the validated responses to identify the nature of the fraud. For example, for non-delivery incidents we coded whether the product was purchased via an online retailer, social media/online marketplace, or using atypical financial instruments such as gift cards or money orders. For banking incidents we additionally coded whether the financial institution (bank or credit card company) or the respondent identified the fraud. Two researchers coded 20% of the validated data, achieving substantial agreement [78] between coders ($\kappa = 0.72$), and one researcher coded the remaining data.

3.6 Analysis

Below, we summarize our analyses by research question. All replication materials are publicly available from: https://osf.io/knufm/?viewonly=c5ef5f5078d04c55ba8295b57df14048.

Computing estimates of cybercrime prevalence (RQ1) & monetary loss (RQ2). We calculate direct estimates of cybercrime prevalence by computing the weighted proportion of people in our survey who had been the victim of each of the six cybercrimes [22]. For common cybercrimes (non-delivery and banking/CC fraud), we used the general sample ($N = 1,002$). To estimate the prevalence of rare cybercrimes (advanced-fee, extortion, non-payment, and overpayment), we pooled the general sample and rare-incident sample ($N = 11,953$). The large sample size allows for accurate and precise direct estimation of all six cybercrime incidence rates. We calculate the median, 10th quantile, and 90th quantile dollar monetary loss for each of the 6 incidents separately. We report the median because of its robustness to outliers.

Demographic analysis of cybercrime victimization (RQ3). We fit logistic regression models to investigate the association between sociodemographics and the likelihood of being the victim of a cybercrime. For all models, the dependent variable is whether an individual has been the victim of a cybercrime. Our predictors are basic demographic covariates and, when available, a measure of internet-based skills (dichotomous high/low). We fit three separate models grouping similar cybercrimes into pairs – one model to predict banking/non-delivery, one model to predict non-payment/overpayment, and one model to predict advanced-fee and extortion – in order to offer appropriate sample size for regression modeling while retaining granularity of analysis.

Computing Network Scale-up Prevalence Estimates (RQ4).

We use the *generalized* network scale method to estimate the proportion of U.S. adults who had been the victim of each of the six cybercrimes. We perform variance estimation using a standard bootstrap procedure with 10,000 bootstrap samples [27]. For more details on our implementation of the generalized network scale-up method and internal consistency checks, see Appendix Section 7.

Annualizing Estimates (RQ1, RQ2, RQ4). Finally, we annualized all estimates of cybercrime incidence and monetary loss. By annualizing our estimates, we make the assumption that respondents are equally likely to (1) be the victim of and (2) report scams in each year of the observation window. We use the following equation:

	Amazon Mechanical Turk			NORC Amerispeak Panel	
Sample	Pretest 1	Pretest 2	Pretest 3	General Sample	Rare-Incident Sample
N	100	301	659	1,002	10,951

Table 4: We conducted three pretests to refine and validate our survey instrument. Our final survey collected 1,002 responses. A shorter version of the questionnaire, focusing on rare-incident cybercrimes, collected an additional 10,951 responses.

$$P_a(scam) = 1 - (1 - P_t(scam))^{1/t} \quad (3)$$

where $P_a(scam)$ is the annualized rate, $P_t(scam)$ is the rate for t years of the observation window, and t is the length in years of the observation period.

4 RESULTS

Table 5 and Figure 4a show the prevalence of cybercrime based on direct estimates (based on respondents' reports about their own experiences); Table 7 gives the network scale-up estimates (based on respondents' reports about the experiences of their network).

4.1 RQ1 & RQ2: Incidence and Impact of Cybercrime

We analyze the direct estimates of cybercrime prevalence first. Banking or credit card scams clearly dominate: we estimate that 12.1% (95% confidence interval (CI) [10.3%, 14.1%]) of Americans experienced such scams annually.[5] However, only 1.08% (95% CI, 0.6% - 1.8%) of Americans actually lost money as a result. In other words, only 1-in-13 of those who experienced banking or credit card scams actually lost money. The remainder, 91.1% of victims suffered no monetary loss.

Those who suffered no monetary loss commonly reported that their bank either a) reimbursed losses or b) detected the fraud before the victim noticed anything. While banks and credit-card issuers reveal little of their internal fraud-detection algorithms, clearly they perform well. A partial explanation is that many banking transactions are reversible and/or traceable, so that access to an account (e.g., with a stolen password) does not lead to instant loss [29] Our qualitative coding of respondents' incident reports reveals that for 58% of respondents their bank or financial institution discovered the fraud and alerted them:

> "International travel charges [were] put on my credit card but [were] identified by the credit card company fraud department. [The credit card company] called us, verified [that the] charges were fraudulent, reversed the charges, and closed out our card and issued [us] a new card."

The remaining respondents identified the fraudulent charges themselves and in many cases received a refund, "someone attempted to charge/make purchases from Walmart to my credit card. I noticed the charge and contacted my creditor."

[5]We asked respondents to report experiences of themselves and their networks over the past two years, due to the rarity of these incidents. We have annualized all estimates following the method in SI, section 8 for simplicity of reading and comparison with measurements from prior work.

	Prevalence	Money Lost (Dollars)		
Cybercrime	Direct Estimate (%)	Median	Q_{10}	Q_{90}
Bank/CC (any)	12.110			
Bank/CC (lost money)	1.082	265.95	32.34	1000.00
Non-Delivery	3.205	57.05	15.00	300.00
Advanced Fee	0.280	500.00	14.32	3000.00
Non-Payment	0.344	100.00	13.66	700.00
Extortion	0.116	300.00	56.65	1442.25
Overpayment	0.052	88.01	35.00	854.27

Table 5: Annualized cybercrime prevalence estimates in the U.S. from our direct survey. The banking and non-delivery categories are estimated with $N = 1,002$, all other categories with $N = 11,953$.

The median[6] loss for those who did lose money from a banking or credit card scam was $266. Table 5 lists the median and bottom and top ten percentiles of money lost per scam; Figure 2 illustrates the distribution of money lost.

Of banking or credit card scams respondents reported, 6.68% involved withdrawal or transfer of money from the victim's account, while the remainder involved fraudulent charges. Of those who experienced fraudulent charges and provided details regarding the nature of those charges, 57.0% described the scammer purchasing products; the remainder reported that the scammer placed charges (e.g., for gas) in a location far from the respondent's residence.

Non-delivery of purchased goods is the second most frequently experienced cybercrime amongst those we measured. We estimate that 3.21% (95% CI, 2.2% - 4.5%) of Americans experienced this annually. Typical experiences reported were ordering goods online through an unfamiliar seller: "A website advertised a tent for $30, I paid and never received it." Americans lost a median of $57 from non-delivery scams. Of these scams, 70.1% occurred when the victim made a purchase from an online retailer, 23.9% occurred when they made a purchase on social media or from an online marketplace, and the remainder involved atypical financial instruments such as gift cards or money orders: "both were older adults who purchase[d] something via money order online and never received the item."

The remaining four categories of cybercrime – advance-fee, non-payment, and overpayment scams, as well as extortion – are far rarer, with fewer than 0.40% of Americans (i.e., 4 out of every 1000) experiencing such scams annually (confidence intervals are listed in Table 7). The distribution of money lost from non-payment scams and overpayment scams was similar to that of non-delivery scams: the majority of victims lost less than $100. However, advanced fee

[6]We report medians, because prior work shows that means are very easily skewed by even a single low or high report, which are known to be highly likely in cases of cybercrime [30].

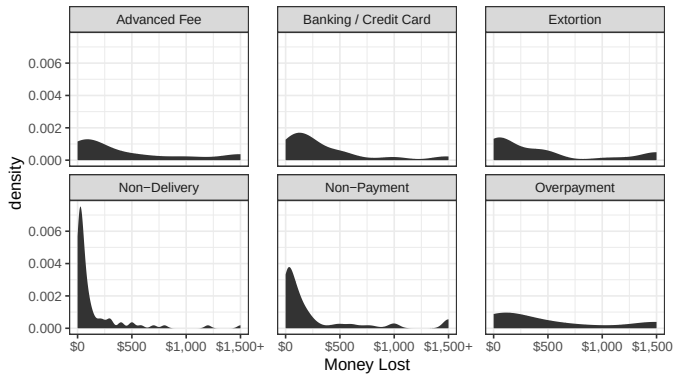


Figure 2: Distribution of money lost per directly-reported cybercrime incident. Note that cases where money was not lost are not included (e.g., 12.1% of respondents experienced a banking or credit card crime, but we show only the 1.08% who lost money.

scams and extortion resulted in higher reported losses: a median loss of $500 for advanced fee and a median of $300 lost by extortion.

All but three of the non-payment scams reported involved selling an item in an online marketplace. Of the other three non-payment scams reported, two involved housing rentals via online marketplaces and one involved the sale of cryptocurrency: "I sold bitcoins and the bank took the money back after 2 weeks, and I had already sent the bitcoin." All overpayment scams involved the sale of products online. Of advanced fee scams, 43.5% involved winning a trip or time share, 41.3% involved winning money or a gift, and 15.2% involved financial instruments such as investments or loans:

> "A guy called said I was approved for a loan and I had to pay a process fee on a prepaid card. Sent it didn't receive loan just keep saying they need more money to approve. Told my daughter and she called the place; they just hung up on her many times."

Finally, of extortion scams, 59.3% involved holding the victim's digital files hostage: "My computer locked up and I received an email that if I wanted my information on to be unlocked then I had to pay the fee." 33.3% involved a threat to post false or harmful information about the victim – "said they would release their porn to their contact list" – while the remainder involved fake digital threats such as computer viruses. Regarding the latter, one respondent explained:

> "My computer froze and I called the phone number on the screen. The person showed me all the viruses and threats that were on my computer and said all my personal info could be stolen, if I didn't have him run software to get rid of the problems. He needed payment before he could clean the computer. [I] couldn't use my credit card because that could be stolen if I put it on the internet, he said. So he asked me to get gift cards in $100 denominations, which I stupidly did (twice). He said the first gift card numbers were invalid. He got me at a vulnerable time because my Facebook account had been breached a few times (maybe they did it, I don't know). Gave them the money and never got notification that they ran any software...I reported it to my local police."

Figure 3 places our results in the context of cybercrime measurement from the U.S. and Europe from the last five years.[7] While there are substantial limitations to comparing these data – they were measured via different methodologies (in the case of self-report measurements, with different questions), at different periods of time, and in different countries – we observe that our measurements bracket or fall within these existing estimates. Specifically, our data and past data suggest that the frequency of credit card and banking scams is between 3.5% and 12.5%, but the frequency of losing money from such scams is below 1.1%. The annual frequency of non-delivery scams is between 1% and 3.5%, while the annual frequency of extortion, and non-payment, advanced fee, and overpayment scams are all less than 1.25%. While there is some heterogeneity, our estimates broadly align with other survey-based estimates of the prevalence of cybercrime. Converging results across studies using different methodologies further validates estimates from any individual study [37, 69]

4.2 RQ3: Demographic Analysis of Cybercrime

To what extent do cybercrime victimization rates differ across key sociodemographic groups? Table 6 shows the odd ratios, the exponentiated regression coefficients, from three logistic regression models of the relationship between victimization and sociodemographic characteristics in our sample. The odds ratios give the relative odds that an individual was the victim of a scam given a certain covariate compared to our baseline: White males, aged 18-30, with low household income (<50k) and low educational attainment. An odds ratio of 1 means that a given covariate does not affect the likelihood of being the victim of a scam, values greater than 1 correspond to an increased odds of having been the victim of a scam, and values less than 1 correspond to decreased odds of having been the victim of a scam, compared to the baseline.

The clearest insight from our regressions models is that older Americans are more likely to have been the victim of a scam on the internet. The oldest age group (60+) was more than three times as likely to have been the victim of banking, non-delivery, advanced fee, and extortion scams. However, older Americans were less likely to be the victim of nonpayment and overpayment scams. Both nonpayment scams and overpayment scams require the victim to be selling an item, generally online. There is some evidence that older Americans are less likely to sell things on the internet [50], which may explain why older Americans are less likely to be the victim of nonpayment and overpayment scams. We observe no other statistically significant relationship between sociodemographic characteristics and victimization, with the exception that more highly educated people are more likely to be the victims of banking and non-delivery scams as are Black, Non-Hispanic Americans, who

[7] We exclude estimates from FTC Consumer Sentinel for the "Banking / Credit Card" category, as the the low-impact nature of banking / credit card scams (where no money was lost) makes it unlikely it would be reported to the Consumer Sentinel network.

	All Scams	Banking/Nondelivery	Extortion/Advanced Fee	Nonpayment/ Overpayment
	Model 1	Model 2	Model 3	Model 4
Black, non-Hispanic	1.773*	1.761*	2.370*	0.195
	(2.126)	(2.097)	(2.045)	(−1.772)
Hispanic	1.481	1.428	0.550	1.620
	(1.583)	(1.426)	(−0.886)	(1.528)
Other race/ethnicity	0.885	0.890	3.083*	1.569
	(−0.381)	(−0.363)	(2.419)	(1.004)
Gender: Female	1.130	1.155	0.880	1.565
	(0.640)	(0.756)	(−0.377)	(1.544)
Age: 30-44	1.978*	2.114*	3.152	0.894
	(2.138)	(2.309)	(1.599)	(−0.331)
Age: 45-59	2.761**	2.930**	1.743	0.461
	3.125	3.258	0.704	−1.855
Age: 60+	3.063***	3.253***	5.799**	0.305**
	(3.556)	(3.684)	(2.576)	(−2.641)
Educ: Bachelors or Higher	1.751*	1.725*	0.606	0.908
	(2.070)	(2.012)	(−0.884)	(−0.217)
Educ: Some College	1.678*	1.632*	1.444	1.497
	(2.165)	(2.042)	(0.921)	(1.226)
Income: 100k+	1.076	1.101	0.634	1.043
	(0.285)	(0.373)	(−0.883)	(0.112)
Income: 50 - 100k	0.763	0.777	0.503	0.505
	(−1.242)	(−1.155)	(−1.673)	(−1.865)
Internet Skills: High	1.091	1.084		
	(0.441)	(0.406)		
Constant	0.094***	0.088***	0.002***	0.008***
	(−6.498)	(−6.573)	(−8.916)	(−12.455)
Observations	1,002	1,002	11,953	11,953

*p < .05; **p < .01; ***p < .001

Table 6: Logistic regression models predicting being the victim of cybercrime. All models report t-statistics are reported in parentheses, the parameter estimate divided by its standard error. The reference group for all models is White males, aged 18-30, with low household income (<50k), and low educational attainment (high school degree or less).

are also more likely to be the victims of advanced fee and extortion scams.

Broadly, our results suggest that victims of cybercrimes are more likely to be older, more highly educated, and have higher internet skills; we find that Black, non-Hispanic Americans are also more likely to be the victims of banking, non-delivery, advanced fee, and extortion scams, but not non-payment and over-payment scams (the two scams that require the internet users to be involved in selling items online). This pattern — the opposite of inequities in physical crime — has been found in past security victimization studies [63].

Since only two of our categories overlap with the 2017 FTC survey, only partial comparison with their demographic analysis is possible [4]. Additionally, the FTC conducts bi-variate comparisons with individual-level demographics (they look at correlations between victimization and a single demographic), while our analysis controls for a wide range of demographic variables (and in the case of banking and non-delivery scams, internet skill).

For non-delivery fraud, the FTC survey found an inverse correlation between age and victimization rate; this is the reverse of our finding. They also found that women were slightly more likely than men to be victimized, which agrees with our finding. They found African-Americans and Hispanics were victimized at a higher rate than the rest of the population, which is consistent with our finding that Black Americans are more likely to be victimized by banking and non-delivery scams (see Figure 6(a)).

For advance fee fraud, the FTC survey found no significant correlation with age; they found that women were almost twice as likely as men to be victimized (while we found little correlation); they found African-American's and Hispanics were significantly more likely to be victimized (we found the former more likely to be victimized, and no significant relationship for the latter).

4.3 RQ4: Network Scale-up Estimates of Cybercrime

We asked our entire nationally-representative general sample (N = 1,002) a series of network scale-up questions to estimate both the size of their personal networks and to generate scaled-up cybercrime estimates. Additionally, to generate generalized network

Cybercrime	Network scale-up (%)	Network Scale-up CI	Direct (%)	Direct CI (%)
Bank/CC (any)	3.904	1.601-12.692	12.110	10.339, 14.061
Bank/CC (lost money)	0.786	0.291-2.712	1.082	0.618, 1.754
Advanced Fee	0.018	0.004-0.074	0.280	0.167, 0.441
Non-Payment	0.017	0.000-0.061	0.344	0.243, 0.472
Extortion	0.060	0.021-0.212	0.116	0.031, 0.299
Non-Delivery	0.576	0.019-1.811	3.205	2.209, 4.481
Overpayment	0.032	0.002-0.163	0.052	0.013, 0.136

Table 7: Annualized cybercrime prevalence estimates from our network scale-up survey, in which respondents answered about the experiences of their friends and acquaintances, and our direct report survey in which respondents answer about their own experiences. The banking and non-delivery categories are estimated with $N = 1,002$, all other categories with $N = 11,953$.

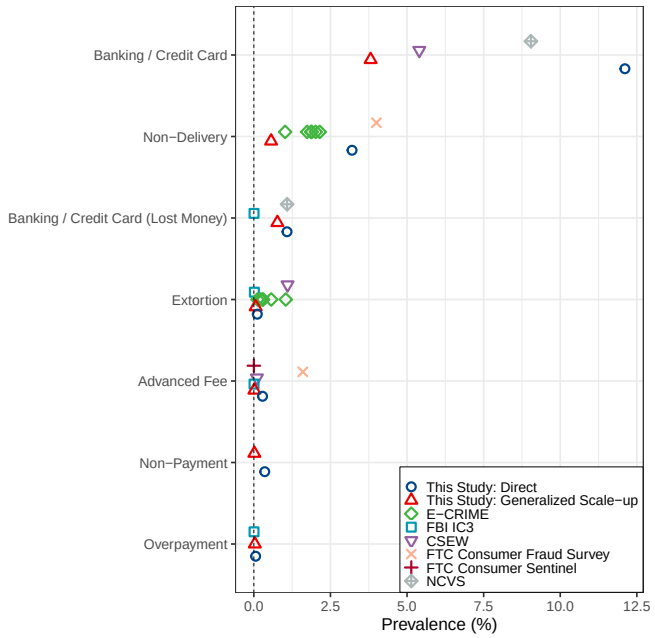


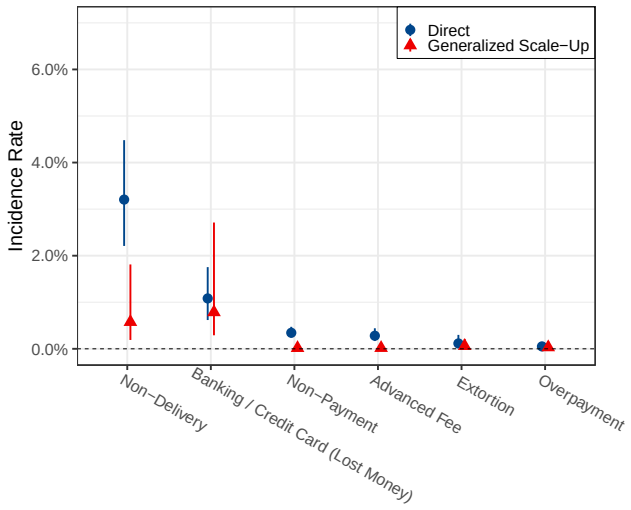
Figure 3: Comparison of cybercrime prevalence estimates generated from different data sources: (i) our own direct and network scale-up surveys (U.S., surveys) (ii) E-Crime (7 European countries, survey), (iii) Federal Bureau of Investigation (FBI) IC3 (U.S., crime reports), (iv) Crime Study of England and Wales (CSEW) (England and Wales, survey), (v) Federal Trade Commission (FTC) Consumer Sentinel (U.S., crime reports), (vi) Federal Trade Commission (FTC) Consumer Fraud Survey (U.S., survey) and (vii) Bureau of Justice Statistic's National Crime Victimization Study (U.S., survey).

scale-up estimates (which adjust for the low visibility factor and differential network sizes of cybercrime victims as described in further detail in Section 3.3), we conducted a second nationally-representative survey (N = 10,951) to calculate adjustment factors for the generalized network scale-up estimates [27, 68]. The network scale-up estimates of cybercrime frequency are shown in Table 7. The estimates generated from the network scale-up data trend lower than those obtained from direct estimation (see Figure 4a; however we note that the confidence intervals for the estimates overlap for banking/CC, extortion, and overpayment scams.

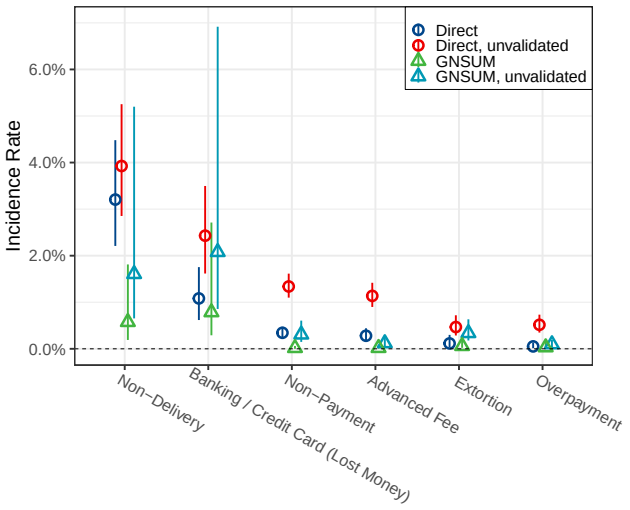
In situations where direct estimation produces underestimates because of social desirability bias, the network scale-up method generally produces higher estimates because it avoids social desirability bias; respondents report about others, not themselves. There are several potential explanations for the difference between our direct and network scale-up estimates. First, as we elaborate in the Discussion, this difference may be related to the low *visibility* of these experiences. The visibility is the proportion of people in a member the target populations' personal network who know about their cybercrime experiences. A visibility of 75% means that on average, 75% of someone's personal network knows that they are a member of the target population. In comparison to past network scale-up studies [35], we find very low visibility factors ranging from 0.8%-1.4% (see Table 9). Visibility factors vary from study to study, but are generally between 25%-75% [35].

We estimate an adjustment factor to correct for this low visibility, but this adjustment factor relies on people who were the victim of cybercrime being able to accurately report whether others in their social network know they were the victim of a cybercrime. Survey methodology research finds that people are subject to recall bias: decreased ability to recall precise details of experiences (e.g., how many people they told about the incident) [74]. Thus, participants may not have been able to provide perfectly accurate estimates. While some network scale-up surveys address specific crime incidents like ours [48], others address lifestyle situations such as whether someone works in the sex industry or uses intravenous drugs [45, 68, 77], which are ongoing experiences and thus subject to less recall bias. Investigating how different types of measurements may influence the utility of the generalized scale-up estimator in correcting for low visibility is an important direction for future research in network scale-up methodology.

An second factor that may have affected our network scale-up estimates differently from our direct estimates is our survey response validation procedure. As described in Section 3.5, three coders, two of whom are experts in cybersecurity, evaluated every qualitative description of a cybercrime, whether that crime was experienced by the respondent or experienced by someone in their social network. To better understand the effect of response validation on our final estimates, we show the direct and network scale-up estimates with and without our response validation in Figure 4b. This plot



(a) Direct (blue circle) and network scale-up (red triangle) estimates. Note that all but the banking/credit card and non-delivery categories have annual prevalence below 0.4%.



(b) Direct (circle) and network scale-up estates (triangle) with and without response validation.

Figure 4: Annualized estimates of cybercrime prevalence and 95% confidence intervals for our direct and network scale-up estimates.

demonstrates the importance of response validation and its differential effect on the direct and network scale-up estimates. The direct estimates without response validation are substantially higher than the validated direct estimates and both network scale-up results. However, the response-validated direct estimates align closely with the non-validated network scale-up estimates: all confidence intervals overlap. This suggests that people may know of more experiences in their network than they can concretely describe in a way that our response validation would consider a valid description of a cybercrime incident.

5 DISCUSSION

Overall, we find that our estimates of cybercrime, both the network scale-up and direct measurements, bracket the prior estimates of cybercrime from crime reports and self-report surveys. Our measurements and measurements from prior work suggest that only two crimes occur with greater than 1% prevalence: credit card or bank account scams (1.08% prevalence annually) and non-delivery of goods purchased online (3.21% prevalence annually). Moreover, the median loss reported by victims for all scams, except extortion (0.113% prevalence annually) was $300 or less.

Thought Experiment: Typical Consumer Losses. To understand what these measurements mean for typical consumer losses from cybercrime, we conduct a thought experiment, using our data to reason about typical consumer losses. We use the direct estimate statistics to reason about the typical and worst case monetary losses from cybercrime that an American might expect to sustain annually. We treat the probability of each cybercrime occurring as independent. Thus, we compute the following for Q_{50} and Q_{90} monetary losses.

$$\sum_{n=1}^{6} P_a(scam) \times loss \tag{4}$$

To represent the losses a typical consumer suffers from the six cybercrimes we measure, we sum the product of the incidence rate and the median monetary loss across the six cybercrimes. To represent the worst losses a typical consumer might suffer, we calculate prevalence rate multiplied by the 90th percentile loss and sum across all six categories. We find that in the typical case, an American is at risk of losing $6.87 annually from these six cybercrimes, while the 90th percentile case would result in a $33.56 annual loss from cybercrimes.

Based on the most recent FBI crime report statistics, the six cybercrimes we study represent 30% of cybercrimes against individuals. Thus, we can estimate that these losses represent 30% of potential consumer losses. If the remaining crimes follow a similar loss pattern, a typical consumer stands to lose $22.90 (= $6.87 ÷ 0.3) and in the worst 90th percentile case a consumer stands to lose $111.87.

Comparison with Prior Cybercrime Estimates. For the categories that we have in common with the 2017 FTC survey [4] agreement is within the margin of error. The FTC found that 4.0 ± 0.9% of consumers experienced non-delivery of goods they had paid for, which aligns closely to our estimate of 3.2%, (95% CI, 2.2%-4.4%). For advanced fee fraud, the FTC study found a 1.6 ± 1.3% incidence rate. However, the FTC survey includes phone and in-person fraud,

in addition to online fraud. They estimate that a little over half of the fraud reported in this category occurred online, and thus their estimate is comparable to our direct estimate of 0.3% (95% CI, 0.16%-0.46%).

We note that, when direct comparison is possible, our estimates show good agreement with previous studies that ask about well-defined incidents and clearly specify their methodology. This is the case for all of the estimates in Figure 3. Such consistency supports the scientific validity of our respective results [37, 69].

Our numbers are harder to reconcile with other estimates, such as the Gartner estimate pegging US phishing losses at $3.2 billion [1], the FTC Identity Theft estimate of $57 billion [26], the Norton $114 billion estimate [56], or the McAfee claim that Cybercrime cost $1 trillion in 2018 [15]. First, survey-based estimates that do not sanitize self-reported numbers (such as the Gartner [1], FTC [26] and Norton [56]) may be subject to extreme over-estimation [30]. Second, some estimates have questionable methodology; e.g., McAfee's bi-annual estimates [14, 15] do not measure or survey anything but simply take a fraction (decided in an unspecified manner) of GDP as their estimate. Finally, when numbers are offered for economy-wide cybercrime losses as a whole (e.g., the Norton and McAfee estimates) it is difficult to know precisely what is being estimated.

Beyond Monetary Loss: Discussing Cybercrimes. A common criticism of characterizing the impact of crime based only on monetary loss is that such characterizations do not capture the full spectrum of victims' experiences, including the time necessary to mitigate a loss and the emotional experience of being a victim [29]. Another way of characterizing the impact of an experience is whether or not victims speak about that experience to those in their personal network. Prior work on physical crime has demonstrated that whether or not victims do so may correlate with the severity of the crime [73] and that most victims of serious crimes reach out for such support [31, 33]. Further, prior work on digital security has found that many people learn digital security strategies from friends who describe stories of their own negative experiences / crime victimization [60, 62, 65].

Given this prior work, it is interesting that we find that the network scale-up estimates are in all cases lower than the direct estimates. We asked respondents about their own experience to estimate the former and the experience of their network to estimate the latter. Thus, the network scale-up survey queries the experiences of a population that is many times larger. For example, if the average respondent has 60 people they know well, the network scale-up estimates are effectively querying the experiences of a group 60× larger than the direct for matters where people have perfect visibility into their network. For activities like intravenous drug use and sex work, the network scale-up estimates are higher than direct [68]. However, we find that in all cases our network scale-up estimates are lower than our direct estimates.

Our estimates of the visibility factor indicates that victims' social networks have poor visibility into their experiences, and conversely, suggests that cybercrime victims – of the six cybercrimes we studied – talk about their experiences rarely and/or to few other people [35]. This could either be because the emotional impact of these cybercrimes for most victims is low, as suggested in prior work [71][8], or that people are embarrassed to admit their experiences to friends. As aforementioned, multiple prior studies suggest that people do talk about – and their friends learn from – their negative experiences [60, 62, 65]. At the same time, prior work on romance scams in particular found that scam victims did not discuss their experiences with others out of embarrassment [18]. This could suggest a general trend toward not discussing more severe cybercrime experiences, or that romance scams with their connection to the societally-taboo topics of romance and sex [2] are uniquely sensitive.

Given people's receptiveness to learning protective behaviors from other's stories [79] – especially those from lower socioeconomic status backgrounds [62, 63] – to learn security behaviors, future work is needed to further investigate when and for which types of cybercrimes people are and are not willing to discuss their cybercrime experiences. Further, future work is merited measuring the impact of cybercrime via measures other than monetary loss such as time spent mitigating the crime or emotional impact of the crime. Such measurements may lead to novel prioritizations as compared to existing measurements based on monetary loss.

5.1 Implications for Design

The two most prevalent cybercrimes we identify both relate to purchasing behavior, suggesting that future work on cybercrime protection may seek to focus specifically on behavioral interventions at the time of purchase, a relatively unexplored design space [57]

Further, we find that older Americans and Black Americans are significantly more likely to be the victims of cybercrimes, with the exceptions of scams that involve the victim selling goods on the internet, where they are significantly less likely to be victims. Thus, future work may seek to prioritize research and design focused on protecting these groups in particular, who have rarely been the focus of security research (as notable exceptions that echo the need for more research centering these communities see [11, 32]).

Finally, we find that people rarely discuss cybercrimes with others in their network. Investigating non-disclosure of cybercrimes is a promising area for future work, which has been conducted on non-disclosure of other non-security related digital experiences [3]. For example, future work may explore how to design mechanisms of post-crime support for victims while respecting victims' desire for privacy and mitigating shame.

5.2 Limitations

This study has several limitations. First, we focus on a subset of common cybercrimes against individuals that can be clearly defined and understood in the context of a survey, and thus we do not measure cybercrimes against organizations nor the total amount of cybercrime in the U.S. However, the advantage of this approach is that focusing on common, easily-defined cybercrimes is that it allowed us to ensure the reliability of our definitions and avoid respondent fatigue. Building on our evaluation of how to most robustly measure cybercrime, future work can use our open source materials to extend our survey instrument to include new cybercrimes.

[8] We do not argue that the emotional impact for all cybercrime victims, especially those who fall for sensitive scams such as romance scams or who lose large amounts of money, is low [19].

Second, our study is subject to the typical limitations of survey research. Respondents may have experienced social desirability bias – selecting the answer choice they perceived as desired by the researchers or by society – or they may have engaged in satisficing behavior – they may have selected the easiest answer – when reporting their answers to our survey questions. To mitigate these biases, we conducted extensive pretesting of our survey and conducted qualitative coding on all incident reports as aforementioned.

Third, respondents may not have been aware that they experienced a cybercrime incident and thus such an incident may not have been reported in our survey. However, it is critical to privilege people's subjective realities in the development of technology including cybercrime protections [59]. For this reason, and due to the measurement limitations of other potentially more "objective" approaches detailed in Section 2.1, we chose to maintain a self-report approach to cybercrime measurement as is the gold standard in the measurement of physical crimes [52].

Finally, our network scale-up analysis had lower visibility than past network scale-up studies. We calculated an adjustment factor to account for the low visibility [27], but this calculation relies on victims of cybercrimes being able to accurately report whether someone in their network knows they were the victim of a cybercrime. Critically, our findings suggest that there may be more significant recall bias in the use of network scale-up surveys for specific incidents (like crimes) than for ongoing lifestyle experiences (like working in the sex industry or using intravenous drugs), which may erode the correction power of the generalized correction factors used in our work. This is an important direction for future work in the statistics community.

5.3 Conclusion

This study provides several methodological and substantive insights into the study of cybercrime. Our large-scale, nationally representative survey of consumer cybercrime in the U.S. finds that cybercrime against individuals is rare and generally low-impact. Only two of the cybercrimes we studied occurred with an incidence rate over 1%; the median loss for the cybercrimes we studied was $100. Except for scams that involve selling goods online, older and Black Americans are more likely to report being victims of cybercrime.

Methodologically, this work makes two key contributions to the cybercrime measurement literature. First, we demonstrate that with an appropriate survey instrument, researchers can accurately and precisely estimate the cybercrime incidence rates. However, our results highlight that relying on respondent reports alone is not sufficient. A response validation procedure is needed to systematically confirm that reported incidents weren't reported inaccurately. This is especially important for scams with low incidence rates, where even a small number of false reports will have large implications for the final estimates. However, different response validation procedures may be necessary for direct reports vs. reports about a respondents' social network, as undercounting may occur in the latter case due to respondents' lack of specificity when reporting on the experiences of others. The second methodological contribution is the evaluation of a new approach to measuring cybercrime, the network scale-up method, which uses sampled social network data to estimate the incidence rates. Our network scale-up results suggest promising directions for future research and design related to the low visibility of cybercrime victimization in respondents' networks. In future network scale-up surveys related to cybercrime, we recommend focusing on closer relationships — household members, close friends, or co-workers rather than the entire personal network as the network scale-up method works best when people have high visibility into the traits of others in their social networks. We place additional, smaller, lessons learned for the construction of future measurement instruments for cybercrime in the Appendix.

ACKNOWLEDGMENTS

The authors wish to thank Dennis Freehan, James Bono, and the Amerispeak team for their feedback on this work. A portion of this work was completed while the third author was at Microsoft Research.

REFERENCES

[1] T Almeida. 2007. *Gartner Survey Shows Phishing Attacks Escalated in 2007/More than $3 Billion Lost to These Attacks.* Technical Report N/A. Gartner. N/A pages.

[2] Teresa Almeida, Rob Comber, and Madeline Balaam. 2016. HCI and Intimate Care as an Agenda for Change in Women's Health. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. Association for Computing Machinery, New York, NY, USA, 2599–2611. https://doi.org/10.1145/2858036.2858187

[3] Nazanin Andalibi. 2020. Disclosure, Privacy, and Stigma on Social Media: Examining Non-Disclosure of Distressing Experiences. *ACM transactions on computer-human interaction (TOCHI)* 27, 3 (2020), 1–43.

[4] Keith B Anderson. 2019. *Mass-Market Consumer Fraud in the United States: A 2017 Update.* Technical Report. Federal Trade Commission.

[5] Ross Anderson, Chris Barton, Rainer Boehme, Richard Clayton, Carlos Ganan, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the Changing Cost of Cybercrime. In *Workshop on the Economics of Information Security*, Vol. WEISS 2019. WEISS, Boston, MA, 32. https://doi.org/10.17863/CAM.41598

[6] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. 2013. Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy*, Rainer Böhme (Ed.). Springer, Berlin, Heidelberg, 265–300. https://doi.org/10.1007/978-3-642-39498-0_12

[7] Eric P.S. Baumer and M. Six Silberman. 2011. When the Implication Is Not to Design (Technology). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2271–2274. https://doi.org/10.1145/1978942.1979275

[8] Paul C Beatty and Gordon B Willis. 2007. Research Synthesis: The Practice of Cognitive Interviewing. *Public opinion quarterly* 71, 2 (2007), 287–311.

[9] Ingolf Becker, Alice Hutchings, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Steven J Murdoch, M Angela Sasse, and Gianluca Stringhini. 2017. International Comparison of Bank Fraud Reimbursement: Customer Perceptions and Contractual Terms. *Journal of Cybersecurity* 3, 2 (June 2017), 109–125. https://doi.org/10.1093/cybsec/tyx011

[10] Rosanna Bellini, Nicola Dell, Monica Whitty, Debasis Bhattacharya, David Wall, and Pamela Briggs. 2020. Crime and/or Punishment: Joining the Dots between Crime, Legality and HCI. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–8. https://doi.org/10.1145/3334480.3375176

[11] Maia J. Boyd, Jamar L. Sullivan Jr., Marshini Chetty, and Blase Ur. 2021. Understanding the Security and Privacy Advice Given to Black Lives Matter Protesters. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3411764.3445061

[12] Karoline Busse, Mohammad Tahaei, Katharina Krombholz, Emanuel von Zezschwitz, Matthew Smith, Jing Tian, and Wenyuan Xu. 2020. Cash, Cards or Cryptocurrencies? A Study of Payment Culture in Four Countries. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Genoa, Italy, 200–209. https://doi.org/10.1109/EuroSPW51379.2020.00035

[13] David Cantor and James P Lynch. 2000. Self-Report Surveys as Measures of Crime and Criminal Victimization. *Criminal justice* 4, 2000 (2000), 85–138.

[14] Center for Strategic and International Studies. 2014. Net Losses: Estimating the Global Cost of Cybercrime.

[15] Center for Strategic and International Studies. 2020. The Hidden Costs of Cybercrime.

[16] Linchiat Chang and Jon A Krosnick. 2010. Comparing Oral Interviewing with Self-Administered Computerized Questionnaires: An Experiment. *Public Opinion Quarterly* 74, 1 (2010), 154–167.

[17] Federal Trade Commission et al. 2020. Consumer Sentinel Network Data Book 2019.

[18] Cassandra Cross. 2015. No Laughing Matter: Blaming the Victim of Online Fraud. *International Review of Victimology* 21, 2 (May 2015), 187–204. https://doi.org/10.1177/0269758015571471

[19] Cassandra Cross, Kelly Richards, and Russell G Smith. 2016. The Reporting Experiences and Support Needs of Victims of Online Fraud. *Trends and issues in crime and criminal justice* 1, 518 (2016), 1–14.

[20] J. Michael Dennis. 2020. Technical Overview of the Amerispeak Panel.

[21] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. Association for Computing Machinery, New York, NY, USA, 1065–1074. https://doi.org/10.1145/1357054.1357219

[22] Greg Freedman Ellis, Thomas Lumley, Tomasz Żółtak, Ben Schneider, and Pavel N. Krivitsky. 2021. Srvyr: 'Dplyr'-Like Syntax for Summary Statistics of Survey Data.

[23] Cori Faklaris, Laura Dabbish, and Jason I. Hong. 2019. A Self-Report Measure of End-User Security Attitudes (SA-6). In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19)*. USENIX Association, USA, 61–77.

[24] Federal Bureau of Investigation. n.d.. The Nation's Two Crime Measures.

[25] Federal Bureau of Investigation. n.d.. Nigerian Letter or "419" Fraud.

[26] Federal Trade Commission. 2007. *Identity Theft Survey Report.* Technical Report. Federal Trade Commission.

[27] Dennis M. Feehan and Matthew J. Salganik. 2016. Generalizing the Network Scale-Up Method: A New Estimator for the Size of Hidden Populations. *Sociological methodology* 46, 1 (Aug. 2016), 153–186. https://doi.org/10.1177/0081175016665425

[28] Dennis M. Feehan and Matthew J. Salganik. 2016. Networkreporting: Tools for Using Network Reporting Estimators.

[29] Dinei Florêncio and Cormac Herley. 2012. Is Everything We Know about Password Stealing Wrong? *IEEE Security Privacy* 10, 6 (Nov. 2012), 63–69. https://doi.org/10.1109/MSP.2012.57

[30] Dinei Florêncio and Cormac Herley. 2013. Sex, Lies and Cyber-Crime Surveys. In *Economics of Information Security and Privacy III*. Springer, Economics of information security and privacy III, 35–53.

[31] Kenneth Friedman. 1982. *Victims and Helpers: Reactions to Crime.* US Department of Justice, National Institute of Justice, Washington, DC.

[32] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and Security Threat Models and Mitigation Strategies of Older Adults. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. SOUPS, Santa Clara, CA, 21–40.

[33] Martin S. Greenberg and R. Barry Ruback. 1992. *After the Crime: Victim Decision Making.* Plenum Press, Springer Science & Business Media.

[34] Robert M. Groves, Floyd J. Fowler Jr, Mick P. Couper, James M. Lepkowski, Eleanor Singer, and Roger Tourangeau. 2009. *Survey Methodology.* John Wiley & Sons, Hoboken, NJ, USA.

[35] Aliakbar Haghdoost, Milad Ahmadi Gohari, Ali Mirzazadeh, Farzaneh Zolala, and Mohammad Reza Baneshi. 2018. A Review of Methods to Estimate the Visibility Factor for Bias Correction in Network Scale-up Studies. *Epidemiology and Health* 40 (Aug. 2018), e2018041. https://doi.org/10.4178/epih.e2018041

[36] Eszter Hargittai and Yuli Patrick Hsieh. 2012. Succinct Survey Measures of Web-Use Skills. *Social Science Computer Review* 30, 1 (2012), 95–107.

[37] Roberta Heale and Dorothy Forbes. 2013. Understanding Triangulation in Research. *Evidence Based Nursing* 16, 4 (Oct. 2013), 98–98. https://doi.org/10.1136/eb-2013-101494

[38] Michael J. Hindelang, Travis Hirschi, and Joseph G. Weis. 1979. Correlates of Delinquency: The Illusion of Discrepancy between Self-Report and Official Measures. *American Sociological Review* 44, 6 (1979), 995–1014. https://doi.org/10.2307/2094722

[39] HMD. 2021. Human Mortality Database. (2021).

[40] Danny Yuxing Huang, Maxwell Matthaios Aliapoulios, Vector Guo Li, Luca Invernizzi, Elie Bursztein, Kylie McRoberts, Jonathan Levin, Kirill Levchenko, Alex C. Snoeren, and Damon McCoy. 2018. Tracking Ransomware End-to-end. In *2018 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 618–631. https://doi.org/10.1109/SP.2018.00047

[41] Connor Huff and Dustin Tingley. 2015. "Who Are These People?" Evaluating the Demographic Characteristics and Political Preferences of MTurk Survey Respondents. *Research & Politics* 2, 3 (2015), 2053168015604648.

[42] Internet Crime Complaint Center. 2019. *Internet Crime Report.* Technical Report. Federal Bureau of Investigation.

[43] Lilli Japec, Frauke Kreuter, Marcus Berg, Paul Biemer, Paul Decker, Cliff Lampe, Julia Lane, Cathy O?Neil, and Abe Usher. 2015. Big Data in Survey Research: AAPOR Task Force Report. *Public Opinion Quarterly* 79, 4 (2015), 839–880.

[44] Josine Junger-Tas and Ineke Haen Marshall. 1999. The Self-Report Methodology in Crime Research. *Crime and justice* 25 (1999), 291–367.

[45] Charles Kadushin, Peter D. Killworth, H. Russell Bernard, and Andrew A. Beveridge. 2006. Scale-Up Methods as Applied to Estimates of Heroin Use. *Journal of Drug Issues* 36, 2 (April 2006), 417–440. https://doi.org/10.1177/002204260603600209

[46] Steven Kemp, David Buil-Gil, Asier Moneva, Fernando Miró-Llinares, and Nacho Díaz-Castaño. 2021. Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice* 37, 4 (Nov. 2021), 480–501. https://doi.org/10.1177/10439862211027986

[47] Peter D. Killworth, Eugene C. Johnsen, Christopher McCarty, Gene Ann Shelley, and H.Russell Bernard. 1998. A Social Network Approach to Estimating Seroprevalence in the United States. *Social Networks* 20, 1 (Jan. 1998), 23–50. https://doi.org/10.1016/S0378-8733(96)00305-X

[48] Peter D. Killworth, Christopher McCarty, H. Russell Bernard, Gene Ann Shelley, and Eugene C. Johnsen. 1998. Estimation of Seroprevalence, Rape, and Homelessness in the United States Using a Social Network Approach. *Evaluation Review* 22, 2 (April 1998), 289–308. https://doi.org/10.1177/0193841X9802200205

[49] Jooyoung Lee, Sarah Michele Rajtmajer, Eesha Srivatsavaya, and Shomir Wilson. 2021. Digital Inequality through the Lens of Self-Disclosure. *Proc. Priv. Enhancing Technol.* 2021, 3 (2021), 373–393.

[50] Amanda Lenhart. 2005. About 25 Million People Have Used the Internet to Sell Something.

[51] Eric Lin, Saul Greenberg, Eileah Trotter, David Ma, and John Aycock. 2011. Does Domain Highlighting Help People Identify Phishing Sites?. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. Association for Computing Machinery, New York, NY, USA, 2075–2084. https://doi.org/10.1145/1978942.1979244

[52] James P Lynch. 2006. Problems and Promise of Victimization Surveys for Cross-National Research. *Crime and justice* 34, 1 (2006), 229–287.

[53] Mary Madden. 2017. Privacy, Security, and Digital Inequality. *Data & Society* N/A, N/A (2017), 125.

[54] Tyler H. McCormick, Matthew J. Salganik, and Tian Zheng. 2010. How Many People Do You Know?: Efficiently Estimating Personal Network Size. *J. Amer. Statist. Assoc.* 105, 489 (March 2010), 59–70. https://doi.org/10.1198/jasa.2009.ap08518

[55] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-Rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–23.

[56] NortonLifeLock. 2019. *Cyber Safety Insights Report.* Technical Report. Norton. 3–9 pages.

[57] Simon Parkin, Elissa M. Redmiles, Lynne Coventry, and M. Angela Sasse. 2019. Security When It Is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change. In *Proceedings 2019 Workshop on Usable Security*. Internet Society, San Diego, CA, 2–10. https://doi.org/10.14722/usec.2019.23024

[58] Pew Research Center. n.d.. Questionnaire Design.

[59] Kathleen H. Pine and Max Liboiron. 2015. The Politics of Measurement and Action. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. Association for Computing Machinery, New York, NY, USA, 3147–3156. https://doi.org/10.1145/2702123.2702298

[60] Emilee Rader, Rick Wash, and Brandon Brooks. 2012. Stories as Informal Lessons about Security. In *Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS '12)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/2335356.2335364

[61] Elissa M. Redmiles. 2019. "Should I Worry?" A Cross-Cultural Examination of Account Security Incident Response. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, San Francisco, CA, 1107–1121. https://doi.org/10.1109/SP.2019.00059

[62] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2016. How I Learned to Be Secure: A Census-Representative Survey of Security Advice Sources and Behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16)*. Association for Computing Machinery, New York, NY, USA, 666–677. https://doi.org/10.1145/2976749.2978307

[63] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2017. Where Is the Digital Divide? A Survey of Security, Privacy, and Socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 931–936. https://doi.org/10.1145/3025453.3025673

[64] Elissa M. Redmiles, Sean Kross, and Michelle L. Mazurek. 2019. How Well Do My Results Generalize? Comparing Security and Privacy Survey Results from MTurk, Web, and Telephone Samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, Shanghai, China, 1326–1343. https://doi.org/10.1109/SP.2019.00014

[65] Elissa M. Redmiles, Amelia R. Malone, and Michelle L. Mazurek. 2016. I Think They're Trying to Tell Me Something: Advice Sources and Selection for Digital Security. In *2016 IEEE Symposium on Security and Privacy (SP)*. IEEE, Glasgow,

Scotland, 272–288. https://doi.org/10.1109/SP.2016.24
[66] Elissa M. Redmiles, Noel Warford, Amritha Jayanti, Aravind Koneru, Sean Kross, Miraida Morales, Rock Stevens, and Michelle L. Mazurek. 2020. A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX, Virtual, 89–108.
[67] Markus Riek, Rainer Bohme, Michael Ciere, Carlos Ganan, and Michel van Eeten. 2016. Estimating the Costs of Consumer-Facing Cybercrime: A Tailored Instrument and Representative Data for Six EU Countries. *Workshop on the Economics of Information Security (WEIS), University of California at Berkeley* 2016 (2016), 1–43.
[68] Matthew J. Salganik, Dimitri Fazito, Neilane Bertoni, Alexandre H. Abdo, Maeve B. Mello, and Francisco I. Bastos. 2011. Assessing Network Scale-up Estimates for Groups Most at Risk of HIV/AIDS: Evidence From a Multiple-Method Study of Heavy Drug Users in Curitiba, Brazil. *American Journal of Epidemiology* 174, 10 (Nov. 2011), 1190–1196. https://doi.org/10.1093/aje/kwr246
[69] Neil Salkind. 2022. Encyclopedia of Research Design. *SAGE Publications* Vols. 1-0 (Feb. 2022), N/A. https://doi.org/10.4135/9781412961288
[70] Yukiko Sawaya, Mahmood Sharif, Nicolas Christin, Ayumu Kubota, Akihiro Nakarai, and Akira Yamada. 2017. Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. Association for Computing Machinery, New York, NY, USA, 2202–2214. https://doi.org/10.1145/3025453.3025926
[71] Russell G Smith and Tabor Akman. 2008. Raising Public Awareness of Consumer Fraud in Australia. *Trends and issues in crime and criminal justice* AIC Trends & Issues in Crime and Criminal Justice, 349 (2008), 1–6.
[72] Elizabeth Sully, Margaret Giorgio, and Selena Anjur-Dietrich. 2020. Estimating Abortion Incidence Using the Network Scale-up Method. *Demographic Research* 43 (Dec. 2020), 1651–1684. https://doi.org/10.4054/DemRes.2020.43.56
[73] Rob Thomson and John Langley. 2004. Who Do Young Adult Victims of Physical Assault Talk to about Their Experiences? *Journal of Community Psychology* 32, 4 (2004), 479–488.
[74] Roger Tourangeau. 2003. Cognitive aspects of survey measurement and mismeasurement. *International Journal of Public Opinion Research* 15, 1 (2003), 3–7.
[75] UK Data Service. 2019. Crime Survey for England and Wales [Data File].
[76] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True" the Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. *Proceedings of the ACM on human-computer interaction* 2, CSCW (2018), 1–25.
[77] Jun Wang, Ying Yang, Wan Zhao, Hualin Su, Yanping Zhao, Yue Chen, Tao Zhang, and Tiejun Zhang. 2015. Application of Network Scale Up Method in the Estimation of Population Size for Men Who Have Sex with Men in Shanghai, China. *PLOS ONE* 10, 11 (Nov. 2015), e0143118. https://doi.org/10.1371/journal.pone.0143118
[78] Matthijs J Warrens. 2015. Five Ways to Look at Cohen's Kappa. *Journal of Psychology & Psychotherapy* 5, 4 (2015), 1.
[79] Rick Wash and Molly M. Cooper. 2018. Who Provides Phishing Training? Facts, Stories, and People Like Me. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. Association for Computing Machinery, New York, NY, USA, 1–12.
[80] Rick Wash and Emilee Rader. 2015. Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. SOUPS, Ottawa, Canada, 309–325.

APPENDIX

6 SURVEY PRETESTS

In pretest #1 (N=100), we tested the precision of our questions by first asking respondents to report any experience with a particular type of cybercrime incident (e.g., bank or credit card compromise) and then asking them to report in open-text if they had ever experienced other, similar incidents. This was to determine if our wording was adequately capturing each surveyed cybercrime category. Pretest #1 revealed that our initial question related to digital blackmail / extortion was too specific in the examples that we gave ("scammer threatens to release a victim's confidential information (e.g., passwords, photographs, browsing history) to friends, family, or the public"), and thus respondents were not reporting extortion incidents, which they mentioned in other sections of the survey, under the digital blackmail question. We refined our question wording to address this issue: "A scammer threatens to release a victim's confidential information (e.g., passwords, photographs, browsing history) to friends, family, or the public *or* holds a victim's computer, account, or confidential information hostage." Further, pretest #1 also revealed that the answer options for our banking and credit card compromise question were insufficiently specific: respondents were unsure how to report incidents in which their bank or credit card ultimately refunded them. Hence, for the bank account and credit card scams, we added an additional response option so that the choices were: the respondent was (1) a victim and lost money, (2) a victim but did not lose money, or (3) not a victim.

In pretest #2 we retested our survey to ensure our wording revisions were successful (n=301). While our wording revisions addressed specificity issues, in pretest #2 we identified another issue: respondents tended to report incidents as soon as they found a category that somewhat matched their experience (e.g., reporting credit card scams in the advanced fee section). We hypothesized that if we asked about the most common categories first, respondents would be less likely to misassign experiences. Someone who has experienced some form of cybercrime may be eager to describe that experience when participating in a survey on cybercrime victimization. A common type of cybercrime mis-categorized as a rare type will affect the accuracy of our estimates considerably. Thus, in pretest #3 (n=659) we ordered questions so that respondents were asked about the common categories first. When evaluating the accuracy of total reports across all categories we find that ordering the questions by rarity from most to least rare significantly improved reporting accuracy ($p = 0.01$, χ^2 statistic = 7.66, see Table 10 in the Appendix).

7 NETWORK SCALE-UP ESTIMATION

We calculate scale-up estimates of cybercrime prevalence by first computing the basic scale-up estimate, $\widehat{P}_H$:

$$\widehat{P}_H = \frac{\sum_{i \in s_F} y_{i,H}}{\sum_{i \in s_F} \hat{d}_i} \tag{5}$$

where $\hat{d}_i$ is the total degree (size of personal network) for person i, $y_{i,H}$ is person i's total number of connections to hidden population, and s_F is the sampling frame [28]. Respondents' degree is calculated using the *known population method* [47]. The known population

method involves collecting aggregate relational data for groups of known size and using this information to estimate respondents' personal network size. Intuitively, respondents who report more connections to these groups are more likely to have larger social networks. For this study, we use 12 groups of known size defined by first name (e.g., "Tina" or "Alan"); see Table 8 for the full list. We selected these names as they satisfy the scale-down condition [54], intuitively: they are representative of the demographic distributions of names in the U.S. For example, if 20% of the population is women between the ages of 30 and 50, approximately 20% of the people asked about should be women between the ages of 30 and 50.

As there is no publicly available demographic profile of first names in the U.S. [54], we estimated the number of people in the U.S. over age 18 with a given first name using the Social Security Administration baby names file, a 100% sample of persons born in the U.S. We use a life table from the Human Mortality Database to calculate the probability that a person survived to 2017 [39]. We then sum this estimate over all birth cohorts to estimate the total number of persons with a given name over age 18. We multiply the count of each name by 1.015 to account for population growth between 2017 and 2020.

To estimate a respondent's degree (personal network size), we use the known population estimator:

$$\hat{d_i} = \sum_{j=1}^{K} y_{ij} \times \frac{N}{\sum_{j=1}^{k} N_j} \tag{6}$$

where d_i is a degree (personal network size) of respondent i, y_{ij} is the number of connections between respondent i and group of known size j (e.g., people with first name "Rachel"), N is the total size of the population, and N_j is the known size of the subpopulation j [48]. Following past studies, we top-code all responses for the groups of known size to 30 to minimize sensitivity to outliers.

Names	
Adam	Paula
Alan	Rachel
Bruce	Ralph
Emily	Rose
Kyle	Tina
Martha	Walter

Table 8: Set of 12 names used in this network scale-up study. This set of names is recommended for scale-up studies as it satisfies the "scale-down" condition[54].

To assess the validity our network scale-up estimator, we perform an internal consistency check. As our survey asks respondents about how many people they know in 12 groups of known size (e.g., number of people named "Tina"), we can use network scale-up method to estimate the size of these 12 groups, holding out any knowledge of the true size of the group [68]. Figure 5 shows how the hold-out network scale-up estimates compare to the true known population size. Reassuringly, the estimates align closely with the true known values. This suggests that respondents, to the best of their ability, made accurate reports about others in their networks.

We next calculate the adjustment factors for the generalized network scale-up estimates. To calculate the visibility factor, we asked respondents who reported they were the victim of a cybercrime whether any of the people with the 12 names from the beginning of the survey knew that they had been a victim of the cybercrime.[9]

For our final analysis, we calculated two separate sets of adjustment factors, one for rare incidents, and one for common incidents. By pooling together data for the rare scam incidents, we can calculate a more stable estimate of the adjustment factors. However, this pooling has a cost; we are assuming that the average visibility and degree ratio are comparable within the rare scam group and common scam group. We perform variance estimation with a standard bootstrap procedure using 10,000 bootstrap samples.

Category	Degree Ratio	Visibility Ratio	Adj. Factor
Common Incidents	1.01	0.00872	113.02
Rare Incidents	1.31	0.0139	54.93

Table 9: Adjustment factors for generalized network scale-up (pooled).

8 LESSONS LEARNED FOR MEASURING CYBERCRIMES.

While we measured prevalence of six of the highest volume cybercrimes reported to law enforcement [42], in an effort to create an evidence-based practice of cybersecurity, future work should continue to assess the impact of cybercrime on individual internet users. The work presented here has revealed several methodological difficulties, and potential solutions, for ongoing measurement of cybercrimes by both governments [42] and researchers.

First, we underscore the importance of question wording. Technical terms like "advance fee fraud" or "non-delivery scam" (often used by security professionals to describe incidents) are unclear to users, and should be avoided. There were many cases of respondents lumping experiences into inappropriate categories in their responses. Some respondents will say they have been victim of non-delivery scam when what they received simply did not meet their expectations. Further, it is important to explicitly communicate to respondents whether they should report experiences that did not involve monetary loss. Some respondents answer affirmatively to questions about being a victim even if they simply received a phishing email or a Nigerian scam solicitation, but never actually engaged with the scammer or lost money. It is important for the computer security community and governmental bodies focused on measuring crime rates to align not only on the language used to carefully describe cybercrimes to respondents, but on which cybercrimes are important to measure. In our efforts to place our measurements in context with past work, we found significant discrepancies in how various cybercrimes were described and grouped, and found that some reports, especially those from the FBI and FTC

[9] In calculating visibility factors, we omitted three outlier cases where respondents reported telling every person in their 1,000+ person social network that they were the victim of a cybercrime.

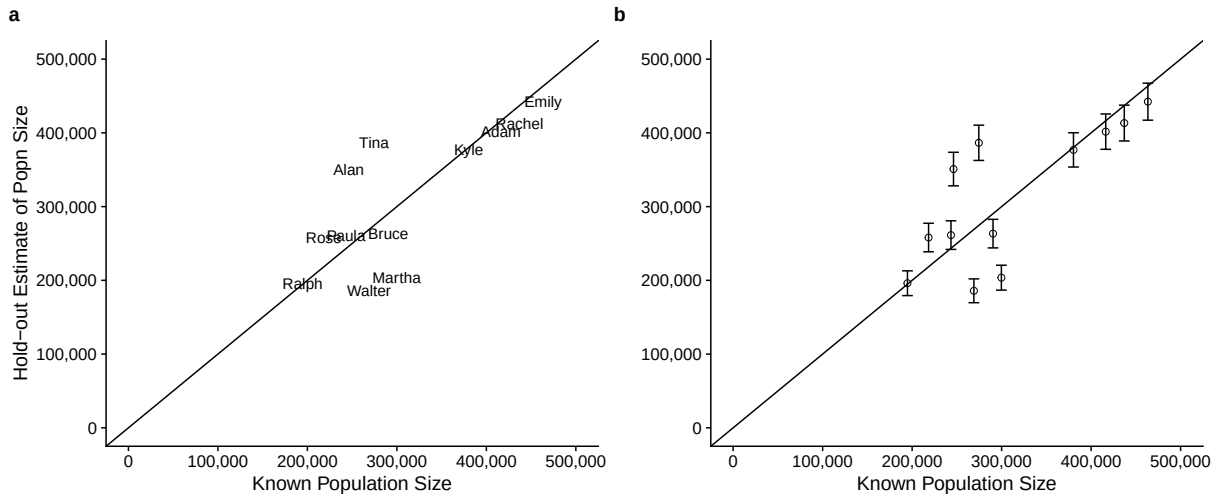


Figure 5: Internal validation check: Panel (a) shows comparison of the (hold-out) network scale-up estimates to true known population size for 12 groups. Panel (b) shows point estimates with 95% confidence intervals. The hold-out network scale-up estimates are generally similar to their true value, with no clear pattern of under or over-estimation.

in the U.S., changed their categories of cybercrime quite frequently, making longitudinal and comparative analysis very challenging.

Second, no matter how much care goes into recruiting high quality respondents and constructing the survey instrument, some respondents will answer carelessly. Respondents have incentives to complete the survey as quickly as possible. Most make good faith efforts to read, understand and answer carefully, but it is inevitable that a small percent will be hasty or careless. Respondents who give nonsense answers or enter random text (e.g., "asdf" etc) can be filtered out by a survey vendors quality control mechanisms, but careless or inattentive responses can be hard to detect. If 1-2% of respondents answer carelessly it would have minor effect when estimating phenomena that affect a large portion of the population, but it has a much more serious effect on estimates of rare things. Since several of the phenomena we study were experienced by less than 0.5% of the population annually, there is considerable need to sanitize the data.

Consider, for example, binary answers about experiencing a crime that actually affects 1% of the population. The number of respondents who can artificially inflate estimated prevalence is 99× the number who can artificially deflate it. For example, if 0.5% of respondents respond carelessly (or at random) it will have a small effect on the estimate of a phenomenon experienced by 15% of the population, but can have a catastrophic effect on the estimate of one experienced by 0.3%.

These issues suggest the need to replicate approaches taken in this work to: (a) be as precise as possible in describing incidents in lay terms, e.g., avoiding overly general questions such as "have you been the victim of identity theft", (b) create a comprehensive set of closed-answer choices to disambiguate how respondents characterize themselves as victims (e.g., have they lost money), (c) verify reports through coding of respondents' qualitative descriptions of the incident, and (d) carefully order questions to avoid respondents describing an experience under the first category they encounter that seems remotely relevant.

9 QUESTION ORDER

Our pretests demonstrated that respondents would often preemptively report an incident as soon as they found a category that loosely aligned with their experience. To avoid this, we reordered the questions in terms of frequency to minimize how often respondents preemptively reported a scam. Table 10 shows that in aggregate, reordering reduced the number of false positives reported in our pretests (χ^2 = 7.66, p = 0.01). For our final analysis, we ordered questions from most to least frequent.

10 WEIGHTED SAMPLE DEMOGRAPHICS

Table 11 presents the weighted sample demographics used in our analysis. Separate sets of statistical weights were constructed for the general sample and total sample.

	Ordered			Random				
Incident	Accepted	Reported	Accuracy	Accepted	Reported	Accuracy	χ^2 Statistic	P-Value
CC/Banking	165	206	80.1%	45	61	73.8%	1.12	0.29
Non-delivery	20	33	60.6%	7	16	43.8%	1.24	0.27
Non-payment	11	29	37.9%	4	16	25.0%	0.78	0.38
Advanced Fee	9	18	50.0%	1	8	12.5%	3.29	0.07
Overpayment	0	13	0.0%	1	7	14.3%	0.57	0.45
Total	205	299	68.6%	58	108	53.7%	7.66	0.01

Table 10: Comparison of coding accuracy for ordered pretest (N = 669) and random pretest (N = 301).

	General Sample		**Rare-Incident Sample**		**Total**	
	No.	%	No.	%	No.	%
Gender						
Male	484	48.3	4988	47.0	5773	48.3
Female	518	51.7	5632	53.0	6180	51.7
Age						
18-29	206	20.5	2023	19.0	2453	20.5
30-44	255	25.4	2706	25.5	3087	25.8
45-59	243	24.3	2625	24.7	2856	23.9
60+	298	29.8	3266	30.8	3557	29.8
Education						
<HS Equivalent	98	9.8	1032	9.7	1167	9.8
HS Equivalent	283	28.2	2892	27.2	3377	28.2
Some college	278	27.7	2884	27.2	3313	27.7
Bachelors	218	21.8	2178	20.5	2359	19.7
Advanced degree	125	12.5	1634	15.4	1736	14.5
Race						
White, non-Hispanic	629	62.8	6760	63.7	7506	62.8
Black, non-Hispanic	119	11.9	1252	11.8	1425	11.9
Other, non-Hispanic	16	1.6	143	1.3	163	1.4
Hispanic	167	16.7	1655	15.6	1992	16.7
2+, non-Hispanic	19	1.9	318	3.0	341	2.9
Asian, non-Hispanic	51	5.1	491	4.6	526	4.4
Income						
<$29,999	223	22.3	2629	24.8	2965	24.8
$30,000 to $74,999	373	37.2	4060	38.2	4579	38.3
$75,000 to $124,999	273	27.3	2463	23.2	2809	23.5
>$125,000+	133	13.2	1468	13.8	1600	13.4
Metro						
Non-Metro Area	123	12.2	1793	16.9	1967	16.5
Metro Area	879	87.8	8827	83.1	9986	83.5
Marital Status						
Married	519	51.8	5195	48.9	5790	48.4
Widowed	31	3.1	394	3.7	422	3.5
Divorced	103	10.3	1072	10.1	1184	9.9
Separated	44	4.4	474	4.5	529	4.4
Never married	247	24.6	2666	25.1	3111	26.0
Living with partner	58	5.8	819	7.7	917	7.7
Total	1002	100	10951	100	11953	100

Table 11: Sample descriptive statistics (weighted). Sample collected from NORC's Amerispeak panel.

11 SURVEY QUESTIONS

The full survey instrument is presented on the following pages.

Intro

Thank you for taking the time to consider volunteering in a Microsoft Corporation research project. This survey we will be asking you about your online experiences in the past two years.

People have many different experiences online, understanding your experiences will help us do better science and keep people safer online. Please do your best to answer these questions completely.

Screener Question

We are now going to ask about a few experiences you've had online. Please answer to the best of your ability.

Have you had any of the following experiences in the past two years?

	Yes	No	I don't know
Someone made fraudulent charges on your credit or debit account or stole money directly by accessing your bank account. (Either resolved by the bank or you lost money.)	○	○	○
Someone overpaid for something you sold online, and asked for the excess amount to be refunded. After you refunded the excess amount, you found out the original payment method was invalid (credit card stolen, check bounced, etc.) and lost money.	○	○	○
You sold a product or service online, but never received payment from the buyer.	○	○	○

	Yes	No	I don't know
You paid an advanced fee for a promised monetary reward (e.g., $1,000) or product (e.g., TV, cruise). After paying the advanced fee, you never received the money or product promised and lost money.	○	○	○
You paid someone money in exchange for either not releasing your confidential information (e.g. passwords, photographs, browsing history) to the public and/or to return computer / account / information.	○	○	○
You bought a product online and paid using an unexpected payment mechanism (e.g., Western Union, gift cards, Bitcoin). After being paid, the product or service was never delivered.	○	○	○

Web use skills

How familiar are you with the following computer and Internet-related items? Please choose a number between 1 and 5 where 1 represents "no understanding" and 5 represents "full understanding" of the item.

	1 - None	2	3	4	5 – Full
Advanced Search	○	○	○	○	○
PDF	○	○	○	○	○
Spyware	○	○	○	○	○
Wiki	○	○	○	○	○
Cache	○	○	○	○	○
Phishing	○	○	○	○	○

Personal Network Size Block 1

We are now going to ask some questions about people you know.

These people should be:

- **People over 18 who live in the United States**
- **People you know, by sight and by name, and who also know you by sight and name**
- **People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years**

Please write the total number in the box below. Please consider only people who have this *exact* name (spelled in the way shown).

Giving accurate answers to these questions is extremely important for the accuracy of our science! Thank you for your help.

How many people named **Kyle** do you know?	
How many people named **Walter** do you know?	
How many people named **Ralph** do you know?	
How many people named **Bruce** do you know?	

Personal Network Size Block 2

We are now going to ask some questions about people you know.

These people should be:

- **People over 18 who live in the United States**
- **People you know, by sight and by name, and who also know you by sight and name**

- **People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years**

Please write the total number in the box below. Please consider only people who have this *exact* name (spelled in the way shown).

Giving accurate answers to these questions is extremely important for the accuracy of our science! Thank you for your help.

How many people named **Emily** do you know?	
How many people named **Martha** do you know?	
How many people named **Rachel** do you know?	
How many people named **Paula** do you know?	

Personal Network Size Block 3

We are now going to ask some questions about people you know.

These people should be:

- **People over 18 who live in the United States**
- **People you know, by sight and by name, and who also know you by sight and name**
- **People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years**

Please write the total number in the box below. Please consider only people who have this *exact* name (spelled in the way shown).

Giving accurate answers to these questions is extremely important for the accuracy of our science! Thank you for your help.

How many people named **Rose** do you know?

How many people named **Alan** do you know?

How many people named **Adam** do you know?

How many people named **Tina** do you know?

Advanced Fee Description Qn

In the past two years, have you been the victim of an advanced fee scam?

Advanced fee scams occur when a scammer asks the victim for fees before providing a promised prize or reward (e.g., $1,000, a TV, a cruise). After the victim pays the fees, the scammer never actually sends the prize or reward that they promised.

- ○ Yes, I have been the victim of an advanced fee scam (and lost money)
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Non-Payment Description Qn

In the past two years, have you been the victim of a non-payment scam?

Non-payment scams occur when the victim sells a product or service, but never receives payment from the scammer buying the goods.

- ○ Yes, I have been the victim of a non-payment scam (sold goods and never received payment)
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Extortion Description Qn

In the past two years, have you been the victim of an extortion scam on the internet?

Extortion scams occur when a scammer either:

- Threatens to release a victim's confidential information (e.g. passwords, photographs, browsing history) to friends, family, or the public
- Holds a victim's computer, account, or confidential information hostage

The scammer then asks for money in exchange for either not releasing the victim's information or returning the computer/account/information to the victim.

- ○ Yes, I have been the victim of an extortion scam on the internet (and lost money)
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Overpayment Description Qn

In the past two years, have you been the victim of an overpayment scam?

Overpayment scams occur when a scammer overpays for something a victim is selling online. The scammer then asks for the excess amount to be refunded. Once the excess amount is refunded, it is discovered that the original payment method is invalid (credit card stolen, check bounced, etc.)

- ○ Yes, I have been the victim of an overpayment scam (and lost money)
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Overpayment Visibility Qn

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with an **overpayment scam** to describe what happened?

- Yes
- No
- I don't know

How many of these [ ] people do you think know enough information about your experience with an **overpayment scam** to briefly describe what happened?

How sure are you about your answer to the last question?

Extortion Qn Visibility

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with an **extortion scam** to briefly describe what happened?

- ○ Yes
- ○ No
- ○ I don't know

How many of these [ ] people do you think know enough information about your experience with an **extortion scam** to briefly describe what happened?

How sure are you about your answer to the last question?

Advanced Fee Visibility Qn

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with an **advanced fee scam** to briefly describe what happened?

- ○ Yes
- ○ No
- ○ I don't know

How many of these [ ] people do you think know enough information about your experience with an **advanced fee scam** to briefly what happened?

How sure are you about your answer to the last question?

Non-Payment Visibility Qn

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with a **non- payment scam** to briefly describe what happened?

- ○ Yes
- ○ No
- ○ I don't know

How many of these [ ] people do you think know enough information about your experience with a **non-payment scam** to briefly describe what happened?

How sure are you about your answer to the last question?

Banking / Credit Card Description

In the past two years, have you been the victim of a banking, credit, or debit card scam?

Banking scams occur when a scammer makes fraudulent charges on the victim's credit or debit account or directly steals money by accessing their bank account.

- ○ Yes, I have been the victim of a banking, credit, or debit card scam (and lost money)
- ○ Yes, I have been the victim of one of these scams **but** my bank or credit card company paid me back or the charges never cleared
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Banking / Credit Card Network Scale-up

Do you know anyone who was the victim of a banking, credit, or debit card scam on the internet in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name
- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years
- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have paid or lost money in a banking, credit, or debit card scam in the last two years.

You reported that you know [ ] person(s) who have been the victim of a banking, credit, or debit card scam on the internet.

Can you describe to us the scam(s) these people experienced?

How many of these **[ ]** people lost money (were **not** paid back by the bank or credit card company)?

In total, how much money would you estimate that
these **[ ]** people lost (were **not** paid back by the bank or credit card company) from these experience(s)?

Non-Delivery Description Qn

In the past two years, have you been the victim of a non-delivery scam?

Non-delivery scams occur when a scammer requires the victim to use an unexpected payment mechanism (e.g., Western Union, gift cards, Bitcoin). After being paid, the scammer never delivers the product or service.

- ○ Yes, I have been the victim of a non-delivery scam (paid money and did not receive the goods)
- ○ No
- ○ I don't know

How much money would you estimate you lost in total from this experience?

Can you describe to us what happened?

Non-Delivery Scale-up

Do you know anyone who was the victim of a non-delivery scam on the internet in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name
- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years
- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have paid or lost money in a non-delivery scam in the past two years.

You reported that you know [ ] person(s) who have been the victim of a non-delivery scam on the internet.

In total, how much money would you estimate that these people lost from these experience(s)?

Can you describe to us the scam(s) these people experienced?

Non-Payment Scale-Up

Do you know anyone who was the victim of a non-payment scam on the internet in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name
- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years
- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have paid or lost money in a non-payment scam in the last two years.

You reported that you know [ ] person(s) who have been the victim of a non-payment scam on the internet.

In total, how much money would you estimate that these people lost from these experience(s)?

Can you describe to us the scam(s) these people experienced?

Advanced Fee Scale-up

Do you know anyone who was the victim of an advanced fee scam on the internet in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name
- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years
- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have paid or lost money in an advanced fee scam in the last two years.

You reported that you know [ ] person(s) who have been the victim of an advanced fee scam on the internet.

In total, how much money would you estimate that these people lost from these experience(s)?

Can you describe to us the scam(s) these people experienced?

Overpayment Scale-up

Do you know anyone who was the victim of an overpayment scam in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name

- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years
- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have paid or lost money in an overpayment scam in the past two years.

You reported you know [ ] person(s) who have been the victims of overpayment scams.

In total, how much money would you estimate that these people lost from these experience(s)?

Can you describe to us the scam(s) these people experienced?

Extortion Scale-up

Do you know anyone who was the victim of an extortion scam on the internet in the last two years?

These people should be:

- People over 18 who live in the United States
- People you know, by sight and by name, and who also know you by sight and name
- People you have had some contact with — in person, over the phone, or over the computer — in the past 2 years

- People who told you enough information about the scam that you can describe their situation

Please report the number of people you know who have been the victim of an extortion scam on the internet in the last two years.

You reported that you know [ ] person(s) who have been the victim of an extortion scam on the internet.

In total, how much money would you estimate that these people lost from these experience(s)?

Can you describe to us the scam(s) these people experienced?

Non-Delivery Visibility Qn

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with an **non- delivery scam** to briefly describe what happened?

- ○ Yes
- ○ No
- ○ I don't know

How many of these [ ] people do you think know enough information about your experience with an **non-delivery scam** to briefly describe what happened?

How sure are you about your answer to the last question?

Banking / Credit Card Visibility Qn

To help us better understand scams on the internet, we're going to ask a few questions about the [ ] people you reported knowing named Adam, Alan, Bruce, Emily, Kyle, Martha, Paula, Rachel, Ralph, Rose, Tina, or Walter.

We'll never use this information to try to identify these people. We only want to better understand scams on the internet.

Do any of these [ ] people know enough information about your experience with a **banking, credit, or debit card scam** to briefly describe what happened?

- ○ Yes
- ○ No
- ○ I don't know

How many of these 0 people do you think know enough information about your experience with a **banking, credit, or debit card scam** to briefly describe what

happened?

How sure are you about your answer to the last question?