

USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

Quantifying Risk Perception and Scam Response Among International and Domestic US University Students

Alexandra Xinran Li, Elijah Bouma-Sims, Lily Klucinec, and Ray Liu, *Carnegie Mellon University;* Ayesha Binte Mostofa, *University of Massachusetts, Amherst;* Arjun Arunasalam, *Florida International University;* Lorrie Faith Cranor, *Carnegie Mellon University;* Pubali Datta, *University of Massachusetts, Amherst;* Lucy Simko, *Barnard College, Columbia University;* Karen Sowon, *Indiana University*

https://www.usenix.org/conference/soups2026/presentation/li

This paper is included in the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security.

August 24–26, 2026 • Hannover, Germany

ISBN 978-1-939133-59-5

Open access to the Proceedings of the Twenty-Second Symposium on Usable Privacy and Security is sponsored by USENIX.

Quantifying Risk Perception and Scam Response Among International and Domestic U.S. University Students

Alexandra Xinran Li[1], Elijah Bouma-Sims[1], Lily Klucinec[1], Ray Liu[1], Ayesha Binte Mostofa[2], Arjun Arunasalam[3], Lorrie Faith Cranor[1], Pubali Datta[2], Lucy Simko[4], Karen Sowon[5]

[1]*Carnegie Mellon University* [2]*University of Massachusetts, Amherst* [3]*Florida International University*
[4]*Barnard College, Columbia University* [5]*Indiana University*

alexandrali@cmu.edu, {eboumasi, laklucin, ruiyang3}@andrew.cmu.edu, amostofa@umass.edu, aarunasa@fiu.edu, lorrie@cmu.edu, pdatta@umass.edu, lsimko@barnard.edu, ksowon@iu.edu

Abstract

We conducted an online survey of 1,074 students from five U.S. universities to examine and quantify the differences between domestic and international students' scam encounters, engagement behaviors, reporting tendencies, and exposure to anti-scam training. International students were significantly more likely than domestic students to say they would engage with scammers when presented with suspicious phone-call and text-message scenarios, but also more likely to disengage in our suspicious-rental email scenario. We found no difference in their ability to detect suspicious cues, but international students may require more evidence before disengaging in certain scenarios. While domestic students are more likely to encounter generic scams, international students reported more loss from authority-based, rental, and "unknown language" scams. International students reported a greater reliance on social media and peer support to avoid scams. They were significantly more likely to report incidents to law enforcement than domestic students, but less likely to report overall, use call filters, or online platform tools. We provide recommendations for improving both scam training offered by universities and digital scam reporting platforms.

1 Introduction

Approximately 6% of university students in the United States are international students, defined here as students who are not U.S. citizens or permanent residents who have come to the country to pursue higher education [30]. Although all university students are targeted by scams [43], international students face a distinct vulnerability profile. Prior work suggests that the lack of structural social support for immigrants contributes to vulnerability due to unfamiliarity with legal, linguistic, and cultural norms, and pressure to achieve and maintain financial security [60, 61]. In addition, scammers deliberately target non-citizens' needs for legal support by falsely claiming to offer naturalization or other visa-related services [50]. International students may be especially vulnerable to these scams due to the requirements for maintaining a student visa [70]. Recent changes in U.S. immigration policy have also generated uncertainty for non-citizens, potentially creating additional opportunities for scammers to exploit visa-related fears [38, 56].

There is little work exploring international students' encounters with scams in the U.S. [3, 75] and, to our knowledge, there is no large-scale quantitative study comparing the scam experiences of international and domestic students. We address this gap by asking the following research questions:

1. How do domestic and international university students in the U.S. engage with benign and suspicious parties requesting personal information across different communication channels?
2. How do domestic and international students differ in their scam experiences and reporting behaviors?
3. How do domestic and international students differ in their engagement with scam-related training and in the sources they consult for advice or support?

To address these questions, we conducted a large-scale survey ($n = 1,074$) of international and domestic students at five U.S. universities. We presented each participant with five scenarios spanning four communication channels and featuring both benign and fraudulent messages. To assess scam vulnerability, participants described their intended actions and reasoning for each scenario. Additionally, we gathered data on participants' prior scam encounters, reporting behaviors, and history with anti-scam training to provide context on their experiences.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2026.
August 23–26, 2026, Hannover, Germany.

We found that, overall, domestic and international students do not differ greatly in their ability to detect suspicious cues or in their exposure to scams, but they are vulnerable in structurally different ways. International students were more likely to engage with hypothetical scam scenarios involving phone calls and text messages. While domestic students reported encountering certain types of scams at higher rates, a higher proportion of international students reported losses across several scam categories. International students were more likely to seek scam-related advice but less likely to use tools to block or report scams. International students appear to have a higher threshold for disengagement in certain contexts. We therefore recommend recurring, scenario- and simulation-based training across communication channels, complemented by mock reporting exercises that familiarize students with different reporting pathways.

2 Background and Related Work

2.1 The Evolving Scam Landscape

We define a scam as a deceptive scheme to manipulate users into giving up money or sensitive information, resulting in financial, informational, or emotional loss [40]. Phishing is a widely studied form of scam that lures users to spoofed sites impersonating trusted entities [36], including text-message or SMS-based variants (smishing) [53]. Other common scams include telephone-based impersonation [65], fraudulent real estate listings [10], and fake job offers [18].

Scams have grown more sophisticated over time. Annual reports from the Federal Bureau of Investigation Internet Crime Complaint Center (IC3) consistently show rising losses associated with digital crimes [11].

Scams targeting the general population. Across communication channels, scams succeed by exploiting recipients' trust, attention, and situational relevance. Email phishing attacks especially exploit factors such as workload, attentional limitations, and perceived relevance [76], while telephone scams impersonate trusted entities and often create a sense of urgency or fear to bypass recipients' vigilance [65]. In a study on smishing, participants reported that the mentioning of personalized information significantly influenced their assessment of messages' legitimacy [53]. Government and authority impersonation schemes capitalize similarly on fear of legal consequences [13]. Beyond these channel-based attacks, scams exploit specific life circumstances: investment and "pig-butchering" schemes cultivate long-term financial trust [45, 46], online marketplace fraud capitalizes on peer-to-peer commerce [52], and romance scams build emotional trust before financial exploitation [28]. A common thread is that susceptibility is not uniform but context-dependent: scams are more effective when they align with a target's circumstances, and these vulnerabilities differ across populations [26, 48].

College student–specific scams. University students are exposed not only to broadly applicable scams but also to threats specific to academic life. Their vulnerability spans a diverse and evolving range of scam modalities. Demographic analyses found that younger users aged 18–25, which includes most university students, are especially vulnerable to phishing [34, 59], and students remain vulnerable even when they have prior awareness of phishing concepts [6, 7]. In addition, students frequently encounter rental and housing scams [17], as well as employment and internship scams [16, 66], which exploit financial need and limited work experience. While domestic students may be particularly vulnerable to federal student loan scams [71], international students seem to be disproportionately targeted by government impersonation and visa-related fraud [3, 75]. These divergent exposure patterns suggest susceptibility may depend on how well a scam aligns with each group's circumstances, motivating a scenario-based design to present both broadly-targeted and population-specific scams to international and domestic students alike.

2.2 Demographic and Sociocultural Factors

Certain populations face a higher risk of being targeted by digital safety threats due to structural, social, or personal vulnerabilities. In digital security research, these groups are often described as "at-risk users"—individuals or communities who face a higher likelihood of harm, exploitation, or adverse outcomes when interacting with digital systems [1]. Despite the growing recognition of at-risk users, the needs of marginalized populations are frequently overlooked in privacy and security research [61]. Prior work has begun to address this gap by examining the security and privacy challenges faced by refugees [60], sex workers [42], queer individuals [24], and survivors of intimate partner violence (IPV) [39].

Age-related vulnerabilities. Older adults are disproportionately represented in government fraud reports [11]. This may stem from less familiarity with digital fraud prevention [58] or cognitive decline with age [32]. Minors may also face elevated security risk in online threat contexts, particularly those involving phishing or account compromise, due to weaker password management practices [63], parental mediation patterns in digital media use [25], and documented susceptibility to phishing attacks [44]. While teens may not necessarily be less capable than adults when it comes to scam identification, they may more often encounter and be victimized by specific scam types such as giveaway scams due to their greater interest in the purported giveaways [5]. Not all targeted individuals necessarily fall victim to scams: engagement with fraudulent schemes exists along a behavioral spectrum, shaped by cognitive, emotional, and situational factors. While older adults may be more vulnerable to emotional manipulation, younger users may be at risk due to their impulsivity and high online exposure [49].

Socioeconomic and immigrant vulnerabilities. Migrant populations have been characterized as at-risk users, as they

lack support networks in their host country and must navigate stressful and confusing visa processes [64]. Undocumented immigrants often maintain a low profile, but qualitative research suggests that their understanding of government surveillance and related risks may be limited [27]. Individuals with lower socioeconomic status (lower-SES) experience disproportionate privacy and security risks [74], frequently because of lower levels of digital literacy and reduced confidence in navigating online systems.

2.3 Risk Profile of International Students

International students occupy a unique socio-legal position, balancing their primary goal of attending school [73] with the constraints imposed by temporary immigration status. Prior research has shown that visa requirements, including maintaining full-time enrollment, complying with employment rules, and fulfilling reporting obligations, may make them particularly vulnerable to scams that impersonate government or immigration officials [3], as fear of jeopardizing their status adds significant pressure [75].

International students face a range of challenges upon arriving in the U.S. [8], including the need to adapt to an unfamiliar culture while arranging housing [54] in a new country. Remote apartment searches can expose them to fraudulent listings or deposit scams [9], adding to the stress of an already complex transition. Financial transactions, including paying for transportation or moving to new housing, can also be difficult, as foreign debit and credit cards may not be accepted, and accessing U.S. financial services requires a credit history they often do not yet have. To apply for a U.S. Social Security Number (SSN), which is generally required for financial services, students must first gather all necessary documentation, a process that can take several weeks [64]. Employment options, including on-campus work, Curricular Practical Training (CPT), Optional Practical Training (OPT), and employer-sponsored visas, are highly regulated and competitive. Thus, international students may be especially susceptible to fraudulent job offers or sponsorship scams [47].

While prior work has examined college students' susceptibility to phishing [6, 7] and used small-scale interviews and surveys to study international students' scam experiences [75], no large-scale study has directly compared international and domestic students across a broad spectrum of scams.

3 Methods

3.1 Recruitment

We recruited participants from five public and private universities across five U.S. states where the authors are based: Carnegie Mellon University (CMU), Barnard College, Columbia University (Barnard), Florida International University (FIU), Indiana University (IU), and the University of Massachusetts, Amherst. We distributed messages to student mailing lists, posted on social media and student online communities (e.g., Reddit and Discord), placed flyers around campus, and asked departmental contacts to share information. We also recruited through international student organizations.

The recruitment materials described the survey as an effort to address the gap in understanding scam experiences among international and domestic students. We mentioned scams in the recruitment materials to attract participants interested in sharing their scam experiences. The materials also outlined the eligibility criteria, included a link and QR code to the survey, and informed participants of the survey length (20 minutes) and compensation (a digital gift card of $5).

Participants had to be 18 years or older, reside in the U.S., and be a full-time, in-person student at one of the five participating universities. These criteria were intended to ensure that participants had sufficient recent exposure to the scam environment faced by U.S. university students.

We conducted a power analysis for logistic regression using *G*Power*. Effect size estimates (odds ratio and baseline probability) were derived from an early wave of survey responses from Carnegie Mellon University (n = 125). Assuming a two-tailed test with $\alpha = .05$ and 80% power, and targeting an odds ratio of 1.5, the analysis indicated a required sample size of 1,040 participants.

To ensure adequate representation of international students, we initially set a minimum quota of 100 international students per university and capped domestic student participation at 100 students per university. However, during recruitment, we observed that domestic students were not enrolling substantially faster than international students, and we relaxed the domestic student cap. Our recruitment strategy prioritized maximizing overall sample size and statistical power rather than enforcing demographic proportionality. Moreover, the underlying population distribution, such as the concentration of international students in certain fields (e.g., technical disciplines) [30], is itself non-uniform. To account for potential demographic differences, we included relevant variables as covariates in our regression analyses.

3.2 Ethics Statement

Our study was approved by the Institutional Review Boards (IRBs) of all five participating universities. Participants were required to read and electronically agree to a consent form before proceeding to the main survey. Survey responses were stored in a secure Google Drive accessible only to authorized research team members and were assigned unique identifiers. Email addresses, collected for compensation and student verification purposes, were stored in a separate file and deleted after compensation was distributed. Open-ended responses were reviewed to ensure that no personally identifiable information was disclosed. Because the survey involved recalling experiences with potential scams, the consent form explic-

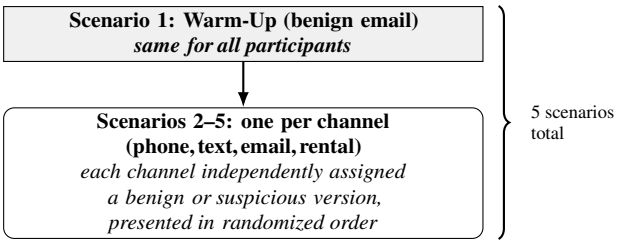


Figure 1: Scenario presentation for each participant.

itly noted the possibility of minor psychological discomfort associated with such recall. To reassure participants that the survey itself was legitimate, we provided contact information and website details for the lead author's institution and hosted the survey on a server maintained by that institution.

3.3 Survey Procedure

3.3.1 Screening and Verification

Participants reported residency status (U.S. citizen, permanent resident, or non-permanent resident) and the country in which they spent the majority of their time before the age of 18. We classified U.S. citizens or permanent residents as domestic students, and non-permanent residents as international students. The country-of-origin measure was used to explore differences in engagement patterns among international students.

To prevent responses from individuals who were not current students at the participating universities and to ensure data validity, we required participants to provide their university-issued email address for verification and compensation. Only respondents whose email domain matched that of the relevant university were permitted to proceed in the survey. In cases where we identified invalid email addresses (e.g., when compensation delivery failed), we removed those responses from the dataset prior to analysis. Participants were informed in the consent form that responses generated using external AI tools, containing nonsensical or low-effort content, or duplicate submissions would be deemed invalid and ineligible for compensation. We also implemented technical measures (e.g., disabling copy-paste) to discourage the use of AI tools.

3.3.2 Suspicious and Benign Scenarios

To examine participants' engagement behavior when interacting with parties requesting information in different communication channels, we asked students to review five realistic scenarios and indicate how they would respond. Each scenario included multiple response options, and participants were asked to select the action they would most likely take if facing a similar situation in real life. To encourage authentic responses, we reiterated that there were no right or wrong answers and asked participants to choose the option that best reflected what they would actually do. To avoid potential declines in attention associated with longer surveys, we presented only five scenarios to each participant. Figure 1 shows the presentation of the scenarios.

All participants started the survey with the same benign warm-up scenario (*Warm-Up-Benign*) where they were asked to imagine that they had previously emailed their university's career center for resume advice, and that they received a reply requesting their availability for a meeting and a draft of their resume. We presented this scenario first to set participants' expectations and encourage careful evaluation of subsequent scenarios. By presenting a benign scenario first, we sought to reduce priming participants to engage in defensive behaviors, such as selecting options that avoid sharing any information.

Each participant was then shown four scenarios, one from each communication channel, presented in a random order. This design was intended to mitigate potential order effects (e.g., influencing responses if a particular channel consistently appeared later). We recorded the order of the scenario and included it as a control variable in our analyses to account for any order effects. For each channel, we developed both suspicious and benign scenarios. Participants were randomly assigned to view one scenario per channel, with balanced allocation to ensure approximately equal representation of each version. We designed the suspicious and benign versions within each communication channel to be comparable by incorporating red flags in the suspicious scenarios and removing them in the benign counterparts while keeping the context as similar as possible. This allowed us to examine whether participants could detect and respond appropriately to embedded red flags. The inclusion of benign scenarios also signaled to the participants that subsequent scenarios could be either suspicious or legitimate. Furthermore, it enabled us to assess whether certain student groups were more likely to exhibit defensive or information-withholding behaviors even in benign situations.

Each scenario was presented as a single-choice question, with response options reflecting three types of engagement. Participants could select from several responses relevant to each scenario that aligned with one of three response types: (1) fully engage with the other party without seeking external assistance; (2) engage cautiously by consulting others or searching online while maintaining the communication (e.g., not hanging up or blocking the sender); or (3) disengage by ignoring, blocking, or reporting the communication. We defined these engagement categories for data analysis purposes; participants were presented only with concrete behavioral response options. We also included an "Other, please specify" option to allow participants to report actions not captured by the existing response options. After each scenario question, we asked participants to explain the reasoning behind their choice. Below, we describe the sources informing each scenario, provide a brief overview of their content, and outline the red flags embedded in the suspicious versions.

Phone Call. We designed two suspicious scenarios to reflect differences in the tactics used to target international and domestic students. The international student scenario was informed by scams documented by the U.S. Citizenship and Immigration Services (USCIS) and the U.S. Department of Homeland Security (DHS) [69, 72], while the domestic-student scenario drew on consumer alerts published by the Federal Trade Commission (FTC) [19].

In *Phone-Sus-USCIS*, the caller impersonated a USCIS officer and alleged a failure to update information in the Student Exchange Visitor Information System (SEVIS) and requested passport number and date of birth. This scenario incorporated several red flags: (1) caller ID spoofing; (2) immediate identity confirmation; (3) vague system claims; (4) urgency and threat framing; and (5) requests for sensitive personal information.

In *Phone-Sus-Police*, the caller impersonated a local police officer and claimed the participant had missed jury duty, requesting their date of birth and the last four digits of their SSN. This scenario incorporated red flags, including: (1) caller ID spoofing; (2) identity confirmation pretexting; (3) vague reference to prior communication; (4) urgency and threat framing; and (5) requests for sensitive personal information.

Although *Phone-Sus-USCIS* reflects a scam that is specific to international students (who are required to maintain SEVIS records) and *Phone-Sus-Police* reflects a jury-duty scam that typically applies only to U.S. citizens and permanent residents, participants were not restricted to scenarios aligned with their residency status. Domestic participants could be assigned *Phone-Sus-USCIS*, and international participants could be assigned *Phone-Sus-Police*. This design allowed us to examine whether participants would engage with a scenario that was not directly applicable. For each suspicious scenario, we incorporated multiple co-occurring red flags to reflect the layered cues present in real-world scams, rather than isolating individual red flags to test which cue matters most.

To construct a realistic, benign phone scenario, we consulted the Carnegie Mellon University police department about situations in which they might legitimately contact students to request limited personal information. They described a scenario involving a lost wallet containing a student ID, in which officers would call the student to confirm their university ID number before logging the item. We adapted this example as our benign phone scenario *Phone-Benign*).

Text Message. We designed the text-message scenario around a failed delivery notification during the time a package is expected, one of the most frequent messages university students may receive [20], informed by the Federal Communications Commission (FCC)'s delivery scam page [12] and FedEx's page on paying Duties & Taxes on Imported Goods [23].

In *Text-Sus*, the sender presented themselves as UPS and stated that a package was being held due to missing documentation, requesting that the recipient click a link to pay a release fee of $45.20. This scenario incorporated several red flags, including: (1) a lookalike sender domain (`ups-secure-cx.com`) rather than an official UPS domain; (2) an insecure `http` link; (3) an unexpected fee to release a held package; (4) a vague customs/paperwork pretext; and (5) a request to pay through an embedded link rather than an official channel.

In *Text-Benign*, the sender presented themselves as FedEx, stating that $45.20 of duties and taxes were due for a package, with a link on an official FedEx domain and a notice that FedEx never requests personal information by text. We used FedEx here because its website publicly documents legitimate text-based duties-and-taxes requests [23], and UPS for the suspicious version, as UPS-branded scams are commonly reported.

Email. In this scenario, participants received an email from an individual claiming to be a recruiter at Google while they were actively seeking employment [15, 18]. To design a realistic, benign counterpart, we drew on real examples shared in online communities in which legitimate recruiters had sent unsolicited outreach emails [55].

In *Email-Sus*, the sender informed participants of a full-time opportunity that included visa sponsorship and requested that they click a link to apply and submit their resume. This scenario incorporated several red flags, including: (1) a non-official sender email address; (2) a non-official application portal; (3) a non-official email signature; (4) emphasis on visa sponsorship; and (5) a vague job description.

In *Email-Benign*, the sender provided a link to apply and invited participants to reply with their availability to schedule a meeting for further discussion before applying.

Rental Platform. Participants were asked to imagine that they were searching for housing while physically located in another city, identified a suitable listing on Zillow, and completed a satisfactory virtual tour. This scenario was informed by the FBI's press release on rental and real estate scams [10] and Zillow's FAQs regarding lease-signing procedures [77].

In *Rent-Sus*, participants received an email from a property manager with whom they had previously exchanged messages and completed a virtual tour, requesting the first month's rent and a $500 security deposit via Zelle in order to receive the lease. This scenario incorporated several red flags, including: (1) a non-official sender email address; (2) use of an informal payment method; (3) urgency framing; and (4) a request for payment before lease signing.

In *Rent-Benign*, participants also received a message from the property manager with whom they had previously exchanged messages and completed a virtual tour with, but via Zillow's Rental Manager platform, requesting them to click into a link to review and sign the lease.

3.3.3 Scam Encounter, Response, and Loss

In the second part of the survey, we presented participants with ten scam types curated from government scam glossaries

and prior research on scams that are applicable to college students [3, 13, 14, 21, 22, 31, 64], scam warnings issued by state officials [37, 51], as well as scam information maintained by U.S. universities [57, 67, 68]. Our goal was to understand university students' experiences with these scam types and to examine potential differences between international and domestic students in terms of targeting, response behaviors, and losses incurred. For each of the ten listed scam types, participants answered whether they had encountered the scam, whether they responded or engaged with the other party (if applicable), and whether they experienced any form of loss (financial, informational, emotional, or time-related). We then presented participants with a list of potential scam reporting channels and asked them to select all that they had used. The list included formal authorities (e.g., government websites and law enforcement), institutional channels (e.g., university offices), financial institutions (e.g., banks), and technical reporting tools (e.g., phone spam filters), as well as an "Other" option. We asked them to describe their reasons for reporting and selecting that report channel.

3.3.4 Training and Advice

We curated two lists of scam-related resources and training opportunities: university-provided and external (e.g., social media). Participants selected all resources they had used and identified those they found most helpful. International student participants were asked to describe any training tailored to international students at their university. We also asked participants whether they had sought scam-related advice from various online communities or individuals.

3.3.5 Demographics

We asked demographic questions at the end of the survey to minimize potential identity priming effects. Participants reported their age, gender, field of study, academic program, residency status, years in the U.S., and English proficiency. International student participants also reported their visa type. These variables were used to characterize the sample and were included as covariates in data analyses.

3.4 Data Analysis

3.4.1 Quantitative Analysis

To address RQ1, we conducted multinomial logistic regression analyses [29] on the five suspicious scenarios, with student type (international vs. domestic) as the primary predictor and gender, age, tech background, and scenario presentation order included as covariates. We ran separate regressions for each scenario question, so each participant contributed only one data point per regression. Response options were binned into three engagement levels defined before administering the survey ("fully engage," "cautiously engage," and "disengage"; see Section 3.3.2). For each benign scenario, we applied binary logistic regression using the same predictors and covariates, grouping "fully engage" and "cautiously engage" together. Participants selecting "disengage" were modeled separately, as disengagement would forgo the potential benefit of the situation.

We applied Signal Detection Theory (SDT) [62] to quantify participants' behavior across scenarios. We defined *hits* as selecting "disengage" in suspicious scenarios and *correct rejections* as selecting "engage" or "cautiously engage" in benign scenarios. False alarms were defined as disengaging in benign scenarios, and misses as engaging or cautiously engaging in suspicious scenarios. From these rates, we computed sensitivity (d') and response bias (c) for each participant. We conducted Wilcoxon rank-sum tests (Mann–Whitney U tests) to examine differences between international and domestic students in sensitivity (d') and response bias (c) [41].

We conducted two parallel analyses restricted to international students. First, using the country where participants spent the majority of their time before age 18 as the primary predictor, we compared the three largest national-origin subgroups in our sample (India, mainland China, and Bangladesh). Second, to assess whether the international/domestic gap reflects time spent in the U.S. rather than student status, we ran scenario-level regressions among international students with time in the U.S. (Recent, <1 year vs. Established, 1+ year) as the primary predictor, with gender, age, scenario order, and technical background as covariates.

For RQ2, we further conducted mixed-effects binary logistic regression analyses predicting scam encounter, response conditional on encounter, and loss outcomes with participant as a random intercept, accounting for within-participant dependence across the 10 scam types. Student type, scam type, and their interaction were included as predictors, with age, gender, and tech background entered as covariates. We used additional logistic regression models to examine whether a report was filed and the reporting channels used.

Finally, for RQ3, we used logistic regression to model the advice sources participants consulted (social media platforms and interpersonal sources), with student type as the predictor and age and gender as covariates; training resources were summarized descriptively.

We applied the Benjamini–Hochberg procedure to control the false discovery rate across multiple statistical tests [2].

3.4.2 Qualitative Analysis

Many multiple-choice questions in our survey included an "Other, please specify" option. Two researchers independently coded all of these responses. They assessed whether each response could be mapped to an existing category (i.e., deductive thematic analysis). For example, scenario actions were categorized into one of three engagement levels, or new cat-

egories were generated when the response did not fit within the existing schema. The coders met to resolve disagreements and agreed on a final code for each response.

Our survey included three sets of open-ended questions that were analyzed through inductive thematic analysis: participants' explanations for scenario actions, experiences (not) reporting scams, and training/other resources participants have experienced or would like. For all three sets, the first author developed an initial codebook using a subset of the data (n=40). Two team members reviewed the codebooks and the subset of coded data. Disagreement about the coding and codebook was discussed with the first author to refine the initial codebook.

Full coding of the data differed across question categories. For scenario reasoning, four team members independently coded an additional subset of the data (n=50), refined the codebook accordingly, and resolved all disagreements through discussion. Two of the four then double-coded the remaining data, resolving all disagreements. For the scam reporting reasoning and the training/other resources responses, two pairs of coders iteratively coded 50-response subsets and met to resolve disagreements and modify the codebook as needed. This process was repeated until the codebook stabilized, at which point they split the remaining data for independent coding. Substantial agreement was defined as Krippendorff's $\alpha \geq 0.8$. Krippendorff's α is suitable when multiple codes may be applied to the same response [35].

It should be noted that the highest α reached on responses for scam reporting reasoning was slightly below the threshold (0.79), falling into the range for "tentative" conclusions [35]. To account for this, the coders dual-coded all reporting reasoning responses. Differences in coding were reconciled collaboratively.

3.5 Limitations

Conclusions about differences between international and domestic students are specific to the scenarios presented and should not be generalized to other scenarios. Nevertheless, this approach allows for controlled comparisons while preserving ecological validity. We also prioritized comparison power over mirroring population proportions, which constrains population-level claims. In addition, although we tried to simulate realistic scenarios and elicit authentic responses, participants' reported actions may not fully reflect their behavior in real life due to a lack of pressure and time constraints. We recruited participants interested in sharing their experience with scams, which may introduce self-selection bias.

4 Results

4.1 Participants

We received 1,097 complete survey submissions. After excluding duplicates and participants with invalid institutional email addresses, we included 1,074 responses in our final data set: 333 from CMU, 96 from Barnard, 244 from FIU, 201 from IU, and 200 from Amherst. Of these, 391 participants identified as non-permanent residents or non-U.S. citizens, 653 identified as U.S. citizens, and 30 identified as U.S. permanent residents (green card holders) but not U.S. citizens. Our final sample consisted of 391 international students and 683 domestic students. Overall, 444 participants identified as men, 568 as women, 11 as non-binary, and 52 preferred not to disclose their gender. Our participants were 53% undergraduate students ($n = 567$), 29% master's students ($n = 308$), 17% PhD students ($n = 187$), and 1% enrolled in professional or other programs (DDS/DMD, JD, MD/DO, MBA, and other; $n = 12$). A total of 648 participants reported studying computer science or engineering-related disciplines, while 426 reported studying non-technical fields. The fields of study most commonly represented were computer science ($n = 366$), engineering ($n = 207$), data science ($n = 119$), biology ($n = 39$), and information systems ($n = 33$).

Our international student participants reported spending most of their time before age 18 in 56 countries, with the top three being India ($n = 165$), mainland China ($n = 46$), and Bangladesh ($n = 25$). Among them, 129 had been in the U.S. for less than one year, 222 for one to five years, and 40 for more than five years. 120 identified as native English speakers, while 271 identified as non-native speakers. Most reported currently holding an F-1 student visa ($n = 374$), followed by J-1 exchange visitor visas ($n = 8$) and other visa types ($n = 9$). International students self-reported their English proficiency across reading, listening, writing, and speaking. Although the majority of non-native speakers indicated being at least "quite" proficient in all domains, 13.3% and 16.3% reported moderate or lower proficiency in speaking and writing, respectively.

We refer to participants with a code that indicates their university and whether they are a domestic (d) or international (i) student (e.g., B24d refers to participant 24 from Barnard, a domestic student).

4.2 RQ1. Scenarios

4.2.1 International vs. Domestic Students

We conducted multinomial logistic regression analyses to compare domestic and international students' engagement behaviors across our five suspicious scenarios. "Disengage" was used as the reference category, with "cautiously engage" and "fully engage" as comparison categories. For suspicious scenarios, we treated "fully engage" as the highest-risk response. However, "cautiously engage" was also considered unsafe, as continuing the interaction may still cause participants to disclose their personal information. Figure 2 shows participants' engagement behaviors across all 10 scenarios by student type. We observed significant differences between international and domestic students in four of the five suspicious scenarios. No

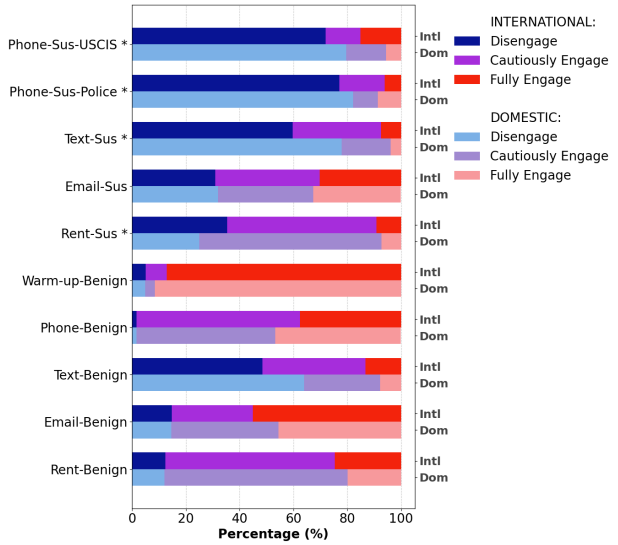


Figure 2: Engagement behavior across scenarios for international and domestic students. * indicates the difference between the two student groups is statistically significant.

significant differences were found in the suspicious email scenario or in any of the five benign scenarios. See Table 3 (supplementary materials) for all scenario statistics.

For the two suspicious phone call scenarios, participants performed relatively well: over 70% of both domestic and international students chose to immediately disengage. Specifically, 79.6% of domestic students and 72.0% of international students disengaged in *Phone-Sus-USCIS*, while 82.2% of domestic students and 77.1% of international students disengaged in *Phone-Sus-Police*. Interestingly, although each scenario was designed to be applicable primarily to one student group, a non-trivial proportion of participants from the non-target group still indicated engagement: 14.8% (cautious) and 5.7% (full) of domestic students engaged with callers claiming to be USCIS officers, referencing documents unlikely to be relevant to them. Similarly, 16.8% (cautious) and 6.1% (full) of international students engaged with a jury duty-related scenario that would not typically apply to them.

We found that international students were significantly more likely than domestic students to fully engage with the suspicious caller in the USCIS scenario rather than disengage. They were also significantly more likely to cautiously engage in the jury duty scenario rather than disengage.

We observed a substantial difference between international and domestic students in their likelihood of disengaging from the suspicious text scenario. Specifically, 78.0% of domestic students chose to disengage compared to 59.7%of international students. Correspondingly, a higher proportion of international students selected cautiously engage (32.8% vs. 18.1%) and fully engage (7.5% vs. 3.9%). In this fake delivery scenario, international students were significantly more likely to both cautiously engage and fully engage compared to domestic students.

Compared to the suspicious call and text message scenarios, participants were less likely to disengage in the email and rental scenarios. Only 32.0% of domestic students and 30.9% of international students immediately disengaged in the email scenario, while 25.0% and 35.4% disengaged in the rental scenario, respectively. We did not observe a significant difference in the engagement behavior of domestic and international students in the email scenario. In contrast, international students were significantly less likely than domestic students to cautiously engage rather than disengage in the rental scenario. This suggests that international students were more cautious than domestic students in the rental context.

We conducted binary logistic regression analyses to compare domestic and international students' engagement behaviors across the five benign scenarios. We treated "disengage" as the reference category and combined "cautiously engage" and "fully engage" into a single engagement category.

We observed a high baseline level of trust in both student groups across all benign scenarios, except for *Text-Benign*. In the remaining benign scenarios, fewer than 15% of participants chose to immediately disengage. In contrast, participants were more likely to disengage in the *Text-Benign* scenario, with 63.9% of domestic students disengaging compared to 48.4% of international students, though this difference was not statistically significant. This pattern may reflect heightened skepticism overall toward unsolicited text messages, possibly due to the prevalence of text-based scams.

We found no statistically significant differences between domestic and international students in engagement behavior across any of the benign scenarios. This suggests that the heightened engagement observed among international students in suspicious scenarios is not attributable to a general tendency to engage across contexts, but rather reflects a context-specific response to deceptive cues.

In addition, we applied signal detection theory to compute sensitivity (d') and response bias (c) for each group (see Table 12). Both groups demonstrated comparable sensitivity (domestic $d' = 0.816$; international $d' = 0.807$), indicating a moderate and similar capacity to distinguish between suspicious and benign scenarios. Although international students exhibited a slightly higher response bias (domestic $c = 0.282$; international $c = 0.341$), this was not statistically significant after multiple testing correction. This suggests a slight tendency for international students to require stronger evidence before disengaging or classifying a scenario as a scam.

4.2.2 Gender, Age, Tech Background, Scenario Order, and Advice Seeking

While age was initially identified as a significant factor in four out of the ten scenarios, suggesting that older participants generally exercise more caution, only the *Phone-Sus-Police* sce-

nario remained significant after correction ($p = 0.021$). Similarly, while women were found to be significantly more cautious in two scenarios (*Phone-Sus-USCIS* and *Text-Benign*) prior to correction, this significance disappeared after adjusting for multiple testing. This suggests that age and gender are not consistent predictors of engagement behavior across the scenarios presented. Across all scenarios, we found no significant differences in engagement behavior based on technical background. The scenario ordering was largely non-significant, with the exception of the *Rent-Sus* scenario ($p = 0.030$). In this case, participants were more likely to cautiously engage rather than disengage if the scenario appeared later. We added student-type × advice-seeking interactions to the four scenarios with significant international/domestic differences; after BH correction, no interaction reached significance, indicating that advice-seeking does not moderate the international/domestic engagement gap (see Table 4).

4.2.3 International students only

We ran scenario-level regressions among international students for scenarios where we observed a significant difference between the two student groups, using two predictors: country of origin and time in the U.S. Comparing the three largest national-origin subgroups (India, mainland China, Bangladesh), we found no significant differences in engagement, though small cell counts warrant caution in interpreting this null. We did not include English proficiency as a predictor, since 86% of non-native speakers reported average proficiency >= 4.0 ("Quite Well"; median=5.0), and this limited variation caused model separation. Using time in the U.S. (Recent, <1 year vs. Established, 1+ year), results were scenario-specific: recent and established students showed comparable engagement in both phone scenarios and the rental scenario, while recent arrivals were significantly more likely to engage in the Text-Sus scenario.

4.2.4 Scenario Reasoning

For each scenario they were shown, participants briefly stated the reasoning behind their engagement decision. For suspicious scenarios, the most commonly cited reason involved identifying common red flags, particularly the request for sensitive information or money ($n = 371$); the only scenario where this reasoning was not commonly used was the suspicious email scenario, in which participants were asked to click on a link and send their resume as opposed to providing information deemed sensitive (e.g., SSN). Additionally, participants mentioned their own personal rules ($n = 337$) such as never clicking links they did not recognize or refusing to share certain information if contacted unsolicited. Participants also choose to disengage or cautiously engage as a result of the sender/caller's unverified identity ($n = 313$) and a mismatch between the situation and their expectation regarding how similar situations should work in real life ($n = 311$).

For benign scenarios, participants most commonly said their decisions were based on a sense of trust in the person requesting their information ($n = 596$), often due to recognizing legitimate email addresses or domains Participants also mentioned trusting communications they perceived as stemming from their request ($n = 504$), especially in the warm-up scenario. Even when considering the scenario as benign, many participants still used caution and indicated that they hoped to verify the person's identity($n = 314$), or verify the situation by initiating contact via a separate channel ($n = 280$).

4.3 RQ2. Scam Experience and Response

4.3.1 Scam Types

We examined participants' prior encounters with, responses to, and losses resulting from 10 scam types, as summarized in Table 1. Job, delivery, and tech support scams were the most frequently reported and were also associated with the highest percentage of loss. Unknown-language, job, and delivery scams had the highest response rates. Note that we define loss broadly to include financial losses, exposure of both sensitive and non-sensitive information, emotional distress, and time loss. As a result, even participants who did not report responding to a scam may still have experienced some form of loss.

We found statistically significant differences (see Table 5) in reported encounters for five scam types: delivery, financial aid, tech support, job, and non-immigration authority scams. In each case, the odds ratio (International vs. Domestic) was below 1, indicating that domestic students were significantly more likely than international students to report encountering these scam types. No statistically significant differences in the likelihood of responding were found among those who encountered each of the ten scam types (see Table 6).

International students reported significantly higher odds of experiencing loss in five of the ten scam types (see Table 7). These included two authority-based scams—foreign authority and immigration authority—as well as rental, unknown-language, and job scams. As shown in Table 8, participants most commonly reported time loss (9.2%) and emotional distress (5.8%), while financial loss (1.7%) and sensitive information loss (1.3%) were less frequent.

4.3.2 Scam Reporting

We asked participants to select all channels they had used to report a scam (see Table 2). Overall, 73.9% of domestic students and 64.5% of international students indicated using at least one of the reporting channels presented. This difference was statistically significant, with domestic students more likely to report a scam overall (see Table 10 for statistics).

Phone or app-based filters/blockers were the most frequent reporting method for both groups (63.3% among domestic

Table 1: Scam encounter, response, and loss rates by student type. Significant differences are highlighted in blue.

Scam Category	Encounter		Respond		Loss	
	Dom.	Intl.	Dom.	Intl.	Dom.	Intl.
Foreign Authority	6.6%	10.3%	0.3%	1.8%	7.5%	16.1%
Immigration Authority	12.0%	15.1%	0.9%	2.3%	4.7%	9.7%
Non-Immigration Authority	27.5%	17.1%	1.6%	2.0%	9.8%	10.2%
Unknown Language	37.9%	38.4%	7.0%	7.2%	11.1%	18.7%
Relationship	15.4%	20.7%	3.5%	4.1%	7.3%	10.5%
Job	81.9%	65.6%	10.0%	7.4%	24.2%	32.5%
Financial Aid	27.6%	22.1%	3.1%	1.0%	9.5%	10.7%
Delivery	82.4%	50.4%	7.3%	7.4%	22.1%	21.5%
Tech Support	78.3%	49.0%	6.3%	5.6%	25.3%	23.3%
Rent	23.1%	27.4%	4.7%	7.7%	10.0%	19.2%

Table 2: Reporting channel used by student type and victim status. Significant differences are highlighted in blue.

Reporting Channel	Total Group		Victims Only	
	Dom. ($N = 683$)	Intl. ($N = 391$)	Dom. ($n = 354$)	Intl. ($n = 224$)
Any Report Made	73.9%	64.5%	79.7%	68.3%
Law Enforcement (Police)	3.7%	11.5%	4.2%	13.4%
Phone/App Filters	63.3%	45.5%	63.8%	47.8%
Online Platforms	34.6%	26.3%	41.2%	29.9%
University Department	15.5%	21.5%	18.6%	20.5%
Bank/Financial Inst.	12.2%	11.0%	17.2%	14.3%
Gov. Websites (FTC/FCC)	6.0%	4.1%	8.5%	4.9%

students vs. 45.5% among international students), followed by reporting through the online platform where the scam occurred (34.6% vs. 26.3%, respectively). Government websites and law enforcement were least frequently used for reporting. However, a significantly higher proportion of international students reported contacting law enforcement compared to domestic students (11.50% vs. 3.70%). In contrast, domestic students were significantly more likely to use built-in phone/app filters or blockers and to report directly to online platforms. We conducted a follow-up analysis limited to victims (i.e., participants who reported experiencing any form of loss), and the observed pattern remained unchanged. Table 2 presents the number of domestic and international student participants who selected each reporting channel, both overall and among victims only.

We asked participants to explain their reasoning behind their reporting decisions in order to contextualize and better interpret these findings. Participants report scams out of loss, vengeance, altruism, or convenience, with convenience mentioned most frequently ($n = 259$). Many who reported via a built-in phone or app feature did so because "it is easy and convenient to report this way" (C23d), and those who did not report cited "a very time consuming process that just doesn't seem worth it in my opinion" (B18i). Those who did report scams via one method sometimes explained that they did not report further because of the additional effort involved.

Participants' belief in the usefulness of their report was central. Many reported scams altruistically to protect others ($n = 127$), with one noting, "I want to let other people know so that they can avoid the scam" (A84i). Others expressed a moral sense of responsibility ($n = 15$), describing reporting as "the least I could do" (C58d). Some said that they reported for accountability, hoping the scammers "will get caught and stop" (I28d).

Participants also reported scams to prevent more messages from the same scammer ($n = 219$). I72i, who used the reporting feature on their phone, explained that "I don't want to have same scam message being sent again and again."

Loss (or lack thereof) was also a factor. Participants who had suffered significant losses (by their definition) ($n = 55$) reported their scams both to recoup their losses (B29d wrote, "I contacted my bank in order to get [my money] back") and for retribution (C245d wrote, "I was desperate to get back at the scammers"). Conversely, those who experienced little or no loss often did not report ($n = 117$).

Some participants were also unaware of how to make a report ($n = 43$). For example, B94d stated, "I do not know who to report to if I receive scams." Others seemed to be unaware that reporting was an option. C48d stated, "I... didn't know we were supposed to report scams oops."

These findings align with prior work that found convenience and loss as major factors in scam reporting [33]. We did not observe qualitative differences between international and domestic student motivations, except for the former sometimes mentioning their identity (e.g., C229i stating "I am an international student and I have to take care of any danger").

4.4 RQ3. Resources, Training, and Advice

4.4.1 Internal Training

Over 80% of students reported receiving anti-scam training from their universities (83.6% of domestic students and 89.0% of international students). The most frequently recalled types of training include general scam awareness during orientation (56.1% domestic, 60.1% international), reminder or warning emails (58.0% domestic, 53.2% international), and phishing simulation emails (43.8% domestic, 50.1% international). 55.8% of international and 53.8% of domestic students stated that they felt somewhat or well prepared as a result of their university's anti-scam training, while 7.2% of international students and 6.2% of domestic students said they did not feel prepared despite the training and 15.7% of domestic and 22.9% of international students did not remember receiving any training. In addition, 24.3% of domestic students and 14.1% of international students said they already felt well prepared, and training did not change that.

When asked about the types of university resources that would be most helpful, students most frequently mentioned phishing simulations ($n = 168$), in which they receive realistic test emails. Some students preferred this approach due

to it being memorable, with one participant sharing that this "teach[es] you about scams in a way embarrassing enough that you might remember" (C33d). One participant drew a comparison between phishing training and "fire drills," suggesting that this training needed to occur more often at universities because they "encounter fire less often than scams" (C52i).

Participants expressed a desire for greater depth in scam education, including detailed case studies ($n = 69$), exposure to sophisticated scam tactics, and explicit demonstrations of common red flags ($n = 88$). Several participants noted that the "examples provided by universities are too simplistic" (B22d) and wanted to see how scams unfold in practice. They also preferred structured, potentially in-person classes or workshops ($n = 36$), as opposed to the "Security 101" format, which is usually self-paced and asynchronous.

International students were asked whether they had received training specifically tailored to international students. Of the 391 international student participants, 157 reported that they did not remember or were unsure, and 144 indicated that they had not received such training. Only 90 participants reported having received international-student–specific training (including at least 9 from each of the universities), suggesting that such training was probably provided, but students may not have attended, or it may not have been memorable.

4.4.2 Advice Seeking and External Training

We asked participants where they had sought advice related to scams (see Table 9). A higher proportion of international students reported seeking help from other people (77.2% domestic vs. 88.0% international), as well as from social media platforms (68.5% domestic vs. 77.0% international).

Reddit was the most frequently used online source for scam-related advice, with more than half of participants reporting that they had consulted Reddit ($n = 592$). A few students also shared that they turned to LLMs for support ($n = 9$), such as copying and pasting the email in question to ChatGPT, or searching online ($n = 47$) for "other users that have encountered the same issue and how they dealt with it" (F85d). Family (52.3%) and friends (51.6%) were the two most commonly reported interpersonal sources of support, whereas government websites (6.5%) and student communities (2.0%) were among the least frequently used.

International students were significantly more likely to seek help from friends (45.8% vs. 61.6%) and peers (18.3% vs. 32.2%). Similarly, international students were significantly more likely to seek advice from YouTube (13.6% vs. 27.4%) and Instagram (9.1% vs. 14.6%). This suggests that international students may rely more heavily on their interpersonal and online networks compared to domestic students when navigating scam-related incidents.

We asked participants to comment on additional resources they would find helpful. One common theme was the desire for a comprehensive list or up-to-date database of common scam types ($n = 44$) to support quick verification. This approach would allow for "[a] more reliable/accessible list of new and common scams" (F132d) to be accessed when faced with a potentially risky situation.

Similarly, participants wanted dedicated scam support platforms ($n = 43$). C91d suggested a "hotline for if you got scammed" and B50d suggested a government website "where each type of scam is cataloged for easy access/search, and appropriate reporting channels." While government websites for scam reporting and education already exist in multiple places (e.g., [13, 21, 69, 71, 72]), the U.S. does not currently have a central place for scam reporting and information.

Finally, participants noted the usefulness of engaging videos ($n = 39$), including content primarily designed to be "entertaining," such as "[scam-baiting] videos," (C56d) where creators deliberately waste a scammers' time and post the interaction online. Though not explicitly for educational purposes, such content can still help shape viewer perceptions.

5 Discussion

5.1 Higher Baseline for Disengagement

Our findings argue against framing international students as uniformly more vulnerable to scams. Both groups were susceptible, but not in the way commonly assumed. Detection ability was comparable, and domestic students reported higher exposure to common scam types. International students' vulnerability, therefore, does not stem from greater exposure or weaker detection. What differed was engagement in specific contexts and patterns of loss and reporting.

Interestingly, when asked to recall prior scam encounters, international students were not more likely than domestic students to report responding. However, when presented with hypothetical scam scenarios, international students demonstrated a greater likelihood of engagement in certain contexts, particularly phone call and text-based scenarios, while being less likely to engage in rental scenarios. As neither self-reports of behavior nor hypothetical scenarios may fully capture context-specific engagement behaviors, we combine these approaches to form a more nuanced and authentic picture of scam vulnerability.

International students appeared to require stronger cues before disengaging in certain contexts—often authority-related or involving compelling lures or threats, with higher perceived stakes of ignoring the message. This pattern is consistent with the Protection Motivation Theory [4], which holds that protective behavior depends on both *threat appraisal* and *coping appraisal*. The comparable detection we observed suggests intact coping appraisal across groups. For international students, however, authority- and immigration-framed scenarios carry unusually high perceived stakes: failing to heed a message that could affect legal status feels costly, so engagement may reflect a threat-driven attempt at resolution rather than a

failure to recognize the scam.

5.2 Strong Support but Fewer Reports

Although many international students in our sample had been in the U.S. for only a limited time, some for less than 1 year ($n = 129$), they reported having strong peer support networks, which they relied on more often for scam-related advice than domestic students. They also reported greater use of online resources. This pattern may reflect greater uncertainty when navigating suspicious situations or responding to losses.

Despite stronger advice-seeking tendencies and higher losses in certain scam categories, international students were less likely overall to report scams, including through phone filters/blockers and online platforms, though they were more likely to report to the police. While more than half of participants recalled receiving university-provided training, over one-third of international students could not recall any international-specific training and another third reported receiving none, suggesting such training may be insufficiently delivered or salient. Recognizing scam patterns and red flags is likely easier when students can draw on prior exposure to similar formats. These findings suggest that existing training, with generic orientation training and warning emails mentioned most often, may not effectively increase awareness of reporting channels or guide decision-making. Both student groups also reported limited familiarity with formal reporting mechanisms, with some unaware of reporting as an option.

5.3 Recommendations

Identifying High-Risk Scenarios. In both phone-based authority impersonation and text-based delivery scams, international students were more likely to continue engaging even after spotting "red flags." Future research should explore a wider range of contexts and communication channels to identify others to which international students are especially vulnerable. Consequently, intervention materials should clearly identify red flags in these scenarios to help international students disengage faster, especially if their judgment is clouded by high-pressure lures or the fear of missing out.

Recurring, Scenario-based, Multi-Channel Training. Current university scam training is often generic, limited to orientation periods, and fails to leave a lasting impression on students. We recommend transitioning to a recurring training model that incorporates engaging, interactive content. Our results suggest that presenting students with hypothetical scenarios featuring carefully embedded red flags can be an effective tool for observing engagement behavior. We therefore recommend integrating these scenario-based simulations into university scam training and leveraging interactive approaches that have been used successfully for email phishing awareness training [36]. Notably, in the email job scam scenario, international students were no more likely to engage, despite the inclusion of "visa sponsorship" as a lure, many of which recognized the offer as too-good-to-be-true, suggesting that prior exposure to similar scam formats effectively deters against further engagement. We therefore recommend expanding simulations beyond email to text- and phone-based scenarios, in collaboration with campus police and information security offices. Future work should evaluate whether such multi-channel training reduces engagement and whether tailoring it to international and domestic students' distinct vulnerabilities improves effectiveness.

Multi-Platform Mock Reporting Simulations. International students should receive technical guidance on built-in security features, such as call-blocking and message-filtering tools, tailored to different platforms (e.g., Android, iOS). Students should also be introduced to specific reporting channels, including both platform-based tools and government resources. Furthermore, we recommend a training component that allows students to practice reporting scams. Students may be less likely to use a channel that they are unfamiliar with when they are already in distress. We suggest that universities, in conjunction with federal reporting sites and online platforms such as Zillow or Facebook Marketplace, design training modules that allow users to simulate the reporting process, thus building the necessary procedural familiarity for students to act effectively during real-world scam encounters.

6 Conclusion

We conducted an online survey of 1,074 students across five U.S. universities to examine scam engagement behaviors, prior encounters and reporting experiences, perceptions of anti-scam training, and advice-seeking. Our findings reveal that international students were more likely to engage in phone- and text-based scam scenarios, but less likely to engage in rental platform scenarios. Although domestic students reported encountering more generic scams, we observed no differences in response likelihood. However, international students reported significantly higher loss in foreign-authority, immigration-authority, rental, and unknown-language scams. Despite similar ability to detect suspicious cues, international students were less likely to disengage in high-stakes or authority-related contexts. Domestic students were more likely to report scams overall, particularly through built-in blockers and online platforms, whereas international students were more likely to contact law enforcement. International students reported greater reliance on peer networks and online sources. We find that vulnerability differences arise not from exposure or detection ability, but from context-specific engagement and reporting patterns. This study offers one of the first quantitative comparisons of scam experiences between international and domestic students and underscores the need for scenario-based, multi-channel training.

Acknowledgments

This work was supported in part by the Hima and Jive Fellowship in Computer Science at Carnegie Mellon University. We also thank the Carnegie Mellon University Police Department for consulting on the scenario design.

References

[1] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L Mazurek, Dana Cuomo, et al. Sok: Safer digital-safety research involving at-risk users. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 635–654. IEEE, 2024.

[2] Yoav Benjamini and Yosef Hochberg. Controlling the false discovery rate: a practical and powerful approach to multiple testing. *Journal of the Royal Statistical Society: Series B (Methodological)*, 57(1):289–300, 1995.

[3] Morvareed Bidgoli and Jens Grossklags. "Hello. This is the IRS calling.": A case study on scams, extortion, impersonation, and phone spoofing. In *2017 APWG Symposium on Electronic Crime Research (eCrime)*, pages 57–69. IEEE, 2017.

[4] Hendrik Boer and Erwin R Seydel. Protection motivation theory. In *Predicting Health Behaviour: Research and Practice with Social Cognition Models. eds. Mark Conner, Paul Norman*, pages 95–120. Open University Press, 1996.

[5] Elijah Robert Bouma-Sims, Lily Klucinec, Mandy Lanyon, Julie Downs, and Lorrie Faith Cranor. The kids are all right: Investigating the susceptibility of teens and adults to YouTube giveaway scams. In *NDSS*, 2025.

[6] Roderic G Broadhurst, Katie Skinner, Nicholas Sifniotis, Bryan Matamoros-Macias, and Yuguang Ipsen. *Phishing and cybercrime risks in a university student community*. Australian Institute of Criminology, 2020.

[7] Alejandra Diaz, Alan T Sherman, and Anupam Joshi. Phishing in an academic community: A study of user susceptibility and behavior. *Cryptologia*, 44(1):53–67, 2020.

[8] Prakriti Dumaru, Ankit Shrestha, Rizu Paudel, Arezou Behfar, Hanieh Atashpanjeh, and Mahdi Nasrullah Al-Ameen. "I have learned that things are different here": Understanding the transitional challenges with technology use after relocating to the USA. In *International Conference on Human-Computer Interaction*, pages 201–220. Springer, 2023.

[9] Editorial Team. Student housing scams in 2026: How students can rent safely in a digital-first world. https://www.theblueground.com/blog/find-your-home/student-housing-scams-2026/, n.d. Accessed: 2026-02-18.

[10] Federal Bureau of Investigation. FBI warns of spike in rental and real estate scams. https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-spike-in-rental-and-real-estate-scams, 2023. Accessed: 2026-02-15.

[11] Federal Bureau of Investigation. FBI releases annual internet crime report. https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report, April 2025. Accessed: 2026-02-16.

[12] Federal Communications Commission. How to identify and avoid package delivery scams. https://www.fcc.gov/how-identify-and-avoid-package-delivery-scams, n.d. Accessed: 2026-02-15.

[13] Federal Communications Commission. Scam glossary. https://www.fcc.gov/scam-glossary, n.d. Accessed: 2026-02-15.

[14] Federal Student Aid. Scams. https://studentaid.gov/resources/scams, n.d. Accessed: 2026-02-15.

[15] Federal Trade Commission. Scammers impersonate well-known companies to recruit for fake jobs on linkedin and other job platforms. https://consumer.ftc.gov/consumer-alerts/2023/08/scammers-impersonate-well-known-companies-recruit-fake-jobs-linkedin-other-job-platforms, 2023. Accessed: 2026-02-15.

[16] Federal Trade Commission. College students: Avoid scammers while you job hunt. https://consumer.ftc.gov/consumer-alerts/2025/05/college-students-avoid-scammers-while-you-job-hunt, June 2025. Accessed: 2026-02-16.

[17] Federal Trade Commission. FTC analysis shows consumers have lost millions to rental scams. https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-analysis-shows-consumers-have-lost-millions-rental-scams, December 2025. Accessed: 2026-02-16.

[18] Federal Trade Commission. Job scammers are looking to hire you! https://consumer.ftc.gov/consumer-alerts/2025/07/job-scammers-are-looking-hire-you, 2025. Accessed: 2026-02-15.

[19] Federal Trade Commission. Scammers are using fake websites to twist jury duty scams. https://consumer.ftc.gov/consumer-alerts/2025/08/scammers

-are-using-fake-websites-twist-jury-duty-scams?utm_source=govdelivery, 2025. Accessed: 2026-02-15.

[20] Federal Trade Commission. Think that text message is from USPS? It could be a scam. https://consumer.ftc.gov/consumer-alerts/2025/04/think-text-message-usps-it-could-be-scam, 2025. Accessed: 2026-02-15.

[21] Federal Trade Commission. Top scams of 2024. https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024, 2025. Accessed: 2026-02-15.

[22] Federal Trade Commission. How to avoid scholarship and financial aid scams. https://consumer.ftc.gov/articles/how-avoid-scholarship-and-financial-aid-scams, n.d. Accessed: 2026-02-15.

[23] FedEx. How to pay duties & taxes on imported goods. https://www.fedex.com/en-si/customer-support/faq/duties-taxes-imported-goods/paying-duties-taxes/how-to-pay-duties-taxes.html, n.d. Accessed: 2026-02-15.

[24] Christine Geeng, Mike Harris, Elissa Redmiles, and Franziska Roesner. "Like lesbians walking the perimeter": Experiences of U.S. LGBTQ+ folks with online security, safety, and privacy advice. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 305–322, 2022.

[25] Arup Kumar Ghosh, Karla Badillo-Urquiola, Mary Beth Rosson, Heng Xu, John M Carroll, and Pamela J Wisniewski. A matter of control or safety? examining parental use of technical monitoring apps on teens' mobile devices. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2018.

[26] Kristen K. Greene, Michelle P. Steves, Mary F. Theofanos, and Jennifer A. Kostick. User context: An explanatory variable in phishing susceptibility. In *Proceedings of the Workshop on Usable Security (USEC)*, February 2018.

[27] Tamy Guberek, Allison McDonald, Sylvia Simioni, Abraham H Mhaidli, Kentaro Toyama, and Florian Schaub. Keeping a low profile? technology, risk and privacy among undocumented immigrants. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2018.

[28] LD Herrera and John Hastings. The trajectory of romance scams in the US. In *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, pages 1–6. IEEE, 2024.

[29] David W Hosmer Jr, Stanley Lemeshow, and Rodney X Sturdivant. *Applied logistic regression*. John Wiley & Sons, 2013.

[30] Institute of International Education. International students in the united states: 2023/24 open doors report, 2024. Accessed: 2025-09-01.

[31] Internet Crime Complaint Center. Public service announcement: 2025 internet crime report preparations. https://www.ic3.gov/PSA/2025/PSA250513, 2025. Accessed: 2026-02-15.

[32] Rebecca A Judges, Sara N Gallant, Lixia Yang, and Kang Lee. The role of cognition, personality, and trust in fraud victimization in older adults. *Frontiers in Psychology*, 8:248182, 2017.

[33] Steven Kemp. Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*, 19(5):994–1015, 2022.

[34] Jennifer Klütsch, Jasmin Schwab, Christian Böffel, Verena Zimmermann, and Sabine J Schlittmeier. Friend or phisher: how known senders and fear of missing out affect young adults' phishing susceptibility on social media. *Humanities and Social Sciences Communications*, 11(1):1–14, 2024.

[35] Klaus Krippendorff. Reliability. In *Content Analysis: An Introduction to Its Methodology*. Sage publications, 4th edition, 2019.

[36] Ponnurangam Kumaraguru, Steve Sheng, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Teaching johnny not to fall for phish. *ACM Trans. Internet Technol.*, 10(2), June 2010.

[37] Jesse Leavenworth. Connecticut officials warn of job recruitment scams targeting college students. https://www.ctinsider.com/connecticut/article/job-recruitment-scam-warning-ct-ag-tong-21020124.php, 2025. Accessed: 2026-02-15.

[38] Matthew Lee. Trump administration is reviewing all 55 million foreigners with U.S. visas for any violations. *The Associated Press*, August 2025. Accessed 27 August 2025.

[39] Roxanne Leitão. Digital technologies and their role in intimate partner violence. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, pages 1–6, 2018.

[40] Xiao Fan Liu, Yushi Ai, Li Crystal Jiang, Xiaohui Wang, and Ye Wu. Understanding the human element in scams: a multidisciplinary approach. *Journal of Information Technology Case and Application Research*, 27(1):9–24, 2025.

[41] Henry B Mann and Donald R Whitney. On a test of whether one of two random variables is stochastically larger than the other. *The Annals of Mathematical Statistics*, pages 50–60, 1947.

[42] Allison McDonald, Catherine Barwulor, Michelle L Mazurek, Florian Schaub, and Elissa M Redmiles. "It's stressful having all these phones": Investigating sex workers' safety goals, risks, and practices online. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 375–392, 2021.

[43] Ethan Morrow. Scamming higher ed: An analysis of phishing content and trends. *Computers in Human Behavior*, 158:108274, 2024.

[44] James Nicholson, Yousra Javed, Matt Dixon, Lynne Coventry, Opeyemi Dele Ajayi, and Philip Anderson. Investigating teenagers' ability to detect phishing messages. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 140–149. IEEE, 2020.

[45] Rajvardhan Oak and Zubair Shafiq. "Hello, is this Anna?": Unpacking the lifecycle of pig-butchering scams. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 1–18, 2025.

[46] Rajvardhan Oak and Zubair Shafiq. Victims, vigilantes, and advice givers: An analysis of scam-related discourse on reddit. In *Twenty-First Symposium on Usable Privacy and Security (SOUPS 2025)*, pages 57–71, 2025.

[47] Office of International Services, North Carolina State University. Scam information & alerts. https://internationalservices.ncsu.edu/scam-information-alerts/, 2025.

[48] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. Dissecting spear phishing emails for older vs young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 6412–6424, 2017.

[49] Katalin Parti. "Elder scam" risk profiles: Individual and situational factors of younger and older age groups' fraud victimization. *International Journal of Cybersecurity Intelligence & Cybercrime*, 5(3), 2022.

[50] Juan Manuel Pedroza. Making noncitizens' rights real: Evidence from immigration scam complaints. *Law & Policy*, 44(1):44–69, 2022.

[51] Pennsylvania Office of the Attorney General. Beware of scams targeting college and graduate students. https://www.attorneygeneral.gov/protect-yourself/consumer-advisories/beware-of-scams-targeting-college-and-graduate-students/, n.d. Accessed: 2026-02-15.

[52] Pew Research Center. About a third of Americans say they've had an online shopping scam happen to them. https://www.pewresearch.org/short-reads/2025/11/19/about-a-third-of-americans-say-theyve-had-an-online-shopping-scam-happen-to-them/, November 2025. Accessed: 2026-02-16.

[53] Md Lutfor Rahman, Daniel Timko, Hamid Wali, and Ajaya Neupane. Users really do respond to smishing. In *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, pages 49–60, 2023.

[54] Reddit user u/Unknown. "how do international students usually find accommodation…". Post on the *r/expats* subreddit, https://www.reddit.com/r/expats/comments/1oi16pz/how_do_international_students_usually_find/, n.d. Accessed: 2026-02-15.

[55] Reddit user u/Unknown. "random email about software opportunities at…". Post on the *r/cscareerquestions* subreddit, https://www.reddit.com/r/cscareerquestions/comments/2nmrb9/random_email_about_software_opportunities_at/, n.d. Accessed: 2026-02-15.

[56] Reuters. Trump administration moves to tighten duration of visas for students and media. *Reuters*, August 2025. Accessed 27 August 2025.

[57] San Diego State University Information Security. Phishing scams & financial aid scams. https://security.sdsu.edu/be-cyber-smart/phishing-scams/financial-aid-scams, n.d. Accessed: 2026-02-15.

[58] Jingjin Shao, Qianhan Zhang, Yining Ren, Xiying Li, and Tian Lin. Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud. *Journal of Elder Abuse & Neglect*, 31(3):225–243, 2019.

[59] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 373–382, 2010.

[60] Lucy Simko, Ada Lerner, Samia Ibtasam, Franziska Roesner, and Tadayoshi Kohno. Computer security and

privacy for refugees in the united states. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 409–423. IEEE, 2018.

[61] Julia Slupska, Selina Cho, Marissa Begonia, Ruba Abu-Salma, Nayanatara Prakash, and Mallika Balakrishnan. "They look at vulnerability and use that to abuse you": Participatory threat modelling with migrant domestic workers. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 323–340, 2022.

[62] Harold Stanislaw and Natasha Todorov. Calculation of signal detection theory measures. *Behavior Research Methods, Instruments, & Computers*, 31(1):137–149, 1999.

[63] Mary Theofanos, Yee-Yin Choong, and Olivia Murphy. 'Passwords keep me safe'–Understanding what children think about passwords. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 19–35, 2021.

[64] Mindy Tran, Collins W Munyendo, Harshini Sri Ramulu, Rachel Gonzalez Rodriguez, Luisa Ball Schnell, Cora Sula, Lucy Simko, and Yasemin Acar. Security, privacy, and data-sharing trade-offs when moving to the United States: Insights from a qualitative study. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 617–634. IEEE, 2024.

[65] Huahong Tu, Adam Doupé, Ziming Zhao, and Gail-Joon Ahn. Users really do answer telephone scams. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 1327–1340, 2019.

[66] UC Berkeley Information Security Office. Students: Beware of employment scams via email. https://security.berkeley.edu/news/students-beware-employment-scams-email, December 2023. Accessed: 2026-02-16.

[67] University of Cincinnati Public Safety. Housing scams. https://www.uc.edu/about/publicsafety/services/crime-prevention/housing-scams.html, n.d. Accessed: 2026-02-15.

[68] University of Washington Information Technology. Employment scams targeting students. https://it.uw.edu/guides/security-authentication/scams-malware-phishing/employment-scams-targeting-students/, n.d. Accessed: 2026-02-15.

[69] U.S. Citizenship and Immigration Services. Common scams. https://www.uscis.gov/scams-fraud-and-misconduct/avoid-scams/common-scams, 2025. Accessed: 2026-02-15.

[70] U.S. Citizenship and Immigration Services. Students and employment. https://www.uscis.gov/working-in-the-united-states/students-and-exchange-visitors/students-and-employment, 2025. Accessed: 2026-02-15.

[71] U.S. Department of Education, Federal Student Aid. Avoid scams and protect yourself. https://studentaid.gov/resources/scams, 2025. Accessed: 2026-02-16.

[72] U.S. Department of Homeland Security. Students: Read these tips to avoid scams. https://studyinthestates.dhs.gov/2018/08/students-read-these-tips-avoid-scams, 2018. Accessed: 2026-02-15.

[73] U.S. Department of Homeland Security. International student life cycle. https://studyinthestates.dhs.gov/students/get-started/international-student-life-cycle, n.d. Accessed: 2026-02-16.

[74] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. "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):1–25, 2018.

[75] Katherine Zhang, Arjun Arunasalam, Pubali Datta, and Z. Berkay Celik. International students and scams: At risk abroad. In *Proceedings of the 47th IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2026.

[76] Sijie Zhuo, Robert Biddle, Lucas Betts, Nalin Asanka Gamagedara Arachchilage, Yun Sing Koh, Giovanni Russello, and Danielle Lottridge. The impact of workload on phishing susceptibility: An experiment. In *Symposium on Usable Security and Privacy (USEC)*, 2024.

[77] Zillow. Leases and marketing FAQ. https://www.zillow.com/rental-manager/leases-marketing-faq/, n.d. Accessed: 2026-02-15.

Appendix

Survey Materials

Headings and words in italics were not shown to participants verbatim.

A. Consent

- Present the consent form
- 4 consent form questions

B. Screening

B.1 Which of the following best describes your citizenship/residency status?

- I am a U.S. citizen
- I am a U.S. permanent resident (green card holder) but not a U.S. citizen
- I am not a U.S. citizen or a U.S. permanent resident (green card holder)

B.2 Please select the country where you spent the majority of your time before turning 18. If you lived in multiple countries for a similar amount of time, choose the one that you feel influenced you the most.

- Insert Qualtrics' built-in **list of countries**: single-choice as a drop-down question

B.3 For verification purposes, please enter the email address associated with your official school account (typically ending in *.edu*). This address will also be used to deliver your compensation. Once the study is complete, we will delete the email address from our records, and it will not be connected to your survey responses.

B.4 Where did you find this survey link?

- Through a university mailing list or newsletter
- From a campus flyer or poster
- From a friend or classmate
- Through social media
- Other (please specify)

C. Official Survey

C.1 Scenarios

Each participant was randomly assigned one scenario from each of these delivery channels below, making it 5 scenarios per participant. The order the scenarios was randomized. Options indicating disengagement are shown in blue; cautious engagement options are shown in black; full engagement options are shown in red. These colors were not shown to participants. Email addresses in the scenarios below are defanged to prevent accidental interaction; participants saw the original unmodified versions.

In this part of the survey, you will be asked to imagine yourself in 5 scenarios where you receive or encounter a form of communication, including a phone call, text, email, or online platform. Please select or describe the actions you would most likely take in each case.

Warm-up benign scenario

Imagine you recently emailed the University Career Center from your university account to ask for advice on your resume. You later receive the following email:

From: careers@<youruniversity>.edu
Subject: Re: Resume help appointment

Hello [Your Name],
Thanks for reaching out for help with your resume. I would be happy to meet with you to review your current resume draft and offer suggestions. This week I am available on Thursday and Friday afternoon from 1 to 5 pm to meet over Zoom. Please reply to this email with your preferred time to meet and you will be added to my schedule and receive a Zoom invite. Please attach the current draft of your resume to your email so I can review it before we meet.
Best regards,
Pat Lopez
Career Consultant
YOURUNIVERSITY Career Center
careers@<youruniversity>.edu

- Reply with your preferred time and attach your resume
- Reply with your preferred time
- Search online for advice
- Contact someone you trust for help
- Block the sender or report the email
- Ignore the email and take no further action
- Other (please specify):

Why did you choose to *(insert option)*? *[Open response]* (*this question was asked for all scenarios, but is not repeated in the Appendix*)

Phone calls

Phone-Sus-USCIS

You receive a phone call and notice that the caller ID displays "USCIS". Once you answer the call, the caller says:

"Hello, are you [Your Name], currently a student at [Your University]?" After you confirm, they continue: "I'm Officer Martinez with U.S. Citizenship and Immigration

Services. Our system indicates your SEVIS information hasn't been updated since your last I-94 renewal. If this isn't corrected, your I-20 could be at risk of termination. Just a quick verification—could you please confirm your date of birth and passport number for our records?"

How would you most likely initially react in this scenario? There's no right or wrong answer; please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- End the call and contact the law enforcement or campus IT department
- End the call and block the caller
- End the call and take no further action
- Stay on the call while searching online for guidance
- Stay on the call while contacting someone you trust for help
- Stay on the call and continue the conversation before deciding what to do
- Share your birthday and passport number
- Other [Please Specify]

Phone-Sus-Police

You receive a phone call and notice that the caller ID displays your city police department. Once you answer the call, the caller says:

"Hello, are you [Your Name]?" After you confirm, they continue: "I'm Officer Martinez with the [Your City] Police Department. Our records show that you have missed your jury duty summons after several reminders. If this isn't resolved immediately, a bench warrant will be issued for your arrest, and you may face a fine. To clear your record today, could you please verify your date of birth and the last four digits of your Social Security Number?"

How would you most likely initially react in this scenario? There's no right or wrong answer; please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- End the call and contact the law enforcement or campus IT department
- End the call and block the caller
- End the call and take no further action
- Stay on the call while searching online for guidance
- Stay on the call while contacting someone you trust for help
- Stay on the call and continue the conversation before deciding what to do
- Share your birthday and last four digits of Social Security Number
- Other [Please Specify]

Phone Benign

Imagine your wallet is missing since yesterday. Today, you receive a phone call, and the caller ID shows your university's campus police. Once you answer the call, the caller says:

"Hi, this is Officer Martinez from the [Your University] Campus Police Department. Someone turned in a wallet with your student ID inside. You can pick it up at our station do you have your student ID number handy so I can confirm it's yours before we log it under your name?"

How would you most likely initially react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- End the call and block the caller
- End the call and take no further action
- End the call and contact campus police directly
- End the call and contact the law enforcement or campus IT department afterward
- Stay on the call while searching online for guidance
- Stay on the call while contacting someone you trust for help
- Stay on the call and continue the conversation before deciding what to do
- Share your student ID number
- Other [Please Specify]

Text messages (SMS)

Text-Sus

Imagine you receive a text message around the time you are expecting a package from overseas. The message says:

"UPS Alert:" Your package **#1Z999AA10123456784** is currently held at customs for missing paperwork. When you have a moment, please review and pay the **$45.20 release fee** here to complete processing:
`http://ups-secure-cx.com/release?ref=1Z999AA10123456784`

How would you most likely initially react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Block the sender
- Use a feature in your text messaging app to report the message
- Ignore the message and take no further action
- Search online for guidance
- Contact someone you trust for help
- Click the link to view the delivery details

- Pay the 45.20 release fee right away, or save the message to pay later
- Other [Please Specify]

Text-Benign

Imagine you receive a text message around the time you are expecting a package from overseas. The message says:

"FedEx: Duties & taxes of USD 45.20 are due for Tracking **#123456789012**. Review & pay securely via FedEx Import Tool `https://c2p.clearance.fedex.com/duty-tax/ui/public/en-si/payment/trknbr`. FedEx will never ask for personal info via text."

How would you most likely initially react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Block the sender
- Use a feature in your text messaging app to report the message
- Ignore the message and take no further action
- Search online for guidance
- Contact someone you trust for help
- Click the link to view the delivery details
- Pay the 45.20 release fee right away, or save the message to pay later
- Other [Please Specify]

Email

Email-Sus

Imagine you are currently looking for job opportunities in software engineering and receive the following email sent to your university email account.

From: **david.nguyen[at]google-careers.com**
Subject: Software Engineer Position at Google – H-1B Sponsorship Available

Hello [Your Name],
I hope you're doing well. I'm David Nguyen from Google Careers. We have an opening for a **Software Engineer** on our AdTech team at the Mountain View, CA office, and your experience looks like a great fit. This is a full-time role with a competitive salary, standard benefits, and **H-1B visa sponsorship** for qualifying candidates. To begin the process, please send over your resume and complete a brief application here: `http://google-apply-career.com/start?ref=XYZ476`

Feel free to reply if you have any questions. We look forward to reviewing your application!

Best regards,
David Nguyen
Google Careers Team

How would you most likely initially react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Block the sender
- Use your email client to report the email
- Ignore the message and take no further action
- Search online for guidance
- Contact someone you trust for help
- Click the link to see more details or reply to the email for more information
- Send your résumé and apply right away, or save the email to apply later
- Other [Please Specify]

Email-Benign

Imagine you are currently looking for job opportunities in software engineering and receive the following email sent to your university email account.

From: **david.nguyen[at]google.com**
Subject: Software Engineer, AdTech – Mountain View, CA

Hello [Your Name],
I hope you're doing well. My name is David Nguyen, Senior Technical Recruiter on the AdTech team at Google. We are looking for a **Software Engineer** to help scale our ad-serving platform at our Mountain View, CA office, and your background aligns very well with what we're looking for. Please let me know if you will be interested in chatting or exploring more about this opportunity.
Apply here:
`https://careers.google.com/jobs/results/123456789-software-engineer-adtech/`

If you'd like to discuss the role before applying, just reply to this email with a few time slots that work for you, and I'll set up a call on our end.

Best regards,
David Nguyen
Senior Technical Recruiter, Google Inc.
david.nguyen[at]google.com | +1 (650) 555-1234
LinkedIn: `linkedin.com/in/david-nguyen-recruiter`

How would you most likely initially react in this

scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Block the sender
- Use your email client to report the email
- Ignore the message and take no further action
- Search online for guidance
- Contact someone you trust for help
- Click the link to see more details, or reply to set up a call to discuss further
- Apply right away, or save the email to apply later
- Other [Please Specify]

Rental Platform

Rent-Sus

Imagine you're looking for an apartment to rent before starting a new program. You find a promising listing on Zillow, exchange a few messages with the property manager, and it seems like a good fit. Since you're out of town, they offer a virtual Zoom tour. After the tour, you tell them you'd like to proceed, and they email you the lease. The email reads:

From: 245Grove.rentals[at]gmail.com
Subject: Lease & Deposit for 245 Grove Street
Hello [Your Name],
Thanks again for your interest in 245 Grove Street, Apt. 3B, I've attached the lease for your review. To secure the apartment, please send the first month's rent and a $500 security deposit via Zelle to **245Grove.rentals[at]gmail.com**. Once payment is received, I'll countersign the lease and email you move-in instructions.

How would you most likely initially react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Do not sign the lease and report to Zillow
- Do not sign the lease and take no further action
- Search online for advice
- Contact someone you trust for help
- Verify the landlord's identity online before proceeding
- Send the requested payment via Zelle
- Proceed to sign and return the lease
- Other [Please Specify]

Rent-Benign

Imagine you're looking for an apartment to rent before starting a new program. You find a promising listing on Zillow, exchange a few messages with the property manager, and it seems like a good fit. Since you're out of town, they offer a virtual Zoom tour. After the tour, you tell them you'd like to proceed, and they send you the lease through Zillow's secure Rental Manager platform. The message says:

Hello [Your Name],
Thanks again for your interest in 245 Grove Street, Apt. 3B. I've uploaded the lease to Zillow Rental Manager. Since we've received several applications, please review and sign the lease by [a date one week from now] to secure the unit. You can access it here: `https://rental.zillow.com/lease?leaseId=A92F7C1B`
Let me know if you have any questions!

How would you most likely react in this scenario? There's no right or wrong answer, please select the option that best reflects how you think you would respond in the moment. [Single-choice]

- Do not sign the lease and report to Zillow
- Do not sign the lease and take no further action
- Search online for advice
- Contact someone you trust for help
- Verify the landlord's identity online before proceeding
- Proceed to sign and return the lease
- Other [Please Specify]

D. Actual Experience with Scams

We define scams as deceptive activities that use technology to trick people into giving up money or personal information — for example, phishing emails, fake job offers, or fraudulent phone calls — which can lead to identity theft or financial loss. In this study, we focus on scams, not spam. Spam refers to unwanted but generally harmless messages, like bulk promotional emails, that are more annoying than dangerous.

In the next section, you'll see a list of common scams. Each will include a brief definition, followed by a few questions for you to answer.
Scam List

- **Job Scams:** Scammers may pretend to be recruiters or professors, offering fake jobs or internships through text, email, or ads. They may even hold fake interviews before asking for money or personal information.
  - **[If yes]** In those encounters, did the scammers mention visa sponsorship or offer immigration assistance, such as expedited green cards?
- **Rental and Online Transaction Scams:** Scammers post fake housing or sublet listings, asking you to pay deposits or rent for places they don't actually own or control. They may also pose as buyers or sellers on platforms like Facebook Marketplace, using tactics such as fake invoices or payment requests to steal money.
- **Tech Support / Account Security Scams** Scammers

may say there's suspicious activity on your account or device, such as unauthorized logins or charges, even if that is not true. They use this to trick you into giving personal information or contacting fake tech support.
- **Delivery Scam:** Scammers impersonate delivery services or banks, claiming an issue with a package or account to trick you into giving payment or personal information.
- **Scholarship / financial-aid & student-loan relief scams:** Scammers claim they can get you scholarships, help with the Free Application for Federal Student Aid (FAFSA), or forgive your student loans. They ask for upfront fees or sensitive info (e.g., SSN or FAFSA login) and may pretend to be the U.S. Department of Education or your loan servicer.
- **Online Relationship & Investment Scams:** Scammers befriend students online or via dating apps, then lure them into fake investment schemes—or romance scams that lead to financial exploitation.
- **Unknown Language / Chinese Robocalls:** Scammers may send robocalls or messages in a language other than English, often Chinese, to confuse you or pressure you into responding.
- **Impersonation of Immigration-Related U.S. Authorities:** Scammers may pretend to be from government agencies like U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), or the Department of Homeland Security (DHS). They claim you've broken visa rules or have legal problems and demand money or personal information to "fix" the issue.
- **Impersonation of Non-Immigration U.S. Authorities:** Scammers pretend to be officials from the police, the FBI, the Social Security Administration (SSA), the Internal Revenue Service (IRS), or other U.S. government agencies. They say you've done something illegal or owe money, and threaten to arrest or fine you unless you pay.
- **Impersonation of Foreign Authorities:** Scammers impersonate authorities from countries outside the U.S., such as foreign embassies or police, and claim you are involved in a crime or legal matter, demanding money or personal information.
  - **[If yes]** Did the scammers claim to be authorities from your home country?

The following questions were asked for each of the scam types

D.1 Have you personally encountered this type of scam in the U.S. after turning 18?

- No
- Yes, but I did not respond in any way (aside from blocking or indicating I wasn't interested).
- Yes, and I responded in some way (e.g., clicked a link, spoke on the phone, exchanged messages, etc.)
- I'm not sure [Please Specify]

D.2 Did you experience any of the following types of loss? Please select all that apply.

- **Financial loss:** I lost money or assets (e.g., sent payment, unauthorized transactions)
- **Information loss (less sensitive)**: I shared general or personal information (e.g., name, email address)
- **Information loss (more sensitive)**: I shared sensitive or high-risk information (e.g., Social Security number, credit card number, address)
- **Emotional distress**: I felt stress, anxiety, embarrassment, or fear as a result
- **Time loss:** I spent a lot of time dealing with the situation
- Other [Please specify]
- I did not experience any loss or distress

repeat for 10 scam types

D.11 [Multi-select] Which of the following channels have you used to report or respond to a scam? Please note that even if you experienced no loss, you may still want to make a report. Select all that apply.

- Local police, campus police, or other law enforcement
- Online platform or service where the scam occurred (e.g., Facebook, eBay)
- University office or department (e.g., IT, student affairs)
- Official government websites (e.g., FTC, FCC, IC3)
- Phone's built-in reporting/blocking feature
- Bank/other financial platforms
- Other [Please Specify]
- I have not made a report

D.12 What was the main reason for the above decision? [Open Response]

E. Resources

E.1 Which of the following types of scam-related training or information do you recall receiving from your current university? [Select all that apply.]

- General scam awareness during orientation (e.g., overview of common scams via online or in-person sessions)
- Links to external resources (e.g., government websites like the FTC or the FCC for scam prevention)
- Phishing simulation emails (fake scam emails followed by an explanation to raise awareness)
- Reminder or warning emails (e.g., alerts about recent scams, tips on what not to share)
- Informational videos or animations (e.g., short educational clips)
- Interactive content (e.g., quizzes, games, or workshops)
- Posters or flyers on campus

- Other types of training [Please Specify]
- I have not received or do not remember receiving any scam-related training

E.2 (*international students only*) Have you received any scam-related training or support specifically tailored for international students from your current university?

- No
- I don't remember, or I'm not sure
- Yes, I received training or support specifically for international students

E.2.1 (*if answered yes for the previous question*) Could you briefly describe the training or support specifically provided for international students at your current university? [Open Response]

E.3 How do you feel about the scam prevention training you received from your university?

- I feel well prepared to protect myself because of the training I received
- I feel somewhat prepared because of the training I received
- I do not feel very well prepared, even with the training
- I do not remember receiving any scam prevention training from my university
- I already felt well prepared, and the training did not change that

E.4 What types of university support, training, or resources do you think would be most helpful for better identifying and responding to potential scams? [Open Response]

E.5 Which of the following social media platforms **have you personally visited** to look for advice related to scams? [Select all that apply.]

- Reddit
- Instagram
- TikTok
- YouTube
- Other: [please specify]
- I have not/would not seek support from social media

E.6 Who **have you personally gone** to for advice related to scams? [Select all that apply.]

- Family members
- Friends
- Other students at your university (i.e., upperclassmen, student mentors, residential advisors)
- Student communities (online or offline): [please specify]
- Government websites or official sources: [please specify]
- Other: [please specify]
- I have not/would not seek support from anyone

E.7 What types of support or resources from **outside the university** (e.g., government, community, or online sources) would be most helpful for identifying and responding to potential scams?

F. Demographic Info

F.1 What is your gender?

- Woman
- Man
- Non-binary
- Genderqueer / Gender non-conforming
- Prefer to self-describe: [text entry]
- Prefer not to say

F.2 What is your age? [Dropdown list]

F.3 What type of program are you currently enrolled in?

- Undergraduate
- Master's
- PhD
- JD (Law)
- MD / DO (Medicine)
- DDS / DMD (Dentistry)
- MBA (Business)
- Other: [text entry]

F.4 What is your main area of study? [Insert Qualtrics' built-in dropdown list of fields of study]

F.5 Do you identify with a cultural or ethnic background that is different from the country you selected in Q B.2 (the country where you spent most of your time before age 18)? For example, you grew up in Japan but identify as Korean; you grew up in Brazil but identify as Japanese; or you grew up in Canada but identify as Indian.

- Yes
- No

F.5.1 (*if answer yes for previous question*) How would you describe your cultural or ethnic background? (e.g., Chinese, Nigerian, German, Brazilian, American) [Open Response]

F.6 What is/are your native language(s)? [Insert a list of common languages together with the other option (allow for multi-select)]

F.7 How long have you been in the U.S.? [Insert dropdown list: # of years, less than one year]

F.8 (*international students only*) What type of visa are you currently on?

- F-1 Student Visa
- J-1 Exchange Visitor Visa
- OPT (Optional Practical Training)

- STEM OPT Extension
- Other: [text entry]

F.9 (*non native speakers only*) How well can you do the following in English? (1 = Not at all, 5 = Very well). [Likert Scale, compute the mean]

- **F.9.1 Listening:** Understand virtually any spoken English, live or broadcast, even at fast native speed, once I'm familiar with the accent.
- **F.9.2 Reading:** Read almost any text with ease, including abstract or highly complex materials (manuals, specialized articles, literary works).
- **F.9.3 Speaking:** Join any conversation easily, use common idioms, and express subtle ideas clearly. If I get stuck, I can quickly rephrase. I can also give clear, well-organized explanations or arguments that fit the situation and help people remember the main points.
- **F.9.4 Writing:** Write clear, easy-to-read text in the right style. I can create longer letters, reports, or articles with a simple, logical structure that helps readers remember the main points. I can also write summaries and reviews of professional articles and literary works.

End of Survey Message

Thank you for completing the survey!
Your responses have been recorded. Eligible participants will receive their digital gift card soon. We truly appreciate your time and contribution to our study.
If you have any questions, please contact us at alexandrali@cmu.edu
If you know other students at your university who might be interested, please feel free to share this survey link with them: [Link]

Supplementary Materials

Due to space constraints, Tables 3–12 are available in our supplementary materials on the Open Science Framework: https://osf.io/3brhx/. Table numbering in the supplementary materials matches the main paper.