Cybersecurity Education Outreach to Immigrant Communities in the U.S.: A Case Study

Kevin Huang
Computing & Software Systems
University of Washington
Bothell, USA
huangk12@uw.edu

Marc J. Dupuis
Computing & Software Systems
University of Washington
Bothell, USA
marcjd@uw.edu

***Abstract*—Cybersecurity education equips individuals with the essential knowledge and skills to navigate the digital world safely. However, not all consumers have equal access to this information. In the United States, Asian minority groups face significant barriers to obtaining cybersecurity education, largely due to language and cultural challenges. Our project aimed to address this gap by designing targeted cybersecurity education and training programs for Chinese and Vietnamese communities. To achieve this, we developed training materials based on the latest research and best practices in password security and social engineering prevention. Participants for these sessions were recruited with the support of nonprofit organizations. Following the training sessions, our findings revealed a strong demand for cybersecurity education among these communities. Furthermore, the sessions positively influenced participants' intentions to adopt better password practices and remain alert to social engineering threats. The insights gained from this initiative highlight the importance of expanding tailored cybersecurity education to other minority groups and extending these efforts to additional cities across North America.**

***Index Terms*—cybersecurity, minority education outreach, Asian immigrant communities, password security, social engineering**

I. Introduction

Cybersecurity knowledge has become indispensable in today's digital era. The Internet serves as a vital global connector, bringing numerous advantages but also presenting opportunities for malicious activities. Cybercriminals exploit this technology to employ social-engineering tactics and scams that prey on the human factor in cybersecurity. These tactics enable them to steal personal information and data remotely, without being physically near their victims. In 2023, the Federal Trade Commission (FTC) reported that consumers lost $10 billion to scams [1]. To combat such threats, it is crucial for consumers to understand the strategies employed by cyber-criminals and the tools they can use to strengthen their cybersecurity defenses [2], [3].

Despite the importance of cybersecurity awareness, there is a significant shortage of training programs tailored to racial minority groups in the U.S. [4]. While organizations often provide cybersecurity training for employees to safeguard corporate data, systems, and networks, similar resources for consumers are scarce. Existing programs are predominantly designed by and for the majority population, which can lead to unintentional exclusion. Research evaluating the effectiveness of cybersecurity training for racial minority populations highlights that these programs often reflect the perspectives of dominant racial groups, resulting in challenges such as language and cultural barriers [4]. This lack of inclusivity underscores a gap in cybersecurity education for minority communities and presents an opportunity to develop more accessible and culturally relevant training initiatives.

A. Goals

The aim of our project is to develop tailored cybersecurity education and training programs for Asian minority groups, with a particular focus on the Chinese and Vietnamese communities. The education and training materials center on two fundamental topics: password security and social engineering prevention. These areas are essential to cybersecurity, straightforward to understand, and actionable for consumers to implement.

The success of the project is evaluated based on two key factors: participant attendance and the effectiveness of the training in influencing behavior. We established a minimum requirement of 25 participants to provide sufficient data for meaningful analysis. While 50 participants was our target goal, any attendance above that threshold was considered an aspirational achievement. Beyond attendance, the effectiveness of the training is assessed by measuring changes in cybersecurity behaviors before and after the education sessions. We anticipated a noticeable improvement in participants' cybersecurity practices as a result of the training.

This project serves as an initial step toward increasing cybersecurity resources for Asian minority populations. By showcasing the effectiveness of customized education and training programs for Chinese and Vietnamese consumers, the initiative aims to encourage the development of similar programs for other under-served groups.

B. Paper Structure

This paper is structured as follows. We begin with a review of recent research on password security and social engineering prevention, as well as an overview of existing training programs related to these topics. Next, we detail

the design and implementation process of the education programs developed specifically for Chinese and Vietnamese audiences. Following this, we present the results of the project and assess its overall success. Lastly, we summarize the key accomplishments, address the project's limitations, and propose directions for future research and development.

II. Related Work

Developing effective cybersecurity education and training programs requires both current knowledge of cybersecurity topics and an efficient delivery method. This section begins by identifying the latest guidelines and best practices for password security and social engineering prevention. Next, we review and analyze the methodologies used in existing research and industry resources related to these two areas. Finally, we examine a study that integrates psychological principles into the evaluation of cybersecurity awareness campaigns.

A. Passwords

Authentication involves verifying the identity of users within a system and plays a critical role in controlling access to information and data. This process is especially important when dealing with private resources that should not be accessible to the general public. Access should be restricted to individuals who have been authenticated and authorized. Authentication methods can be categorized into five types: knowledge (something you know), ownership (something you have), characteristics (something unique to you), location (somewhere you are), and action (something you do or how you do it) [5]. Each category has its own strengths and weaknesses that users should consider.

Passwords represent a form of authentication by knowledge, as they rely on something the user knows. They are the oldest and most widely used authentication method. Passwords are advantageous because they are simple to implement and cost-effective. However, they are user-created, which introduces variability in their strength depending on the effort and knowledge of the user. Factors such as password length, reuse, and sharing significantly impact the security of this authentication method.

1) Password Length: The National Institute of Standards and Technology (NIST) identifies password length as the most important factor in determining password strength [6]. Longer passwords provide more permutations, making them significantly harder to crack using brute force methods. While NIST sets a minimum password length of 8 characters, many organizations recommend longer passwords [7]. For our educational materials, we opted for a minimum length of 14 characters to enhance security further.

Although NIST acknowledges password complexity as a consideration, it does not regard it as a reliable indicator of password strength. Password composition rules, such as requiring a special character, are often ineffective because users tend to follow them in predictable ways. For instance, when prompted to include a special character, many users simply add an exclamation mark ("!") at the end of their password. Due to this predictability, password complexity does not consistently improve security. As a result, we chose not to emphasize this factor in our training materials.

2) Password Reuse: A 2014 study examined the extent of password reuse and found that 43% of participants reused the same password across multiple websites [8]. Additionally, some participants created only minor variations of their passwords for use on different platforms. One contributing factor to password reuse is the growing number of online accounts and services that users need to manage. Since individual companies can only enforce password policies on their own platforms, they cannot address this issue on a broader scale. The responsibility ultimately falls on users to understand and mitigate the risks associated with password reuse. This challenge remains significant, with estimates from 2023 indicating that 65% of consumers reuse passwords [9].

As part of our project, we emphasize the importance of creating unique and substantially different passwords for each website in our educational materials. To help address the issue of password reuse, we also introduce the use of password managers, which provide a practical solution for securely managing multiple strong passwords.

3) Password Sharing: Another important topic that is listed in many password best practices is to not share passwords [5]. Password sharing is relevant because it is another aspect of password security that the user is in charge of. Passwords can be shared intentionally or accidentally and to friends and family or attackers. It is advised to not share passwords under any circumstances because the user relinquishes the full control that they have over their accounts. The consequences of leaked passwords can be detrimental, including loss of ownership of the account and assets, negligence from those whom you have shared your password with, and privacy breaches [10]. This topic is included in our educational material to deter participants from password sharing.

B. Social Engineering

Social engineering refers to manipulating legitimate users into performing actions that benefit unauthorized individuals [5]. While attackers employ a variety of techniques, their ultimate focus is on exploiting the human element. Unlike employees within organizations who are bound by security policies, consumers are solely responsible for safeguarding their own information. Negligent behaviors, such as failing to verify the identity of individuals before sharing private information or interacting with malicious links and attachments, are common vulnerabilities that attackers frequently exploit [11].

C. Identity Confirmation

The effectiveness of social engineering stems from its ability to prompt users to take specific actions. A literature review examined various prevention methods, models, and

frameworks designed to address social engineering attacks [12]. The review highlighted that impersonation is a key component of many social engineering techniques, including phishing, grooming, pretexting, and profile cloning. Sharing sensitive information with attackers not only jeopardizes the individual but can also have broader implications for the organizations and communities they belong to. Information obtained through these attacks can be leveraged to launch additional social engineering campaigns. In our project, we emphasize the critical importance of verifying an individual's identity before sharing any sensitive or private information.

1) Suspicious Links and Attachments: A research study analyzed the increase in various types of cyber-attacks and threats that emerged during the COVID-19 pandemic [13]. The study identified phishing as the most prevalent method, accounting for 35% of attacks. Other commonly observed techniques included scamming, spamming, smishing, and vishing. These findings underscore the growing prevalence of social engineering attacks and highlight the need for consumers to recognize and counter these tactics. In our project, we address these widespread methods, focusing on their delivery via email, phone calls, and text messages. Additionally, we emphasize the importance of avoiding suspicious links and refraining from downloading questionable attachments to reduce vulnerability to such attacks.

D. Existing Cybersecurity Education

A study was conducted to gather and compile the latest recommendations for password best practices [14]. The researchers sourced information from government entities in the UK and USA, as well as organizations associated with these governments.

The resulting ontology provides a comprehensive framework of essential knowledge for password usage. It addresses all facets of password management, including creation, storage, and practical application. This ontology can be tailored to suit specific audiences, as demonstrated by the researchers who adapted it for educating children. In our case, we utilize the original version of the ontology, as our project focuses on educating adults. This serves as a foundational guide for the development of our password security training materials.

The CompTIA Security+ certification, designed for IT security professionals, includes extensive coverage of various security topics, including social engineering. Study guides for this certification are valuable resources as they provide in-depth information and up-to-date guidelines on these topics [15]. Regarding social engineering, the guides cover different types of attacks, impersonation tactics, and the underlying principles of social engineering. In our project, we utilized this resource to develop comprehensive social engineering education materials for our participants.

E. Effective Education

A research study explored the factors contributing to the failure of cybersecurity training programs [16]. The findings highlighted that individuals must not only understand and apply the advice but also be motivated and willing to act on it. Using an interdisciplinary approach, the study applied psychological theories to identify elements that facilitate behavioral change, ultimately aiming to create more effective cybersecurity training. One key factor identified was culture. People from collectivist cultures, often found in Eastern societies, place greater importance on relationships and social group memberships than on individual needs. This contrasts with individualistic cultures, which emphasize personal independence. As a result, individuals from collectivist cultures prioritize avoiding behaviors that could disrupt social harmony. Given that our target groups—Chinese and Vietnamese populations—are part of collectivist cultures, our educational materials emphasize prevention and the potential negative consequences of unsafe behaviors [17].

Another critical factor in effective cybersecurity education is the delivery method. The medium through which training is provided significantly influences its success. A study evaluating information security awareness programs compared text-based, game-based, and video-based delivery methods. The results showed that a blended approach combining multiple delivery methods was more effective than any single method [18]. In our project, we leverage this insight by utilizing a combination of delivery methods. Our approach includes educational videos, which provide both visual and auditory content, along with interactive activities to teach key concepts in password security and social engineering prevention. This multi-method strategy is designed to maximize engagement and learning outcomes for participants.

Beyond general cybersecurity training literature, research on culturally and linguistically tailored interventions underscores the importance of adapting content for immigrant communities. Studies of health education programs demonstrate that interventions aligned with cultural values and delivered in the participants' language produce stronger behavioral outcomes, including increased adoption of protective practices [19]–[21]. Community-based organizations and schools have been identified as trusted delivery venues that enhance engagement and overcome access barriers for immigrant populations [22], [23]. In parallel, research highlights that immigrant groups face heightened risks of cyber-victimization, such as cyberbullying and fraud, suggesting a need for targeted cyber awareness and resilience training [24], [25]. These findings provide a foundation for our approach of partnering with nonprofits to deliver linguistically adapted cybersecurity education, designed to build on cultural strengths while addressing specific vulnerabilities.

III. METHODS

To develop effective cybersecurity education and training programs tailored for Chinese and Vietnamese audiences, we organized our efforts into three distinct phases. The first phase involved the creation and preparation of educational materials. This included not only the core instructional content but also the tools necessary for evaluating the success

of the training sessions. In the second phase, we recruited volunteers who expressed interest in participating in the project. Finally, in the third phase, we conducted the training sessions and collected data from participants, which was then used for analysis.

A. Educational Material

1) Surveys: In this project, surveys were utilized to assess the impact of the cybersecurity education on participants. Four distinct survey variations were developed: pre- and post-education surveys for both password security and social engineering prevention. The pre-education surveys included questions on demographics, as well as topic-specific and general cybersecurity questions. In contrast, the post-education surveys focused solely on topic-specific and general cybersecurity questions.

a) Demographic Questions: The demographic questions provided insights into the diversity of our participants. These questions addressed participants' gender, age, ethnicity, and whether English was their first language. For ethnicity, we included specific response options for Chinese and Vietnamese, as these were the target populations for our project. Similarly, the English language question was tailored to identify participants who did not speak English as their first language, aligning with the focus of our study. These demographic questions were included in the pre-education surveys for both topics since participants were not required to attend sessions for both password security and social engineering prevention.

b) Password Security Questions: The password security questions in the surveys were designed to assess participants' practices related to password hygiene. These questions corresponded to three key factors identified as critical for maintaining strong password hygiene: password length, password reuse, and password sharing. In the pre-education survey, the questions focused on participants' existing habits, while the post-education survey shifted to explore their intentions and perspectives on improving these practices moving forward.

c) Social Engineering Prevention Questions: The social engineering prevention questions in the surveys aimed to evaluate participants' behaviors and responses during potential social engineering attempts. These questions were aligned with best practices, emphasizing the importance of verifying identities and avoiding interaction with suspicious content.

d) General Cybersecurity Questions: Two survey questions focused on participants' perspectives on cybersecurity. The first question explored their views on the importance of cybersecurity, while the second inquired about their interest in learning more about the subject. These questions were intended to gauge participants' engagement with the topic and their enthusiasm for further education. Both questions were included in all four survey variations.

2) Password Security Education: The educational portion of the sessions included a video on the topic and interactive activities to reinforce the material. In the password security sessions, the video was divided into sections covering: the purpose of passwords, challenges associated with using passwords, the consequences of compromised passwords, best practices for password creation and retention, proper password usage, and tools to enhance password security. These sections addressed all the topics outlined in the password ontology from the study by Prior and Renaud [14].

The first hands-on activity involved testing password strength using the website https://www.security.org/how-secure-is-my-password/, allowing participants to practice creating robust passwords. The second activity focused on setting up an account and learning to use the Bitwarden password manager. Password managers help address key password security challenges, such as ensuring sufficient password length and reducing password reuse. Bitwarden was selected for its strong reputation, availability of a free version, and compatibility across a wide range of platforms and devices.

3) Social Engineering Prevention Education: The social engineering prevention sessions followed the same structure as the password security sessions, consisting of a topic-focused video and interactive activities. The video was divided into sections covering why attackers use social engineering, the various types of attacks, impersonation tactics, the principles behind social engineering, and strategies for preventing phishing, vishing, and smishing. The educational content was sourced from the CompTIA Security+ Study Guide, Kaspersky, and the Cybersecurity & Infrastructure Security Agency (CISA) [15] [26] [27].

The first hands-on activity involved participants reviewing examples of social engineering attempts delivered via email, phone calls, and text messages. This exercise provided an opportunity to practice recognizing and identifying such attacks. The second activity encouraged participants to share their personal experiences or stories they had heard about social engineering incidents. These activities were designed to give participants practical experience and increased familiarity with social engineering tactics, helping them better prepare for future attempts targeting them.

4) Translation: The survey questions and educational materials were translated into Chinese (Mandarin and Cantonese) and Vietnamese. To ensure accurate and reliable translations, professional translators were hired through the American Translators Association (ATA). These translators provided translations for the survey questions, the text displayed in the educational videos, and the instructions for the hands-on activities. Additionally, they delivered audio interpretations for the videos. Examples of the translations for the Chinese and Vietnamese videos are shown in Figures 1 and 2, respectively. The translated videos can be accessed at the following URLs: [redacted for review] (Password Security in Chinese), [redacted for review] (Password Security in Vietnamese), [redacted for review] (Social Engineering Prevention in Chinese), and [redacted for review] (Social

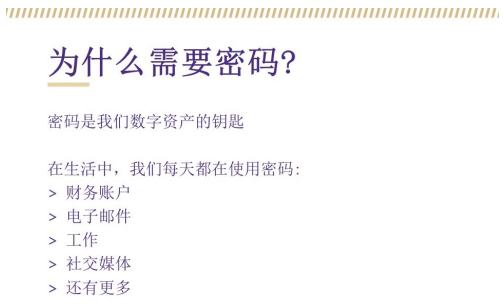

Fig. 1: Screenshot from Chinese Password Security Video

Fig. 2: Screenshot from Vietnamese Password Security Video

Engineering Prevention in Vietnamese).

B. Participants

1) IRB Approval: Approval from an Institutional Review Board (IRB) was secured before commencing any activities involving participants. It qualified for exempt status from full board review.

2) Recruiting: The target populations for this project were Chinese and Vietnamese minority groups residing in Seattle, Washington. To recruit participants, we first identified local nonprofit organizations serving these communities. This approach was chosen because such organizations often have established relationships and deep connections with the communities they support, making it easier to reach individuals from our target populations. We specifically sought nonprofits focused on serving the Chinese and Vietnamese communities, contacting them via email and phone to explain the project's purpose and request assistance with participant recruitment.

Two organizations, the Chinese Information and Service Center (CISC) and Kandelia, agreed to assist with the project. CISC is a nonprofit organization dedicated to supporting immigrant families by creating opportunities for their success. While primarily serving the Chinese immigrant community, CISC also offers resources to immigrants from Eastern Europe, Latin America, and other parts of Asia. Kandelia, initially founded as the Vietnamese Friendship Association (VFA), has evolved into a nonprofit organization serving all immigrant and refugee communities. Both organizations promoted the educational sessions and provided their facilities for hosting them. CISC hosted the sessions for the Chinese community, while Kandelia hosted the sessions for the Vietnamese community.

Due to facility and staff availability, the sessions were conducted in group settings. Participation was entirely voluntary, and no monetary compensation was provided to attendees for their time.

C. Education Sessions

A total of four group education sessions were conducted, with one session dedicated to each education topic—password security and social engineering prevention—and each language, Chinese and Vietnamese. The password security sessions were held first, followed by the social engineering prevention sessions one month later.

Staff members from the respective nonprofit organizations hosting the sessions were present at their facilities during the events. They served as the primary communication bridge between us and the participants. Their responsibilities included interpreting instructions for the education sessions, translating participants' questions, and conveying our responses. Additionally, the staff assisted with administrative tasks such as setting up the education video and facilitating the distribution and collection of surveys.

Each session followed the same structured format and lasted approximately one hour. The sessions began with participants signing in, during which they were assigned unique identification numbers. This allowed us to track whether a participant attended both the password security and social engineering prevention sessions. Participants then spent 10 minutes completing the pre-education survey, which was administered in physical form using pen and paper.

Following the survey, participants watched a 15-minute educational video presented via a projector with accompanying audio. The next 25 minutes were dedicated to hands-on training exercises, during which participants were encouraged to ask questions. Each session concluded with a post-education survey, which also took 10 minutes to complete.

IV. Results

A. Participant Demographics

In total, 45 unique participants attended our education sessions. Among them, 30 participated in the password security education, and 32 took part in the social engineering prevention education. The majority of participants, 40 in total, were aged 60 and above. Four participants were between the ages of 41 and 50, and one participant was in the 31 to 40 age range.

Regarding gender, 34 participants identified as female, nine as male, one as other, and one preferred not to disclose their gender. In terms of ethnicity, 38 participants identified as Chinese, six identified as Vietnamese, and one identified as other or multi-racial. All participants indicated that English was not their first language.

B. Pre-Post Analyses

Analytic Approach and Error Control: We treated each item as a paired outcome, mapping Likert responses to

integers (1=Strongly Disagree to 5=Strongly Agree) and estimating within-participant change from pre- to post-session. Primary analyses used one-sided paired t-tests with α=0.05 given the directional hypothesis (improvement post-education). For each comparison, we report t, p, and the paired standardized mean change d_z with 95% CIs (Figure 3). We also comment on potential ceiling effects and practical significance. To guard against inflated Type I error across related endpoints, we applied a Holm–Bonferroni correction within topic blocks (Passwords; Social Engineering). All behavior-focused outcomes that were significant in the unadjusted analyses remained significant after correction. As a robustness check, we repeated the analyses using Wilcoxon signed-rank tests; inferences were unchanged. As a sensitivity check, we repeated all tests two-sided at $\alpha = 0.05$; all inferences for behavior-focused outcomes were unchanged.

Table II summarizes pre–post changes with standardized effect sizes and confidence intervals. The largest effect was observed for *password length* ($d_z = 0.93$, 95% CI [0.54, 1.31]), indicating a large improvement in intentions to create longer passwords. Medium effects were seen for *password reuse* ($d_z = 0.70$) and *password sharing* ($d_z = 0.54$), consistent with stronger commitment to better hygiene practices. In the social engineering sessions, improvements in *identity confirmation* ($d_z = 0.51$) and *avoiding suspicious links/attachments* ($d_z = 0.62$) were also in the medium-to-large range. General attitudes such as *importance of cybersecurity* and *interest in learning more* shifted modestly (small effects, $d_z \approx 0.3$–0.5), reflecting ceiling effects from already-high baseline scores. Together, the pattern highlights that the strongest gains were in specific, actionable behaviors rather than general attitudes.

1) Password Security Sessions (Interpretation): As shown in Table II and Figure 3, the strongest gains were in concrete password hygiene behaviors, led by password length (large effect), with meaningful reductions in reuse and sharing (both medium). General attitudes (importance, learning interest) showed little additional movement, consistent with ceiling effects from already-high baselines.

TABLE I: Participant Demographics (N=45)

Characteristic	n	%
Age		
31–40	1	2.2
41–50	4	8.9
60+	40	88.9
Gender		
Female	34	75.6
Male	9	20.0
Other	1	2.2
Prefer not to disclose	1	2.2
Ethnicity		
Chinese	38	84.4
Vietnamese	6	13.3
Other/Multi-racial	1	2.2
English as First Language		
No (ESL)[a]	45	100.0

Note. Percentages may not sum to 100 due to rounding.
[a] ESL = English as a second language.

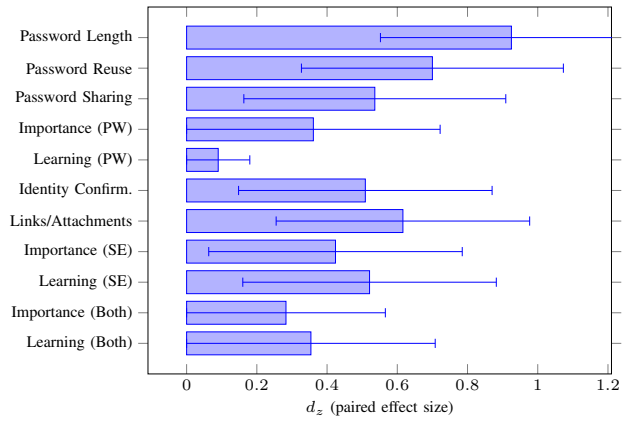

Fig. 3: Paired effect sizes (d_z) with 95% CIs across measures. These values correspond to the results summarized in Table II. Reference lines at $d = 0.2$, 0.5, and 0.8 denote small, medium, and large effects, respectively.

2) Social Engineering Prevention Sessions (Interpretation): Behavioral intentions improved on both focal practices—verifying identity and avoiding suspicious links/attachments—with effects in the medium to medium–large range (Table II, Figure 3). Attitudinal items moved modestly, suggesting the training primarily shifted specific, actionable behaviors rather than broad attitudes.

3) Participants Attending Both Sessions: Among participants who attended both topics (N=17), changes in general attitudes (*importance*, *learning interest*) were directionally positive but not statistically significant at α=0.05 (Table II). Given pre-session means > 4.4, a ceiling effect likely constrained additional detectable movement. Practically, the second session appears to deepen specific behaviors more than shift already-high global attitudes (Table II, Figure 3).

V. Discussion

We established a minimum attendance goal of 25 participants and met it across both topics (30 in password security; 32 in social engineering), providing sufficient data for analysis. Recruitment nonetheless fell short of the aspirational target (50), partly because only two immigrant-serving nonprofits partnered on outreach. The sample skewed older (mostly 60+) and predominantly female (75%), with most respondents from the Chinese-language sessions, which may limit generalizability.

Quantitatively, the education sessions produced small-to-medium improvements on targeted cyber-hygiene intentions, with the largest gains on concrete, teachable behaviors (e.g., adopting longer passwords), and medium gains for reducing reuse and sharing (Table II, Figure 3). Social

engineering behaviors (identity confirmation; avoiding suspicious links/attachments) showed medium to medium–large improvements. In contrast, general attitudes (importance of cybersecurity; interest in learning more) changed only modestly. This pattern is consistent with ceiling effects, given already-high pre-education means (e.g., importance M=4.17 and 4.53; learning M=4.33 and 4.53 on a 5-point scale), leaving limited headroom for further movement.

Comparison with Prior Work

Consistent with prior awareness programs in general U.S. populations [28]–[32], we observed small-to-medium improvements on targeted cyber-hygiene behaviors, but here within linguistically tailored sessions delivered through trusted community nonprofits. This extends evidence from culturally adapted health and education programs [19]–[22], [33] and immigrant-focused cyber risk research [23]–[25], demonstrating that culturally and linguistically adapted content can yield comparable or larger gains on specific protective behaviors in immigrant communities, even when global attitudes start high.

Practical Implications

Partnering with community-based organizations enabled language access, trust, and attendance. The largest effects centered on concrete behaviors (longer passphrases; reduced reuse/sharing; link hygiene), suggesting programs should prioritize hands-on tools (e.g., password manager setup) and rehearsed responses to common scams. Materials and facilitator scripts should remain culturally and linguistically adapted to sustain engagement.

Limitations

Recruitment through two nonprofits constrained reach and diversity. The single-group pre–post design with immediate post-tests limits causal attribution and does not assess durability; follow-ups and control groups are warranted. Responses are self-reported and may diverge from realized behavior [34], [35]. Likert outcomes were treated as interval for t-tests; robustness checks using Wilcoxon signed-rank yielded the same substantive conclusions. Sensitivity analyses with two-sided tests at α=0.05 did not change inferences for behavior-focused outcomes. Finally, results reflect Seattle-based Chinese and Vietnamese cohorts and may not generalize uniformly to other regions or language communities.

Future Work

Future efforts should expand translation to additional languages (e.g., Japanese, Korean) and sites across the U.S. to assess regional effects. Methodologically, longitudinal follow-ups and behavioral telemetry (e.g., password manager adoption/usage logs) can test whether intention gains translate into sustained practice. Richer models (e.g., ordinal mixed-effects or predictive classifiers) could identify subgroups that benefit most and adapt curricula accordingly. Content-wise, expanding topics (e.g., MFA usage, VPNs, anti-phishing cues) may yield broader protection while preserving the practical, hands-on emphasis.

The understanding and use of various cybersecurity tools do vary based on demographic factors [36]. Future research could explore whether such factors may involve language barriers or being part of an immigrant community. Additionally, it is unclear if they could perhaps be more susceptible to other threat vectors, such as certain IoT devices and the vulnerabilities they pose [37], or the spread of disinformation that is prevalent on social media [38].

VI. Conclusion

This case study evaluated linguistically tailored cybersecurity education for Chinese- and Vietnamese-speaking immigrant communities delivered via trusted nonprofits. Participants reported the largest pre–post gains on specific, actionable behaviors—longer passwords, reduced reuse/sharing, identity confirmation, and avoiding suspicious links/attachments—while global attitudes shifted only modestly, plausibly due to ceiling effects. The results align with prior awareness programs in general populations yet extend the evidence base by demonstrating comparable or larger behavior-focused gains in immigrant cohorts when

TABLE II: Paired Sample Results with Effect Sizes and 95% Confidence Intervals

Session / Measure	**Pre (M±SD)**	**Post (M±SD)**	t**(df)**	p	d_z	**95% CI**	**Sig.**
Password Security Sessions (N=30)							
Password Length	2.83 ± 1.09	4.03 ± 0.89	$t_{29} = -5.067$	<0.001	0.93	[0.54, 1.31]	***
Password Reuse	3.13 ± 1.04	3.87 ± 0.57	$t_{29} = -3.832$	<0.001	0.70	[0.32, 1.09]	***
Password Sharing	3.43 ± 1.22	4.20 ± 0.48	$t_{29} = -2.935$	0.003	0.54	[0.17, 0.92]	**
Cybersecurity Importance	4.17 ± 0.91	4.50 ± 0.51	$t_{29} = -1.980$	0.029	0.36	[0.02, 0.70]	*
Learning Cybersecurity	4.33 ± 0.61	4.27 ± 0.58	$t_{29} = 0.494$	0.313	0.09	[-0.28, 0.46]	ns
Social Engineering Prevention Sessions (N=32)							
Identity Confirmation	4.19 ± 0.90	4.59 ± 0.50	$t_{31} = -2.881$	0.004	0.51	[0.16, 0.86]	**
Links/Attachments	4.13 ± 0.83	4.50 ± 0.51	$t_{31} = -3.483$	<0.001	0.62	[0.27, 0.98]	***
Cybersecurity Importance	4.53 ± 0.57	4.69 ± 0.47	$t_{31} = -2.396$	0.011	0.42	[0.09, 0.75]	*
Learning Cybersecurity	4.53 ± 0.51	4.75 ± 0.44	$t_{31} = -2.946$	0.003	0.52	[0.17, 0.87]	**
Both Sessions (N=17)							
Cybersecurity Importance	4.41 ± 0.62	4.65 ± 0.49	$t_{16} = -1.167$	0.130	0.28	[-0.09, 0.66]	ns
Learning Cybersecurity	4.47 ± 0.51	4.71 ± 0.47	$t_{16} = -1.461$	0.082	0.35	[-0.05, 0.75]	ns

Note. d_z = paired standardized mean change; 95% CIs from noncentral-t approximation. Significance: * $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$, ns = not significant.

content and delivery are culturally and linguistically adapted. These findings support scaling community-partnered, hands-on, tailored programs to help close cybersecurity awareness gaps in underserved populations.

REFERENCES

[1] L. Bungo, "Think you know what the top scam of 2023 was? take a guess," *https://consumer.ftc.gov/consumer-alerts/2024/02/think-you-know-what-top-scam-2023-was-take-guess*, 2024. [Online]. Available: https://consumer.ftc.gov/consumer-alerts/2024/02/think-you-know-what-top-scam-2023-was-take-guess. Accessed 2024-02-15.

[2] Y. Peker, L. Ray, and S. da Silva, "Online Cybersecurity Awareness Modules for College and High School Students," in *2018 National Cyber Summit (NCS)*, 2018.

[3] S. S. Tirumala, M. R. Valluri, and G. Babu, "A survey on cybersecurity awareness concerns, practices and conceptual measures," in *2019 International Conference on Computer Communication and Informatics (ICCCI)*, 2019.

[4] S. Wongkrachang, "Cybersecurity Awareness and Training Programs for Racial and Sexual Minority Populations: An Examination of Effectiveness and Best Practices," *Contemporary Issues in Behavioral and Social Sciences*, vol. 7, pp. 35–53, Feb. 2023.

[5] D. Kim and M. G. Solomon, *Fundamentals of Information Systems Security*. Jones and Bartlett Learning, 3rd ed., 2016.

[6] P. Grassi, R. Perlner, E. Newton, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, and M. Theofanos, *Digital Identity Guidelines: Authentication and Lifecycle Management [including updates as of 12- 01-2017]*. Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, Dec 2017.

[7] G. Orenstein, "3 tips from nist to keep your passwords secure," *https://bitwarden.com/blog/3-tips-from-nist-to-keep-passwords-secure/*, 2023. [Online]. Available: https://bitwarden.com/blog/3-tips-from-nist-to-keep-passwords-secure/. Accessed 2023-10-13.

[8] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang, "The tangled web of password reuse," in *Proceedings of NDSS*, 2014.

[9] S. Laborde, "Password reuse statistics: Over 60 [Online]. Available: https://techreport.com/statistics/password-reuse-statistics/.

[10] I. Garakh, "The 5 risks of sharing your password," *https://www.techopedia.com/the-5-risks-of-sharing-your-password/2/34897*, 2023. [Online]. Available: https://www.techopedia.com/the-5-risks-of-sharing-your-password/2/34897. Accessed 2023-10-13.

[11] V. Gomes, J. Reis, and B. Alturas, "Social engineering and the dangers of phishing," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020.

[12] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 39325–39343, 2022.

[13] M. Hijji and G. Alam, "A Multivocal Literature Review on Growing Social Engineering Based Cyber-Attacks/Threats During the COVID-19 Pandemic: Challenges and Prospective Solutions," *IEEE Access*, vol. 9, pp. 7152–7169, Jan. 2021.

[14] S. Prior and K. Renaud, "Age-appropriate password "best practice" ontologies for early educators and parents," *International Journal of Child-Computer Interaction*, vol. 23-24, p. 100169, June 2020.

[15] M. Chapple and D. Seidl, *CompTIA Security+ Study Guide: Exam SY0-601*. Sybex, 8th ed., 2021.

[16] M. Bada, A. M. Sasse, and J. R. C. Nurse, "Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," Jan. 2019. arXiv:1901.02672 [cs].

[17] P. Lockwood, T. C. Marshall, and P. Sadler, "Promoting success or preventing failure: Cultural differences in motivation by positive and negative role models," *Personality and Social Psychology Bulletin*, vol. 31, no. 3, pp. 379–392, 2005.

[18] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behaviour & Information Technology*, vol. 33, no. 3, pp. 237–248, 2014.

[19] M. Sánchez, P. Rojas, T. Li, G. J. Ravelo, E. Cyrus, W. Wang, M. Kanamori, N. Peragallo, and M. D. La Rosa, "Evaluating a culturally tailored hiv risk reduction intervention among latina immigrants in the farmworker community," *World Medical & Health Policy*, 2016.

[20] N. Peragallo, R. M. González-Guarda, B. E. McCabe, and R. Cianelli, "The efficacy of an hiv risk reduction intervention for hispanic women," *Aids and Behavior*, 2011.

[21] E. L. Tuthill, L. Butler, J. M. McGrath, R. M. Cusson, G. N. Makiwane, R. K. Gable, and J. D. Fisher, "Cross-cultural adaptation of instruments assessing breastfeeding determinants: A multi-step approach," *International Breastfeeding Journal*, 2014.

[22] S. E. Jones, C. Pezzi, A. Rodríguez-Lainz, and L. Whittle, "Health risk behaviors by length of time in the united states among high school students in five sites," *Journal of Immigrant and Minority Health*, 2014.

[23] E. Hall and N. G. Cuellar, "Immigrant health in the united states," *Journal of Transcultural Nursing*, 2016.

[24] K. S. Kenny, L. Merry, D. A. Brownbridge, and M. L. Urquía, "Factors associated with cyber-victimization among immigrants and non-immigrants in canada: A cross-sectional nationally-representative study," *BMC Public Health*, 2020.

[25] R. C. Forgas, J. S. Negre, and A. Calvo-Sastre, "Characteristics of cyberbullying among native and immigrant secondary education students," *International Journal of Cyber Behavior Psychology and Learning*, 2017.

[26] "Ways to avoid social engineering attacks," *https://usa.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks*. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/how-to-avoid-social-engineering-attacks. Accessed 2023-10-13.

[27] "Avoiding social engineering and phishing attacks," *https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks*, 2021. [Online]. Available: https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks. Accessed 2023-10-13.

[28] A. Tick, D. Cranfield, I. M. Venter, K. Renaud, and R. Blignaut, "Comparing three countries' higher education students' cyber related perceptions and behaviours during covid-19," *Electronics*, 2021.

[29] B. Khamzina, N. Roza, G. Zhussupbekova, K. Shaizhanova, A. Aten, and A. Baikulova, "Determination of cyber security issues and awareness training for university students," *International Journal of Emerging Technologies in Learning (Ijet)*, 2022.

[30] K. F. McCrohan, K. L. Engel, and J. W. Harvey, "Influence of awareness and training on cyber security," *Journal of Internet Commerce*, 2010.

[31] W. He, I. K. Ash, M. Anwar, L. Li, X. Yuan, L. D. Xu, and X. Tian, "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training," *Journal of Intellectual Capital*, 2019.

[32] F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gounaris, A. Georgiadou, A. Michalitsi-Psarrou, G. Doukas, M. Kontoulis, Y. Nikoloudakis, S. Marin, R. Cabecinha, and C. Ntanos, "A cybersecurity culture survey targeting healthcare critical infrastructures," *Healthcare*, 2022.

[33] N. M. Edwards, Z. Isik-Ercan, H. Lu, M. Fall, and L. Sebti, ""do the best you can with resources you have to offer": Community stakeholder views on supporting immigrant families," *Journal of Community Psychology*, 2022.

[34] S. MacKenzie and P. Podsakoff, "Common method bias in marketing: Causes, mechanisms, and procedural remedies," *Journal of Retailing*, vol. 88, pp. 542–555, 2012.

[35] J. Wu and H. Du, "Toward a better understanding of behavioral intention and system usage constructs," *European Journal of Information Systems*, vol. 21, no. 6, pp. 680–698, 2012.

[36] M. Dupuis and E. Jones, "Cyber victimization: Tools used to combat cybercrime and victim characteristics," in *International Congress on Information and Communication Technology*, pp. 141–162, Springer Nature Singapore Singapore, 2024.

[37] M. Khadeer, M. Dupuis, and S. Khadeer, "Educating consumers on the security and privacy of internet of things (iot) devices: A quantifiable security compliance measurement system to aid in purchasing decisions," in *Journal of The Colloquium for Information Systems Security Education*, vol. 5, pp. 20–20, 2018.

[38] L. Crouse and M. Dupuis, "A dangerous infodemic: an examination of the impact social media misinformation has on covid-19 vaccination status," in *Proceedings of the 23rd Annual Conference on Information Technology Education*, pp. 37–43, 2022.