Interacting with Computers, 2025, 1–21
https://doi.org/10.1093/iwc/iwaf055
Article

I Know, Therefore, I Trust? quantitatively modelling how knowledge shapes the reliance on trust and confidence in the case of internet voting usage in Estonia

Bogdan Romanov [1,*], David Duenas Cid [2] and Mihkel Solvak [1]

[1]Lossi 36, Tartu University, Johan Skytte Institute of Political Studies at University of Tartu, 51003, Tartu, Estonia
[2]Kozminski University, Pub-Tech Research Center (Public Sector Data-Driven Technologies), Warsaw, Poland
*Corresponding author: Email: bogdan.romanov@ut.ee

Abstract

Internet voting is widely adopted in Estonia, yet psychological factors influencing its acceptance remain underexplored. The increasing complexity of digital voting systems raises concerns about whether voters rely on institutional trust or personal confidence driven by knowledge. This study applies Simmel's concept of trust, bridging ignorance and certainty, and Giddens' differentiation between trust and confidence. These frameworks help understand how different knowledge levels influence the mechanisms voters use to decide whether to use Internet voting or not.

Using post-election survey data from the 2021 local and 2023 parliamentary elections in Estonia ($N = 1{,}153$, $N = 1{,}001$), this study examines how technical knowledge moderates the relationship between trust in institutions and confidence in one's own knowledge when it relates to Internet voting. The key independent variables include technical knowledge, confidence in the system, and trust in political institutions; the dependent variable is binary Internet voting usage. Logistic regressions are employed to assess the effects of the variables, including the set of standard socio-economic controls.

Results show that confidence is the decisive factor for individuals with high levels of technical knowledge, significantly increasing their likelihood of voting online. Trust in government does not exert a consistent effect overall, with significance emerging only among respondents with high knowledge. By contrast, both trust in system performance and trust in Internet voting show robust positive main effects across the electorate, without evidence that their influence differs by knowledge level. These findings enrich the literature by influencing how knowledge conditions the role of confidence, while trust complements adoption more broadly.

RESEARCH HIGHLIGHTS

- Trust and confidence influence Internet voting behavior and actual usage of technology.
- Technical knowledge level dictates reliance on confidence or trust in political institutions and technology itself.
- High-knowledge users rely primarily on confidence, leading to a greater likelihood of informed usage.
- Trust in political institutions shows an effect only among high-knowledge users, while trust in Internet voting and its performance exert positive effects across the electorate but are not stronger among low-knowledge users.

Keywords: *user characteristics; internet voting; trust; knowledge; Estonia*

Researching trust has been an important topic for social sciences (Hardin, 2006) and has sparked a new wave of renewed interest stemming from the digitalization of societies (Bodó, 2021). The technological development of societies brings along with it an increasing complexity and, in parallel, a renovation of the understanding of certain vital elements for societal cohesion, such as equity (Ruijer et al., 2023) and solidarity (Duenas et al., 2023). Similarly, the foundations of trust have been shaken by technological developments, and the research examining the relationship between trust and, more recently, distrust and technology are long and diverse, covering the main recent technological developments, including, e.g., blockchain (Hawlitschek et al., 2018) or artificial intelligence (Benk et al., 2024; Kleizen et al., 2023).

The role of trust is strongly associated with the growth of complexity concerning modern technological systems, including digital governance (digital governance and e-governance are used interchangeably). For instance, citizen attitudes toward e-governance adoption are significantly influenced by trust in institutions and the perceived benefits of technological systems (Al-Hujran et al., 2015). As systems grow more advanced and usually more complex, trust becomes essential for managing

Received: May 5, 2025. **Revised:** October 24, 2025. **Accepted:** November 14, 2025

uncertainty and imperfect knowledge (Mayer et al., 1995). Trust serves as a mechanism for reducing complexity (Luhmann, 1979), enabling people to use technologies without the need to have constant questions regarding their functioning or a complete understanding of the inner workings, relying, for example, instead on the reliability of the system and designers (Glikson and Woolley, 2020; Hawlitschek et al., 2018) whose expertise allows for overcoming the lack of own knowledge (Giddens, 1990).

Paradoxically, this increase in technological systems' complexity is coupled with efforts to make them more convenient and user-friendly: users are invited to utilize simple interfaces with a complex system behind the screen that remains invisible. Trust, then, is the dialogue between the inherent complexity of technological systems and the ease of their use (Kim et al., 2024; Mirabdolah et al., 2023; Savioja et al., 2014), and users are enticed to trust complex systems merely because they are sufficiently efficient and paint over the fact that the underlying complexity is not fully understood (Caloyannides, 2004). This so-called "blind" trust, stemming mainly from usage convenience, simplifies access to the services but obscures potential risks, like security vulnerabilities, which might erode trust if the system fails to perform its work, i.e., when convenience-driven trust fails (Octasia, 2018).

Parallel to trust, confidence has been defined as the certainty that something will occur as expected based on previous knowledge and experience (Giddens, 1991). Similarly, Luhmann (1988) understands confidence as the expectation that something will occur where no risks are considered (Meyer et al., 2008). Both approaches relate confidence to knowledge, assuming that confidence appears when there is a certitude based on some form of reflection relying on previous knowledge or a risk assessment. This differs significantly from the understanding of trust and its relationship with knowledge. Simmel (1950) describes trust as an antecedent of knowledge, a bridge that allows for the connecting of ignorance and knowledge and the taking of action in situations of imperfect knowledge by relying on other inputs. In contemporary technologically driven societies, although the connection between trust, knowledge, and confidence has become more complex (e.g., due to the increase in available information (Buckland, 2017) and the lack of verifiability of some of these information sources (van Zoonen et al., 2024), knowledge still appears as a crucial concept in the cornerstone between trust and confidence.

This intertwinedness between knowledge, trust, and confidence will be studied in detail. To do so, a critical field of research is approached: Internet voting use. Internet voting, casting ballots for elections using a remote Internet system, represents an electoral innovation with supporters and detractors. The reason for both positions is commonly related to trust factors. Internet voting is implemented in a few countries and relies upon very developed cryptographic systems, but at the same time, it relates to critical societal actions such as deciding to whom power will be delegated within and after the elections. As such, it is a field prone to discussions of political, societal, and technical nature and represents an interesting field for research on trust-related issues (Dueñas-Cid, 2024).

The purpose of the article is to answer the question, how does knowledge latently affect the usage of Internet voting technology via confidence and trust-infused factors? In order to structure the answer to the research question, the following hypotheses were tested:

Hypothesis 1: At high-knowledge levels, confidence in technology is the primary predictor of Internet voting usage.

Hypothesis 2: At low-knowledge levels, trust-related factors, i.e., trust in Internet voting, trust in political institutions, and Internet voting's performance are the primary predictors of Internet voting usage.

In other words, this study investigates the interplay between trust, confidence, and knowledge in shaping the adoption of Internet voting in Estonia, an only democratic country enabling its citizens to cast a vote during the election for all election types (Use of E-Voting Around the World, 2023). While Internet voting offers significant benefits, including convenience and efficiency, its adoption hinges on psychological and societal factors, such as users' trust in the system and their confidence in its reliability. The central problem explored in this paper is the extent to which technical knowledge influences these mediating factors, trust and confidence, and how they, in turn, drive Internet voting usage. Using survey data from two Estonian elections, the local elections of 2021, and the parliamentary elections of 2023, logistic regression models are applied to test the hypotheses and uncover the nuanced relationships among these variables.

The article adheres to a structured academic framework to unveil the narrative behind the findings. The second section establishes the core theoretical concepts (i.e., trust, confidence, and knowledge) and explores their interconnections, from which two key hypotheses are derived. The third section outlines the methodological approach, detailing the data collection process, survey design, and the operationalization of theoretical concepts into measurable variables. In the fourth section, two hypotheses are rigorously tested using binary logistic regression analysis to uncover the relationships driving Internet voting adoption. The discussion section provides an in-depth interpretation of the findings, linking them to existing literature and highlighting their broader implications. Finally, the conclusion synthesizes the study's key insights, emphasizing the role of confidence and trust in Internet voting adoption, and suggests avenues for future research, while the limitation section acknowledges the study's constraints, such as reliance on self-reported data and the scope of variables.

1 Theoretical background

An essential component of increasing the complexity of the current societies and, therefore, reforming the forms of trust has been the adoption of technologies (Duenas and Calzati, 2023). Technology development has reduced the capacity to control and understand essential elements of the everyday lives while increasing convenience. Internet voting serves as an excellent example of that; it represents a technology that makes the voting process and overall election management simpler and more convenient by using complex technologies. Given the sociotechnical nature of technology (van Dijck, 2013), the elements that might influence the creation of trust in aspects related to Internet voting span from cryptographic elements to the legal framework or politically related aspects, being technological elements enmeshed with societal ones (Dueñas-Cid, 2024).

Here comes the crux of the matter and the pivotal element of this paper. Internet voting systems are complex technologies that are not easy to understand, requiring essential knowledge in particular topics like voter identification and eligibility verification methods, exchange of encrypted messages, in-depth cryptography and security protocols, voter registration, storage services, and vote tabulation methods. However, the eminently practical nature of such technology, purposefully designed to emulate regular on-paper voting, makes it easy for voters to use, who can cast their ballots more conveniently due to possessing a certain level of practical knowledge in using technology. The difficulty in understanding Internet voting lies at the bottom of some of the leading critics of the system (Licht et al., 2021; Volkamer et al., 2011). Internet voting systems are more complex than paper voting systems, making it much more challenging to observe and ascertain the system's security and, therefore, hard for nontech-savvy users to follow (Willemson, 2018). This scenario depicts knowledge as an important element in relation to the use of Internet voting, but how it intersects with the creation of trust in Internet voting remains an open question.

The relationship between knowledge and trust has already been approached in the past. Simmel (1950) understood trust as the link between the absolute lack of knowledge (faith) and the absolute knowledge (certainty), serving as a sort of bridge connecting the unknown with the known and allowing taking risks. Luhmann (1979) linked trust with dealing with uncertainty so that familiarity (knowledge based on experience) helps reduce the inherent uncertainty involved in any complex societal activity and allows for creating trust or distrust and transforming reality into something manageable with identifiable risks. Connecting these ideas to the paper's topic, one does not necessarily need to understand the insights into technology or have advanced knowledge on electoral management to use Internet voting, since one can rely upon the trust posited in the government and/or based on previous experiences with this or similar technologies. Similarly, Zinn places trust as a semi-emotion that is put between rational and nonrational certainties (2008, 2016), having one foot on factual knowledge and another in emotions, and serving to deal with uncertainty.

The concept of knowledge is also present in Giddens' (1990) understanding of trust when it connects trust to knowledge asymmetry. Individuals cannot fully understand every aspect of complex societies and technologies, and they need to rely on those with the necessary expertise to understand them. As a result, trust is transferred from those holding specific knowledge to those who do not possess it, becoming knowledge-holders (experts), a form of trust mediator. Trust appears as a third-party legitimized element based on trusted parties: one might not have absolute knowledge about how things work, but enough knowledge to know who to trust or distrust. In this context, political parties act as legitimate actors for their audience, helping shape the positions of their voters regarding trust in Internet voting. In this regard, party cues have been identified as trust mediators, influencing citizens' perceptions, and acceptance of new technologies (Ehin and Solvak, 2021a). Giddens (1990) adds more complexity to this scenario when introducing "confidence" in his definition of trust as "the link between faith and confidence." In his approach, faith is such a scenario in which one has no knowledge and needs to put the expectations into faith. Confidence is a scenario in which one has complete certitude and, therefore, does not need to trust. In other words, the more one knows, the less one needs to rely on trust, and the more one can rely on confidence, and thus, the more one can engage with the technology (Cegarra-Navarro et al., 2014).

More recently, De Filippi et al. (2020) used a similar understanding of the relation between trust and confidence, putting the distinction not necessarily on the actual knowledge available but on the individual's attitude concerning the available knowledge and the certainty that something will occur. Confidence, in this case, would result from the fact that the available knowledge and experience would create a feeling of security and predictability in the use of technology.

While the use of the concept of trust has been widely used in the research on information systems, the way it has been approached has been based on simplistic conceptual approaches to trust (Duenas and Calzati, 2023; Marsh and Dibben, 2005), on occasions being trust considered as a predictor of usage of technology (Li et al., 2008) in others as a consequence of its use (Janssen et al., 2018), as the result of the adoption of complex technical elements (Barthe, 2015), or as the result of using complex self-surveillance systems (i.e., blockchain) (Jemielniak and Przegalinska, 2020), ignoring the need of societal legitimation of such systems (Bodó, 2021). The relationship between trust, confidence, and knowledge has yet to be underexplored in digital technologies, with some exceptions (De Filippi et al., 2020), and remains unresolved in Internet voting.

Internet voting might be the most appropriate technology case, which merges trust, knowledge, and confidence in its core due to several unique characteristics of elections (Duenas et al., 2022). Elections are not continuous services but discrete events with rigid time constraints, meaning voters must trust that everything will perform correctly on a single day or throughout the election period. Additionally, the structural complexity of elections, which involve numerous temporary actors and networks, amplifies the challenge of ensuring public confidence (Krimmer et al., 2021; Montjoy, 2008). For voters, these managerial complexities are often invisible, but for electoral administrations, ensuring a correct unfolding of elections plays a crucial role in building citizens' trust. Internet voting further complicates these dynamics, requiring the seamless integration of technological systems with traditional electoral frameworks (Duenas et al., 2020; Krivonosova, 2022).

The stakes are further raised by the political significance of elections, which are central to democratic governance (Dueñas–Cid, 2024). For voters, trust in Internet voting is about trusting the system's performance and trusting that their vote will be accurately counted and that the process will be transparent (Agbesi et al., 2024). Given the central role of elections in distributing and delegating political power, trust in Internet voting overpasses technical aspects (Wolf et al., 2011) and dialogues directly with elements related to the broader trust in democratic institutions (Sharma, 2020). Additionally, the conceptual framework is intentionally limited to trust, confidence, and usage, without including the verification tool/mechanism, which allows users to check if the vote was recorded as cast. It must be admitted that it is compulsory for trust building (Marky et al., 2021), but how this technology is integrated in the framework is cumbersome to define—its use rate is extremely low, about 4%, and the image of the verifying users is not clear and poses a different research angle (Solvak, 2020). Do users verify because they distrust the technology and/or the institutions maintaining it, or is verification used by trusting users, aiming to solidify their trust? As a result, within the research verification logic is kept aside, and attention is paid to trust, confidence, and actual usage.

Even if previous research approached several elements contributing to the understanding of trust in Internet voting, understanding how different levels of knowledge shape voter confidence and trust in Internet voting is still an open question, a question ultimately key to ensuring the legitimacy and acceptance of such systems in future democratic processes. With this idea in mind, a following set of hypotheses are suggested:

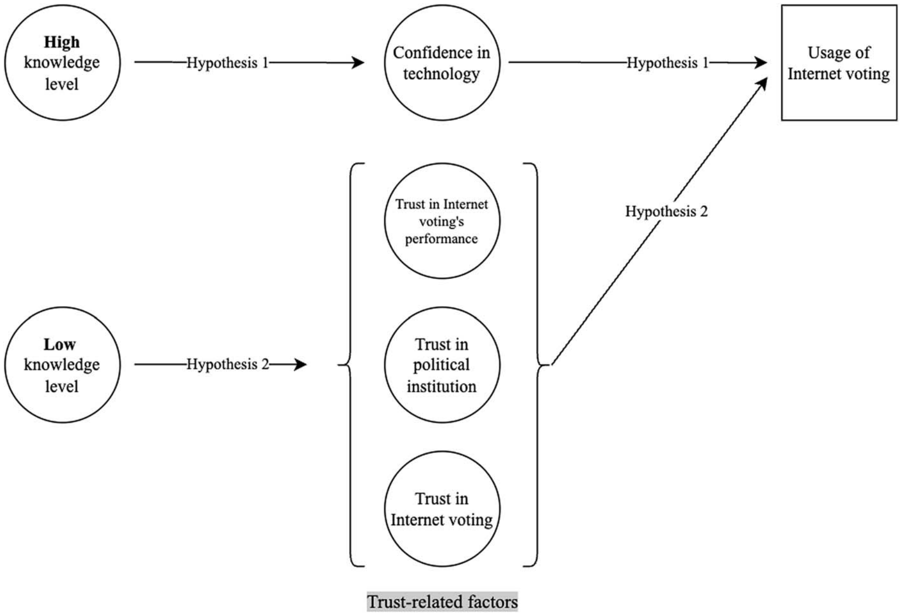


Figure 1. The visualization of the theoretical expectations

Hypothesis 1: At high-knowledge levels, confidence in technology is the primary predictor of Internet voting usage.

Individuals with higher knowledge levels are less dependent on the "blind" trust factors, as their understanding of cryptographic measures, security protocols, and less technically complicated notions allows them to have greater confidence in the reliability and integrity of the Internet voting system.

Hypothesis 2: At low-knowledge levels, trust-related factors, i.e., trust in Internet voting, trust in political institutions, and Internet voting's performance (concepts to which trust is delegated) are the primary predictors of Internet voting usage.

In contrast to hypothesis 1, individuals with lower knowledge rely heavily on external signals of trustworthiness to navigate the uncertainties associated with Internet voting. These signals include previous experiences using the system, the reputation of electoral bodies, rumors, and scandals related to the Internet voting platform and its administrators, as well as recommendations from trusted political figures. Additionally, Wang et al. (2020) demonstrate that well-performing government applications foster citizen compliance by influencing their perceptions of system effectiveness and trustworthiness. This finding supports the notion that Internet voting performance, as perceived by users, plays a critical role in driving adoption, especially among those with limited technical understanding.

This reliance is closely linked to practical knowledge associated with the use of the system and the societal context. Practical knowledge refers to individuals' hands-on experience and familiarity with Internet voting technologies, which can compensate for their lack of technical understanding. In societies with high digital literacy and widespread technology adoption, even individuals with low technical knowledge can feel confident using Internet voting systems due to their everyday interactions with similar technologies (Vassil et al., 2016). Thus, societal norms and the general acceptance of digital platforms play a crucial role in shaping trust and adoption among less knowledgeable users.

By connecting trust-related factors to practical knowledge and societal influences, the goal of the study is to better understand how individuals with higher and lower knowledge levels decide about using Internet voting systems. Their reliance on practical experiences and societal cues underscores the importance of fostering a trustworthy environment and enhancing digital literacy to encourage the adoption of Internet voting. The overall theorertical argument presented in Figure 1.

2 Methodology

2.1 Source

Estonia is selected as a critical case for the Internet voting usage as the only democratic country arranging regular, legally binding elections via the Internet across the entire country. Since its introduction in 2005, Estonian Internet voting has matured into a routine part of elections, supported by robust legal, technical, and institutional frameworks. This long-term institutionalization allows the study to test hypotheses related to user behavior and attitudes over time.

Moreover, Estonia's high level of digitalization and its strong emphasis on e-governance mean that the population is generally accustomed to interacting with complex digital systems. This creates a favorable context to explore how different levels of technical knowledge mediate the role of trust and confidence in technology adoption. Thus, Estonia offers not only the empirical conditions necessary for rigorous analysis but also a sociotechnical environment where the influence of knowledge on trust and confidence can be meaningfully assessed.

2.2 Data

The article's main focus is unpacking the intertwined association between trust, knowledge-confidence, and the usage of Internet voting. In order to test these mechanisms, individual-level survey data from two elections over the period from 2021 to 2023 is utilized. The 2021 elections were local elections, while the 2023 elections decided on the composition of the national parliament. The studies used in this analysis were cross-sectional post-election surveys representative of the voting-eligible population in terms of age, gender, ethnicity (language spoken at home), education, and region. Timeframes 2021 and 2023 are justified by the absence of variable operationalizations in the iterations prior to 2021. As the modeling below involves only self-reported voters, with respondents reporting nonvoting excluded, Internet voters are contrasted with paper voters by pooling both datasets to achieve a higher case number, and all subsequent analysis is conducted on the pooled dataset. The total sample was 2,142, excluding nonvoters left. Nonvoters made up 18.7% of the total sample of 2,142, after excluding them, the sample consist of 1,743 respondents, adding relatively many control variables, plus running interactions with variables that have missing values for some respondents leads to a final sample of 1,155 for the combined models. The original pooling decision is therefore justified, otherwise leading to the variables-to-cases ratio problem. In the modeling below, standard errors were, however, clustered by election to account for the fact that despite having repeated random samples from the same population over time and accurate mean effect of the population could be calculated as well, there is a theoretical possibility that outcomes could be clustered depending on the election year, i.e., the could be a sampling design that causes clustering (Abadie et al., 2023). The missing data were not imputed; the total sample size used in the analysis is hence reduced by involving voters only and leaving out respondents with missing values on any variable included in the modeling. For details on the data gathering of the surveys, see Appendix A.

Despite the fact that the 2021 survey wave could have been affected by the COVID-19 outbreak, the design intentionally disregards this exogenous shock for two main reasons. Firstly, COVID-19 did not have a substantial effect on the usage of the Internet voting systems, see Figure 2. The predicted share of Internet votes for the 2021 election does not differ from the actual number. Secondly, the authors of this paper prepared a more detailed analysis of the impact of COVID on the usage of Internet voting across Estonia, and the effect observed is considerable only among particular age groups—the share of the senior population has switched from paper voting to Internet voting.

The main predictors stem from theoretical discussion and previously published studies exploring the phenomenon of Internet voting. The operationalization is presented in Table 1 below. Most explanatory variables are dichotomized to allow larger qualitative differences between the theorized groups to emerge. Continuous variables would reflect smaller quantitative unit differences and could potentially obscure the mechanism under investigation. There is a clear position in the literature on why routine dichotomization entails problems, which mostly focus on the statistical artefacts it creates (Altman and Royston, 2006; MacCallum et al., 2002). But there are also positions on why it is defendable, or even desirable under certain conditions when variables have either skewed distributions or expected nonlinear associations with third variables, or when there is a substantive reason for splitting a scale at a point that might contravene with the most optimal cut-off from a statistical point of view (DeCoster et al., 2009; Streiner, 2002). The study justifies dichotomization on three grounds. First, for four to five item Likert scale variables, there are clear substantive cut-off points that separate respondents who have or do not have the measured attribute regardless of the most optimal statistical cut-off value. Second, for almost all variables

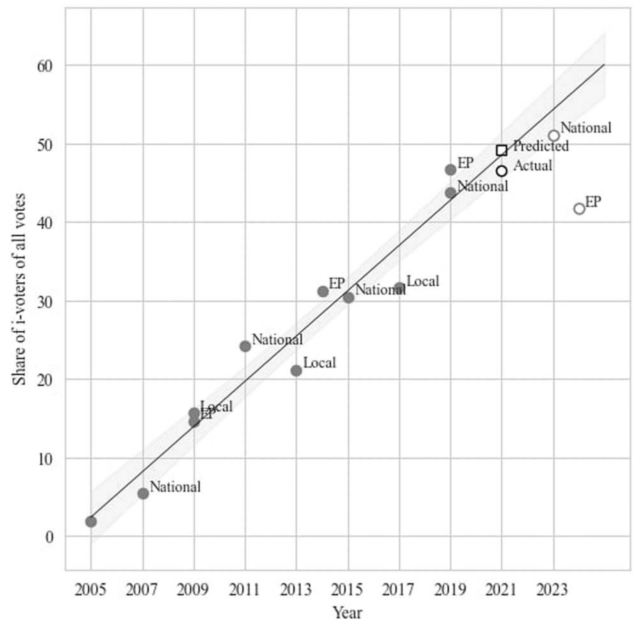


Figure 2. Share of Internet voters 2005–2024 with a superimposed trendline and predicted 2021 Internet voter share based on the data for 2005–2019, with turnout depicted in the parentheses. Values for 2023 and 2024 are not included in the training data and are presented for the overall trend. Source: Valimised | Elections in Estonia. (n.d.). Retrieved March 4, 2025, from https://www.valimised.ee/.

on trust, we have a significant positive skew, violating uni-, and most likely multivariate normal distribution assumptions, this is especially pronounced for the trust in Internet voting variable. Dichotomizing is a viable fix in such situations (Streiner, 2002, p. 265). Third, for 0 to 10 scale items, we evaluated different dichotomization cut-off points for the original 0–10 scale survey items (cutoff at <5, <6, or assigning respondents with mid-values 5 and 6 randomly into either of the binary categories) were tested, but no differences in results were observed. Variables were also recoded into four-category ordinal items in an additional specification, but this led to substantially more difficult interpretation of the interaction terms without noticeable changes in the observed empirical associations.

The correlation matrix for the dependent variables, independent predictors, and control variables is presented in Appendix B, Table B1; while the VIF values are listed in Table B2.

2.3 Methods

To test the hypotheses derived from the literature and theoretical framework, a series of binary logistic regression models was developed, including the variables listed above, for data from 2021 and 2023. The choice of logistic regression is methodologically grounded in the binary nature of the dependent variable, whether or not an individual used Internet voting. Logistic regression enables the estimation of the probability of this dichotomous outcome based on a set of binary and categorical predictors, without requiring the assumption of normally distributed errors or linear relationships in the raw data.

The primary aim of the study is to assess whether the likelihood of Internet voting is affected differently by trust and confidence, depending on an individual's level of technical knowledge. Logistic regression is particularly appropriate for testing such conditional relationships through the inclusion of interaction terms. These interactions enable the modeling of how

Table 1. Detailed information on the conceptualization and operationalization of the variables.

Variable names	Conceptualization	Operationalization in survey
Internet voting usage, binary, dependent variable	Through which mode of vote casting the respondent has cast their vote during the current elections. The same concept was used in the design exploring the turnout via the electoral technology usage (Ehin and Solvak, 2021a; Vassil and Weber, 2011).	"How did you vote in the current election?" Internet voting in the current elections (coded 1) and any other mode of voting (coded 0).
Technical knowledge level, ordinal	This variable captures the individual's general computer skills, technical knowledge, which may range from basic tasks such as writing emails to more advanced skills like programming (Cegarra-Navarro et al., 2014; Sindermann et al., 2023). The qualitative meaning of this variable extends beyond mere technical ability; it encompasses the individual's comfort and familiarity with technology. Higher levels of knowledge are indicative of greater ease in navigating digital environments, which can contribute to a more informed and confident use of Internet voting systems. In essence, this variable reflects not only the technical competence of the individual but also their broader capability to engage with digital tools effectively.	"How do you evaluate your computer skills?" The variable was recoded from ordinal 5 ("no computer skills")—1 ("very good") to: 1) Low knowledge—answers 5 and 4, no and basic technical knowledge; 2) Medium knowledge—answer 3, medium knowledge; 3) High knowledge—answer 2 and 1, good and very good knowledge.
Confidence in Internet voting, binary	This variable captures the respondent's perception of the system's reliability and accuracy. High confidence levels suggest that the individual believes the system is secure and trustworthy, which can significantly influence their willingness to use it (Fisher and Savani, 2023; Hilt et al., 2023). Conversely, low confidence levels indicate doubts or skepticism about the system's integrity, potentially deterring individuals from opting for Internet voting. The qualitative aspect of this variable lies in its reflection of the individual's trust in the technological processes and institutional assurances surrounding Internet voting. In the analysis, the variable was converted to the binary.	"How confident are you that the digital votes of all voters were correctly taken into account the way they voted?" The variable was recoded from ordinal 0 ("Not confident at all")—10 ("Very confident") to binary: 0 ("Not confident")—answers from 0 to 5, not confident in the internet voting; 1 (Confident)—answers from 6 to 10, confident in the internet voting.
Trust in government, binary	Trust in the Estonian government represents trust in the government's role in organizing election (Abdala et al., 2025; Ehin and Solvak, 2021a). Higher political trust may correlate with greater acceptance of election processes, including Internet voting. It reflects the individual's general faith in governmental structures and their effectiveness.	The respondents have to place their attitude on a scale from 0 ("Do not trust at all") to 10 ("Trust completely"). The variable was recoded from ordinal 0–10 to binary: 0 (No trust)—answers from 0 to 5, do not trust the Estonian government; 1 (Trust)—answers from 6 to 10, trust the Estonian government.
Trust in Internet voting, binary	Trust in Internet voting is crucial as it represents the individual's general belief in the system's safety, fairness, and effectiveness. Within the research, the concept of technological trust is presented by one variable of trust in the Internet voting (Abdala et al., 2025; Ehin and Solvak, 2021a). Trust, in this context, goes beyond confidence in specific technical aspects and encompasses a broader sense of reliability and dependability in the system as a whole. High trust levels suggest that the individual is more likely to perceive the system as legitimate and worthy of use, whereas low trust levels may indicate concerns about potential vulnerabilities or misuse.	The respondents have to place their attitude on a scale from 0 ("Do not trust at all") to 10 ("Trust completely"). The variable was recoded from ordinal 0–10 to binary: 0 (No trust)—answers from 0 to 5, do not trust the Estonian online voting; 1 (Trust)—answers from 6 to 10, trust the Estonian online voting.

(Continued)

Table 1. Continued.

Variable names	Conceptualization	Operationalization in survey
Internet voting performance, binary	This variable captures the individual's subjective evaluation of the effectiveness and efficiency of the Internet voting system. It reflects their personal experiences or perceptions regarding how smoothly the system operates, including factors like usability, reliability, and accessibility (Farooq et al., 2024; Marky et al., 2021). Qualitatively, this variable goes beyond mere technical assessment; it encompasses the user's overall satisfaction with the Internet voting process. A higher rating indicates a positive perception, suggesting that the individual believes the system functions well and meets their expectations. Conversely, a lower rating points to perceived deficiencies or frustrations with the system's performance.	"In your opinion, how well or badly has Internet voting worked in Estonia?" The variable was recoded from ordinal 0 (Very badly)—10 (Very well) to binary: 0 (Bad)—answers from 0 to 5, Internet voting works badly; 1 (Good)—answers from 6 to 10, Internet voting works well.
Age, continuous	Continuous measure of respondent's age in years, reflecting life-cycle differences in digital adoption and political participation (Bakon and Ward, 2015; Vassil and Weber, 2011).	Age of respondent, open-ended question, answer is provided in years.
Gender, binary	Binary categorical indicator controlling for gender-related variation in technology use and political behavior (Mendez and Serdült, 2017; Volkamer et al., 2011).	Gender of respondent. 1) Male 2) Female
Education, ordinal	Ordinal variable for social status and general knowledgebase (Mendez and Serdült, 2017; Vassil et al., 2016).	"What is your level of completed education?" 1) Elementary/basic 2) Secondary education/gymnasium 3) Vocational secondary education 4) Higher
Left–right self-position, ordinal	Ideological orientation capturing hypothetical political trust variance (Sindermann et al., 2023).	"In politics it is spoken about "left" and "right." Where would You locate Yourself on a political scale from 0 (standing for totally left) to 10 (standing for totally right)." Used as continuous.
Ethnicity, categorical	Categorical control for linguistic and socio-cultural cleavages in Estonia's electorate (Mendez and Serdült, 2017; Vassil et al., 2016). Within the study, language is equal to the ethnicity.	"What language do you usually speak at home?" 1) Estonian 2) Russian 3) Others
Internet usage intensity, continuous	The variable brings additional conceptualization of the technical knowledge of the Internet voting users and nonusers (Sindermann et al., 2023; Vassil and Weber, 2011).	"On how many days over the last week have you used the Internet, for example, surfed on the World Wide Web, sent an e-mail, or used e-banking?" Open-ended question, answer is provided in days.

the effect of one predictor, such as confidence in the Internet voting system, changes depending on another variable, such as technical knowledge. The resulting estimates can be used to calculate predictive margins and visualize differences in predicted probabilities, offering a nuanced understanding of how combinations of knowledge and attitudinal factors jointly influence voting behavior.

All analyses were conducted using STATA, and marginal effects were computed to facilitate the interpretation of interaction terms. As an additional control, all models were estimated separately for the two elections to examine whether the direction of the observed effects remained consistent across both survey waves. No discernible differences were found, apart from variations in significance values and confidence interval ranges resulting from the reduced statistical power of the smaller individual samples. A generalized linear structural equation modeling (SEM) model was also estimated (see Appendix C) to provide a comprehensive test of the assumed associations. As the SEM and regression models yielded very similar results, the regression models are reported and interpreted in the main text, as they represent a more straightforward technique to implement and explain.

Table 2. Baseline model for Internet voting (dependent variable: Internet voting usage. Logit coefficients with standard errors clustered by election in parentheses).

	Coefficient (SE)
Confidence in Internet voting	0.96***(0.17)
Perceived performance of Internet voting	1.36***(0.00)
Trust in Internet voting	0.68***(0.06)
Trust in government	0.18*(0.10)
Technical knowledge level: medium(base: low)	0.98(0.85)
Technical knowledge level: high(base: low)	1.45**(0.80)
Age	−0.00(0.00)
Gender: male	0.43***(0.03)
Ethnicity: Estonian	0.58(0.48)
Left–right self-position	−0.03(0.00)
Education level: vocational(base: basic)	0.49***(0.03)
Education level: secondary(base: basic)	−0.46***(0.13)
Education level: high(base: basic)	−0.30*(0.15)
Internet usage days per week	0.03(0.04)
Intercept	−3.69***(0.01)
Pseudo R^2	0.26
N	1,155

Note: *$p < 0.1$; **$p < .05$; ***$p < .01$. Standard errors clustered by election year.

Table 3. Predicted probabilities of using Internet voting at fixed knowledge and trust levels.

	Predicted probability (SE)
Low knowledge, at no trust	0.24*(0.13)
Low knowledge, at trust	0.37**(0.15)
Medium knowledge, at no trust	0.43***(0.00)
Medium knowledge, at trust	0.57***(0.02)
High knowledge, at no trust	0.53***(0.01)
High knowledge, at trust	0.66***(0.00)

Note: *$p < 0.1$; **$p < .05$; ***$p < .01$. Standard errors clustered by election year.

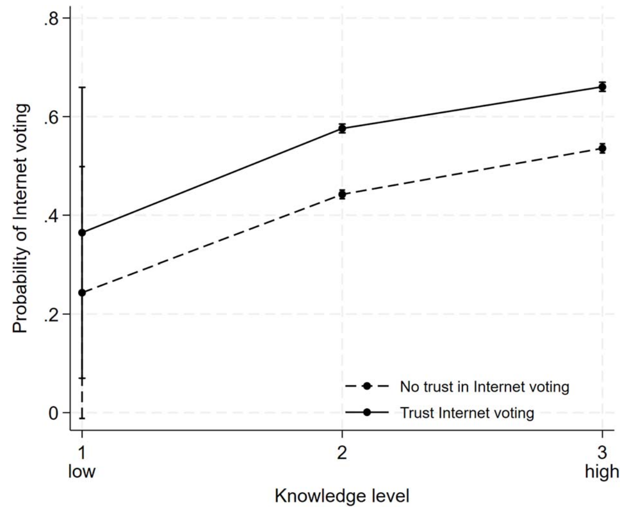


Figure 3. Visualization of predictive margins for the baseline model.

3 Results

3.1 Analysis of the baseline model without interactions

Baseline model:

$$\log\left(\frac{P\left(\text{ivote}=1\right)}{1-P\left(\text{ivote}=1\right)}\right)=\beta_0+\beta_1\text{confidence\_ivote}+\beta_2\text{ivote\_perform}+\beta_3\text{trust\_gov}+\beta_4\text{trust\_ivote}+\beta_5\text{knowledge}$$

The analysis begins by constructing and interpreting the baseline model to understand the additive effects of key predictors—knowledge, confidence, and trust—on Internet voting usage. In addition, the analysis includes age, gender, ethnicity (language spoken at home), left–right self-position, education level, and Internet usage intensity as controls in all the models, as these have been shown in the past to affect Internet voting usage (Sindermann et al., 2023). While hypotheses suggest interactions, the baseline model isolates the main effects to provide an initial overview of the relationships between variables.

The results of logistic regression, presented in Table 2, allow for preliminary estimations of the aforementioned hypotheses. Firstly, most of the key predictors are statistically significant, including confidence in Internet voting, perceived performance of the system, trust in the Internet voting technology itself, and self-assessed technical knowledge. These results support the theoretical expectations. Citizens who trust Internet voting, have confidence in the voting system's fairness, perceive the system's performance as good, and have better technical knowledge are more likely to use Internet voting for elections. These findings are particularly relevant in comparison with the baseline values of citizens who do not trust Internet voting, have low confidence in the system, perceive it as poorly functioning, and possess limited technical knowledge. The only variable that does not reach statistical significance is trust in government, used here as a proxy for political trust. This result suggests that generalized political trust in government does not directly translate into a higher likelihood of using Internet voting. A possible explanation is that voters distinguish between institutional trust in specific systems (e.g., internet voting) and broader political trust, which may be more diffuse or affected by short-term political attitudes.

Table 3 presents the marginal effects of knowledge on the probability of using Internet voting at different levels of trust in Internet voting. The marginal effects show a clear and significant influence of self-assessed technical knowledge on the likelihood of Internet voting across different levels of trust in the mode of voting, see Figure 3.

At low-knowledge levels, there actually is not a statistically significant difference in Internet voting probabilities between the no-trust and trust groups. There are, however, statistically significant differences for the two other groups. At medium knowledge levels, the trusting group has a 14-percentage point higher, and at high-knowledge levels, a 12-percentage point higher Internet voting probability compared to the no-trust group at the same knowledge level. It is also apparent that the additional knowledge makes one more likely to vote via the Internet within both the not-trusting and trusting groups, as the confidence intervals of the estimations do not overlap when knowledge increases from medium to high. There is hence evidence that knowledge matters, but the picture is nuanced and possibly conditioned by other factors, which will be tested further.

3.2 The effect of confidence on internet voting usage

The next stage of the analysis is direct hypothesis testing; analysis starts with hypothesis 1, which claims that confidence in Internet

Table 4. Logistic regression model with confidence-knowledge interaction (dependent variable: Internet voting usage; all socio-demographic controls included, effects not shown).

	Logit coefficient (SE)
Confidence in Internet voting	0.74**(0.37)
Technical knowledge level: Medium(base: low)	1.18(0.94)
Technical knowledge level: High(base: low)	0.98**(0.45)
Confidence × Knowledge level interaction	
Confident (1) × Medium knowledge (2)	−0.27(0.23)
Confident (1) × High knowledge (3)	0.60*(0.36)
Perceived performance of Internet voting	1.29***(0.06)
Trust in Internet voting	0.70***(0.01)
Trust in government	0.16**(0.06)
Age	0.00(0.00)
Gender: male	0.41***(0.03)
Ethnicity: Estonian	0.55(0.52)
Left–right self-position	−0.03(0.05)
Education level: vocational(base: basic)	0.51***(0.03)
Education level: secondary(base: basic)	−0.43**(0.13)
Education level: high(base: basic)	−0.29*(0.13)
Internet usage days per week	0.03(0.03)
Pseudo R^2	0.26
N	1,155

Note: *$p < 0.1$; **$p < .05$; ***$p < .01$. Standard errors clustered by election year.

Table 5. Predicted probabilities of using Internet voting at different confidence and knowledge levels.

	Predicted probability (SE)
Confidence in Internet voting:	
Not confident	0.42***(0.01)
Confident	0.64***(0.01)
Technical knowledge level	
Low	0.34**(0.16)
Medium	0.54***(0.01)
High	0.63***(0.00)
Confidence × Knowledge level	
Not confident (0) × Low knowledge (1)	0.22***(0.08)
Not confident (0) × Medium knowledge (2)	0.46***(0.10)
Not confident (0) × High knowledge (3)	0.41***(0.02)
Confident (1) × Low knowledge (1)	0.36**(0.18)
Confident (1) × Medium knowledge (2)	0.56***(0.03)
Confident (1) × High knowledge (3)	0.69***(0.01)

Note: *$p < 0.1$; **$p < .05$; ***$p < .01$. Standard errors clustered by election year.

voting will have the largest effect size or will be the statistically significant variable for the cohort of electorate with a high level of knowledge, as shown in Table 4. The interaction term is significant only for one term, but it reveals a very specific group difference, as confidence is binary and knowledge is a three-value ordinal variable. It makes more sense to investigate the postestimation output shown in Table 5 and Figure 4 with the help of predicted Internet voting probabilities.

In the baseline model, the output highlights the role of standalone confidence in regard to Internet voting usage. However, once the interaction with the technical knowledge is added, the picture becomes more sophisticated. The interaction between confidence and technical knowledge at high levels deserves additional attention. First of all, it is statistically significant in comparison to interaction with the medium level as well as the low level of knowledge. Secondly, it indicates that confidence in Internet voting significantly enhances the effect of high technical knowledge on the likelihood of Internet voting. Specifically, for high-knowledge individuals, having confidence in Internet voting increases the probability of voting via the Internet. This finding is aligned with the theoretical expectations listed above and proves hypothesis 1.

Regarding the effect size on the likelihood of using online voting, the emphasis will be placed on the interaction between confidence in Internet voting and a high level of knowledge. The margins are visually represented in Figure 4.

- At no confidence, those with low technical knowledge have a predicted probability of using Internet voting at 22%.
- For individuals with medium knowledge, the likelihood increases substantially to 46%.
- The probability slightly decreases to 41% for those with high knowledge.

On the other hand, for individuals who possess high confidence in Internet voting, the predicted probabilities reflect a different trend:

- Low-knowledge individuals exhibit a lower predicted probability of 35%. But confidence levels overlap with the probability at high confidence—it is clear that there is no statistical difference between those with low and high confidence in Internet voting.
- The likelihood of voting via the Internet rises to 56% among those with medium knowledge.
- The highest probability of Internet voting usage is observed in individuals with high knowledge, reaching 69%.

These findings highlight that while knowledge generally enhances the probability of voting via the Internet, the effect is more pronounced and statistically significant among those who are confident in Internet voting. A high-knowledge level, coupled with high confidence in Internet voting, significantly boosts the likelihood of using Internet voting systems. This suggests that fostering both confidence and knowledge could be key strategies in promoting the adoption of Internet voting.

3.3 The effect of trust-related variables on internet voting usage

Moving to the testing of hypothesis 2, which assumes that trust-related factors, such as trust in Internet voting, trust in political institutions, and Internet voting's performance, will be driving variables for Internet voting usage for citizens with low levels of technical knowledge.

In order to test hypothesis 2, three models were created, illustrated in Table 6, each having an interaction term with trust-related factors and knowledge, as well as the main terms. Since the analysis has evaluated the effects of the noninteracted variables in the baseline model, closer attention will be paid to the interactions in the following analysis. In order to save space and streamline the results, the analysis examines the postestimation coefficient graphically with Figures 5–7 and does not report predicted probabilities in a separate table.

Though the interaction terms in the table are not significant, the postestimation of Model 1 in Figure 5 reveals that high-knowledge users are more likely to leverage performance trust to engage with Internet voting, while medium-knowledge users exhibit a significant weakening in this relationship. Low-knowledge users display no significant interaction, indicating that belief in good performance alone is insufficient to encourage their adoption of Internet voting. In sum, Figure 5 shows that

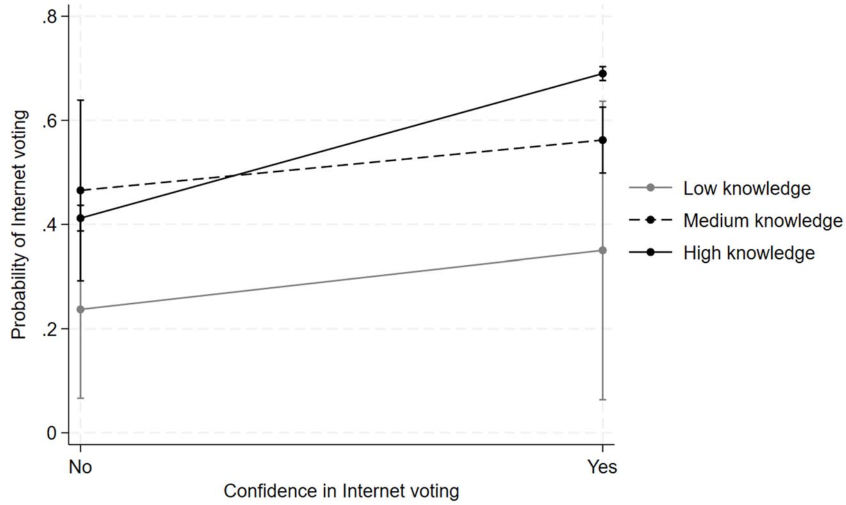


Figure 4. Visualization of predictive margins for the confidence-knowledge model.

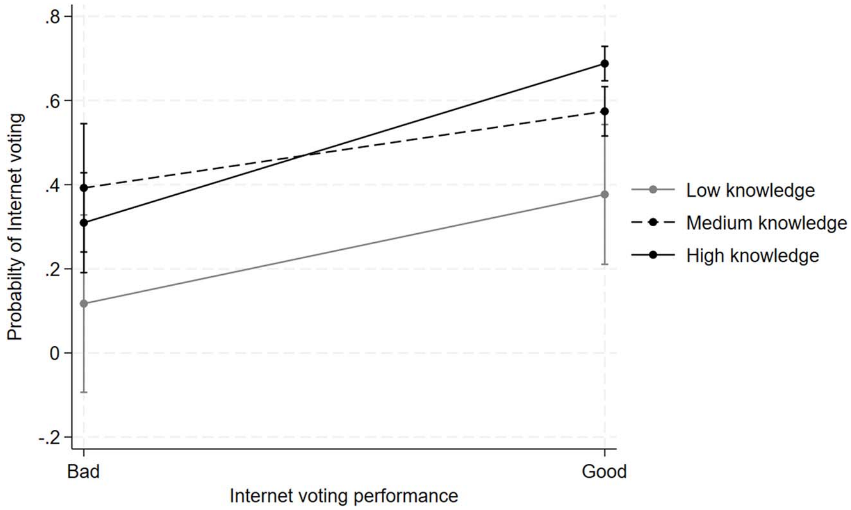


Figure 5. Visualization of predictive margins for trust in Internet voting performance and knowledge interaction.

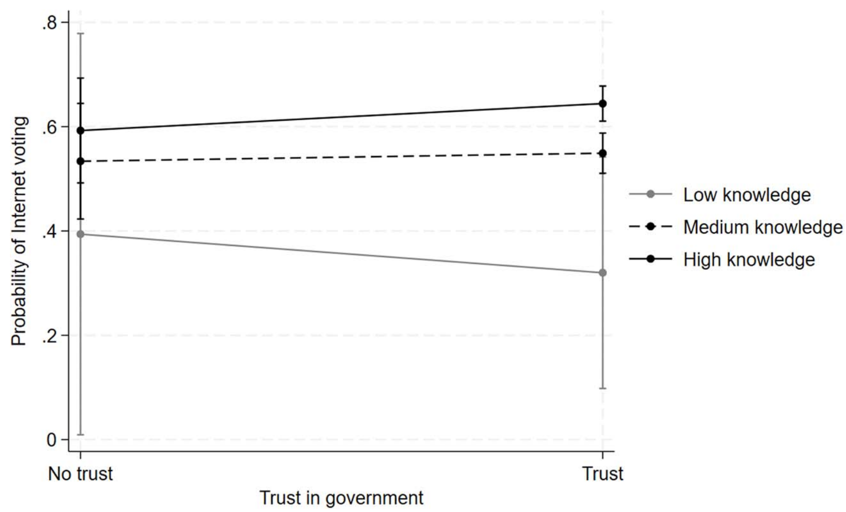


Figure 6. Visualization of predictive margins for trust in government and knowledge interaction.

belief in internet voting performance increases the usage for all knowledge groups; the effect is strongest and significant among the high-knowledge respondents.

In Model 2, one interaction term is significant. Figure 6 tells us that Internet voting probability differs between high- and medium-knowledge level, and high- and low-knowledge level

Table 6. Logistic regression models of trust-related factors (dependent variable: Internet voting usage; all socio-demographic controls included, effects not shown).

	Coefficient (SE)		
	Model 1 **Perceived performance and knowledge interaction**	**Model 2** **Trust in government and knowledge interaction**	**Model 3** **Trust in Internet voting and knowledge interaction**
Trust in performance	1.60*** (0.62)	—	—
Trust in government	—	−0.37 (0.39)	—
Trust in Internet voting	—	—	0.25 (0.83)
Confidence in Internet voting	0.95*** (0.15)	0.99*** (0.16)	0.96*** (0.16)
Technical knowledge level: Medium	1.69 (1.78)	0.70 (1.24)	0.79* (0.48)
Technical knowledge level: High	1.40 (1.24)	1.00*** (0.64)	1.00*** (0.02)
Trust in performance × Knowledge			
Good performance (1) × Medium knowledge (2)	−0.83 (1.08)	—	—
Good performance (1) × High knowledge (3)	0.04 (0.47)	—	—
Trust in government × Knowledge			
Trust in government (1) × Medium knowledge (2)	—	0.45 (0.79)	—
Trust in government (1) × High knowledge (3)	—	0.67*** (0.03)	—
Trust in Internet voting × Knowledge			
Trust in Internet voting (1) × Medium knowledge (2)	—	—	0.20 (0.39)
Trust in Internet voting (1) × High knowledge (3)	—	—	0.64 (0.83)
Age	0.00 (0.00)	0.00 (0.00)	0.00 (0.00)
Gender: male	0.42*** (0.03)	0.42*** (0.02)	0.42*** (0.03)
Ethnicity: Estonian	0.56 (0.51)	0.57 (0.50)	0.56 (0.52)
Left–right self-position	−0.04 (0.05)	−0.03 (0.05)	−0.03 (0.05)
Education level: vocational (base: basic)	0.54*** (0.08)	0.49*** (0.05)	0.51*** (0.07)
Education level: secondary (base: basic)	−0.43** (0.15)	−0.44** (0.21)	−0.44** (0.18)
Education level: high (base: basic)	−0.28* (0.14)	−0.29** (0.09)	−0.29** (0.12)
Internet usage days per week	0.03 (0.04)	0.03 (0.03)	0.03 (0.03)
Constant	−3.94*** (0.88)	−3.32*** (0.47)	−3. 36 *** (0.31)
Pseudo R^2	0.26	0.28	0.28
N	1,155	1,155	1,155

Note: *$p < 0.1$; **$p < .05$; ***$p < .01$. Standard errors clustered by election year.

when trust in government is high, but not when trust is not there. It also shows that trust in government itself is not sufficient to increase usage among any of the knowledge groups as the confidence intervals overlap between the no trust and trust ends. This suggests that while trust in government is a relevant factor, it is not sufficient to overcome the barriers posed by lower levels of technical knowledge. Thus, hypothesis 2 is not supported; trust in government either somewhat decreases or does not influence the likelihood of online voting usage among the electorate with low and medium levels of technical knowledge.

Finally, Model 3 also demonstrates that the interaction terms are not significant. The postestimation results in Figure 7 shows that similarly to the effect of trust in government, trust in Internet voting increases the likelihood of voting via the Internet for high-knowledge people more than for those with medium levels, but not for the low-knowledge group. Also, the medium- and high-

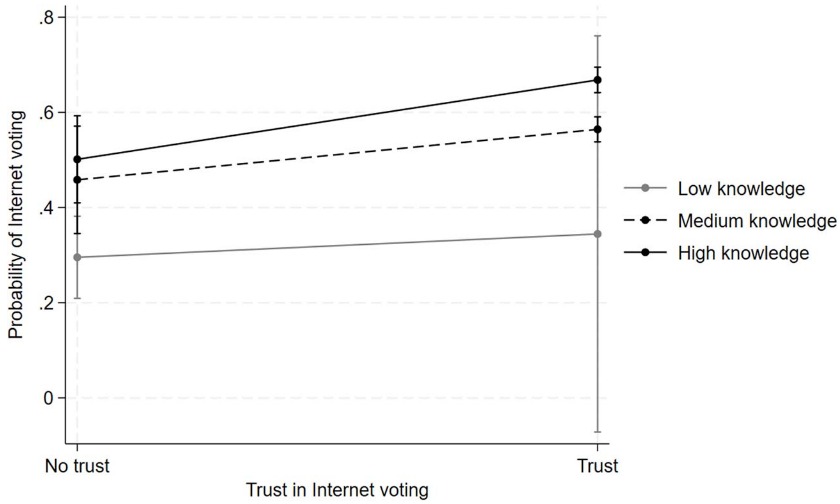


Figure 7. Visualization of predictive margins for trust in Internet voting and knowledge interaction.

knowledge groups have a significant difference in voting probability when they trust Internet voting as such.

As a summary of the hypothesis 2 analysis, the produced results do not support the initial theoretical assumption that low-level citizens delegate their trust to other entities, such as trust in Internet voting performance, trust in government, and trust in Internet voting itself. While trust in Internet voting performance and trust in Internet voting integrity increase usage among respondents with both high levels of knowledge, the effects are mostly statistically insignificant for the low-knowledge group. At the same time, trust in the Estonian government decreases the likelihood of usage among those with low-knowledge levels and does not affect usage among medium-level users.

4 Discussion

The study's findings shed light on the interconnection between the conceptual triangle of trust, knowledge, and confidence and their relationship with using Internet voting. The crucial takeaway stemming from the analysis, and a novelty not yet present in the existing literature, is that the knowledge level serves as a cornerstone to determine whether voters should rely on confidence or trust-related factors when approaching the use of Internet voting in elections.

Knowledge plays a central role in shaping how individuals engage with Internet voting systems. Trust and confidence act as intermediary variables that mediate the relationship between knowledge and the decision to use Internet voting. Trust refers to reliance on external factors like the reputation of the voting system or political institutions, while confidence is based on an individual's personal assessment of the system's security and reliability. Comparable distinctions appear in Giddens' (1990) notion of "confidence" as knowledge-based predictability and in recent empirical studies of Estonian Internet voting that differentiate between technological trust and institutional trust (Duenas and Calzati, 2023; Ehin and Solvak, 2021b; Romanov et al., 2025).

Initially, the research hypothesized that individuals with higher technical knowledge are more likely to rely on confidence, as their understanding of the system allows them to make informed judgments about its safety and functionality. In contrast, individuals with lower levels of knowledge tend to depend more on trust-related indicators, such as societal cues, previous experiences, or trust in the institutions managing the election, to overcome uncertainties about the system.

The first hypothesis, assuming that confidence would be the primary predictor of Internet voting usage at higher knowledge levels, is supported by the results. The significant interaction between confidence and knowledge illustrates that the electorate members, who are more familiar with the technologies in general, are also more likely to engage in Internet voting when they are confident in the system's integrity. This finding is aligned with the existing literature, which suggests that when people possess greater technical understanding, they are less reliant on, dependent on the external signals of trust, and more on their own assessments of the system's security and reliability, stemming from various sources, including their knowledge (Cegarra-Navarro et al., 2014; Sindermann et al., 2023). Even among individuals with high technical literacy, a lack of confidence in the system significantly reduces the likelihood of using Internet voting, which echoes evidence from usability and verification studies showing that even expert users abstain when confidence in technical integrity is shaken (Hilt et al., 2023; Marky et al., 2021). This suggests that technical proficiency alone is not sufficient; confidence in the system's security and reliability remains essential for adoption. Conversely, when individuals with high knowledge also have confidence in the system, they are much more likely to engage in Internet voting. Their technical expertise and confidence reinforce their decision to trust the system and use it for voting purposes, consistent with observations that habitual users of Estonia's digital state infrastructure internalize procedural confidence over time (Ehin et al., 2022, p. 202; Solvak and Vassil, 2018).

Turning to the trust-related indicators, the results do not provide the expected support for hypothesis 2, which predicted that trust would play a more important role among citizens with low levels of technical knowledge.

The second hypothesis, which posits that trust-related factors hold more influence on individuals with lower levels of technical knowledge, is not supported by the findings in the current design. This partly contradicts earlier assumptions that institutional trust could substitute for technical competence (Li et al., 2008) or that it could serve as the main adoption driver (Romanov et al., 2025), and aligns instead with findings that generalized political trust has limited predictive value once citizens have long-term exposure to stable e-voting institutions (Abdala et al., 2025).

The regression model with the interaction between trust in government and knowledge shows that the main effect of political trust is not statistically significant, and neither is the interaction for medium knowledge. Only the interaction term for high knowledge reaches significance. This means that trusting the government increases the likelihood of Internet voting only among respondents with high technical knowledge. Similar conditional patterns have been reported in other advanced democracies (i.e., the case of Canada), where political trust reinforces usage only among those already confident in digital systems (Reddick and Roy, 2013) or that a higher degree of understanding of the technology leads to higher trust (Zollinger et al., 2025); however, the interaction still remains underexplored.

For low- and medium-knowledge voters, trust in government does not significantly affect adoption. Margins in Figure 6 mirror this: confidence intervals overlap for the lower-knowledge groups, while a gap emerges among high-knowledge individuals. Additionally, same Figure 6 depicts that electorate with low-level of technical knowledge that trust the government is less likely to vote via the Internet, in comparison to those with low-knowledge level and who do not demonstrate political trust. Thus, generalized political trust cannot compensate for low technical knowledge; its influence is limited to those who already possess advanced knowledge.

In the model with perceived system performance, neither interaction term is statistically significant. The main effect of performance, however, is positive and highly significant in the baseline model. This indicates that perceiving the Internet voting system as working well increases the likelihood of adoption across the electorate as a whole, but there is no evidence that this effect is stronger for low-knowledge voters. Figure 5 illustrates that the positive association is most pronounced among high-knowledge respondents, while the effect for medium-knowledge voters is weaker and not significant for low-knowledge voters. The regression results therefore only suggest that performance evaluations drive adoption generally, as confirmed by long-term Estonian trend analyses (Ehin et al., 2022; Vassil et al., 2016).

Finally, trust in Internet voting, neither of the interaction terms with knowledge levels is statistically significant. The main effect of trust in Internet voting, however, is consistently positive and significant in the baseline model (Table 2) and in the interacted model. This means that trusting the Internet voting system itself increases the probability of usage across knowledge groups, but not in a way that is systematically conditioned by knowledge levels. The margins in Figure 7 suggest that the effect is more pronounced for medium- and high-knowledge voters, while among low-knowledge respondents the difference between trusting and nontrusting groups is indistinguishable within confidence intervals. Given the absence of significant interaction effects, the most reliable interpretation is that trust in the Internet voting system generally enhances the likelihood of adoption across the electorate, rather than exerting a particular influence among low-knowledge voters. These findings are in line with comparative insights that technology-specific trust (trust in the application) tends to exert uniform positive effects across populations (Ehin and Solvak, 2021b; Janssen et al., 2018; Romanov and Babayan, 2025).

Taken together, the regression models do not support hypothesis 2. None of the trust-related factors significantly increases the probability of Internet voting among low-knowledge citizens. Trust in government matters only for high-knowledge voters. Trust in performance and trust in Internet voting both exert positive and significant main effects, but without significant interactions—meaning they encourage adoption generally, not specifically among the less knowledgeable. The visual patterns in Figures 5–7 hint that these effects are stronger at medium- or high-knowledge levels, but regression evidence confirms that trust and trust-related factors do not substitute for a lack of technical understanding.

In summary, the results emphasize the dynamic relationship between trust, knowledge, and confidence in influencing the adoption of Internet voting. The analysis indicates that individuals possessing higher technical knowledge tend to depend more on confidence, arising from their capacity to evaluate the system's reliability through their own understanding. This observation corresponds with previous research suggesting that greater knowledge fosters confidence by mitigating perceived uncertainty (Cegarra-Navarro et al., 2014; Majid et al., 2020; Vassil et al., 2016). Conversely, the analysis shows no consistent evidence that individuals with lower technical knowledge rely more strongly on trust in external signals such as system performance or institutional endorsements. Instead, the positive effects of trust appear mainly among medium- and high-knowledge respondents. These results therefore underscore that while both confidence and trust matter for technology adoption, their influence is conditioned by knowledge levels in ways that differ from the original expectations.

The findings offer key contributions to the literature on digital technology adoption and trust, particularly in the realm of Internet voting. While prior studies have often treated trust and confidence interchangeably or as unidimensional predictors (Janssen et al., 2018 Li et al., 2008), this study provides a more nuanced understanding by demonstrating their interaction with knowledge.

From a policy and design perspective, although the analysis does not provide consistent evidence that low-knowledge voters rely more heavily on trust, the positive main effects of performance-related and system-related trust (in some cases, political trust among high-knowledge respondents) suggest that communication strategies should nonetheless be tailored to different levels of technical literacy. For individuals with lower technical knowledge, the results indicate that trust factors alone do not significantly increase the likelihood of Internet voting. However, this does not diminish the importance of making trust-building communication accessible and transparent, since clear assurances may still help reduce uncertainty and address skepticism among this group. This could include plain-language explanations of institutional safeguards, assurances framed in everyday terms (e.g., system and portal with results tally uptime, reports on the system updates, contingency procedures), and highly visible channels of support such as hotlines or chat-based assistance during the voting period. A useful reference is the Estonian Election webpage (*Valimised | Elections in Estonia*, n.d.), which addresses "city legends" and myths, but similar efforts should be provided in plain terms and with regular updates. In other words, while trust effects were not statistically significant for low-knowledge citizens, campaigns that emphasize the reliability of the service, reinforced by promotion from trusted institutions and community figures, remain important for fostering perceptions of legitimacy.

Since the study deals with knowledge as "levels," the state and NGO could focus on empowering low-knowledge users to become more informed voters through structured digital and civic literacy training and bringing them to next knowledge levels as a result. Such training could enable these users to move toward medium or high technical literacy, hence moving to the confidence as rationale. For examples, Estonia's commitment to building digital skills through lifelong learning programs, early tech education with the AI leap project, and teacher development initiatives demonstrates a strong foundation for such efforts (*e-Estonia*, 2024, 2025). Implementing tailored training sessions, for example, community workshops, or online modules that demystify Internet voting mechanics could resolve the digital divide issue and bridge knowledge gaps while enhancing perceptions of reliability.

Finally, for the electorate with lower technical knowledge, the practice of organizing training courses on observing online voting could be useful and beneficial (State Electoral Office Is Offering a Training Course on Observing Online Voting | Elections in Estonia, 2024). In the case of Estonia, this is a two-day workshop that simulates the real-life implementation of Internet voting with all procedures and checks, accompanied by guidance and explanations from the organizers. Observers can monitor the process from an appropriate distance and ask questions about the procedures. This format of interaction between the Election Management Body and the electorate is more engaging than one-way information published online. However, the current issue that Estonia faces with Internet voting observation training lies in the low attendance and limited outreach. Undoubtedly, the number of attendees is not the core aspect in this context, but in practice, this format is ideal for citizens who are doubtful or skeptical about the technology, since it allows them to challenge their concerns and receive answers directly from practitioners.

For more knowledgeable users, initiatives aimed at enhancing confidence are paramount. Here, confidence can be cultivated through "how it works" explanations of the cryptographic and procedural safeguards, verifiable status updates when a vote is cast (as done via the verification application in Estonia (Solvak, 2020); return codes via SMS in Norway (Duenas-Cid and Misev, 2024; Koenig et al., 2013); and verification codes sent via the mail in Switzerland (Marky et al., 2020; Maximum Security for E-Voting | Swiss Post, 2025)), and clear messaging on what verification tools do and do not guarantee. In the Estonian context, confidence could also be fostered by opening the system to greater expert scrutiny, for instance, through structured "bug hunting" programs (for reference, see the Swiss Post initiative (Swiss Post—E-Voting Bug Bounty Program—YesWeHack, n.d.)) or responsible disclosure schemes that invite security researchers and white-hat hackers to test the robustness of the Internet voting platform. Such initiatives would demonstrate that the government has nothing to hide, reinforce the transparency that is crucial for citizens with lower levels of technological knowledge, and provide technically literate voters with additional reasons to be confident in the system's integrity.

Ultimately, the findings emphasize the importance of a dual strategy: reinforcing trust cues for less knowledgeable citizens and cultivating confidence for technically literate users. Embedding these strategies into the communication and interaction design of the Estonian Internet voting system can foster broader acceptance and legitimacy. More generally, these lessons illustrate how civic technologies must adapt explanations and signals to heterogeneous publics, which is of central interest to HCI researchers and practitioners.

5 Conclusion

5.1 Findings

The study's findings offer valuable insights into the complex interplay between trust, knowledge, and confidence in the adoption of Internet voting systems. The analysis shows that individuals with higher levels of technical literacy are significantly more likely to engage in Internet voting when they also possess confidence in the system's integrity. This underscores the importance of fostering not only technical understanding but also public confidence in electoral technology for broader adoption.

By contrast, the expectation that trust would act as the primary driver of adoption among low-knowledge voters is not supported. The regression models demonstrate that neither trust in government, nor trust in system performance, nor trust in Internet voting itself consistently increases the likelihood of adoption for this group. Instead, the positive and significant effects of performance- and system-related trust appear mainly among medium- and high-knowledge respondents, while generalized political trust demonstrates an effect only among those with high technical knowledge.

Importantly, the results support the first hypothesis that confidence, more than trust, becomes the decisive factor for individuals with greater technical knowledge. This finding contributes to the literature by showing that knowledge and confidence interact to drive engagement with Internet voting systems. At the same time, the results highlight that trust, while not substituting for low technical knowledge, still plays a reinforcing role at higher knowledge levels, complementing confidence in motivating adoption.

5.2 Limitations

The methodology and the research results have three limitations, which should be mentioned, but they do not undermine the obtained results.

A key limitation of the measurement strategy is the use of single-item self-assessment variables for technical knowledge, trust, and confidence. While such measures are widely used in public opinion research, they are susceptible to individual calibration differences and potential random bias. Future studies would benefit from applying validated multi-item scales such as the Affinity for Technology Interaction for technology engagement (Attig et al., 2018) or the Human-Technology Confidence Scale for trust/confidence in digital systems (Gulati et al., 2019), which can offer greater psychometric reliability.

The operationalization of trust in government may oversimplify the complex nature of trust in political institutions. Trust in government is a multifaceted construct that encompasses various dimensions (e.g., trust in specific government branches, trust in democratic processes, trust in public services). A more nuanced measurement could have provided deeper insights into how different aspects of governmental trust impact Internet voting behavior. The current binary approach may overlook subtle variations in how trust in different political institutions (i.e., courts, parties, politicians, president) influences technology adoption.

The same nuance of limited operationalization is witnessed with the measures of confidence in Internet voting technology and its perceived performance. In this study, both concepts were captured using single survey items, which constitutes a constraint not only of this analysis but also of the underlying survey design. While Appendix B already reports the basic diagnostics, which suggest that the constructs are not perfectly collinear, the use of single-item proxies nevertheless raises concerns about potential conceptual and statistical overlap. No multi-item batteries were available in the survey, which prevented the study from conducting exploratory or confirmatory factor analyses that could more firmly establish empirical separation between trust- and confidence-related measures. Future research should rely on validated multi-item scales that are well established in the HCI literature, such as the TAM (Davis, 1989), when it comes to the technology performance, or the Trust in Automated Systems Scale (Jian et al., 2000). Such instruments would enhance reliability and allow for sharper empirical distinctions and better operationalization of concepts in question. The contribution should therefore be understood as a theoretically grounded demonstration of the distinction, supported by basic diagnostics, but open to refinement through more robust measurement strategies in subsequent studies.

The second comment is that there may be other relevant factors influencing Internet voting usage that were not included in the analysis. For example, socioeconomic status, political ideology, or prior exposure to other digital government services may also influence an individual's trust or confidence in Internet voting systems. Despite admitting the limitation, it shall be noted that the initial design was limited to the variables used in the current version of the analysis.

A final limitation concerns the choice of method. While the analysis relies on logistic regression to test the proposed relationships, alternative modeling strategies such as SEM could provide additional insights (see Appendix C). SEM would enable testing the comprehensive model in a manner that accounts for latent constructs, indirect pathways, and measurement error, providing a richer representation of the interplay between knowledge, confidence, and trust. Future studies could therefore employ SEM to validate and extend the findings, and hopefully unpack further the usage rationales that less tech-savvy citizens use.

5.3 Future research

Future research should continue to investigate how knowledge conditions the effects of trust and confidence in Internet voting, especially in contexts beyond Estonia. Since this study found no consistent evidence that trust compensates for low technical knowledge, further work is needed to examine why trust exerts its most substantial influence among medium- and high-knowledge voters, and under what conditions it might matter more for those with limited digital skills. In addition, comparative research should assess whether the balance between technological trust (in the system's fairness and performance) and political trust (in government or institutions) varies across different political regimes, electoral systems, or levels of digitalization. Expanding the scope of research to include more diverse populations and electoral contexts would provide a richer understanding of how confidence and trust interact with knowledge to shape the adoption of digital voting technologies.

Supplementary material

Supplementary Material is available at *Interacting with Computers* online.

Data availability

Both data and code underlying this article will be shared on request to the corresponding author.

Funding

The work of Mihkel Solvak and Bogdan Romanov was supported by the Estonian Research Council under grant number PRG920 and by the European Union's Horizon 2020 research and innovation program under grant agreement no. 857622 "ERA Chair in EGovernance and Digital Public Services—ECePS". The work of David Duenas-Cid has been funded by the Polish National Research Center's grant OPUS-20 - 2020/39/B/HS5/01661 and EU H2020 MSCA Program, grant agreement no. 101038055.

Conflicts of interest

None declared.

Acknowledgments

The authors express their gratitude to the ECePS project members, who have provided their feedback during the Research Team Meeting presentation.

References

Abadie, A., Athey, S., Imbens, G. W., & Wooldridge, J. M. (2023). When Should You Adjust Standard Errors for Clustering?*. *The Quarterly Journal of Economics*, **138**(1), 1–35. https://doi.org/10.1093/qje/qjac038

Abdala, M. B., Plescia, C., Boyer, M. M., & Brunetti, A. L. (2025). Trust in Government or in technology? What really drives internet voting. *Polit. Res. Q.*, **78**, 783–796. https://doi.org/10.1177/10659129251321424.

Agbesi, S., Budurushi, J., Dalela, A., Nissen, C., & Kulyk, O. (2024). How to increase transparency and trust in internet voting systems: An experimental study. In M. Obrist, J. H. Hornecker, K. Hornbæk, J. Kaye, & A. Schmidt (Eds.), *Proceedings of the 13th Nordic Conference on Human-Computer Interaction (NordiCHI '24)* (pp. 1–18). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3679318.3685362

Al-Hujran, O., Al-Debei, M. M., Chatfield, A., & Migdadi, M. (2015). The imperative of influencing citizen attitude toward e-government adoption and use. *Comput. Hum. Behav.*, **53**, 189–203. https://doi.org/10.1016/j.chb.2015.06.025.

Altman, D. G. & Royston, P. (2006). The cost of dichotomising continuous variables. *BMJ*, **332**(7549), 1080.1. https://doi.org/10.1136/bmj.332.7549.1080

Attig, C., Wessel, D., & Franke, T. (2018). *Human-Technology Interaction from a Personal Resource Perspective: The Affinity for Technology Interaction (ATI) Scale*. Conference poster. Chemnitz University of Technology & University of Lübeck, Germany.

Bakon, K. A. & Ward, T. (2015). *Web 2.0 and Elections: A Study of Factors Influencing Diaspora Voters Adoption of E-Voting System*. International Journal of Information Systems and Engineering, 3(1), 1–10. FTMS College, Kuala Lumpur, Malaysia. https://ssrn.com/abstract=3306306

Barthe, G. (2015). High-assurance cryptography: cryptographic software we can trust. *IEEE Security & Privacy*, **13**(5), 86–89. https://doi.org/10.1109/MSP.2015.112

Benk, M., Kerstan, S., von Wangenheim, F., & Ferrario, A. (2024). Twenty-four years of empirical research on trust in AI: a bibliometric review of trends, overlooked issues, and future directions. *AI & Soc.*, **40**, 2083–2106. https://doi.org/10.1007/s00146-024-02059-y.

Bodó, B. (2021). Mediated trust: a theoretical framework to address the trustworthiness of technological trust mediators. *New Media Soc.*, **23**(9), 2668–2690. https://doi.org/10.1177/1461444820939922

Buckland, M. (2017). *Information and Society*. MIT Press, Cambridge, USA.

Caloyannides, M. A. (2004). The cost of convenience: a faustian deal [computer security]. *IEEE Security & Privacy*, **2**(2), 84–87. https://doi.org/10.1109/MSECP.2004.1281255

Cegarra-Navarro, J.-G., Garcia-Perez, A., & Moreno-Cegarra, J. L. (2014). Technology knowledge and governance: empowering citizen engagement and participation. *Gov. Inf. Q.*, **31**(4), 660–668. https://doi.org/10.1016/j.giq.2014.07.001

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Q.*, **13**(3), 319. https://doi.org/10.2307/249008, 340

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: the problem of trust & challenges of governance. *Technol. Soc.*, **62**, 101284. https://doi.org/10.1016/j.techsoc.2020.101284.

DeCoster, J., Iselin, A.-M. R., & Gallucci, M. (2009). A conceptual and empirical examination of justifications for dichotomization. *Psychol. Methods*, **14**(4), 349–366. https://doi.org/10.1037/a0016956

van Dijck, J. (2013). *The Culture of Connectivity: A Critical History of Social Media*. Oxford University Press, Oxford & New York, NY, USA.

Dueñas-Cid, D. (2024). *Trust and Distrust in electoral technologies: What can we learn from the failure of electronic voting in the Netherlands (2006/07)*. 669–677. https://doi.org/10.1145/3657054.3657262

Duenas-Cid, D. & Calzati, S. (2023). Dis/trust and data-driven technologies. *Internet Policy Review*, **12**(4), 1–23. https://doi.org/10.14763/2023.4.1727

Duenas-Cid, D. & Misev, V. (2024). *Challenging the idea that internet voting verification tools create trust—They serve as distrust mitigation tools*. 109–124. https://dl.gi.de/handle/20.500.12116/45867

Duenas-Cid, D., Krivonosova, I., Serrano, R., Freire, M., & Krimmer, R. (2020). Tripped at the Finishing Line: The Åland Islands Internet Voting Project. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic Voting* (Vol. **12455**, pp. 36–49). Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-030-60347-2_3

Duenas-Cid, D., Janowski, T., & Krimmer, R. (2022). Trust and Distrust in e-Democracy. In L. Hagen, M. Solvak, & S. Hwang (Eds.), *DG.O 2022: The 23rd Annual International Conference on Digital Government Research*, 486–488. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3543434.3543637

Duenas-Cid, D., Estevez, E., & Janowski, T. (2023). Conceptualizing Digital Government for Social Solidarity. *Proceedings of the 24th Annual International Conference on Digital Government Research*, 669–670, Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3598469.3598552

e-Estonia. *Digital skills*. (2024, June 8). https://e-estonia.com/solutions/e-education-and-research/research_iinformation_system/

e-Estonia. *AI Leap 2025: Estonia sets the standard for AI in education*. (2025, March 19). https://e-estonia.com/ai-leap-2025-estonia-sets-ai-standard-in-education/

Ehin, P. & Solvak, M. (2021a). Party Cues and Trust in Remote Internet Voting: Data from Estonia 2005–2019. In Krimmer, R., Volkamer, M., Duenas-Cid, D., Kulyk, O., Rønne, P., Solvak, M., Germann, M. (eds), *Electronic Voting*, pp. 75–90. Springer International Publishing, Cham, Switzerland.

Ehin, P. & Solvak, M. (2021b). Party cues and Trust in Remote Internet Voting: data from Estonia 2005–2019. In R. Krimmer, M. Volkamer, D. Duenas-Cid, O. Kulyk, P. Rønne, M. Solvak, & M. Germann (Eds.), *Electronic Voting. E-Vote-ID 2021: Lecture Notes in Computer Science* (Vol. 12900, pp. 75–90). Springer International Publishing. https://doi.org/10.1007/978-3-030-86942-7_6.

Ehin, P., Solvak, M., Willemson, J., & Vinkel, P. (2022). Internet voting in Estonia 2005–2019: evidence from eleven elections. *Gov. Inf. Q.*, **39**(4), 101718. https://doi.org/10.1016/j.giq.2022.101718

Farooq, A., Warkentin, M., & Virtanen, S. (2024). Role of shared identity and agency trust in online voting among Finnish citizens. *Technol. Soc.*, **76**, 102429. https://doi.org/10.1016/j.techsoc.2023.102429.

Fisher, J. & Savani, M. M. (2023). Who's in charge? The impact of delivery and perception of risk on the willingness to voting online. *Br. J. Polit. Int. Rel.*, **25**(4), 676–700. https://doi.org/10.1177/13691481221120143

Giddens, A. (1990). *The Consequences of Modernity*. Stanford University Press, Stanford, CA, USA.

Giddens, A. (1991). *Modernity and Self-Identity: Self and Society in the Late Modern Age*. Stanford University Press, Stanford, CA, USA.

Glikson, E. & Woolley, A. (2020). Human trust in artificial intelligence: review of empirical research. *Acad. Manag. Ann.*in press, **14**, 627–660. https://doi.org/10.5465/annals.2018.0057.

Gulati, S., Sousa, Sonia, & and Lamas, D. (2019). Design, development and evaluation of a human-computer trust scale. *Behav. Inform. Technol.*, **38**(10), 1004–1015. https://doi.org/10.1080/0144929X.2019.1656779

Hardin, R. (2006). *Trust*. Polity Press, Cambridge, UK.

Hawlitschek, F., Notheisen, B., & Teubner, T. (2018). The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.*, **29**, 50–63. https://doi.org/10.1016/j.elerap.2018.03.005.

Hilt, T., Sein, K., Mällo, T., Willemson, J., & Volkamer, M. (2023). *Voter Perception of Cast-as-Intended Verifiability*. 10.18420/e. https://dl.gi.de/handle/20.500.12116/45433

Use of E-Voting Around the World. (2023). https://www.idea.int/news-media/multimedia-reports/use-e-voting-around-world

State Electoral Office is offering a training course on observing online voting. *Elections in Estonia*. (2024). https://www.valimised.ee/en/state-electoral-office-offering-training-course-observing-online-voting

Janssen, M., Rana, N. P., Slade, E. L., & Dwivedi, Y. K. (2018). Trustworthiness of digital government services: deriving a comprehensive theory through interpretive structural modelling. *Public Manag. Rev.*, **20**(5), 647–671. https://doi.org/10.1080/14719037.2017.1305689

Jemielniak, D., & Przegalinska, A. (2020). *Collaborative Society*. MIT Press, Cambridge, MA, USA.

Jian, J.-Y., Bisantz, A., & Drury, C. (2000). Foundations for an empirically determined scale of Trust in Automated Systems. *Int. J. Cogn. Ergon.*, **4**, 53–71. https://doi.org/10.1207/S15327566IJCE0401_04.

Kim, S., He, X., van Egmond, R., & Happee, R. (2024). Designing user interfaces for partially automated vehicles: effects of information and modality on trust and acceptance. *Transport. Res. F: Traffic Psychol. Behav.*, **103**, 404–419. https://doi.org/10.1016/j.trf.2024.02.009.

Kleizen, B., Van Dooren, W., Verhoest, K., & Tan, E. (2023). Do citizens trust trustworthy artificial intelligence? Experimental evidence on the limits of ethical AI measures in government. *Gov. Inf. Q.*, **40**(4), 101834. https://doi.org/10.1016/j.giq.2023.101834

Koenig, R. E., Locher, P., & Haenni, R. (2013). Attacking the Verification Code Mechanism in the Norwegian Internet Voting System. In Heather, J., Schneider, S., Teague, V. (eds), *E-Voting and Identify*, pp. 76–92. Springer, Berlin, Heidelberg.

Krimmer, R., Duenas-Cid, D., & Krivonosova, I. (2021). New methodology for calculating cost-efficiency of different ways of voting: is internet voting cheaper? *Public Money Manag.*, **41**(1), 17–26. https://doi.org/10.1080/09540962.2020.1732027

Krivonosova, I. (2022). The forgotten election administrator of internet voting: lessons from Estonia. *Policy Studies*, **43**(6), 1254–1276. https://doi.org/10.1080/01442872.2021.1958179

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *J. Strateg. Inf. Syst.*, **17**(1), 39–71. https://doi.org/10.1016/j.jsis.2008.01.001

Licht, N., Duenas-Cid, D., Krivonosova, I., & Krimmer, R. (2021). To i-vote or Not to i-vote: Drivers and Barriers to the Implementation of Internet Voting. In Krimmer, R., Volkamer, M., Duenas-Cid, D., Kulyk, O., Rønne, P., Solvak, M., Germann, M. (eds), *Electronic Voting*, pp. 91–105. Springer International Publishing, Cham, Switzerland.

Luhmann, N. (1979). *Trust and Power: Two Works*. Wiley, Chichester, UK.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In *Trust: Making and Breaking of Cooperative Relations*. Basil Blackwell, Oxford. https://luhmann.ir/wp-content/uploads/2021/07/Familiarity-Confidence-Trust-Problems-and-Alternatives.pdf

MacCallum, R. C., Zhang, S., Preacher, K. J., & Rucker, D. D. (2002). On the practice of dichotomization of quantitative variables. *Psychol. Methods*, **7**(1), 19–40. https://doi.org/10.1037/1082-989X.7.1.19

Majid, U., Wasim, A., Bakshi, S., & Truong, J. (2020). Knowledge, (mis-)conceptions, risk perception, and behavior change during pandemics: a scoping review of 149 studies. *Public Underst. Sci.*, **29**(8), 777–799. https://doi.org/10.1177/0963662520963365

Marky, K., Zimmermann, V., Funk, M., Daubert, J., Bleck, K., & Mühlhäuser, M. (2020). Improving the Usability and UX of the Swiss Internet Voting Interface. In J. McGrenere & A. Cockburn (Eds.), *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3313831.3376769

Marky, K., Zollinger, M.-L., Roenne, P., Ryan, P. Y. A., Grube, T., & Kunze, K. (2021). Investigating usability and user experience of individually verifiable internet voting schemes. *ACM Trans. Comput.-Hum. Interact.*, **28**(5), 30:1–30:36. https://doi.org/10.1145/3459604

Marsh, S. & Dibben, M. R. (2005). The role of trust in information science and technology. *Annu. Rev. Inf. Sci. Technol.*, **37**(1), 465–498. https://doi.org/10.1002/aris.1440370111

Mayer, R. C., Davis, J. H., & Schoorman, D. (1995). *An Integrative Model of Organizational Trust*, **20**, 709–734. Academy of Management, Briarcliff Manor, NY, USA. https://doi.org/10.2307/258792.

Mendez, F. & Serdült, U. (2017). What drives fidelity to internet voting? Evidence from the roll–out of internet voting in Switzerland. *Gov. Inf. Q.*, **34**(3), 511–523. https://doi.org/10.1016/j.giq.2017.05.005

Meyer, S., Ward, P., Coveney, J., & Rogers, W. (2008). Trust in the health system: an analysis and extension of the social theories of Giddens and Luhmann. *Health Sociol. Rev.*, **17**(2), 177–186. https://doi.org/10.5172/hesr.451.17.2.177

Mirabdolah, A., Alaeifard, M., & Marandi, A. (2023). User-centered design in HCl: enhancing usability and interaction in complex systems. *International Journal of Advanced Hum. Comput. Interact.*, **1**(1), Article 1.

Montjoy, R. S. (2008). The public Administration of Elections. *Public Adm. Rev.*, **68**(5), 788–799. https://doi.org/10.1111/j.1540-6210.2008.00919.x

Octasia, D. Y. (2018). The effect of convenience and security on users' trust and Satisfactionof E-commerce in Indonesia (study on customers of TOKOPEDIA in Jabodetabek region). *Journal of Information Engineering and Applications*, **8**(4), 1.

Reddick, C. G. & Roy, J. (2013). Business perceptions and satisfaction with e-government: findings from a Canadian survey. *Gov. Inf. Q.*, **30**(1), 1–9. https://doi.org/10.1016/j.giq.2012.06.009

Romanov, B. & Babayan, V. (2025). Trust in online voting under different regime settings: evidence from public opinion on online voting in national elections in Estonia and Russia. *Journal of Information Technology & Politics*, 1–18. https://doi.org/10.1080/19331681.2025.2486050.

Romanov, B., Cid, D. D., & Leets, P. (2025). *State versus technology:* what drives trust in and usage of internet voting, institutional or technological trust? *Gov. Inf. Q.*, **42**(4), 102068. https://doi.org/10.1016/j.giq.2025.102068

Ruijer, E., Porumbescu, G., Porter, R., & Piotrowski, S. (2023). Social equity in the data era: a systematic literature review of data-driven public service research. *Public Adm. Rev.*, **83**(2), 316–332. https://doi.org/10.1111/puar.13585

Savioja, P., Liinasuo, M., & Koskinen, H. (2014). User experience: does it matter in complex systems? *Cogn. Tech. Work*, **16**(4), 429–449. https://doi.org/10.1007/s10111-013-0271-x

Sharma, S. (2020). Can't change my political disaffection! The role of political disaffection, trust, and resistance to change in internet voting. *Digital Policy, Regulation and Governance*, **22**(2), 71–91. https://doi.org/10.1108/DPRG-07-2019-0049

Simmel, G. (1950). *The Sociology of Georg Simmel*. Simon and Schuster, New York, NY, USA.

Sindermann, C., Rozgonjuk, D., Solvak, M., Realo, A., & Vassil, K. (2023). Internet voting: the role of personality traits and trust across three parliamentary elections in Estonia. *Curr. Psychol.*, **42**(30), 26555–26569. https://doi.org/10.1007/s12144-022-03644-4

Solvak, M. (2020). Does Vote Verification Work: Usage and Impact of Confidence Building Technology in Internet Voting. In R. Krimmer, M. Volkamer, B. Beckert, R. Küsters, O. Kulyk, D. Duenas-Cid, & M. Solvak (Eds.), *Electronic Voting* (pp. 213–228). Springer International Publishing, Cham, Switzerland. https://doi.org/10.1007/978-3-030-60347-2_14

Solvak, M. & Vassil, K. (2018). Could internet voting halt declining electoral turnout? New evidence that E-voting is habit forming: internet voting and habit formation. *Policy Internet*, **10**(1), 4–21. https://doi.org/10.1002/poi3.160

Streiner, D. L. (2002). Breaking up is hard to do: the heartbreak of dichotomizing continuous data. *Can. J. Psychiatr.*, **47**(3), 262–266. https://doi.org/10.1177/070674370204700307

Swiss Post. *Maximum security for e-voting.* (2025). https://digital-solutions.post.ch/en/e-governmenthttps/digital-solutions.post.ch/en/e-government/digitization-solutions/e-voting/security-given-top-priority

Swiss Post—E-Voting bug bounty program—YesWeHack. (2022—2025). YesWeHack #1 Bug Bounty Platform in Europe. Retrieved August 22, 2025, from https://yeswehack.com/programs/swiss-post-evoting

Valimised | Elections in Estonia. (2025). Retrieved March 4, 2025, from https://www.valimised.ee/

Vassil, K. & Weber, T. (2011). A bottleneck model of e-voting: why technology fails to boost turnout. *New Media and Society*, **13**(8), 1336–1354, https://doi.org/10.1177/1461444811405807

Vassil, K., Solvak, M., Vinkel, P., Trechsel, A. H., & Alvarez, R. M. (2016). The diffusion of internet voting. Usage patterns of internet voting in Estonia between 2005 and 2015. *Gov. Inf. Q.*, **33**(3), 453–459. https://doi.org/10.1016/j.giq.2016.06.007

Volkamer, M., Spycher, O., & Dubuis, E. (2011). Measures to establish trust in internet voting. In J. Ramon Gil-Garcia, M. A. Pardo, & T. A. Nam (Eds.), *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, 1–10. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/2072069.2072071

Wang, G., Chen, Q., Xu, Z., & Leng, X. (2020). Can the use of government apps shape citizen compliance? The mediating role of different perceptions of government. *Comput. Hum. Behav.*, **108**, 106335. https://doi.org/10.1016/j.chb.2020.106335.

Willemson, J. (2018). Bits or paper: which should get to carry your vote? *Journal of Information Security and Applications*, **38**, 124–131. https://doi.org/10.1016/j.jisa.2017.11.007.

Wolf, P., Nackerdien, R., Tuccinardi, D. and with International Institute for Democracy and Electoral Assistance (2011). *Introducing electronic voting: Essential considerations*. International Institute for Democracy and Electoral Assistance, Stockholm, Sweden.

Zinn, J. O. (2008). Heading into the unknown: everyday strategies for managing risk and uncertainty. *Health Risk Soc.*, **10**(5), 439–450. https://doi.org/10.1080/13698570802380891

Zinn, J. O. (2016). 'In-between' and other reasonable ways to deal with risk and uncertainty: a review article. *Health Risk Soc.*, **18**(7–8), 348–366. https://doi.org/10.1080/13698575.2016.1269879

Zollinger, M.-L., Rønne, P. B., Schneider, S., Ryan, P. Y. A., & Jamroga, W. (2025). Intelligo Ut Confido: Understanding, Trust and User Experience in Verifiable Receipt-Free E-Voting. In Duenas-Cid, D., Roenne, P., Volkamer, M., Budurushi, J., Blom, M., Rodríguez-Pérez, A., Spycher-Krivonosova, I., Castellà Roca, J., Barrat Esteve, J. (eds), *Electronic Voting*, pp. 158–174. Springer Nature Switzerland, Cham, Switzerland.

van Zoonen, W., Luoma-aho, V., & Lievonen, M. (2024). Trust but verify? Examining the role of trust in institutions in the spread of unverified information on social media. *Comput. Hum. Behav.*, **150**, 107992. https://doi.org/10.1016/j.chb.2023.107992.

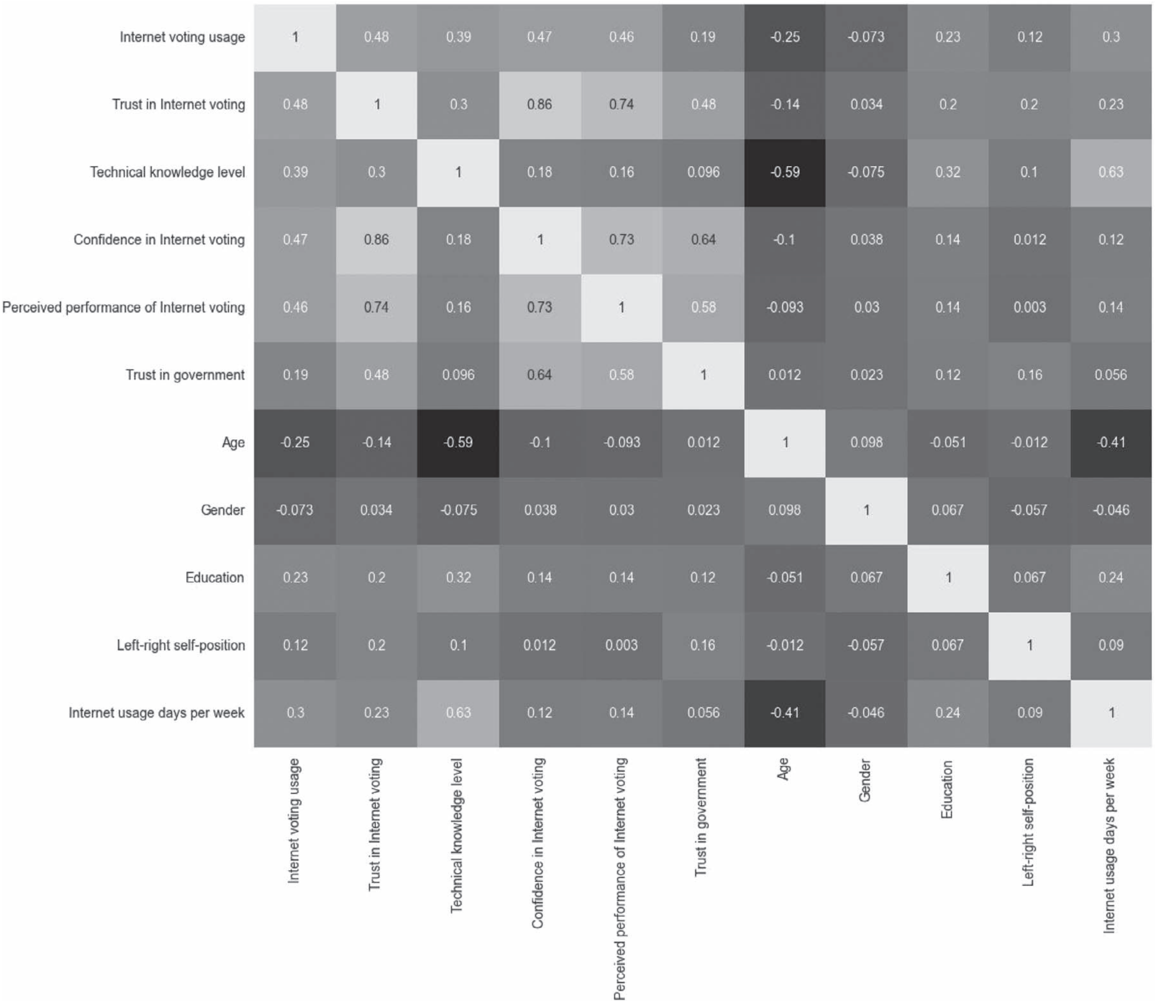
Appendix A.

All surveys are post-election surveys, with fieldwork conducted over 30 days after the election date. The surveys use stratified random samples and are representative of eligible voters in terms of age, gender, citizenship and language, settlement type, and region. The sampling frame was the Estonian Population Registry, which holds demographic data for the whole population, as well as their phone and email addresses. The sampling and surveying were conducted by professional survey companies. Table A1 lists the interview methods and the number of respondents for all the surveys used in this study.

Table A1. Description of post-election surveys used in the study

Post-election survey	Sampling method	Interview method	# of respondents
2021 local	stratified random sample	CATI(30%)/CAWI(70%)	1,153
2023 parliamentary	stratified random sample	CATI(20%)/CAWI(80%)	1,001
Note:	CATI—computer-assisted telephone interview, CAWI—computer-assisted web interview.		

Appendix B.



	Internet voting usage	Trust in Internet voting	Technical knowledge level	Confidence in Internet voting	Perceived performance of Internet voting	Trust in government	Age	Gender	Education	Left-right self-position	Internet usage days per week
Internet voting usage	1	0.48	0.39	0.47	0.46	0.19	-0.25	-0.073	0.23	0.12	0.3
Trust in Internet voting	0.48	1	0.3	0.86	0.74	0.48	-0.14	0.034	0.2	0.2	0.23
Technical knowledge level	0.39	0.3	1	0.18	0.16	0.096	-0.59	-0.075	0.32	0.1	0.63
Confidence in Internet voting	0.47	0.86	0.18	1	0.73	0.64	-0.1	0.038	0.14	0.012	0.12
Perceived performance of Internet voting	0.46	0.74	0.16	0.73	1	0.58	-0.093	0.03	0.14	0.003	0.14
Trust in government	0.19	0.48	0.096	0.64	0.58	1	0.012	0.023	0.12	0.16	0.056
Age	-0.25	-0.14	-0.59	-0.1	-0.093	0.012	1	0.098	-0.051	-0.012	-0.41
Gender	-0.073	0.034	-0.075	0.038	0.03	0.023	0.098	1	0.067	-0.057	-0.046
Education	0.23	0.2	0.32	0.14	0.14	0.12	-0.051	0.067	1	0.067	0.24
Left-right self-position	0.12	0.2	0.1	0.012	0.003	0.16	-0.012	-0.057	0.067	1	0.09
Internet usage days per week	0.3	0.23	0.63	0.12	0.14	0.056	-0.41	-0.046	0.24	0.09	1

Table B1. Correlation matrix

Table B2. VIF values

Feature	VIF
Intercept	79.700749
Trust in Internet voting	5.817638
Technical knowledge level	1.774294
Confidence in Internet voting	4.360131
Perceived performance of Internet voting	2.556583
Trust in government	2.353285
Age	1.537059
Gender	1.040298
Education	1.224891
Left–right self-position	1.071307
Internet usage days per week	1.272194

In order to run the VIF test, all variables were converted to continuous, while the analysis utilizes binary and ordinary versions. Ethnicity was not converted to a continuous variable since the transformation does not make sense.

Appendix C

The SEM model is specified as shown in the theoretical model. First, paths where knowledge level has an effect on Internet voting usage with confidence, performance, and trust in Internet voting (with controls), as well as trust in government. Second, paths where knowledge level affects confidence, performance, and trust in Internet voting, as well as trust in government itself. The model shows a strong effect of knowledge level on voting usage as well as a significant effect for confidence, perceived performance, and trust in Internet voting, with performance playing the strongest role. The direct effect of knowledge itself is significant for confidence, performance perception, and trust in Internet voting. By far the strongest effect exists for confidence, while the effects are smaller and comparable for performance and trust.

Table C1. Path model of Internet voting usage. Generalized SEM coefficients

	Coefficient (SE)
Internet voting ←	
Technical knowledge level: medium*(base: low)*	1.01**(0.39)
Technical knowledge level: high*(base: low)*	1.45***(0.41)
Confidence in Internet voting	0.92***(0.29)
Perceived performance of Internet voting	1.46***(0.27)
Trust in Internet voting	0.64**(0.30)
Trust in government	0.13(0.17)
Age	−0.00(0.00)
Gender: male	0.38***(0.14)
Ethnicity: Estonian	0.52***(0.19)
Left–right self-position	0.00(0.00)
Education level: vocational*(base: basic)*	0.43(0.49)
Education level: secondary*(base: basic)*	−0.37***(0.31)
Education level: high*(base: basic)*	−0.24(0.32)
Internet usage days per week	0.02(0.06)
Constant	−3.82***(0.59)
Confidence in Internet voting ←	
Technical knowledge level: medium*(base: low)*	0.65***(0.18)
Technical knowledge level: high*(base: low)*	1.07***(0.17)
Constant	−0.16(0.16)
Perceived performance of Internet voting ←	
Technical knowledge level: medium*(base: low)*	0.39*(0.21)
Technical knowledge level: high*(base: low)*	0.63***(0.20)
Constant	0.87***(0.18)
Trust in Internet voting ←	
Technical knowledge level: medium*(base: low)*	0.39**(0.17)
Technical knowledge level: high*(base: low)*	0.81***(0.16)
Constant	−0.04(0.15)
Trust in government ←	
Technical knowledge level: medium*(base: low)*	0.19(0.16)
Technical knowledge level: high*(base: low)*	0.66***(0.15)
Constant	0.14(0.14)
Akaike's information criterion	10890.66
Bayesian information criterion	11043.52
N	1,212

Interacting with Computers, 2025, 1–21
https://doi.org/10.1093/iwc/iwaf055
Article