Bryan Gregg

Article Review #2

<<Enséñanos cómo mantenernos seguros en linea.>>

“Hãy dạy chúng tôi cách giữ an toàn trên mạng.”

“Teach us how to stay safe online.”

Cybersecurity Education for Users with Limited English Proficiency

Citation

Ngo, F. T. , Deryol, R. , Turnbull, B. & Drobisz, J. (2024). The need for a cybersecurity education program for internet users with limited English proficiency: Results from a pilot study . International Journal of Cybersecurity Intelligence & Cybercrime, 7(1), - . DOI: https://doi.org/10.52306/2578-3289.1160

Introduction

Computer-based crime is one of the fastest-growing security threats in the U.S. (Johnson, 2021). Between 2019 and 2020, there was a 69% increase in the number of reported cybercrimes (Federal Bureau of Investigation, 2020). This study explores how internet users with limited English proficiency (LEP) are predisposed to becoming victims of cybercrime. It focuses on Spanish-speaking and Vietnamese-speaking participants and how language barriers hinder access to cybersecurity information and online safety. In 2013, Spanish was the predominant language spoken among LEP individuals. Vietnamese Americans are known to be the least proficient in English (Alperin & Batalova, 2018). The research proves that cybersecurity education can provide marginalized people with the tools needed to improve online behaviors, promoting safety as well as social equity (Federal Trade Commission, 2021).

Social Science Principles

1) Social inequality and access to resources (cybersecurity information is unavailable, users are unaware of how to protect themselves, maintaining online safety is difficult).
2) Cultural and linguistic inclusion (outreach education should be specific to the language and culture of different communities).

3) Empowerment and agency (inclusive cybersecurity education supports individuals and communities, giving marginalized users control of their own digital safety).
4) Intersectionality (cybercrime risk depends on several factors, such as language skills, education level, background, and income).
5) Applied social science for public good (finding solutions that help people and promote a fairer and safer society for everyone).
6) Ethics and justice in technology (connecting online safety with fairness, equal access to protection, and user-friendly designs that work for everyone).

Research Question

"How does limited English proficiency affect individuals' ability to recognize, respond to, and protect themselves from cybercrime?"

Hypotheses

1) LEP users are less likely to recognize online threats.
2) LEP users are less likely to follow safe online habits (use strong passwords, avoid suspicious links).
3) Cybersecurity training that is language and culture specific helps LEP users stay safer online.
4) After inclusive training, LEP users feel more confident about handling cyber threats.

Variables

Independent:

1) Language Proficiency Level: Fluency in English or LEP (Spanish- or Vietnamese-speaking).
2) Access to Cybersecurity Education: Training was/was not specific to language and culture.

Dependent:

1) Cybercrime Vulnerability: Ability to recognize and respond to online threats (phishing, scams).
2) Digital Safety Behaviors: Actions taken to protect personal information online (using strong passwords, avoiding suspicious links).
3) Confidence in Cybersecurity Practices: Reported comfort and confidence in maintaining online safety after training.

Research Methods, Data, and Analysis

The study used a mixed-methods approach. Researchers used interviews and surveys to understand how people with limited English skills deal with online safety. Spanish- and Vietnamese-speaking participants joined focus groups and one-on-one interviews to talk about what they knew and needed to learn about cybersecurity. They also filled out questionnaires to show how aware they were of online threats and what safety habits they used.

Data Collection

The participants took a pre-test to see what they knew about cybersecurity. After they received the training, they took a post-test to assess what they had learned and how their behavior changed. The researchers also held focus groups, two with Spanish speakers and one with Vietnamese speakers (Turnbull et al., 2022). The participants discussed their experiences

and struggles with online safety. Surveys were used to gather information about what participants already knew, how they protected themselves online, and how confident they felt about handling cyber threats.

Data Analysis

Quantitative analysis: Researchers compared pre-test and post-test scores to evaluate the effectiveness of the training.

Qualitative analysis: Researchers examined the interview and focus group transcripts and identified recurring patterns (language barriers, lack of resources, increased risk for cybercrime).

Related concepts from Power Point presentation

One related concept is American Sociological Association's definition of sociology as "the study of social life, social change, and the social causes and consequences of human behavior. This study examined the social life (online presence) of two marginalized groups, the social causes (LEP and lack of cybersecurity education), and the consequences of their online behaviors (increased vulnerability to cybercrime) to enact social change (promote equity by providing customized cybersecurity education for all). Also related is the concept of Social Forces and Cybersecurity. Education is considered a strong social force in our society and the type and amount of education we receive affects all aspects of our lives. Cybersecurity education as a social force increases awareness, reduces victimization, and promotes safe behaviors in cyberspace.

Marginalized Groups and Equity Considerations

The researchers focus on how limited English proficiency (LEP) increases risk of cybercrime among marginalized groups. Spanish- and Vietnamese-speaking participants represent communities that may face language barriers, limited computer literacy, and minimal outreach from cyber defense specialists. The study proves that inclusive online education can empower these groups to recognize threats, improve their online behaviors, and advocate for their own digital safety (Sultan, A.H.M.A.D., 2019). This conforms to the fundamental social science principles of equity: ensuring that all users, regardless of language or background, have access to the resources and knowledge needed to maintain safety in virtual environments.

Contributions to Society

This study promotes digital equity by showing how LEP users are predisposed to online threats, and it demands cybersecurity tools that work for all language groups. It empowers marginalized groups by proving that training designed for Spanish- and Vietnamese speakers can improve both safety confidence and safety online. The research supports the need for multilingual programs that protect the public from fraud and identity theft, especially in impoverished areas. It also gives community leaders strong reasons to invest in cybersecurity training. Lastly, the study promotes social science by considering access to technology an issue of equity. It demonstrates the importance of providing digital tools to those who are most at risk.

Conclusion

Ngo et al. (2024) make a strong impact by showing how language barriers can leave people more exposed to online threats. The research emphasizes the need for cybersecurity

education specifically designed for various languages and cultures. It proves that customized training not only enhances participants' knowledge but also increases confidence and improves online safety. LEP users and other vulnerable groups will be better protected in digital spaces. Cybersecurity education must be accessible to everyone.

References

Alperin, E., & Batalova, J. (2018). *Vietnamese immigrants in the United States*. Migration Policy Institute. https://www.migrationpolicy.org/article/vietnamese-immigrants-united-states-5

Federal Bureau of Investigation. (2020). *2020 Internet Crime Report*. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Federal Trade Commission. (2021). *Consumer Sentinel Network Data Book 2020*. Washington, DC: Federal Trade Commission. https://www.ftc.gov

Johnson, J. (2021). *U.S. consumers and cyber crime – Statistics & facts*. Statista. https://www.statista.com/topics/2588/us-consumers-and-cyber-crime/#topicHeader__wrapper

Sultan, A. H. M. A. D. (2019). *Improving cybersecurity awareness in underserved populations*. Center for Long-Term Cybersecurity, UC Berkeley. https://cltc.berkeley.edu/wp-content/uploads/2019/04/CLTC_Underserved_Populations.pdf

Turnbull, B., Ngo, F. T., & Deryol, R. (2022). *Cybersecurity awareness and victimization among internet users with limited English proficiency: A pilot study*. Presented at the American Society of Criminology Annual Meeting, Atlanta, GA.