“Hello. This is the IRS calling.”: A Case Study on Scams, Extortion, Impersonation, and Phone Spoofing

Morvareed Bidgoli
College of Information Sciences and Technology
The Pennsylvania State University
University Park, PA, United States
mbidgoli@psu.edu

Jens Grossklags
Department of Informatics
Technical University of Munich
Munich, Germany
jens.grossklags@in.tum.de

Abstract—**Fraud has existed long before the advent of modern technology; however, we can increasingly observe how this profit-driven enterprise is entering the cyberspace. Our paper focuses on a case study of two scam schemes targeting international students at Penn State. The scams have been perpetrated in either a physical (i.e., phone scam) or online (i.e., Craigslist scam) form. However, this dichotomy becomes blurry when examining the phone scams more closely since they often employ cyber elements (e.g., phone spoofing, requests of electronic payment) to mask the scammer’s tracks and identity. Our study aims to better understand the nature of the scams and how international students contextualize their scam experiences. We place particular emphasis on investigating what students’ decision-making processes are behind filing a report about their scam experiences. We also explore the predominantly used reporting avenues by those international students who filed reports. In the first part of our study, we present a qualitative analysis of Penn State campus police reports of scam incidents covering three years of data (2014-2016). Aside from being able to understand the prevalence and details of the experienced scams, the analysis of the data also helps to unpack the motivations behind why international students file reports to entities like campus police particularly in the event that an inchoate crime was experienced. Furthermore, working with the data lays the groundwork for the second half of our study, a 16-person in-depth interview series with international students who experienced a scam while studying at Penn State. The results of our case study will show the fundamental impact of increased awareness in preventing international students from falling victim to the scams they encountered. However, opportunities still remain in terms of effectively increasing knowledge about how such incidents can be officially reported to law enforcement and how currently existing cybercrime reporting mechanisms can be improved to further bolster cybercrime reporting to take place.**

Keywords—interview study; scams and fraud; cybercrime; international students; victimization, cybercrime reporting; awareness

I. Introduction

We live in a world of constant technological interconnectivity, which increases our susceptibility to becoming victims of cybercrimes. A given cybercrime incident can have severely debilitating effects on its victims as evidenced by statistics provided by the Internet Crime Complaint Center (IC3), a formal U.S. cybercrime reporting entity. According to the IC3’s 2015 Internet Crime Report, the center received 288,012 complaints associated with a reported total loss of $1,070,711,522 [1]. Among the total complaints received, 127,145 complaints (~44%) reported an average financial loss of $8,421 [1].

This data likely underappreciates the true magnitude and diversity of cybercrimes facing computer users and businesses. One of the key reasons for such an incomplete picture is the haphazard reporting of incidents, which has been noted by the literature. This is worrisome since a multitude of important information can be derived from each cybercrime report such as the prevalence of cybercrimes, the types and nature of the cybercrimes present, and the various resulting types of loss or harm (e.g., financial, psychological, emotional). Furthermore, reporting may also foster the development of prevention tips on how to mitigate future cybercrime risk. Therefore, better understanding the reasoning behind cybercrime victims’ reporting behaviors is crucial. Unfortunately, there is a lack of research that has offered solutions to overcoming this problem particularly with regards to encourage reporting by computer users.

In this paper, we present a two-part qualitative case study of international college students at Penn State who have been victims of primarily two scam schemes: (1) telephone scams where the caller impersonates a high level government agency or law enforcement officer and utilizes a combination of techniques that are of physical (i.e., phone) and/or online nature (i.e., phone spoofing) in order to extort payment in return for assurance that the international student in question will not be immediately arrested or deported out of the country, and (2) students who were interested in subleasing their apartments over the summer and were scammed by purported tenants on Craigslist to send back “excess” payment money that was initially sent via fraudulent checks to cover the proposed rent amount. The significance of these scam schemes was initially brought to our attention through a series of informal conversations we have had with Penn State campus police over the course of two semesters.

In the first part of the paper, we analyzed Penn State campus police report data from 2014-2016 (i.e., 79 reports in total, which consisted of over 50 reports from students who have been targeted by scammers). We initially wanted to collect this data in order to understand what the students' motivations were for reporting their scam experiences to campus police. The data also allowed us to gain insights about incidents where an *inchoate* crime occurred; an incident where the student was targeted, but did not fall victim to the crime. To our knowledge, this is an area that has not been thoroughly explored by the literature. An additional purpose of analyzing these reports was to understand the nature of the diverse scam schemes that have specifically affected the *international* student campus community, what the motivations were behind why the victim decided to file a report with campus police, and the avenue in which they decided to file the report (i.e., via telephone, online form, or in-person walk in).

The analysis of the reports laid the foundation for the second part of our study where we report the results of 16 semi-structured interviews with Penn State international college students in order to unpack their scam experiences, which will provide further insights into the students' thought processes during and after they experienced an online scam (e.g., whether and when they recognized they were a victim of a scam scheme and what considerations played a role in deciding whether to report their victimization or not).

The results from this two-part case study address the following research questions:

RQ #1: What is the nature of the recent scam schemes affecting international college students on campus?

RQ #2: How do international college students contextualize their scam experiences (e.g., do they feel specifically targeted by the prevalence of such scam schemes)?

RQ #3: What are the motivations behind international college students' decisions to file a report particularly in the event an inchoate crime was experienced?

RQ #4: Through what avenues (i.e., telephone, online form, in-person walk-in) did international college students report their scam victimizations and which reporting avenues do they generally prefer to file reports through?

RQ #5: What impact have cybercrime awareness campaigns disseminated by on campus entities interacting with international students had?

By focusing on how scammers are targeting and affecting international students, we provide the first study, which focuses on this specific computer user population in the context of cybercrime. International students may be particularly challenged by scam schemes since they find themselves in a new cultural environment and may be unaware of standard U.S. legal procedures and conduct. Furthermore, they may face unique perceived and actual hurdles regarding their willingness and ability to come forward and report incidents to law enforcement. These factors may heighten the importance that awareness plays in effectively educating the international student community about cybercrimes, but may also offer insights into how to communicate with diverse groups to recognize cybercrimes and foster cybercrime reporting.

This paper is structured as follows. We will begin by presenting relevant literature mainly with regards to the issue of cybercrime reporting (Section II). Next, we will present the results from our qualitative analysis of Penn State campus police's 2014-2016 report data (Section III). Subsequently, we will present the results from 16 semi-structured interviews we conducted with international college students (Section IV). Finally, we discuss our findings (Section V) and offer concluding remarks (Section VI).

II. Related Work

In this section, we will discuss related work that is focused on online fraud and the reasons behind why cybercrimes and online fraud are underreported. We place a particular focus on the literature that explains the reasoning behind the underreporting of cybercrimes since it is one of the primary focuses of our study to better understand international college students' decision-making process when it came to reporting the scams they experienced. While there will be some corollaries between the literature and the reasons provided by international students in our study, we provide additional reasons as to why international students made the decision not to file a report about their scam experiences.

A. Defining Cybercrimes and Online Fraud

Since we are introducing and discussing the nature of two scam schemes that have affected the international student campus community, we believe it is worth mentioning the relevant terminology as it pertains to the scams in question. Given that the two scams employ to some extent or entirely online means for financial gain, defining online fraud is pertinent, which the FBI defines as

> "…any fraudulent scheme in which one or more components of the Internet, such as web sites, chat rooms, and e-mail, play a significant role in offering non-existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices, or other items of value to the control of the scheme's perpetrators" [2].

It is worth noting that online fraud comes in various forms some of which are highlighted throughout the IC3's annual Internet crime reports and website. Commonly known examples of online fraud include (but are not limited to) credit card fraud, phishing, pharming, Nigerian prince scam (also known as advance fee fraud), auction fraud, romance scams, and impersonation scams. Since online fraud is an example of a cybercrime, it is also important to state what constitutes a cybercrime. For example, Wall [3] defines cybercrime as acts "in which the perpetrator uses special knowledge of cyberspace." More simply, cybercrime is a term typically used to describe "…the use of computer technology to engage in illegal activity" [4, p. 15]. Cybercrimes have been categorized in various ways as well. For instance, Clifford [4] distinguishes between three categories: crimes in which the computer is the target of the criminal activity, crimes in which the computer is the tool of the criminal activity, and crimes in which the computer is incidental to the criminal activity (only plays a minor role) (pp. 17-21). Based on this categorization, Clifford classifies online fraud as a "tool" cybercrime since technology is viewed as a facilitator to the perpetration of the fraud in question.

Properly defining and classifying cybercrimes is a particularly daunting task notably since the law does not advance at the same rate as technology. With the given case study at hand, we also find it hard to definitively classify a scam scheme such as the phone scams since it utilizes both physical and online means to commit fraud. As we will point out later on, such definitional issues can impact the likelihood that such cybercrimes will be reported to law enforcement.

B. *Online Fraud Victimization*

We observe that there are a number of studies that have tried to account for the various risk factors that make victims susceptible to scams. For example, although telemarketing fraud is not the subject of the study at hand, it exhibits certain similarities with regards to how it is designed to the phone scams we cover in this paper. According to the an AARP survey conducted on 745 telemarketing fraud victims, they found that 56% were 50 years or older [5]. Some reasons as to why elderly people are particularly at risk of experiencing scams is due to their reduced cognitive ability and social isolation [6]. According to the AARP, older adults are also significantly more susceptible to be victims of investment fraud, lottery fraud, and prescription drug/identity theft fraud [7, p. 25]. Additionally, they are less likely to both acknowledge and report such fraud incidents in relation to individuals under the age of 55 [7, p. 5]. While we are not researching elderly people in our study, we do acknowledge that fraud schemes overall set out to exploit certain characteristics of a given population in order to further their criminal agenda whether it be the age or the immigration status of an individual. In terms of mitigating one's susceptibility to such fraud, having knowledge about scams is central [5], [6].

There have been a number of scam studies that have examined the nature of scams somewhat similar to the phone scams covered in our study such as technical support scams (see [8]) and post-transaction marketing scams (see [9], [10]). However, the closest qualitative fraud study we could find that relates to our study's objectives was a study conducted by Cross et al. [11]. In this study, the researchers conducted an 80-person interview study with victims of online fraud who lost $10,000 or more in order to examine the impacts/harm experienced as a result of the fraud they experienced, the reasons for choosing to report the fraud they experienced, and how their support needs can be met. One notable difference between the Cross et al. study and our study is our choice to examine how scams have affected a specific demographic: international college students. We believe that the demographic makeup of our subject pool affects not only the degree to which they are vulnerable to the scams they experience, but also impacts the actions they choose to take post-victimization (i.e., reasoning to report). Moreover, there is also a difference in the types of fraud that are covered in the Cross et al. study (e.g., romance fraud) and ours, which can also be attributed to the fact that there is a difference in the demographic makeup between our studies where they chose to examine adults between the ages of 30-77 and we cover a much younger age demographic. Therefore, it should not come as a surprise that online fraud schemes are tailored in a way so that the scammer can reap the largest rewards from their scam scheme.

C. *Reasons for the Underreporting of Cybercrimes*

The underreporting of cybercrimes is a well-researched issue. The literature provides a number of reasons as to why crimes both online and offline go unreported. Before delving into the reasons behind why online fraud goes unreported, it is worth mentioning the literature that discusses the reasons behind why cybercrimes in general go unreported. One well cited reason why cybercrimes go unreported is that a victim may consider the cybercrime they experienced to lack enough severity to warrant contacting law enforcement [12], [13]. Goucher [14] cites a number of reasons why cybercrimes go unreported such as the victim believing reporting is "a waste of time and effort," that there is a low likelihood the cybercriminal will get caught, that the victim blames themselves for falling for a cybercrime, and that the victim does not want to be labeled as a "victim" (p. 17). Yar [12], Wall [13], and Goodman & Brenner [15] state that a victim may simply be unaware that they experienced cybercrime, which may be explained by Fafinski et al.'s [16] reasoning that computer users lack the proper amount of expertise to understand the nature of currently existing cybercrimes (p. 14). Both Wall [13] and Goodman & Brenner [15] state that a feeling of embarrassment over being a cybercrime victim can also lead to a cybercrime going unreported. Moreover, cybercrime victims may lack the proper expertise to know how to report cybercrimes [13], [14]. Lastly, Wall [17] points out that with the onset of new reporting mechanisms like in countries such as the United States (i.e., the IC3), it will take some time for such mechanisms to gain traction (p. 194).

D. *Reasons for the Underreporting of Online Fraud*

As previously outlined by some of the statistics gathered by the IC3's latest report, online fraud is an increasing issue within the cybercrime context. Not only are instances of online fraud costly for victims, but they also have a history of being unreported by victims. In fact, according to the IC3, "only an estimated 15 percent of the nation's fraud victims report their crimes to law enforcement" [1]. Moreover, a few reasons why online fraud goes unreported were corroborated by previously mentioned reasons for why cybercrimes in general go unreported (i.e., [13]–[15]) such as the victim feeling a sense of self-blame, shame, or embarrassment over falling victim to online fraud [18]–[20]. The perceived embarrassing nature of being an online fraud victim can also contribute to a victim's worry over the stigma they can potentially receive from a fellow family member, which can also contribute to not reporting an online fraud incident [21]. A victim may also not know who to report the online fraud to [13], [18]. A lack of awareness or knowledge of a cybercrime can lead to a particular cybercrime going unreported [22]; for example, Fafinski et al. [16] provides an example where a victim can mistake the hacking of their email for phishing (a form of online fraud) depicting how there is a crucial need to promote proper cybercrime education to computer users (p. 14).

As briefly outlined before, there is also the issue of how cybercrimes are defined and categorized not just in an academic or legal sense, but also how computer users and victims at large perceive them. Al-Nemrat et al. [23] discusses how despite the fact that many believe they know what cybercrimes are, there is a lack of definitional clarity of what it actually constitutes, which can greatly impact both the cybercrime reporting and investigation process. Smith and Budd [22] also discuss the definitional issue by stating that different studies may be researching different types of online fraud, which makes it difficult to compare the results from various studies on the subject. To help illustrate and further elaborate on how problematic this definitional issue can be in terms of contributing to the underreporting of cybercrimes, upon comparing the classification of two different studies on phishing, Wall [20] classified phishing as a form of SPAM involving income generating claims (e.g., Nigerian Advanced Fee scams) email contents while Smith & Budd [22] classified phishing as a form of online fraud. While both of these classifications of phishing seem plausible, it is hard to imagine that computer users and more importantly cybercrime victims will be able to decipher one cybercrime from another if academics cannot seem to do so themselves.

Despite the fact that there have been a multitude of reasons provided by the literature as to why cybercrimes have gone reported, there remains to be research done on better understanding victims' cybercrime reporting behaviors. Thus, it is the focus of this study to further examine victims' cybercrime reporting behaviors by specifically looking at how a sample of the computer user population (i.e., international college students) contextualize their victimizations whether they are choate or inchoate. Vital information can be deduced by qualitatively examining campus police report data such as a reporter's motivation to report, their understanding of computers and cybercrimes, and the resulting impacts the victimization had on them.

III. Campus Police Report Data

After numerous and extensive conversations over the course of two academic semesters with various stakeholders that are involved with the acquisition and storage of campus police report data, Penn State campus police granted us access to a subset of three years of report data from 2014 to 2016. The data was extracted by campus police staff members based on our study objective, which was to analyze relevant reports that entailed instances of scams that affected the campus population. Prior to receiving this dataset, campus police redacted all personally identifiable information (PII); however, basic demographic information such as the age, status of the reporter (i.e., student or employee), race, and gender were provided.

This dataset was qualitatively analyzed while following an approach similar to Amarijo et al. [24] through the creation of basic *victim profiles* including information such as demographics (e.g., gender) and the characteristics of the crime (e.g., means of commission, classification of the crime). However, our analysis goes a step further by also focusing on victims' reporting behaviors. By scrutinizing the report data in its raw form, we could ascertain information such as whether the reported crime was choate or inchoate and what the reporter's motivation was to report the crime. In summary, upon qualitatively analyzing the data, we sought to extract a series of important details from each report, which included the following:

- reporter's gender,
- type of scam scheme (e.g., phone scam, online scam),
- method of reporting (i.e., in-person/walk in, phone, email, web form, in-person response/follow up by officer), and
- whether the crime was completed along with the amount of financial loss or inchoate (i.e., not successful).

In the event that some of these details were unclear or not provided, an "unknown" code was given. Additionally, a number of reports were excluded from analysis because the report in question was not deemed relevant to the study at hand (e.g., the incident was not considered to be a scam, lacked enough detail in order for a proper analysis to be made, or the incident did not involve a student). Campus police provided a total of 79 reports; however, only 53 reports were analyzed (26 reports were excluded from analysis). We would like to note that the report data that was given to us has a few limitations. First, despite the fact that the race of the reporter was provided in many of the reports, we are unable to definitively denote whether the student reports we included in our analysis involved an international student or a domestic student. Additionally, by qualitatively analyzing such reports in their raw form, we noticed that there are variations in the level of detail that was provided between the reports in terms of the information that was provided, which makes it particularly hard for analyses purposes in the event that information is missing or simply unclear (e.g., the avenue to which a report was filed). We conjecture that such variations are simply a byproduct of how report information is collected between officers and the extent to which victims are forthcoming with the information they provide at the time of filing a report. We have consolidated three types of information from the reports: gender, crime type, and method of reporting that are subsequently outlined in Tables I-III below.

The results in Table I indicate that across gender there is an even split between males and females when it comes to the number of reports which suggests that cybercriminals target both genders and that individuals are susceptible irrespective of gender (however, perhaps not in the same way). We observe this finding to be consistent with the breakdown provided by some of the IC3's most recent Internet Crime Reports [25], [26]. While race was a piece of demographic information that was denoted across a number of reports, we cannot conclusively discern what reports were filed on behalf of an international student versus a domestic student on this criteria alone; thus, for the exploratory purposes of utilizing this data we simply decided to include all relevant reports that were reported on behalf of a student.

TABLE I. GENDER (2014-2016)

Female	30 (56.6%)
Male	23 (43.4%)

As evidenced by Table II, the most prevalent reported scams were phone scams. Over the past three years, in these scams scammers frequently employ extortion and/or impersonation techniques. A typical scam caller impersonates a government official (i.e., FBI, local police, campus police, IRS), and, for example, would proceed to claim that the victim owes back taxes in X amount (predominantly about a few hundred or thousands of dollars). The stated threat is that if the targeted victim would not pay their fines immediately then they would be arrested by law enforcement authorities or have their visa revoked and would subsequently be deported out of the country. In order to further legitimize their claims, the scammers also often utilize phone spoofing techniques to mimic legitimate numbers that are affiliated with the governmental agencies they are impersonating. In other instances, the scammers simply block their numbers entirely and appear as an "unknown" caller. As described by the reporters, the callers often had an accent, which to them sounded Middle Eastern or Indian, and they were predominantly male.

TABLE II. CRIME TYPE (2014-2016)

Phone Scams	44 (83.0%)
Online Scams (e.g., phishing, extortion)	6 (11.3%)
Craigslist Scam	2 (3.8%)
Extortion via Phone	1 (1.9%)

Walk-ins at the campus police station, phone, and in-person response/follow ups made by campus police officers were the most prevalent ways in which reports were filed and addressed (see Table III). Interestingly, the web form was among one of the least utilized ways in which reports were filed, which may provide some insights into how formal cybercrime reporting mechanisms like the IC3 may need to rethink the ways in which they choose to allow cybercrime victims to file reports since reports are currently only able to be filed through an online form on the IC3's website.

TABLE III. METHOD OF REPORTING (2014-2016)

Walk-in/In-person	15 (28.3%)
Phone	13 (24.5%)
Web Form	3 (5.7%)
Email	1 (1.9%)
In-person Response/Follow Up by Officer	10 (18.9%)
Combination of Different Report Types	3 (5.6%)
Unknown Report Type	8 (15.1%)

Out of the 53 reports we analyzed, *only* 12 were choate crimes. For the most part loss was either monetary in nature or involved payment through gift cards (e.g., iTunes) and ranged from a couple of hundred dollars to a couple of thousand dollars. In the case with the largest reported financial loss, a male student was a victim of a phone scam where the caller impersonated being an agent from the United States tax office in Philadelphia claiming the student owed current education taxes and threatening that non-payment would result in being sent to jail. The student was given two options: to pay the fines now or go to court and pay the fines. The student subsequently made the decision to pay the fines via MoneyGram at a Walmart store in three different cash amounts (i.e., $1,950.00, $1,750.00, and $1,800.00) ultimately resulting in a total loss of $5,610.00. Additionally, the scammer asked the student to email a photocopy of his passport and a photo of himself to which the student obliged.

In some reports, the reporters provided an indication as to why they were filing a report with campus police. The reasons that were provided included that the reporter wanted to affirm that they were not in trouble, ensure that their information was safe, or help to make sure that no other person would fall for the same scam.

IV. Semi-Structured Interviews

For the second part of our study, semi-structured interviews were conducted with international college students in order to better understand the nature of the scam schemes that are affecting the international student campus community, how international students contextualize their scam experiences, and what their decision-making process was in terms of reporting the incident. Prior to conducting the interviews, IRB approval was attained from Penn State's IRB (Study #: 00006176). The participation requirements were as follows: participants had to be 18 years or older, a current undergraduate or graduate international student at Penn State, have a good command of English, and have experienced a scam during their college experience at Penn State. Recruitment was done through a series of channels such as social media posts, emails sent out to students from professors we knew, and emails sent out by campus entities that support and provide resources specifically to international students (i.e., the Directorate of International Students and Scholar Advising (DISSA)). Prospective participants were screened prior to participating in an interview in order to ensure that they met the study's participation requirements. In the end, 17 semi-structured interviews were conducted; however, one interview (i.e., interviewee #14) was excluded from the analysis process since the student had only experienced scams prior to arriving at Penn State at another institution. Of the 16 subjects that were included in the qualitative analysis, eight students were male and eight students were female. In terms of academic status, there were six undergraduate students and 10 graduate students (7 PhD students, 3 Master's students). The study participants were a diverse sample of the world population with the most represented continent being Asia: India (5), China (3), Hong Kong (1), Iran (1), Venezuela (1), Germany (1), Poland (1), Brazil (1), Israel (1), and South Korea (1).

Upon receiving written (signed) consent from every interviewee, all interviews were audio recorded. Participants were compensated for their time with a $10 Starbucks gift card at the conclusion of the interview. After all interviews were completed, the interviews were subsequently transcribed and coded. The transcripts are anonymous in that each interview is coded with a number in the order they were conducted in (i.e., interviewee #1, interviewee #2, and so forth), and transcripts include no other information that allows for non-trivial linkage to interviewees' identities.

The interview questions that were asked stem from two sources: (1) a subset of questions that we had previously asked in an exploratory mixed methods study focused on better understanding the extent to which undergraduate students are affected by cybercrimes [27], and (2) the main takeaways we gained from our qualitative analysis of the campus police report data. The interviews were semi-structured and allowed for follow-up questions and clarifications.

At the conclusion of the analysis process, five themes emerged from the interview data, which will be described subsequently in detail.

A. Utilization of Preventative Measures

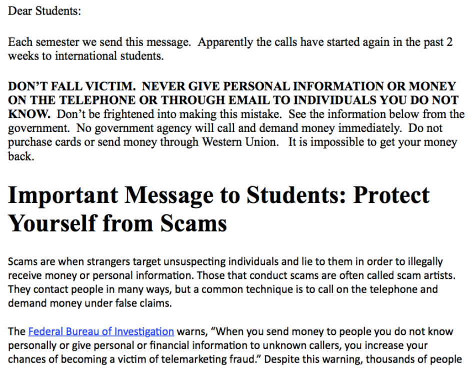
While we recognize that in the context of scams and fraud one of the best preventative resources to mitigate a scam victimization are the individuals themselves, we believe understanding the degree to which students choose to engage in any protective activities of their personal information provides insights into their level of susceptibility to being a victim of various scam schemes. We distinguish between offline (i.e., phone practices) and online (i.e., online security measures) preventative measures.

The first preventative measure we inquired each interviewee about was with regards to how openly they publicize their personal phone number. The purpose of asking this question was to assess a given student's susceptibility to being a victim of a phone scam since a student who openly provides their number to others would have a higher propensity of experiencing a phone scam than a student who kept their personal phone number more private. When we asked them the *general* question whether they keep their number private, most participants professed to do so. In some cases, interviewees stated that they provide their phone number when signing up for online accounts. Interviewee #13 was the only person who acknowledged to openly publicize his number on a personal website. However, we also asked each interviewee the *specific* question if they provided their personal phone number on Penn State's directory that can be easily accessed by anyone and not just Penn State members. Four interviewees stated that they did not post their personal phone number while six interviewees were unsure if their number was listed. Six interviewees acknowledged that they made their phone numbers available in the publicly accessible directory, which is in conflict with their earlier response to the more general question regarding whether they kept their personal phone number private. Interviewees #4 and #12 explained that they shared their phone numbers on the directory in the event that a recruiter or employer was interested in contacting them for a prospective job. Interviewee #7 stated that after losing his debit card and being contacted by a fellow student about his lost card, he decided to ultimately leave his phone number in the directory.

Second, we also asked students whether they employed any online security measures, even though we recognize that taking such measures may only add protection against certain scams (e.g., phishing emails, malware triggering scareware, or false anti-virus scams). There was a high level of uniformity across interviewees' responses in terms of the security measures they employ to protect themselves against cybercrimes. The most prevalent security measures were anti-virus software (16 participants) and having either a biometric or password protection on some or all of their personal devices (14 participants). Another frequently mentioned security measure was checking to see if a connection is secure by looking for the presence of SSL (Secure Socket Layer) or HTTPS (8 participants). Interviewee #16 more generally stated that she made sure that she was only navigating legitimate and reputable websites when entering payment information.

B. Awareness

Raising awareness about the prevalence of certain crimes is another way to mitigate an individual's future crime risk. We first asked interviewees what their level of awareness was with regards to the scam schemes that have affected the international student community on campus particularly and whether they knew of the Penn State awareness campaigns that warn about phone scams. One organization that has taken strides to increase awareness about phone scams that have specifically been affecting international students on campus is the Directorate of International Students & Scholars Advising (DISSA). According to DISSA's mission statement, they are "committed to providing international students and scholars the highest level of expertise in advising, immigration services, and training in support of Penn State's teaching, research and outreach objectives" [28]. DISSA is an important resource that international students on campus rely on with regards to their current immigration and student status while studying in the United States. Importantly, DISSA has been sending out informative emails to their listserv, which has approximately 8,000 students on it. An excerpt from an email DISSA sent out to international students is depicted below in Figure 1.



Dear Students:

Each semester we send this message. Apparently the calls have started again in the past 2 weeks to international students.

DON'T FALL VICTIM. NEVER GIVE PERSONAL INFORMATION OR MONEY ON THE TELEPHONE OR THROUGH EMAIL TO INDIVIDUALS YOU DO NOT KNOW. Don't be frightened into making this mistake. See the information below from the government. No government agency will call and demand money immediately. Do not purchase cards or send money through Western Union.   It is impossible to get your money back.

Important Message to Students: Protect Yourself from Scams

Scams are when strangers target unsuspecting individuals and lie to them in order to illegally receive money or personal information. Those that conduct scams are often called scam artists. They contact people in many ways, but a common technique is to call on the telephone and demand money under false claims.

The Federal Bureau of Investigation warns, "When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud." Despite this warning, thousands of people

Fig. 1. An excerpt from an email DISSA sent out to its listserv on September 27, 2016

All interviewees stated that they were made aware of the scams targeting international students through emails that DISSA was sending out to them. The emails were warning international students about phone scams that have been circulating; for example, one phone scam that was emphasized involved the caller impersonating an IRS official. Additionally, DISSA also advised students to not provide their personal information over the phone to such callers (see Figure 1). When asked whether the emails DISSA sends out are an effective way to raise awareness to international students about such an issue, interviewee #1 stated, "I think it's a good way because DISSA is the main authority for international students…I think because everything they say students heed to it." This statement illustrates the importance of who is the sender of such crucial information and what is their relationship with the receiver (i.e., an on-campus authority and student) when trying to impact adherence to such advice. There were also a few interviewees who mentioned that they were made aware of such scams through other on campus channels such as through their new student orientation (3 participants**),** the daily digest that is sent out to all students on campus (1 participant), and on-campus housing flyers (1 participant). However, one key piece of information that interviewees expressed was missing in the DISSA emails and other stated information sources was how to report such incidents. As we will discuss in further detail later on, despite the fact that virtually all the students we interviewed did not fall victim to the scam they experienced, it is still worth knowing how such crimes can be reported since there are benefits to be gained (e.g., better data availability about the frequency at which students are targeted to guide awareness campaigns in the future and details about the nature of these scams could be made available). For example, interviewee #5 who experienced a phone scam where the caller was impersonating the Philadelphia Treasury Department (but she did not fall victim to the scam) expressed that: "It's good to add to the knowledge base and the society is actually going to take it as something important as long as there are more victims to it."

Additionally, we also asked interviewees about the sources of their cybercrime knowledge. Some of the top sources from which participants mentioned they acquire their cybercrime knowledge from include reading online news articles/media (13 participants), school/coursework they took in college (7 participants) knowing someone personal to them who experienced a cybercrime (e.g., identity theft, credit card fraud) (6 participants), and having had personal experience with a cybercrime before (e.g., credit card fraud, malware) (6 participants). Some of the other sources of their cybercrime knowledge include personal research (4 participants) and work experience (2 participants). Due to the fact that cybercrime is not a subject that is formally taught to everyone (i.e., education as an information source), it does not come as a surprise that the main avenues in which students learned about cybercrimes are informal; such findings have been corroborated by previous studies (see [27], [29]). While informal sources of cybercrime knowledge such as hearing cybercrime victimization stories from a friend or family member may resonate better to an individual, we may question the accuracy, completeness, and reliability of such information.

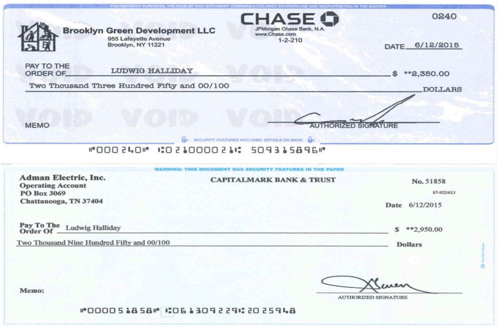
Lastly, we also asked international students whether they shared their personal scam victimization experiences with others. There was not a single interviewee that did not share their scam victimization experience with someone close to them. An overwhelming majority of interviewees chose to share their scam experience with their friends (13 participants); some interviewees mentioned that they particularly set out to share their experiences with their international friends so that they would not fall for such a scam in the future (3 participants). In other instances, interviewees shared their scam experience with others who they also considered to be close to them such as their advisor (2 participants), family (2 participants), or partner (1 participant). Interviewee #11 told a number of people about the phone scams she experienced including the members of her department, friends, and notified DISSA about the incident. While the stated main motivation for sharing was to raise awareness, a few individuals expressed that the nature of the scheme had a funny element to them, which also compelled them to share it with their close friends (3 participants).

C. Scam Schemes

The two main scam schemes reported during the interviews were phone scams and scams perpetrated in response to Craigslist postings. There were also two other instances of cybercrimes that two interviewees experienced, which were auto fraud and scareware. The majority of scams that interviewees experienced were inchoate crimes. Ultimately, only one interviewee fell victim to the scam she experienced. We will discuss the nature of these scam schemes below.

The most prevalent scam scheme interviewees experienced were phone scams, which affected 10 interviewees, but none of them fell victim to it. The phone scams that interviewees described follow a very similar makeup to the description previously mentioned in the campus police report data section: a student receives a phone call from an individual impersonating some high level government agency (i.e., IRS) or law enforcement official (i.e., Sheriff's department) and states that there is either a warrant out for their arrest or that they will be deported if they do not take care of the amount of money they owe (e.g., unpaid taxes); moreover, in order to legitimize themselves the scammers in some instances utilize phone spoofing techniques to appear as if they are calling from a legitimate number of the entity they are impersonating or simply mask their phone number as unknown. A number of interviewees mentioned that they ended up validating the phone number from which the scammer was calling from by either looking it up online or using an app called TrueCaller that detects whether an incoming call is likely legitimate or not based on how it has been reported by others. A few interviewees also mentioned that in order to further elevate their scare tactics (e.g., in the event an arrest warrant was part of the threat) sometimes the scammer would even phone spoof 911; where 911 was an incoming call while the student was on the line with the scammer. Another way the scammers try to legitimate themselves is by mentioning personal details about the student namely their name and in certain instances other key pieces of their private information such as their date of birth or address. In the majority of phone scam cases interviewees experienced, they expressed that the scammer was male and had an accent that predominantly sounded Indian. A few interviewees expressed that they experienced multiple phone scam calls (typically 2-3 scam calls) that they were cognizant of and picked up on. We consider these phone scams to be what Anderson et al. call "transitional fraud" [30] where similar to payment card fraud there are now "online" techniques to support traditional scam schemes (e.g., by phone spoofing or by requesting electronic payment).

The second most prevalent scam scheme interviewees experienced were Craigslist scams, which affected 5 interviewees; none of which fell victim to it. There were also a few instances of Craigslist scams mentioned in the campus police report data we qualitatively analyzed; however, campus police did not highlight this particular scam scheme in our conversations. The overall scheme goes as follows: international students are interested in subleasing their apartment for a few months over the summer so they create a Craigslist post asking for a given monthly rent amount and in some cases to also provide a security deposit. A scammer pretending to be an interested tenant (e.g., claiming to be a foreign exchange student) contacts the student expressing an interest in taking over the lease and immediately mails a check to the student in an amount greater than the student is initially requesting (i.e., with all months' rent instead of simply providing the initial month's rent). The scammer then communicates some heart-wrenching story or matter of urgency, for example, about how the excess money needs to be sent back immediately to them so that it can cover the expense for their flight to the U.S. or to ship their car overseas. The checks that were sent to the students are fraudulent. Thus, the students would have found themselves in a state of debt for any money, which they would have transferred to the scammer upon depositing the check. In fact, interviewee #10 who was on the verge of depositing the fraudulent check (sent by an interested tenant claiming to be a French foreign exchange student coming to Penn State) was immediately informed by a bank teller that she had been sent a fraudulent check and that the bank is already aware of the scams that have been occurring on Craigslist. Interviewee #11 provided scans of two fraudulent checks he received from a scammer as shown in Figure 2 below (note that the name presented on these checks is a pseudonym the interviewee provided to the scammer and not his legal name due to his realization that he was experiencing a scam).



FOR SECURITY PURPOSES, THE FACE OF THIS DOCUMENT CONTAINS A COLORED BACKGROUND AND MICROPRINTING IN THE BORDER

Brooklyn Green Development LLC
955 Lafayette Avenue
Brooklyn, NY 11221

CHASE
JPMorgan Chase Bank, N.A.
www.Chase.com
1-2-210

0240

DATE 6/12/2015

PAY TO THE ORDER OF LUDWIG HALLIDAY $ **2,350.00

Two Thousand Three Hundred Fifty and 00/100 DOLLARS

MEMO

AUTHORIZED SIGNATURE

SECURITY FEATURES INCLUDED. DETAILS ON BACK

000240 021000021 509315896

WARNING: THIS DOCUMENT HAS SECURITY FEATURES IN THE PAPER

Adman Electric, Inc.
Operating Account
PO Box 3069
Chattanooga, TN 37404

CAPITALMARK BANK & TRUST

No. 51858
87-922/613

Date 6/12/2015

Pay To The Order Of Ludwig Halliday $ **2,950.00

Two Thousand Nine Hundred Fifty and 00/100 Dollars

Memo:

AUTHORIZED SIGNATURE

0000051858 061309229 2025948

Fig. 2. Fraudulent checks that were sent by a Craigslist scammer to an international student regarding their rent sublease post on Craigslist

Two interviewees experienced other cybercrimes. Interviewee #2 experienced auto fraud, but did not fall victim to it. He was interested in purchasing a car and contacted the seller of the car via email that he wanted to purchase her vehicle. Upon receiving what he deemed to be a very detailed, professional sounding email from the seller stating that the car would have to be purchased through Amazon's website since she is traveling around, he became suspicious and decided to stop all further communication with the seller. Interviewee #8 experienced an incident resembling scareware and is the only interviewee who fell victim to the crime she experienced. She described receiving a pop-up on her laptop that came with a very unusual sound and that was accompanied by a person's voice. Despite many attempts to remove the problem from her laptop, she was unsuccessful and decided after a week of suffering from the repeated pop-up warnings that she should call the number provided on the pop-up. She was asked to pay approximately $100 via credit card for an anti-virus software that purportedly would secure her computer and remove the pop-up. She accepted the terms and installed the program. Upon taking her laptop to a place on campus that helps troubleshoot computer problems students have, it was made clear to her that she had experienced a scam and the service removed the anti-virus software that was downloaded on to her computer. Additionally, the service also suggested to her that she should try getting her money back. However, after repeatedly calling the scammer's number and explaining her situation, she was unable to have her money returned. She did not undertake any further actions.

Lastly, we would like to note that in some instances the scams that interviewees experienced were emotionally troubling for them. Interviewee #5 expressed that the phone scam she experienced left her traumatized and ultimately resulted in her no longer picking up her phone calls, which her boyfriend now does in place of her. A few interviewees also mentioned the fact that the scammers get particularly aggressive when one does not follow their requests; for example, interviewee #7 who experienced a Craigslist scam felt particularly scared when the scammer began to be threatening with him over the phone for not sending him back the excess money he had sent him going as far as to physically threaten him and emphasizing that he knew where the victim lived. Therefore, we would like to point out that the loss that is felt by such scams should not simply be quantified by monetary figures, but can also result in emotional harm felt by the victim. Thus, pointing out that inchoate crimes are also often not without harm.

D. *Reporting Behaviors*

One of the main objectives of the second part of our study was to better understand the reasons behind international students' reporting behaviors particularly in the event that an inchoate crime was experienced. All but one of our interviewees who experienced a scam did not fall victim (i.e., participant #8; a case which we discussed above); thus, we were particularly interested to see if international students would feel compelled to report attempted scams that did not result in monetary loss and what the reasoning would be behind taking such an action.

The first question we were interested in asking was simply whether international students reported the scams they experienced. We found that 6 students that we interviewed reported their scam experiences while 10 students did not. The top four reasons why students chose not to report their scam experiences were due to a lack of time to file a report (3 participants), lack of any perceived harm or financial loss (2 participants), an absence of knowledge on how to report the incident (2 participants), and finally a fear of visa/academic status being affected (2 participants). Other reasons that were provided included difficulty in tracking the scammer (1 participant), considering the reporting process to be lengthy and a waste of time (1 participant), no personal information was disclosed (1 participant), and a lack of knowledge that a crime took place (1 participant). Some of the justifications as to why students chose not to report their scam experiences can be corroborated by the reasons why cybercrimes and crimes in general are underreported as previously discussed in our related work section (see [12]–[15], [20], [27], [31]). However, several reasons are not cited by previous literature and explain why international students chose not to file a report about their scam experiences. For example, due to their demographic of being an international student, there is a fear that if they file a report with law enforcement that it will in some way jeopardize their visa or academic status in the United States. Interviewee #7 who experienced a Craigslist scam expressed the following as to why he chose not to report his experience to law enforcement, "I don't know I was scared about calling the police…I'm on a visa status in the United States so I'm a non-immigrant alien so I didn't want anything to come on my record which would affect my career or my education studies in the future." Despite contacting DISSA about the phone scam he experienced, interviewee #3 expressed a similar sentiment by explaining "I am not a citizen so I try to minimize my interaction with police. I am legal but I just don't do it." Law enforcement agencies may have to take strides towards reaching out to international students to ameliorate some of these concerns.

Despite the fact that a majority of the interviewees chose not to file a report regarding their scam experiences, there were still several interviewees who chose to report the scam. The entities to which international students reported their scam experiences included a personal bank (1 participant), DISSA (3 participants), campus police (1 participant), local law enforcement (3 participants), and the United State Postal Inspection Service (1 participant). Interestingly, the interviewees who chose to file reports all experienced inchoate crimes; thus, we were particularly interested in understanding what motivated them to report. Among some of the reasons why they chose to report their experiences included to catch the criminal (3 participants), to raise awareness with the hopes that it will prevent others from falling victim to such scams (2 participants), and for the information to be useful for law enforcement (1 participant). Some of these reasons have been corroborated by previous work (e.g., [11]). As previously mentioned in an earlier section, the majority of interviewees felt the need to raise awareness about their scam experiences to those closest to them (i.e., friends and family). We also asked interviewees what their overall satisfaction was with the reporting process. Despite the fact that she did not lose anything financially as a result of experiencing a phone scam, interviewee #11 was dissatisfied by the lack of action that was taken as a result from her filing a report with local police by contextualizing her experience as a personal invasion stating, "people say it's not that big you know because the scam really didn't go through…for example somebody arrived at your house and you just noticed yeah they didn't take anything but they came you know? It increased the feeling of insecurity." Interviewee #12 also echoed her dissatisfaction after filing a report with campus police by stating, "I thought maybe they would call me in to have more details or maybe asking more questions through the phone or have some feedback like okay we are going to do this or whatever, but they're like oh yeah that happens thank you for calling. They were like that happens a lot. Do not take calls from unknown numbers…they were like be careful with your information online." From the sentiments shared by these two interviewees one can infer that individuals may have a preconceived notion of how they wish the reporting process should work, but in absence of the expected level of initiative by law enforcement they are left dissatisfied. Moreover, interviewee #11 adds another point.by arguing that the basis for filing a report and whether action should be subsequently taken by law enforcement should not necessarily be based solely on the presence or absence of financial loss as a crime still occurred. Likewise, when contextualizing how he viewed the reporting process for the Craigslist scam he experienced, interviewee #13 stated: "I really think that the way these scams work the main way to prevent them is really educating people and raising awareness not so much actually getting down on these people." This statement is reflective of the motivations behind taking the step of reporting inchoate crimes by several of our interviewees.

We found that a lack of cybercrime reporting knowledge was central to explaining both the reasoning behind why some international students did not file a report with law enforcement. There was not a single interviewee who had heard of the IC3, which was also corroborated by the results of a previous study we conducted [27]. Thus, we find it very important to rethink how to raise awareness of how to report cybercrimes and scams like those experienced by the international students in this study. We also asked interviewees what the best ways were to raise awareness about how to report scams similar to the ones they experienced and cybercrimes as a whole; some of the suggestions they provided included having DISSA email or post on their website information regarding reporting (7 participants), receiving campus alerts (e.g., via text) (2 participants), incentivizing the reporting process (2 participants), and providing such information during new/international student orientation (2 participants).

As briefly mentioned in a previous subsection, a number of students expressed that despite the informative nature of the emails DISSA sends out to international students regarding the prevalence of scam schemes, there is no mention of how students should report such incidents. We suggest that entities like DISSA can indeed provide such information in future communications especially given the great importance DISSA plays in each international student's academic career. A few interviewees mentioned new/international student orientation would be a good venue to raise awareness about how to report such incidents as interviewee #16 explained, "That's how new people want to learn [and are] willing [to] learn those information to protect themselves. Later on it's harder to get all the people together actually." Thus, the accessibility of such information, but also the convenience behind the delivery of such pertinent information is crucial to students. The idea of providing campus alerts (e.g., through texts) was also a suggestion that was shared by a few interviewees (e.g., alerts sent out by campus police). Currently, Penn State campus police provides alerts to all students regarding occurrences of sexual assault; however, such alerts do not exist for either the scams that have affected international students or cybercrimes that students or staff experience.

Raising awareness about how college students can report scams and cybercrimes is vital since their cybercrime reporting self-efficacy is currently lacking; thus, identifying the most effective way in which relevant information can be shared (e.g., about the existence of the IC3) is important. More generally, aside from acknowledging the importance of both encouraging reporting behaviors and increasing reporting knowledge there also needs to be a broader set of solution approaches on how to mitigate the cybercrime underreporting problem; a sentiment corresponding to an aggregation of interviewees' responses. Some ways in which this can be achieved is by not only better publicizing the resources that are provided by currently existing cybercrime reporting mechanisms such as the IC3 and FTC (e.g., prevention tips), but also providing a better visibility of the tangible output that comes from such mechanisms (i.e., cybercrime victimization statistics, evidence of law enforcement actions towards combatting cybercrimes) [32].

E. Contextualization of Scam Experience

Initially, when the scams were brought to our attention by campus police, it was conveyed to us that the scams predominantly the phone scams were specifically targeting international students. Therefore, we were interested to see how international students contextualized their scam experiences notably whether they felt targeted based on their demographic. Overall, an overwhelming majority of interviewees (13 participants) expressed that they did not feel as if they were the specific target of the scam they experienced. One justification why several of the interviewees expressed such a sentiment was due to the information they found online regarding the scam they experienced in which they came across instances where even domestic individuals had experienced scams similar to the ones they had experienced (2 participants). For the individuals who experienced the Craigslist scam, they believed that such a scam could happen to virtually anyone given the universality of the platform and simply due to the fact that there was no obvious way that the scammers would be made aware of their international status based on their postings (3 participants). In fact, interviewee #10 who experienced a Craigslist scam was particularly adamant about not being considered a target of the scam by sharing that her American roommate had also experienced a similar Craigslist scam.

In general, interviewees expressed the opinion that the phone scams seem more specifically geared towards targeting international students than the Craigslist scam. This sentiment is predominantly based on the nature of the phone scams where the techniques and threats that are employed target an international student's immigration and student status in the U.S. Upon asking interviewees why they might believe international students are the targets of such scam schemes some of the main reasons provided were a lack of awareness regarding U.S. governmental agency procedures/U.S. law (9 participants), fear of jeopardizing their immigration/student status (e.g., threatened with deportation) (6 participants), lack of awareness regarding scam schemes (4 participants), and language barrier (3 participants). Interviewee #3 also pointed out that culture may be a factor why international students are targeted by such scams since an international student's cultural background may impact their susceptibility to falling for such scams if they believe such activities are customary for a government to perform. It is evident that a lack of awareness of U.S. legal and governmental procedure makes a number of international students feel vulnerable to such scam schemes particularly the phone scams; for instance, as pointed out by some interviewees a lack of knowledge that the FBI or IRS will not simply call someone and threaten them with arrest or deportation. In the end an interesting picture emerges. On the one hand, international students are hesitant to acknowledge that they are specifically targeted. On the other hand, they realize that their demographic is likely more vulnerable to such phone scams.

V. Discussion

Given the prevalence of the scam schemes that have affected international students on campus, it was rather surprising to us that we had only one international student in our interview sample who fell for the scam they experienced. We attribute this outcome partially to the power behind spreading awareness about such schemes through informal channels such as the DISSA mailing list. At the time we were conducting our interviews, a number of students mentioned that a shortcoming of the emails DISSA was sending out was that information regarding how to formally report such scams was missing. Fortunately, we observe that this information is now publicized on DISSA's website; however, DISSA only provides instructions on reporting such scams to the FTC and does not mention other valuable formal reporting entities like the IC3 that such scams can also be reported to. We firmly believe that including all the pertinent reporting entities for such scams is information that should be relayed to students since such entities like the IC3 administer more than just a mechanism to report such incidents by also providing valuable resources (e.g., victimization statistics, prevention tips) that can bolster awareness and in turn mitigate such scams from occurring to computer users in the future. Unsurprisingly, we did not come across a single interviewee that had heard of the IC3, an official cybercrime reporting entity, which solicits online scam reports. Including such pertinent information would likely help bolster law enforcement's data availability on such scam schemes and perhaps support the cases for the allocation of further resources to address this problem space. Likewise, one needs to identify strategies to help raise awareness within the general public about reporting mechanisms beyond a localized context such that DISSA achieves. Nevertheless, we also want to add emphasis to the suggestion made by an interviewee regarding the dissemination of occasional campus police text alerts to all students on campus regarding these scams along with information as to how students can report such scams. It is important to leverage local opportunities to understand and reach populations who are likely more vulnerable to specific scams.

Since a number of interviewees did not report their scam experiences, we were curious to know what method of cybercrime reporting international students preferred if given the option between filling out an online form versus making a phone call similar to dialing 911. Thus, we were curious to see if adding more lines of communication between the victim and law enforcement would encourage reporting. Penn State campus police provides a multitude of ways for students to file reports via a web form, phone call, or in person walk-in. There was a fairly even split between interviewees in terms of whether they preferred filling out an online form or making a phone call to law enforcement regarding experiencing an incident like those that they experienced. Some of the reasoning provided for why an online form was preferred was based on its convenience (i.e., a report is completed based on your own time), a feeling of comfort over answering questions in person when English is not your native language, and that it is easier to recall details in order to sort one's thoughts about an incident. Alternatively, some interviewees preferred making a phone call to law enforcement because it was seen as providing more immediate feedback, a more proactive approach, and that someone can help with filling out the report. However, based on the campus police report data we aggregated, we observed that phone reporting was by far a more frequented reporting avenue than filling out an online form with campus police. Therefore, we believe that currently existing reporting mechanisms like the IC3 may want to consider providing alternative options to filing a report other than only presenting one option which is to fill out an online form. Although instituting such a change would come at a cost, we believe the benefits would outweigh the costs in that an increase in reporting would better aid law enforcement efforts towards combatting cybercrimes and provide more information about scam schemes that computer users may face themselves with in the future. Overall, our findings contribute to the discussion on design improvements to currently existing cybercrime reporting entities in order to help encourage victims to report more often [32].

Lastly, the results from our study may also have public policy implications in terms of how cybercrime report data is collated and publicly conveyed to a given university's student body. Presently, only the reporting and tabulation of physical crimes is gathered by participating college campuses, which is set forth by the Clery Act (1990) [33]. Thus, by being the first of its kind, the results providing from the campus police report data analyzed from this study may have the potential to trigger a discussion about an extension of the Clery Act where college campuses across the nation would provide an aggregation of campus cybercrime reports at least on an annual basis, but ideally more frequently given the fluctuating nature of cybercrimes. Additionally, based on the limited scope of our study, we believe there is a great opportunity for future work to be done where a cross comparison study can be conducted on domestic and international college students in order to examine the victimization rates between these two groups since there is evidence to support that these scams (particularly the phone scams) extend beyond the international student context [34], [35]. Beyond providing a comparison of the victimization rates between these two groups, the results from such research would also provide insights on how each group contextualizes their scam experiences and whether the tactics of the scam schemes employed varies across the two groups.

VI. Conclusion

In this paper, we provided the results from a two-part qualitative study we conducted in order to not only better understand the nature of the prevalent scam schemes that have affected international students, but also to unpack the decision-making process behind filing a report particularly in the event an inchoate crime is experienced. We found that the two of the most common scam schemes experienced by international students at Penn State come in the form of phone scams and a Craigslist scam. We found that the majority of international college students we interviewed did not feel as though they were specifically targeted for the scams they experienced, which can be attributed to information they came across online where non-foreign individuals expressed that they too were victims of similar scam schemes such as the phone scams mentioned in our study. However, it is important to note that when comparing the phone scams to the Craigslist scam, the nature of the phone scams were considered to be more geared towards specifically affecting international college students than the Craigslist scam since virtually any individual irrespective of their citizenship status can be susceptible to experiencing a scam on Craiglist. While an overwhelming majority of the students we interviewed did not fall victim to the scam they experienced, we still came across a number of cases where students reported the scam they experienced; predominantly driven by altruistic reasoning so that their peers or friends would not fall victim to similar scam schemes in the future. Based on the results of the campus police report data and our interviews, we believe that currently existing reporting mechanisms like the IC3 may want to reconsider the addition of non-technological reporting avenues (e.g., via phone) since it was shown to be a relatively frequented and preferred reporting avenue utilized by students. Lastly, through this case study we can observe the importance behind raising awareness about such incidents as they promulgate. Many students in our sample were knowledgeable about the scam schemes before being a victim themselves. Likewise, we are motivated to find effective ways in which we can raise more awareness about currently existing cybercrime reporting mechanisms and law enforcement resources to help mitigate computer users' cybercrime risk.

Acknowledgement

We would first like to thank the Penn State campus police officers that provided their insights about the scam schemes that have affected the international student campus community and helped to collate the relevant report data on this pressing matter. We also would like to thank the anonymous reviewers for their suggestions for improvements of this manuscript. This research project (including the interviews we conducted) has been supported by a Google Faculty Research Award, which we gratefully acknowledge. The research activities of Jens Grossklags are also supported by the German Institute for Trust and Safety on the Internet (DIVSI).

References

[1] "2015 Internet Crime Report," 2015. [Online]. Available: https://pdf.ic3.gov/2015_IC3Report.pdf.

[2] T. T. Kubic, "Testimony: Internet Fraud Crime Problems," 2001. [Online]. Available: https://archives.fbi.gov/archives/news/testimony/internet-fraud-crime-problems.

[3] D. Wall, "Cybercrimes and the Internet," in *Crime and the Internet*, 2001, pp. 1–17.

[4] R. D. Clifford, *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime*, 3rd ed. 2011.

[5] M. A. Baginskis, "Telemarketing Fraud upon the Elderly Shows No Signs of Slowing," *Loyola Consumer Law Review*, vol. 11.

[6] J. Langenderfer and T. A. Shimp, "Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion.," *Psychology & Marketing*, vol. 18, no. 7, pp. 763–783, 2001.

[7] K. Pak and D. Shadel, "AARP Foundation National Fraud Victim Study," 2011.

[8] N. Miramirkhani, O. Starov, and N. Nikiforakis, "Dial

One for Scam: A Large-Scale Analysis of Technical Support Scams,” in *Proceedings of the 24th Network and Distributed System Security Symposium (NDSS)*, 2017.

[9] A. Nochenson and J. Grossklags, “An Online Experiment On Consumers’ Susceptibility to Fall for Post-transaction Marketing Scams,” in *Proceedings of the 22nd European Conference on Information Systems (ECIS)*, 2014.

[10] A. Nochenson and J. Grossklags, “I Didn’t Want That! An Experiment on Interventions for Deceptive Post-Transaction Marketing,” in *Workshop on Technology and Consumer Protection (ConPro)*, 2017.

[11] C. Cross, R. Kelly, and R. G. Smith, “The reporting experiences and support needs of victims of online fraud,” *Trends and Issues in Crime and Criminal Justice*, no. 518, pp. 1–14, 2016.

[12] M. Yar, *Cybercrime and the Internet*, 2nd ed. SAGE, 2013.

[13] D. S. Wall, “Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime,” *International Review of Law, Computers & Technology*, vol. 22, no. 1–2, pp. 45–63, 2008.

[14] W. Goucher, “Being a cybercrime victim,” *Computer Fraud & Security*, no. 10, pp. 16–18, 2010.

[15] M. D. Goodman and S. W. Brenner, “Emerging Consensus on Criminal Conduct in Cyberspace,” *International Journal of Law and Information Technology*, vol. 10, 2002.

[16] S. Fafinski, W. H. Dutton, and H. Z. Margetts, “Mapping and Measuring Cybercrime,” 18, 2010.

[17] D. S. Wall, “Policing cybercrimes: Situating the public police in networks of security within cyberspace,” *Police Practice and Research*, vol. 8, no. 2, pp. 183–205, 2007.

[18] J. Kerr, R. Owen, C. M. Nicholls, and M. Button, “Research on Sentencing Online Fraud Offences,” 2013.

[19] C. Cross, “Policing Online Fraud in Australia: The Emergence of a Victim−oriented Approach,” in *Crime, Justice and Social Democracy: Proceedings of the 3rd International Conference 2015*, 2016, pp. 1–8.

[20] D. S. Wall, “Digital Realism and the Governance of Spam as Cybercrime,” no. July, 2016.

[21] A. C. B. Hache and N. Ryder, “’ Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: a critical analysis of the United Kingdom’s legislative provisions and policies to tackle online fraud,” *Information & Communications Technology Law*, vol. 20, no. 1, pp. 35–56, 2011.

[22] R. G. Smith and C. Budd, “Consumer fraud in Australia: costs, rates and awareness of the risks in 2008,” 2009.

[23] A. Al-nemrat, H. Jahankhani, and D. S. Preston, “Cybercrime Victimisations / Criminalisation and Punishment,” *Global Security, Safety, and Sustainability*, pp. 55–62, 2010.

[24] C. L. Amarijo, D. F. Acosta, C. D. Silva, and V. L. de O. Gomes, “Factors Associated with Sexual Violence Against Women: Analysis of Police Reports,” *Skin*, vol. 7, no. 10.3, 2014.

[25] “2013 Internet Crime Report,” 2013. [Online]. Available: https://pdf.ic3.gov/2013_IC3Report.pdf.

[26] “2014 Internet Crime Report,” 2014. [Online]. Available: https://www.fbi.gov/news/news_blog/2014-ic3-annual-report.

[27] M. Bidgoli, B. P. Knijnenburg, and J. Grossklags, “When Cybercrimes Strike Undergraduates,” in *eCrime*, 2016.

[28] “DISSA Mission.” [Online]. Available: https://global.psu.edu/info/internationals-psu/students.

[29] E. Rader, R. Wash, and B. Brooks, “Stories as Informal Lessons about Security,” in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012.

[30] R. Anderson, C. Barton, R. Bhöme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore, and S. Savage, “Measuring the Cost of Cybercrime,” *Workshop on the Economics of Information Security (WEIS)*, pp. 1–31, 2012.

[31] M. Button, C. M. Nicholls, J. Kerr, and R. Owen, “Online frauds : Learning from victims why they fall for these scams,” *Journal of Criminology*, vol. 47, no. 3, pp. 391–408, 2014.

[32] M. Bidgoli and J. Grossklags, “End User Cybercrime Reporting: What We Know and What We Can Do to Improve It,” in *The 4th International Conference on Cybercrime and Computer Forensics (ICCCF)*, 2016.

[33] “Summary of the Jeanne Clery Act.” [Online]. Available: http://clerycenter.org/summary-jeanne-clery-act. [Accessed: 08-Mar-2016].

[34] M. Singletary, “Avoid the scam: That’s not the IRS calling,” *The Washington Post*, 12-Aug-2016. [Online]. Available: https://www.washingtonpost.com/business/get-there/avoid-the-scam-thats-not-the-irs-calling/2016/08/11/ae2636e2-5dae-11e6-8e45-477372e89d78_story.html?utm_term=.4fd0bf300d45.

[35] L. Rein, “Five arrested for impersonating IRS agents in phone scam,” *The Washington Post*, 24-May-2016. [Online]. Available: https://www.washingtonpost.com/news/powerpost/wp/2016/05/24/five-arrested-for-impersonating-irs-agents-in-phone-scam/?utm_term=.eaa2bda8cdfa.