Review Article

Securing Web-Based Surveys: A Three-Stage Strategy for Detecting and Preventing Fraudulent Human and Automated Responses

Irfan Hyder[1,3]; Nashit Chowdhury[1,2]; Mohammad Mojammel Hussain Raihan[1,2]; Tanvir Chowdhury Turin[1,2,4]

[1]Department of Community Health Sciences, Cumming School of Medicine, University of Calgary, 3330 Hospital Drive NW, Calgary, AB, T2N 4N1. Canada; [2]Department of Family Medicine, Department of Community Health Sciences, Cumming School of Medicine, University of Calgary, 3330 Hospital Drive NW, Calgary, AB, T2N 4N1. Canada; [3]Transdisciplinary Research Program, Faculty of Graduate Studies, University of Calgary, 2500 University Drive NW, Calgary Alberta T2N 1N4, Canada; [4]Department of Epidemiology & Research, National Heart Foundation Hospital & Research Institute, Dhaka, Bangladesh.

Abstract

Web-based surveys are efficient and cost-effective methods to collect data from diverse, large, and geographically dispersed populations. They overcome the physical and logistical barriers of in-person or paper-based data collection, enabling broad, rapid, and inclusive participation across geographic and demographic boundaries. However, the increasing automation of online environments exposes these surveys to threats from bots, duplicate entries, and fraudulent responses that can compromise data integrity and study validity. This method-focused paper presents a comprehensive strategy for minimizing these risks through three interrelated stages: Design and Testing, Data Collection, and Data Cleaning and Validation. The structure integrates technical solutions and strategic research design principles to prevent, detect, and remediate survey fraud while safeguarding participant privacy and accessibility. Key preventive measures include eligibility screening, geofencing, device fingerprinting, CAPTCHA implementation, and honeypot traps during instrument design and testing. Real-time monitoring employs personalized survey links, traffic pattern analysis, and consistency checks to identify anomalous behavior during the data collection stage. In the last stage after data collection, rigorous data cleaning involves automated rule-based filters, manual adjudication of suspicious responses, and reliance on composite fraud scoring models to ensure the inclusion of high-quality, bot-free data for analysis. By synthesizing current best practices and emerging challenges, this work provides a practical guide for researchers designing and conducting secure web-based surveys in increasingly complex and adversarial digital environments.

(JNHFB 2025; 14 : 81-86) DOI : 10.61819/jnhfb.v14i3.18

Survey research

Surveys are powerful tools for measuring population characteristics, behaviours, and attitudes, providing valuable insights that inform research, policy, and decision-making across diverse fields[1]. Traditional survey methods such as face-to-face, mail, and telephone surveys continue to be widely used, yet each presents inherent challenges related to cost, logistics, screening difficulties, and response rates that affect their effectiveness and feasibility. These challenges vary by methods, ranging from staffing and geographic limitations in in-person surveys to caller ID screening and rising operational costs in telephone surveys [2]. This evolving landscape necessitates consideration of web-based surveys, which offer various advantages, but also face a distinct set of data quality and security risks.

Corresponding Author
Dr. Tanvir C. Turin
Department of Family Medicine, Cumming School of Medicine, University of Calgary
G012F, Health Sciences Centre, 3330 Hospital Drive NW
Calgary, Alberta, Canada, T2N 4N1
Email: turin.chowdhury@ucalgary.ca

In the current digital era, the reach and convenience of the Internet have transformed survey methodology. Web-based surveys have become a dominant format across a wide range of age demographics [3]. The rise is mainly due to their cost-effectiveness, ability to reach a large audience, and the removal of physical barriers and scheduling constraints, allowing participants to respond at their convenience. In many social research studies involving sensitive questions, respondents are more likely to give accurate responses to an online survey compared to a face-to-face or computer assisted telephone survey [4]. This format helps eliminate survey administrator bias and removes the need for separate data entry, since respondents enter their answers directly into the electronic system [5]. Despite these advantages, online survey administration introduces unique risks to data quality. These risks come primarily from survey fraud, including automated and scripted responses that threaten data validity[6].

Although bot activity is typically considered to be the biggest threat in web-based survey [7], academic reports

rarely detail the survey administration protocol and data cleaning techniques to detect and remove bot and fraudulent responses [7]. This paper addresses this gap by focusing on bot infiltration and presenting a platform-agnostic approach for prevention, real-time detection, and post-field remediation within the broader web-survey workflow. It is increasingly documented in recent literature that addressing these threats is essential, because unchecked fraud can distort samples, bias estimates, and ultimately compromise inference [8].

Web-Based Survey Methods

A survey, in its most fundamental form, involves collecting information from a sample of individuals through their responses to questions [9]. Web-based surveys are often self-administered questionnaires, mostly delivered and completed via the internet. It allows researchers to efficiently collect data from diverse and geographically dispersed populations.

In the late 1990s and early 2000s, leading survey methodologists warned that internet coverage was too limited for the general-population to conduct web surveys [10]. Since then, individuals' access to internet has expanded substantially. In most urban settings today, household internet availability is near-universal, making web-first or web-only designs feasible for many studies, with remaining gaps concentrated among older adults, lower-income households, and rural/remote areas. According to the World Bank's 2024 data[11], over 80% of the population in most high-income nations has regular internet access, making web-based survey designs viable. In methodological terms, web-surveys preserve the classical structure of survey research (design, sampling, recruitment, data collection, and analysis) while introducing digital dependencies that require additional safeguards.

Currently most web-based surveys use prominent platforms such as Qualtrics, SurveyMonkey, Google Forms, REDCap, and others. They offer user-friendly interfaces, customizable question formats, and integrated data analysis tools, addressing a wide range of research needs from basic feedback collection to complex experimental designs. These platforms also enable automated data capture, adaptive branching, and multimedia integration, enhancing convenience and data integrity.

Current Threat Landscape in Web-based Surveys

The modern web-survey environment faces a growing spectrum of threats driven by increasing automation, data exploitation, and participant incentives. Within web-based survey research, these threats can be conceptualized through the Total Survey Error framework, which addresses representation and measurement errors specific to this context 12. Within web-based surveys, 'errors of representation' arise from ineligible or automated respondents such as bots or duplicates, while 'errors of measurement' primarily stem from inattentive or low-effort human responses.

Many web-based surveys are anonymous; therefore, eligibility is easier to spoof, identities can be recycled, and responses can be generated by scripts or language models that look superficially "reasonable." Fraudulent entries are a frequent phenomenon here, which can severely compromise the validity of study estimates. This warrants employment of rigorous safeguards aimed at virtually eliminating such responses. At the same time, these safeguards must be calibrated so they do not erode privacy, reduce accessibility, or undermine participant trust.

Bots and Fraud in Web-Based Surveys: Motives and Mechanisms

Recent studies show that, the web-based surveys can meet or even significantly exceed response rate than the mail questionnaire [13]. However, the trade-off here is exposure that often invites automated bots. These malicious software applications can complete surveys automatically and at scale [14], often motivated by financial gain or manipulation of study outcomes, that can quietly distort estimates or overwhelm recruitment budgets [8].

Bots are created to mimic human interactions in online environments, including surveys. Their motives vary but commonly include financial gain, such as exploiting incentives or rewards for completing surveys, and fraudulent manipulation to distort data or disrupt research validity. Some bots are deployed by profit-driven individuals to inflate participation numbers or harvest data, while others serve political or commercial interests, aiming to influence rankings, public opinion, or policy perception. In severe cases, bot activity is used strategically to undermine data reliability, manipulate consumer insights, or sabotage competitors.

Strategies for Risk Mitigation

This section outlines a practical approaches or safeguarding data quality in web-based surveys. In order to measure and control the quality of the survey, we first need to understand the survey process [1]. In existing literature, survey implementation or execution processes is categorized in diverse ways. Some scholars define the stages as pre-fielding, fielding, and post-fielding stages [15], while others describe them as design, instrument development, and execution [16]. For the purpose of this study, these processes are synthesized into three stages: (1) Design and Testing, (2) Data Collection, and (3) Data Cleaning and Validation. This three-stage conceptualization helps researchers to strategically plan which preventive measures to implement, determine the optimal timing for each, and understand how to effectively apply these controls to combat automated or bot responses throughout the entire survey process.

In the Design and Testing stage, foundational controls focus on eligibility criteria, recruitment strategies, and instrument development to prevent opportunities for fraudulent responses. This stage includes piloting and refining the questionnaire to ensure it deters automation and promotes valid participation while maintaining respondent privacy and accessibility.

During the Data Collection stage, real-time monitoring mechanisms are implemented. These include throttling traffic spikes and using platform-specific links to pinpoint problematic channels. Personalized authentication to enforce participation limitation, while geo–time-zone checks block out-of-scope entries. The continuous oversight facilitates early identification of irregularities, allowing prompt intervention such as restricting access or modifying recruitment channels to uphold data integrity.

The Data Cleaning and Validation stage encompasses post-field rule-based filtering to remove duplicates, illogical or implausible responses, and other low-quality data. Manual reviewer adjudication is needed for contextual insights with flagged entries. Documenting each decision and balancing exclusion thresholds to protect participant inclusion and confidentiality is also a big part of this stage.

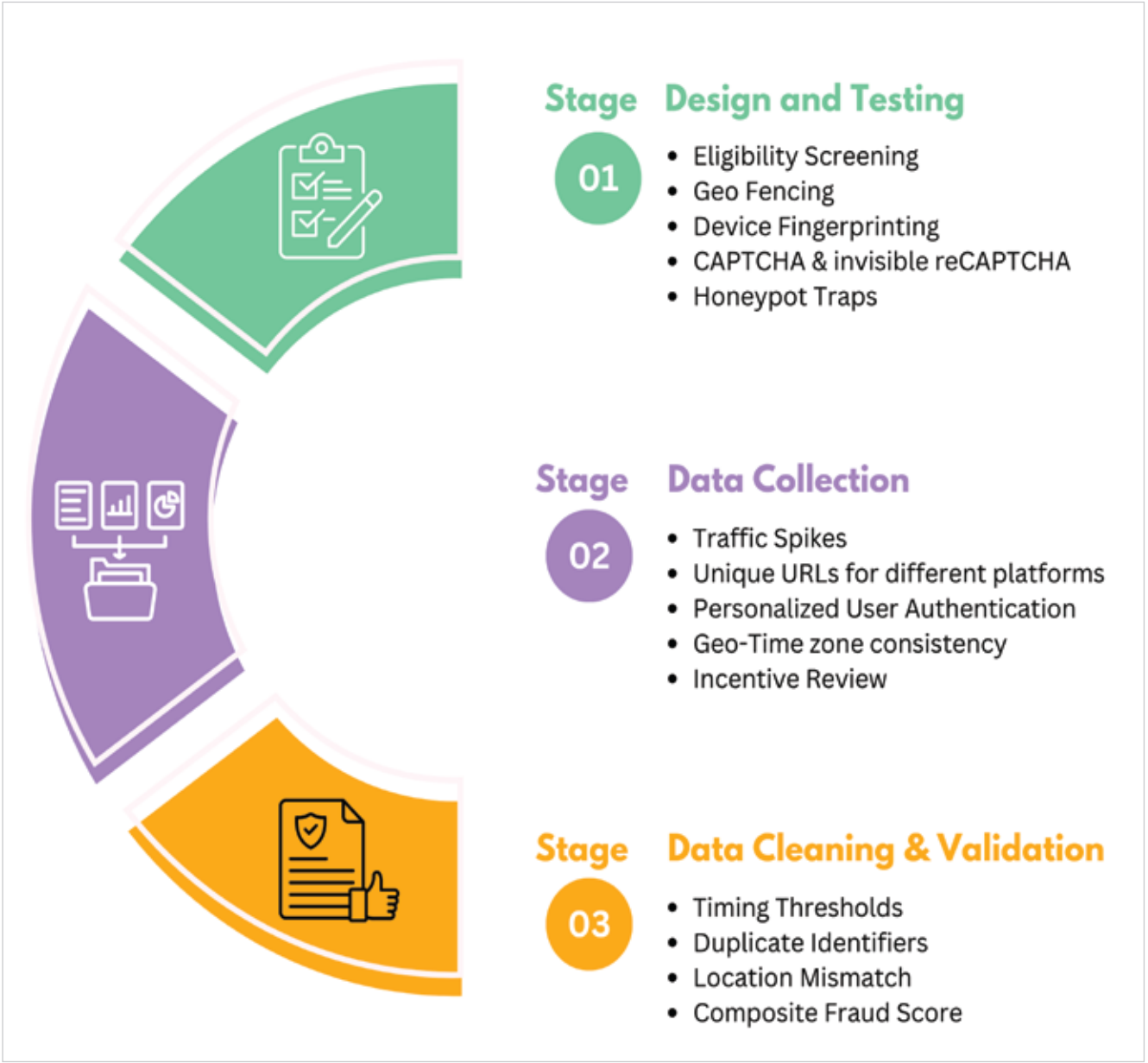

Figure 1: Risk mitigation strategies across the three stages of web-based survey execution

Stage 1: Design and Testing

Eligibility Screening: Effective prevention starts before the survey launch. The survey life cycle begins with designing the survey instrument, where eligibility rules are established, and sampling strategies are defined. At this stage, researchers must anticipate the possibility of unwanted traffic from bots and fraudulent actors and define eligibility criteria that are both verifiable and resistant to manipulation. This strategy is moderately effective in bot detection and prevention [14].

In web-based surveys, researchers also should reveal as little as possible about study purpose before eligibility is established. This can be done by hiding titles and defer introductions until after screeners, so that large language model (LLM) driven bots can't mine context to choose the "right" answers.

Geo-Fencing: Geofencing establishes a virtual boundary around specific geographic areas [17], allowing researchers to ensure that survey responses originate only from eligible locations while automatically blocking out-of-region IPs. This targeted approach enhances data accuracy and prevents unauthorized participation. Nonetheless, sophisticated bots can circumvent geofencing by leveraging technologies such as Virtual Private Networks (VPNs), which allow them to appear as if they are located within the specified boundary despite being elsewhere.

IP or Device based Fingerprinting: Fingerprinting allows anonymous detection of repeated attempts from the same device. This function places a cookie on the respondent's browser after they submit a response that blocks them from submitting a subsequent response [18]. However, Virtual Private Servers (VPS) pose a significant challenge VPS technology can bypass IP and device-based fingerprinting methods because it allows bots to operate behind independently unique IP addresses and manipulate device signatures to evade detection [19]. Additionally, sophisticated bots can modify device fingerprints, and submit multiple survey responses [20]. Researchers need to be aware that restricting survey access by IP address also comes with a cost, as it may also exclude legitimate participants who share the same IP, such as family members or students living in shared housing [21].

CAPTCHA and reCAPTCHA: CAPTCHA has long been used to keep bots from misusing web services [22]. It is an automatic security test to determine whether a user is a real human or a computer program [22], which is said to be easy for humans but difficult for computers [23]. Embedding an invisible reCAPTCHA at the start of the survey adds a human-interaction step that remains a relatively high barrier for automated bots [22]. These systems evaluate cursor movement, scrolling, page dwell time, and input hesitation, which tend to differ between humans and bots. If the system detects suspicious, non-human-like behavior, it may require the respondent to complete an additional test, such as selecting images matching a prompt. This process helps prevent the entry of invalid or fraudulent actors into the survey. While CAPTCHAs serve as an important initial defense against automated bots, they are not foolproof, as many CAPTCHA implementations lack sufficient security to block more sophisticated attacks [14].

Honeypot Traps: Another technique can be used during instrument design is to include hidden questions also known as honeypot fields. This is a form of a trap embedded in a survey, programmed to engage and deceive bot respondents [14]. This can be accomplished by adding the @HIDDEN action tag to an item in REDCap or by adding custom JavaScript code to an item in Qualtrics [19]. These are hidden questions visible only to automated bots help distinguish machine entries from human participants. However, advanced bots may still detect hidden questions and intentionally avoid responding to them to pose as human [14]. Nevertheless, researchers should implement honeypot questions in web-based surveys as they do not require extra effort, but can trap some bots in the process without burdening participants.

Stage 2 - Data Collection

Traffic Spikes: Even with meticulous survey design, real-time monitoring during data collection remains essential. Fraudulent submissions often occur in bursts characterized by atypical completion times, spikes in traffic, or uniform response patterns. Continuous tracking of submission velocity, IP activity, and completion metadata enables early identification of such anomalies.

Unique URLs for different Platforms: It is advantageous to view recruitment channels as an integral part of access control. The initial layer of protection involves identifying who can access the survey and how they gain entry. A key strategy to reduce bot respondents involves issuing personalized, single-use survey links to each participant, ensuring that each link can only be accessed once and cannot be shared or reused [19]. For closed populations, such as university students, panel members, or clinic patients, implementing this strategy is sometimes feasible. However, when the survey is designed for broader audience, links disseminated on public social media platforms typically attract more opportunistic traffic. In this scenario, one possible measure is rotating link variants associated with each channel and monitor if any streams produce unusual activity. When anomalous activity is detected, it is advised to shut down the compromised survey link and replace it with a new link and fresh tokens [14]. This limits rapid, repeated bot submissions and reduces the burden of data cleaning later in the process.

Geo-time zone consistency: Researchers can perform a geo-time zone consistency check in by capturing the participant's local time via JavaScript and comparing it to their reported or expected time zone. For example, Qualtrics allows embedding JavaScript code that retrieves the client's browser time (which reflects their local time zone) and stores it in an embedded data field for later analysis or conditional logic. Other measures during the monitoring phase of a survey include but are not limited to monitoring IP and associated location to find mismatches, Geo-checks and time-zone consistency, and they should be applied judiciously.

Incentive Review: Compensation for survey participation should not be automated. Taking time to screen the received data for potential fraudulent responses before sending incentives can discourage bots [14].

Stage 3 - Data Cleaning & Validation

Even with advanced security, sampling, and in-survey quality checks are in place, some problematic responses may still slip past initial defenses. For this reason, a thorough data cleaning and validation stage is necessary to ensure bot-free responses. This stage involves systematically verifying that all control measures implemented during the survey design phase were effective. By rigorously assessing these controls at the validation stage, researchers can ensure that the survey data is consistent with the intended participant criteria and free from automated or fraudulent responses. For example, if bot detection feature is enabled in Qualtrics, it activates the field Q_RecaptchaScore, where a score of greater than or equal to 0.5 means the respondent is likely a human and a score of less than 0.5 means the respondent is likely a bot [24]. There are some other measures that can be considered during this stage:

Timing Thresholds: Another way to identify bots at this stage is to check for unusually short completion times. Automated filters can flag and remove responses completed too fast to be genuine. Therefore, applying timing thresholds during cleaning can be effective. It helps to exclude both careless and fraudulent submissions without relying on subjective judgment.

Duplicate Identifiers: Rule-based filters can also be applied to make an automated checks to remove duplicate entries, responses that violate survey logic, or submissions that fail critical quality controls (for example, impossible answer combinations). This helps prevent fraudulent responses without human subjectivity.

Location Mismatch: Manual review processes target inconsistencies such as mismatches between declared and IP-based geolocations. These patterns strongly indicate bot activity or respondent attempts to manipulate the survey. Careful adjudication of this metadata strengthens detection beyond automated flags alone.

Composite Fraud Score: Instead of relying on single indicators, researchers can also benefit from composite scoring models (for example, Relevant ID, Q_Recaptcha Score and Q_Ballot Box Stuffing in Qualtrics), which integrate multiple flags to identify probable fraud with high accuracy and minimize false exclusions. For instance, logic based on these fields can be set up (such as screening out possible bots or fraudulent responses), by adding these embedded data fields to the survey flow. Thorough and transparent documentation of all cleaning decisions, including rationale and impact, is vital to maintain ethical standards and scientific rigor throughout data validation.

Additional Measures for Survey Fraud Prevention:

There are additional controls available in all the stages mentioned above that can help flag suspicious activity and prevent bots when the survey is launched. Studies have suggested that lowering incentives would lower fraudulent behavior[18]. However, lowering incentives usually also lowers the participation rates. Researchers can also include a clause offering to interview participants after they complete the survey. However, to maintain anonymity and avoid bias, the contact information collected for scheduling interviews must be stored separately from survey responses. If responses are linked to identifying information, participants may alter their answers, leading to interview bias. Different platforms use common features such as bot-detection scores (RelevantID fraud score for Qualtrics) [24], duplicate-response checks, and "ballot box stuffing" which can guard against automation, identify repeated entries, and block duplicates before they enter the dataset [25].

Some Examples of Scenarios, Signals, and Immediate Actions in Web Surveys:

Table 1 presents some sample scenarios at two evidence levels: soft signals and hard triggers. Soft signals are suspicion cues that require confirmation before exclusion; hard triggers are pre-specified fail conditions that justify immediate containment or removal. For each case, the table lists what is noticed first, the signals (diagnostic confirmations), and the actions that needs to be taken if such cases occur.

Table 1: Detection Signals and Countermeasures for Fraudulent Responses in Web-Based Surveys

Scenario	*Signals*	*Immediate Actions*
Sudden surge in submissions *(soft signal)*	Submissions arrive in large bursts within short period of time; Response quality drop s during an "attack window" ; platform fraud scores spike.	Pause or throttle survey link; mark the suspicious time window; ensure bot controls like reCAPTCHA and fingerprint checks; rotate new channel-specific link.
Claims inconsistent with eligibility/location *(soft signal)*	Claimed eligibility (e.g., region or time zone) doesn't match IP geolocation; entries originate outside the target area.	Enable geofencing or server - side screen -outs where justified.
Incentive requests cluster or repeat *(soft signal)*	Same email/phone/name across multiple entries or waves for repeat incentive request.	Cross-check incentive requests using name/email/phone; queue suspicious cases; withhold rewards pending adjudication.
Hidden item (honeypot) is populated *(Hard trigger)*	Responses appear for hidden items that are invisible to human users.	Exclude per pre -registered rule; flag neighboring time window; consider elevating entry friction (e.g., CAPTCHA) for that channel.
Extreme speeding *(Hard trigger)*	Survey completed in implausibly short time relative to its length or complexity.	Apply soft minimum -time rule; flag for adjudication; exclude if failing multiple criteria
Duplicate submissions from the same agent *(Hard trigger)*	Same device/browser fingerprint used repeatedly; platform flags high duplication scores.	Enforce rate limits per device/ IP address by using survey platform's duplicate detection tools; remove confirmed duplicates during data cleaning.

Conclusion

In an era where bots are rapidly evolving, the threat of fraudulent data in web-based research has never been greater [25]. Despite strong initial safeguards, the emergence of advanced AI agents that are powered by large language model (LLM), has dramatically complicated the challenge.

Recent experiments reveal that these AI bots can outsmart many traditional quality checks: they detect and skip hidden trap questions, slow their pace to evade timing alerts, and craft tailored responses that convincingly mimic human behavior across both closed and open-ended survey items [26]. While each individual control can potentially be defeated, a multi-layered, collective plan remains the most robust defense. Collectively, these measures increase both the technical and resource cost required for fraud or bot attacks and reduce the number and impact of fraudulent responses during the survey's fielding period [26].

Finally, designing and conducting a web-based online survey requires addressing a comprehensive range of security and privacy challenges. At the same time, researchers also need to consider the benefits of each method against its costs and practical challenges [19]. For instance, removing payment for participants might reduce fraud but also discourage people from joining the surveys [18]. Therefore, ensuring data integrity in web-based surveys requires a multi-layered approach that combines technological safeguards with thoughtful instrument design, continuous monitoring, and rigorous data validation.

Conflict of interest: None.
Funding: The authors have no relevant financial or non-financial interests to disclose.

Declarations: We (the authors) take full responsibility for the content of this paper. We acknowledge the use of AI (editgpt) for assistance with English language editing. We used prompts to improve the structure of sentences that we deemed could be further improved. AI was prompted to improve clarity by improving grammar and choice of vocabularies used in the text. All suggestions were critically reviewed and revised to ensure the integrity of our own expressions. The authors have no conflicts of interest, relevant funding, employment, financial or non-financial interests to declare.

Reference

1. Biemer PP, Lyberg L. Introduction to Survey Quality. Wiley; 2003.
2. Traditional vs. Online Survey Research. AIMultiple. Accessed October 25, 2025. https://research.aimultiple.com/online-survey-research/
3. Fitzgerald D, Hockey R, Jones M, Mishra G, Waller M, Dobson A. Use of Online or Paper Surveys by Australian Women: Longitudinal Study of Users, Devices, and Cohort Retention. J Med Internet Res. 2019;21(3):e10672.
4. Arundel A. Survey fundamentals. In: 2023:7-24. doi:10.4337/9781800376175.000065. Van Selm M, Jankowski NW. Conducting Online Surveys. Qual Quant. 2006;40(3):435-456.
6. Bonett S, Lin W, Topper PS, Wolfe J, Golinkoff J, Deshpande A et al. Assessing and Improving Data Integrity in Web-Based Surveys: Comparison of Fraud Detection Systems in a COVID-19 Study. JMIR Form Res. 2024;8(1):e47091
7. Johnson MS, Adams VM, Byrne J. Addressing fraudulent responses in online surveys: Insights from a web-based participatory mapping study. People Nat. 2024;6(1):147-164
8. Dupuis M, Meier E, Cuneo F. Detecting computer-generated random responding in questionnaire-based data: A comparison of seven indices. Behav Res Methods. 2019;51(5):2228-2237.
9. Check JW, Schutt RK. Research Methods in Education. SAGE; 2012.
10. Schaefer DR, Dillman DA. Development of a Standard E-Mail Methodology: Results of an Experiment. Public Opin Q. 1998;62(3):378
11. World Bank Open Data. World Bank Open Data. Accessed October 22, 2025. https://data.worldbank.org
12. Groves RM, Lyberg L. Total Survey Error: Past, Present, and Future. Public Opin Q. 2010;74(5):849-879
13. Kiernan NE, Kiernan M, Oyler MA, Gilles C. Is a Web Survey as Effective as a Mail Survey? A Field Experiment Among Computer Users. Am J Eval. 2005;26(2):245-252
14. Storozuk A, Ashley M, Delage V, Maloney EA. Got Bots? Practical Recommendations to Protect Online Survey Data from Bot Attacks. Quant Methods Psychol. 2020;16(5):472-481
15. Callegaro M, Manfreda KL, Vehovar V. Callegaro, Manfreda, Vehovar. Web Survey Methodology.; 2015.
16. Glasow P. Fundamentals of Survey Research Methodology.
17. Shevchenko Y, Reips UD. Geofencing in location-based behavioral research: Methodology, challenges, and implementation. Behav Res Methods. 2024;56(7):6411-6439
18. Teitcher JEF, Bockting WO, Bauermeister JA, Hoefer CJ, Miner MH, Klitzman RL. Detecting, preventing, and responding to "fraudsters" in internet research: ethics and tradeoffs. J Law Med Ethics J Am Soc Law Med Ethics. 2015;43(1):116-133
19. Pozzer R, Hammer MJ, Underhill-Blazey M, Wright AA, Tulsky JA, Hong F, et al. Threats of Bots and Other Bad Actors to Data Quality Following Research Participant Recruitment Through Social Media: Cross-Sectional Questionnaire. J Med Internet Res. 2020;22(10):e23021
20. Venugopalan H, Munir S, Ahmed S, Wang T, King ST, Shafiq Z. FP-Inconsistent: Measurement and Analysis of Fingerprint Inconsistencies in Evasive Bot Traffic. arXiv. Preprint posted online September 21, 2025
21. Regmi PR, Waithaka E, Paudyal A, Simkhada P, van Teijlingen E. Guide to the design and application of online questionnaire surveys. Nepal J Epidemiol. 2016;6(4):640-644
22. Dinh NT, Hoang VT. Recent advances of Captcha security analysis: a short literature review. Procedia Comput Sci. 2023;218:2550-2562
23. Nerurkar AK, Thampi GT, Motwani D, Chaudhari K, Panhale P. Intelligent robotic process automation that shall make captcha security ineffective. In: 2023:020027
24. Fraud Detection. Accessed November 1, 2025. https://www.qualtrics.com/support/survey-platform/survey-module/survey-checker/fraud-detection/
25. Parker JN, Rager TL, Burns J, Mmeje O. Data Verification and Respondent Validity for a Web-Based Sexual Health Survey: Tutorial. JMIR Form Res. 2024;8:e56788-e56788
26. How To Outsmart Survey Bot Respondents. SurveyMonkey. Accessed October 25, 2025. https://www.surveymonkey.com/curiosity/outsmart-bot-survey-respondent/