Education Impact on Trust in Election Technology & Security: Research Proposal

Gary White
Gw067@txstate.edu

Ju Long
julong@txstate.edu

Texas State University
San Marcos, TX

ABSTRACT

The purpose of this paper is to propose a study to determine if and how education impacts trust on election security and election technology using the TAM and UTAUT models. This study uses a quantitative research design. Data will be collected through surveys administered to a sample of eligible voters. Variables related to TAM and ITAUT models will be measured using a 7-Likert scale. The survey will be administered before and after the educational session.

Keywords: voting systems, security, hash values, digital signatures, Technology Acceptance Model (TAM), Unified Theory of Acceptance and Use of Technology (UTAUT).

1. INTRODUCTION

In recent years, the integrity of electoral processes has come under increased scrutiny, particularly with the growing incorporation of technology in voting systems. The average U.S.A. public trust of the government from 1958 to 1968 was 69%. From 2011 to 2021, the average U.S.A. public trust was 20% (Pew, 2021). In the 2020 U.S. general election, only 65% of voters trusted the initial findings (Mercur & Neumann, 2021; Laughlin & Shelburne, 2021) with less than 25% of Republicans trusting (Coleman, 2020). Election distrust is a political weapon that undermines confidence in elections (Fried & Harris, 2020).

From electronic voting machines to blockchain-based voting applications, technology offers the potential for enhanced efficiency and accessibility in elections. However, these advancements have also raised concerns about security, transparency, and reliability, which, if left unaddressed, can undermine public trust in the electoral process. Education emerges as a critical tool in bridging this trust gap, equipping citizens with the knowledge and understanding necessary to navigate and trust technological advancements in voting systems.

Organizations realize the importance of user security education and awareness training (Dodge et al., 2007; Schultz, 2004). Education makes users more security conscious (Ng et al., 2009) and is needed to counter unrealistic thinking about ideas that sound good but lack evidence.

The integration of education and technology in elections is not merely about informing voters about how to use new systems, but also about instilling a deeper understanding of the underlying principles and safeguards that ensure their integrity. Research suggests that informed citizens are more likely to trust and engage with electoral technologies. This trust is paramount, as perceived vulnerability in electoral systems can lead to decreased voter turnout and increased susceptibility to misinformation (Norris, 2015).

Educational initiatives aimed at improving trust in election technology can take multiple forms, including public information campaigns, school curriculums, and community workshops. For instance, the Carter Center (2020) highlights the importance of comprehensive voter education programs in fostering transparency and confidence in electoral processes. Furthermore, providing voters with accessible information about the technical aspects of election technology, such as encryption and verification methods, can demystify these systems and reduce skepticism.

The necessity of these educational efforts is underscored by the rapid pace at which election technology is evolving. As newer, more complex systems are introduced, the gap between technology developers and the general public's understanding widens, potentially exacerbating distrust. Therefore, ongoing education must be a priority, ensuring that as technology advances, public comprehension and trust advance in tandem.

Can education override the psychological effect of voter fraud propaganda? With education, you can talk from a position of knowledge if you find yourself in a discussion on voter fraud. Having knowledge of election security and technology may increase trust in elections.

This paper explores the multifaceted role of education in enhancing trust in election technology. It analyzes the impact of different educational strategies on trust, and offers recommendations for policymakers. By illuminating the critical connection between education and trust, this research aims to provide a framework for strengthening democratic processes through informed and engaged electorates.

2. THEORETICAL BACKGROUND

To understand how education can impact trust in election technology, it is crucial to delve into theoretical models that explain technology acceptance and usage. Two prominent models in this regard are the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). These models provide a framework for examining the factors that influence individuals' acceptance and trust in technology, highlighting the role of education in this process.

2.1. Technology Acceptance Model (TAM)

The Technology Acceptance Model, developed by Davis (1989), posits that two main factors determine the acceptance of technology: perceived usefulness (PU) and perceived ease of use (PEOU). According to TAM, individuals are more likely to adopt and trust a technology if they believe it will enhance their performance (PU) and if they find it easy to use (PEOU).

Education can significantly influence both PU and PEOU. By providing comprehensive knowledge about the functionalities and benefits of election technology, educational initiatives can enhance voters' perceptions of its usefulness. For example, training programs that demonstrate how electronic voting machines improve accuracy and efficiency in the electoral process can positively impact PU. Additionally, education can simplify the user experience by reducing the perceived complexity of the technology. Workshops and tutorials that familiarize voters with the operation of voting machines or online voting platforms can make these systems appear more user-friendly, thereby enhancing PEOU.

2.2. Unified Theory of Acceptance and Use of Technology (UTAUT)

The Unified Theory of Acceptance and Use of Technology, introduced by Venkatesh et al. (2003), expands upon TAM by incorporating additional determinants of technology acceptance. UTAUT identifies four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. Each of these constructs can be influenced by educational interventions, thereby impacting trust in election technology.

1. Performance Expectancy: Similar to PU in TAM, performance expectancy refers to the degree to which an individual believes that using the technology will help them achieve better outcomes. Education can bolster performance expectancy by clearly communicating the advantages and effectiveness of election technology in ensuring fair and efficient elections.

2. Effort Expectancy: Comparable to PEOU, effort expectancy pertains to the ease of using the technology. Through

targeted educational programs that simplify and demystify the use of election technology, voters are more likely to perceive it as easy to use, thereby increasing their likelihood of acceptance and trust.

3. Social Influence: This construct involves the extent to which individuals perceive that important others (e.g., family, friends, or societal figures) believe they should use the technology. Educational campaigns that include endorsements from trusted community leaders and influencers can positively shape social influence, encouraging broader acceptance and trust in election technology.

4. Facilitating Conditions: These refer to the availability of resources and support needed to use the technology. Education can enhance facilitating conditions by providing access to information, resources, and technical support that enable voters to effectively use election technology. This includes helplines, instructional materials, and community support centers that assist voters throughout the electoral process.

2.3. Integrating Education with TAM and UTAUT

By integrating educational strategies with the constructs of TAM and UTAUT, we can develop a comprehensive approach to fostering trust in election technology. Education serves as a crucial mediating factor that influences perceptions of usefulness, ease of use, performance expectancy, effort expectancy, social influence, and facilitating conditions. Through well-designed educational initiatives, voters can gain the confidence and competence needed to trust and utilize election technology effectively.

For instance, a study by Carter and Bélanger (2005) found that educating users about the security measures and benefits of e-government services significantly increased their trust and adoption rates. Similarly, in the context of election technology, providing voters with transparent information about security protocols, data privacy, and the reliability of electronic voting systems can mitigate concerns and build trust.

2.4. Adapt TAM and UTAUT to Address Election Technologies Challenges

While TAM and UTAUT provide a strong foundation for understanding technology adoption, applying these models to election technology requires specific adaptations to address its unique challenges. Election technology involves higher stakes and public scrutiny compared to other technologies, necessitating a focus on trust, security, and transparency. To enhance the theoretical depth and applicability of this research, we propose that TAM can be extended by incorporating constructs related to perceived security and transparency, which are critical for voter confidence. For instance, we aim to introduce a "Perceived Security" construct to measure the extent to which voters believe that election technology is secure from tampering and fraud. Similarly, we propose that UTAUT can be adapted by emphasizing the role of institutional trust and integrating constructs such as "Institutional Assurance," reflecting voters' trust in the institutions that deploy and manage the technology. These extensions will allow the models to more accurately capture the factors influencing trust in election technology. By addressing these unique challenges, we can develop a more robust theoretical framework that not only explains technology acceptance but also provides actionable insights for enhancing voter trust in election systems. This approach aligns with findings from previous studies on e-government services, where adaptations of TAM and UTAUT to include security and trust-related factors have proven effective in predicting user acceptance (Carter & Bélanger, 2005)

In summary, the TAM and UTAUT models offer valuable insights into how education can impact trust in election technology. By enhancing perceived usefulness, ease of use, performance expectancy, and other key constructs, education plays a pivotal role in promoting the acceptance and trust of technological advancements in elections. As we continue to integrate technology into electoral processes, ongoing educational efforts will be essential in ensuring that voters are informed, confident, and trusting participants in the democratic process.

3. METHODOLOGY

3.1. Research Design

This study employs a quantitative research design to investigate how education impacts trust in election technology using the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). The primary method of data collection will be through structured surveys administered to a sample of eligible voters. The survey will be designed to measure variables related to TAM and UTAUT constructs, as well as participants' levels of trust in election technology.

To ensure the robustness of our research, we will implement a stratified sampling method to ensure a diverse and representative sample that mirrors the demographic composition of the voting population. This approach will involve categorizing participants by key demographic variables such as age, gender, education level, socioeconomic status, and geographic location. By doing so, we aim to capture a broad spectrum of perspectives and experiences, which is crucial for understanding how education impacts trust in election technology across different voter groups. This stratified approach will allow us to conduct subgroup analyses to examine the differential impact of educational interventions on various demographic segments.

3.2. Hypotheses

Based on the theoretical frameworks of TAM and UTAUT, we propose the following hypotheses:

H1: Education on election technology positively impacts perceived usefulness (PU) of election technology.

H2: Education on election technology positively impacts perceived ease of use (PEOU) of election technology.

H3: Perceived usefulness (PU) of election technology positively impacts trust in election technology.

H4: Perceived ease of use (PEOU) of election technology positively impacts trust in election technology.

H5: Education on election technology positively impacts performance expectancy (PE) of election technology.

H6: Education on election technology positively impacts effort expectancy (EE) of election technology.

H7: Performance expectancy (PE) positively impacts trust in election technology.

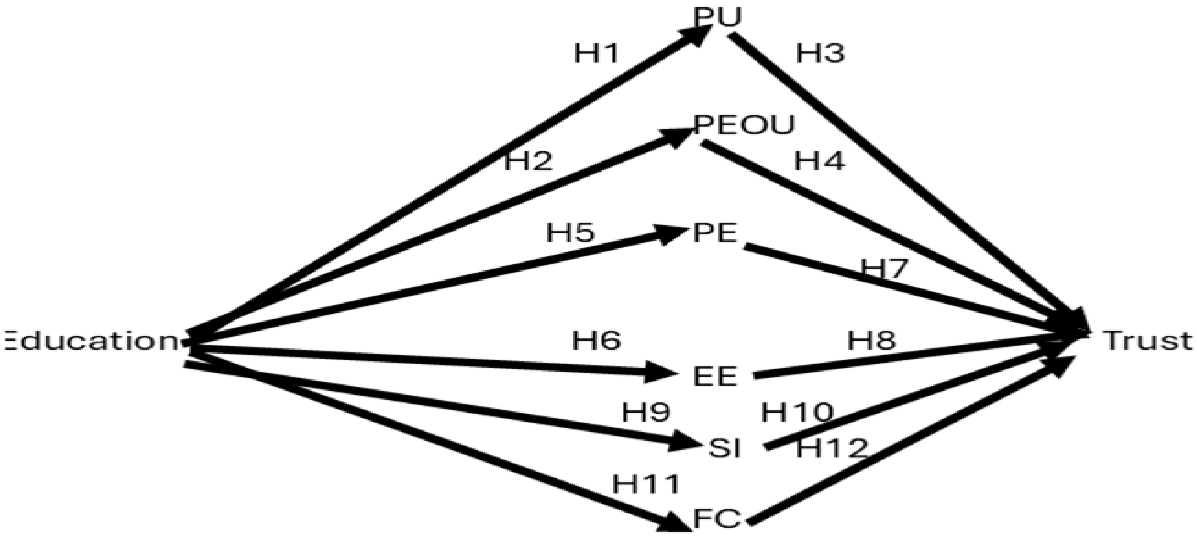

Figure 1. Hypothesis Model

H8: Effort expectancy (EE) positively impacts trust in election technology. (See comment above)

H9: Education on election technology positively impacts social influence (SI) regarding the use of election technology.

H10: Social influence (SI) positively impacts trust in election technology.

H11: Education on election technology positively impacts facilitating conditions (FC) for the use of election technology.

H12: Facilitating conditions (FC) positively impact trust in election technology.

3.3. Survey Instrument

The survey will consist of several sections, each corresponding to different constructs from the TAM and UTAUT models. Participants will respond to statements on a Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree). The survey will include the following sections:

1. Demographics: Age, gender, education level, and voting history.

2. Education on Election Technology: Questions assessing the extent and type of educational interventions participants have received regarding election technology.

3. Perceived Usefulness (PU): Items measuring the degree to which participants believe that election technology enhances the electoral process.
4. Perceived Ease of Use (PEOU): Items assessing how easy participants find the use of election technology.

5. Performance Expectancy (PE): Questions regarding participants' expectations that election technology will improve electoral outcomes.

6. Effort Expectancy (EE): Items evaluating the effort required to use election technology.

7. Social Influence (SI): Questions measuring the influence of social factors on participants' use of election technology.

8. Facilitating Conditions (FC): Items assessing the availability of resources and support for using election technology.

9. Trust in Election Technology: Questions evaluating participants' trust in the security, reliability, and overall integrity of election technology.

3.4. Data Analysis

Data collected from the surveys will be analyzed using structural equation modeling (SEM) to test the hypothesized relationships between constructs. SEM is chosen due to its capability to evaluate complex relationships among multiple variables simultaneously.

1. Descriptive Statistics: Initial analysis will involve descriptive statistics to summarize the demographic data and the distribution of responses for each survey item.

2. Reliability and Validity: Cronbach’s alpha will be used to assess the internal consistency of the survey scales. Confirmatory factor analysis (CFA) will evaluate the validity of the constructs.

3. Hypothesis Testing: Path analysis within the SEM framework will be conducted to test the proposed hypotheses, examining the direct and indirect effects of education on trust in election technology through the TAM and UTAUT constructs.

4. FUTURE RESEARCH

The study's reliance on surveys administered before and after an educational session could raises concerns about capturing long-term changes in attitudes or behaviors, and the use of self-reported data may introduce biases affecting the validity of the findings. To address these concerns, in the future studies, we will incorporate a longitudinal design, following participants over an extended period to assess the persistence of educational impacts on trust in election technology. This approach will involve administering follow-up surveys at multiple intervals to evaluate long-term changes in attitudes and behaviors. Additionally, we plan to complement self-reported data with behavioral measures, such as tracking actual voter turnout and engagement with election technology during subsequent elections. By triangulating self-reported data with objective behavioral data, we can mitigate potential biases and enhance the validity of our findings.

Other interviewing variables to consider in future studies on trusting election technology and security are:

1. Narcissism - a personality trait associated with inflated views of oneself, egotism, and self-promotion.as well as positive and inflated self-views of intelligence, power, and physical attractiveness (Raskin and Terry 1988; Twenge, Konrath, Foster, Campbell, & Bushman, 2008).

2. Technology Readiness Index to measure optimism, innovation, discomfort, and insecurity (Parasuraman & Colby, 2000).

3. Cyber Self-Efficacy to measure confidence with technology. (Claar & Johnson, 2012; White & Ekin & Visinescu, 2017).

5. CONCLUSION

This methodology provides a structured approach to investigating the impact of education on trust in election technology. By leveraging the TAM and UTAUT models, this study aims to identify the key factors that mediate the relationship between education and trust, thereby offering insights into effective educational strategies to enhance public confidence in electoral systems.

6. **REFERENCES**

Carter Center. (2020). Building Confidence in U.S. Elections: A Summary of the Carter Center's Electoral Integrity Assessment Project. The Carter Center.

Carter, L., & Bélanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5-25.

Claar, C. I., & Johnson, J. (2012). Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems,* 52(4), 20-29.

Coleman, J. (Dec. 2020). Poll: Less than one-quarter of Republicans trust election results. *The Hill*, Dec. 9, 2020. (Accessed on 8/31/21) https://thehill.com/homenews/campaign/529476-fewer-than-one-quarter-of-republicans-trust-election-results-poll

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

Dodge, R. C. & Carver, C. & Ferguson, A. (2007). Phishing for user security awareness. *Computers & Security*, 26(1), 73.

Fried, A., & Harris, D. B. (2020). In Suspense: Donald Trump's Efforts to Undermine Public Trust in Democracy. Society, 57(5), 527-533. http://dx.doi.org/10.1007/s12115-020-00526-y.

Laughlin, N. & Shelburne, P. (2021). How Voters' Trust in Elections Shifted in Response to Biden's Victory. *Morning Consult*, Jam. 27, 2021. (Access 8/31/21) (on-line) https://morningconsult.com/form/tracking-voter-trust-in-elections/.

Mercur, R.T.i & Neumann, P.G. (June 2021). The Risks of Election Believability (or Lack Thereof). *Viewpoints: COMMUNICATIONS OF THE ACM*, 64(6), 24-30. DOI:10.1145/3461464.

Ng, B.Y.,& Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief prospective. *Decision Support Systems*, 46(4), 815-825.

Norris, P. (2015). Why Electoral Integrity Matters. Cambridge University Press.

Parasuraman, A. & Colby, C. L. (2000). An Update & Streamlined Technology Readiness Index (TRI). *Journal of Service Research*, 18(1), 59-74.

Pew (2021). Public Trust in Government: 1958-2021. *Pew Research Center*, May 17, 2021. (Accessed 8/31/2021, online) https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/.

Raskin, R. & Terry, H. (1988). A principal-components analysis of the Narcissistic Personality Inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology*, 54(5), May 1988, 890-902.

Schultz, E. (2004). Security training and awareness – fitting a square peg in a round hole. *Computers & Security*, 23, 1-2.

Twenge, J. M., Konrath, S., Foster, J. D., Campbell, W. K., & Bushman, B. J. (2008). Egos inflating over time: A cross-temporal meta-analysis of the Narcissistic Personality Inventory. Journal of Personality, 76(4), 875-902.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.

White, G. & Ekin, T. & Visinescu, L. (2017). "Analysis of Protective Behavior and Security Incidents for Home Computers." *Journal of Computer Information Systems:* **57**(4): 353-363. Online: http://www.tandfonline.com/doi/full/10.1080/08874417.2016.1232991

APPENDIX A:

PILOT STUDIES

Four primary/pilot presentations were made. The first had a negligible positive impact on 8 college students. The second with 10 retirees, had a negligible negative impact. A third presentation, more structured, was made to students attending a high school information technology symposium in San Marcos, Texas (Oct. 8, 2021). Here are the results of their evaluation of the presentation (N = 17).

Presentation:
Excellent 82 %, Great 12%, Good 6%, Fair 0 %, Poor 0%.
Amount learned:
arge 41%, Good 59%, Acceptable 0% Little 0%. Very little if at all 0%

Comments included:

- "You're the only presenter I could understand. I am new to this"
- "This was the only class that I really understood and did not fall asleep"
- "You really connected everything instead of just talking about the topics."
- "I really thought that the entire lessons were deeply described and easily help me understand stuff I have never learned before."
- "Very knowledgeable about the subject, learned a lot. Great."

A fourth presentation was made to computer professionals attending a San Antonio, Texas, cyber summit (Oct. 30, 2021). Here are the results (N = 11):

Presentation:
Excellent 45 %, Great 36%, Good 18%, Fair 0 %, Poor 0%.
Amount learned:
Large 27%, Good 55%, Acceptable 18% Little 0%. Very little if at all 0%

Comments included:

- "This is an important topic, that is critical to preserving our Republic."
- "I understood the technical aspects, but the application of these technologies to detect fraud was new and interesting."
- "Presenter has found group of problems and proves it. Learned problem breakdown."
- "Interesting subject. I'd like to go deeper and learn if the Dominion voting machines were coded to do voter fraud?"
- "I learned how fraud can be proven in court and how fraud can be claimed but is proven false. This is very important for people to know."
- "Good talk"
- "It was an interesting presentation which made me think about and learn about the access of voting digitally.

APPENDIX B: Readings

Background

Hashing is the processing of a unique value for a data file through a mathematical function. An example is a check sum. Given an account number 4545, the digits sum up (4+5+4+5) to a check sum of 18. The hash value is a unique file identifier. If the file changes, the hash value changes. It provides security when the data is shared. It shows integrity, no changes. Hash collisions (different data files calculate the same hash values) are possible. However, this weakness is resolved by using a more powerful hash function or adding an arbitrary value, known as a salt value, to the calculations.

Digital Signatures use hashing functions to show no changes and uses certificates from a third party to show non-repudiation (data came from you and you cannot deny it). Computer laws from many countries have provided greater cyber-security by the acceptance of digital signatures as legal evidence in courts.

To prove in court election software was rigged.

The evidence needed to prove in court the program was rigged are 1) Hash Values of the program, 2) Digital Signature of the program, 3) Test data documentation, and 4) Separation of duties documentation, the testers are independent of the program's developers. The Hash Values show no changes in the program and properly identifies the program used. The Digital Signatures show non-repudiation, you wrote the program.

To prove in court there were Dead Voters

To prove in court that dead people voted requires the comparison of two databases, death certificates from the Department of Vital Statistics database and voter registration records from the Election Commission database. Both databases have common data fields: first name, last name, date of birth, gender, current address, etc.

The compared records from the two databases must be scrub and cleaned (fix mismatches & errors). Hash values of the database files need to be checked to insure nothing was changed so as to show in court. Digital Signatures also need to be presented to the court to show that the sources of the records were from the Dept. of Vital Statistics and the Election Commission.

CYBER SELF-EFFICACY (Claar & Johnson, 2012; White & Ekin & Visinescu, 2017).

Compared to others in the U.S. that are similar age as you, answer the following questions. (NOT at all confident; NOT confident; Somewhat NOT confident; Neutral; Somewhat confident; Confidant; Totally confident).

- I can select the appropriate security software for my home computer.
- I can correctly install security software on my home computer.
- I can correctly configure security software on my home computer.
- I can find the information needed if I have problems using security software on my home computer.
-