

CANADIAN VIEWPOINT

40+ YEARS OF PROVIDING EXCELLENCE

Canadian Viewpoint Panel Quality Assurance Book



1 (888) 770 1770
info@canview.com
www.canview.com

Drop Cookies

Canadian Viewpoint has a very advanced online survey platform – Decipher, which allows our programming team to drop a cookie on a respondent computer, tablet, or phone. This cookie prevents the survey taker from completing the questionnaire a second time. If the cookie is dropped, the respondent will click the survey link and a page will show the statement, "You have already completed this survey".

Check IP Addresses

Canadian Viewpoint has a very advanced online survey platform – Decipher, which allows our programming team to drop a cookie on a respondent computer, tablet, or phone. This cookie prevents the survey taker from completing the questionnaire a second time. If the cookie is dropped, the respondent will click the survey link and a page will show the statement, "You have already completed this survey".

Check for Duplicates

Canadian Viewpoint performs a simple data check to review duplicate cases. Contact information is often collected at the end of a survey. It is important to review the names, emails, or phone numbers for duplicates and identify these records and remove them.

Check for Duplicates

Canadian Viewpoint performs a simple data check to review duplicate cases. Contact information is often collected at the end of a survey. It is important to review the names, emails, or phone numbers for duplicates and identify these records and remove them.

Check for Speeders

Another excellent way to check for data integrity is to review speeders. Our survey platform Decipher logs time to complete for the respondent. This is the exact time it took to complete the survey from start to finish.

Canadian Viewpoint asks clients for their preferred percentage to be applied to the median length. Industry standard ranges from 33% - 40% of the median length. If your survey takes 20 minutes to complete and you have responses that have been completed in less than 8 minutes, this is a red flag for data integrity and these responses may be removed.

Drop a Red Herring Question

Canadian Viewpoint encourages clients to add red herring questions to their surveys as a part of their quality checks. Unlike IP addresses, time to complete, and cookies, this is a purposeful question placed in the survey to identify bad responses. These questions help identify and eliminate speeders.



Examples of Red Herring Questions

1. Add fake brand names – What is your favourite beer
 - a. Heineken
 - b. Labatt's
 - c. Great Orange

2. Outlier answer to an opinionated question - For example, a not-for-profit organization is conducting a long online survey to better understand why people are or are not choosing to donate to their charity. An outlier red herring question to include which does not relate to the survey content may be: Add imaginary roles and responsibilities – Which of the following best describes your role in your company
 - a. Director of IT
 - b. Director of Parties
 - c. Director of Sales

Open-Ended Questions

Canadian Viewpoint does not have an automatic filter for bad open ends. Our skilled Project Managers carefully review our client's data file to catch these responses and will manually remove unwanted open ends.

Canadian Viewpoint employs the following quality measures to address bad open ends:

1. Remove gibberish/non sensical responses - The panelist has entered words or sentences that don't make sense.
2. Remove Profanity - The panelist has used curse words in their response.
3. The answer to the question does not make sense - The panelist's answer does not correlate with the question asked.
4. Bots - The panelist has programmed a system to automatically answer open-ended questions.

Straightliners

Panelists who choose the same response for multi-select and grid questions for the duration of the survey. CVI can program logic into your survey to identify this fraudulent activity.

This logic allows us to track and flag straightliner responses so that the client can decide if these responses should be removed.



Canadian Viewpoint Consumer Panel

Highlights:

- Mixed-mode recruitment strategies (online/phone/in-person) are used to build our panel
- Complex sampling software allows us to draw a sample representative of any required demographics
- Our panelists receive small monetary incentives by cheque, depending on LOI (length of interview) and audience
- Profiling for efficient targeting
- Our average panelists will complete 5-6 surveys a year

Profiling:

We have extensive profiling and are always adding additional list items. Here are some of our most popular profile categories:

- Employment (employment status, type of employment)
- Marital Status
- Financial (credit card/financial institution/bank account type)
- Dwelling Type (own/rent)
- Household Composition (age/gender/number of residents in the household)
- Pets (dog/cat ownership)
- Electronics (currently own tablet, laptop, desktop computers, etc.)
- Smoking (currently smoke, trying to quit, vape and smoking cessation products)

Note: If there is anything specific topics of interest to you, please let us know and we'll set up your question on the next profiling update.

Panel Refreshment Rules:

We have open recruitment as we are constantly refreshing our panel. Our panel team updates panelist information on an ongoing basis to continue to augment the panel within the demographics that are most required.

Updating:

Panelists are immediately removed with the following scenarios:

- Hard-bounced email
- If they request to be unsubscribed/removed
- If they are found to lie or cheat
- 3-strike rule: if a panelist is found providing questionable data 3 times
- If a panelist has ignored 10 consecutive survey invitations



Completion Rates

We have an average completion rate of 80% per study. The overall completion rate is dependent upon the length of the interview and significantly decreases as the survey increases in length. Our average completion rate is based off the number of completes derived from study starts across all projects from the last calendar year.

Response Rate

Typical response rates for online panels ranges between 10%-20%. This number has been averaged from all panelist responses to studies that have been fielded in the last calendar year. Canadian Viewpoint typically has an average response of 20% - 35%. There are 3 options that we can look at for increasing the overall response rate to any project:

1. Increase study incentive
2. Increase the total length of time in field
3. Increase the frequency of reminders

Panel Sourcing, Panel Fatigue & Incentives

Our panel is sourced from several channels to ensure it is as diverse and representative as possible. Our panel does not use incentivized traffic for recruitment purposes to ensure quality. To minimize panel fatigue, our panelists are restricted in the number of studies that they can take part in each month. The incentive that we provide them with is directly proportionate to the amount of time it requires them to complete a study and are comparable to incentives offered by other online panel companies.

Quality Controls – Panel

We use a multi-faceted approach to quality, integrating controls and best practices into every phase of the process: Panel members come from diverse, fully certified sources. A dedicated team monitors performance by source using feedback loops and continuous reporting, which prevents fraud. Our dedicated team monitors the panels for potentially fraudulent behaviour, and blocks these people from ever entering a survey via safeguards which include:

- Double opt-in authentication process
- We use cash incentives, in the form of cheques, which ensures confirmation of our panelist identity
- Respondents provide us with legitimate information about their identity and address and allows them to receive their incentive cheque
- Immediate examination of suspicious email addresses, suspicious behaviour, or unrealistic completion times
- Fast and permanent removal of offenders
- CVI works with our clients to set up customized data quality checks for their surveys that we program. When we are providing Sample Only, the client is ultimately responsible for setting up their own data quality checks
- We limit invitations to 3 x week. The average respondent receives 1.38 surveys a month from us and completes 5 - 6 surveys per year
- CVI keeps participation history, join date and source of respondent on file. A project analysis of such data is available to our clients upon request



- Proprietary Verification is a suite of quality control procedures including digital fingerprinting, address verification against USPS databases (standard in the US and Canada) and third-party verification upon request

Canadian Viewpoint Canadian Server Installation

Complete programming, hosting, and sampling solutions are managed and stored in our datacentres located in Toronto, Ontario, Canada. Our admin and production staff are also located in the Greater Toronto Area (GTA).

Security and Data Protection

Canadian Viewpoint Inc. has a robust Data Security Policy and Cybersecurity Incident Response Plan (CIRT). Our Data Security policy manual establishes guidelines and rules to ensure that Canadian Viewpoint Inc. remains compliant with PIPEDA requirements, as well as managing prevention and detection via ManageEngine.

Canadian Viewpoint Inc. has adopted the CIRA D-Zone Cybersecurity Awareness Training, which offers online education courses related to security for employees, followed by a test on the subject matter. The program reinforces the message of “employee vigilance” by sending periodic and stimulating “phishing” emails, which employees can report. Depending on if employees report, such occurrences are logged within the platform and becomes part of their “risk score”. This enhances security by improving awareness of the need to protect system resources, developing skills and knowledge so employees can perform their job securely. In addition, it builds in-depth knowledge, awareness, and best practices of security responsibilities to help employees improve computer security. With proper security, privacy awareness training, clear communication of data and device use policies, employees are the first line of defense against cybersecurity incidents.

We have implemented all necessary security controls to ensure technology assets, including PII, at risk of inappropriate access, use, and disclosure are protected (i.e., folders are marked ‘secure’, with limited access in cases where PII exists on our network). Our policy has formally appointed and documented the responsibility for specific personnel to serve as security administrator(s) or formally assigned responsibility for creating, implementing, and maintaining security policies and procedures (Tech Lead and Vice President [VP] authors review and authorize policies and procedures; individual Project Managers [PMs] are responsible for ensuring projects with sensitive data or PII are secured and are in access- restricted folders).

CVI has implemented the following security measures to ensure that client personal information is appropriately protected: the use of locked filing cabinets, physically securing offices where personal information is held, the use of user IDs/passwords/encryption/firewalls, restricting employee access to personal information, as appropriate.

Furthermore, we use appropriate security measures when destroying clients’ personal information, by measures including by not limited to shredding documents and permanently deleting electronically stored information. Our security policy manual is continually being reviewed and updated as technology changes to ensure ongoing personal information security.



To safeguard resources(hardware/software/network/data) and to guarantee they are used to best effect, all employees must work to prevent malware and assure physical and information security:

- Do not insert or install any unauthorized media into CanadianViewpoint Inc. resources, including but is not limited to USB sticks/keys, CD/DVD/Blu Rays, external hard drives
- Notify the Tech Lead immediately of any unexplained errors, error messages, tech issues (i.e., protracted slowness, unplanned shutdowns/reboots, etc.), unusual activity, or Malware/Virus alerts that you encounter
- Suspected “social engineering attacks (i.e., suspicious phone calls/emails asking for information)” should be reported in the same manner
- Canadian Viewpoint Inc. will ensure a virus scan/clean program is installed on all PCs. Individual employees should periodically check its status to ensure it is up to date and scans are running daily
- Data files that contain any identifying information (i.e., panel exports, Master Send files, ‘client lists’ etc.) should never be stored outside of Canadian Viewpoint Inc. – don’t create unnecessary copies; pull/save as little information as is required for task; delete any extra/unused data points
- We utilize in-house and remote backups for all data and other materials stored on our in-house servers. Data is backed up to dedicated Canadian servers, encrypted NAS daily, and a remote (off-site). Images are also taken and stored regularly. Backed-up data is encrypted at rest and in transit (using AES-256 and TLS1.2 encryption, respectively); while data backed up ‘off-site’ is encrypted (also using AES-256, and off-site techs do not have the key).
- Least Privilege Access principles guide our action regarding providing access to sensitive resources. This includes giving users access only to the resources they need via Active Directory on our in-house servers, as well as access to elements of the Survey Engine we utilize (FocusVision’s Decipher).

CONTACT US



1 (888) 770 1770
 info@canview.com
 www.canview.com

