Credential Attacks in Ontario's Online Elections*

Eric Klassen[1], James Brunet[2], Nicole J. Goodman[3], and Aleksander Essex[†1]

[1]Department of Electrical and Computer Engineering, Western University
[2]School of Information Technology, Carlton University
[3]Department of Political Science, Brock University

October, 2025

Abstract

We propose two novel voter authentication attacks in the context of the 2022 Ontario Municipal Election, which offered online voting to almost four million voters in over 200 municipalities. One attack exploits a misconfiguration in one of the voting portals used by up to one million voters. It was mitigated through a successful coordinated vulnerability disclosure that we conducted with the affected vendor during the election period. The other attack exploits widespread and insecurely discarded login credentials. This attack affects the vast majority of the deployments examined, and we study and quantify the risk for each city individually. In both cases, the risks were aggravated by unique, context-dependent factors, which we detail. Finally, toward quantifying this risk, and absent the availability of this data elsewhere, we present a comprehensive census of online deployments used in the province.

1 INTRODUCTION

This paper studies online voter authentication mechanisms used in the 2022 Ontario Municipal Election, involving 417 separate local elections, serving a combined 10.7 million eligible voters [1]. Of these municipalities, 219 offered an online voting option, of which 158 cities eliminated the paper ballot altogether.

Owing to the inherently unsupervised nature of remote online voting, strong digital credential mechanisms are necessary to ensure that a digital ballot reflects the

*This document is the authors' full version of the originally published paper:
Klassen, E., Brunet, J., Goodman, N., Essex, A. (2026). Credential Attacks in Ontario's Online Elections. In: Duenas-Cid, D., et al. Electronic Voting. E-Vote-ID 2025. Lecture Notes in Computer Science, vol 16028. Springer, Cham. https://doi.org/10.1007/978-3-032-05036-6_9

[†]Corresponding author: Aleksander Essex, aessex@uwo.ca

genuine intent of the designated voter. Coercion and vote-selling are two well-studied examples of attacks in this setting (among many such works, see e.g. [2–5]). This paper, however, focuses on a different category of credential attacks—those in which voters are unknowing participants.

Our inquiry began with an observation communicated to us by one municipal election official that voter information letters (containing the voter's login PIN) had been observed discarded in a communal trash bin unopened and hence unused. Based on this, we consider the following research questions: Which municipalities offered online voting in the 2022 election, and how did voters authenticate to these systems? What is the potential insecurely discarded voter login credentials, and how can we quantify the risk for each city? What would be the attack complexity required to change an election outcome? Were there any municipalities where this attack could be considered 'easy' under our defined risk metric? Could we observe other vulnerabilities in the online voting portals that allow voter login credentials to be exploited?

Our findings suggest weak authentication methods in Ontario are a weak point in most of the observed systems, highlighting the dilemma faced by 1.6 million eligible voters in cities where paper ballots were eliminated: Accept the cyber risks introduced by the design design decisions of these deployments, or, as one judicial decision from a 2019 election challenge blithely put it, accept "voluntary disenfranchisement" [6].

1.1 Findings and Contributions

The contributions of this work are threefold. First, to facilitate our credential risk analysis, we conducted a comprehensive census of cities and vendors offering online voting. While basic data about online voting adoption was published by the Association of Municipalities of Ontario (AMO) [1], we undertook an intensive supplementary data collection effort to determine which cities used which online voting vendors and how, in each case, they approached voter authentication. Section 2 describes the methods used to collect this data and presents findings about online voting in Ontario, which includes our census of vendors and cities that offered online voting in 2022 and how the landscape has changed since the previous election cycle.

Second, we present a novel effort to quantify the cyber risk of discarded credentials in Section 3, correlating each municipality's credential scheme against their electoral outcomes, combined with additional context-dependent factors to compute an overall risk score in each case. Of the 219 Ontario cities offering online voting, we found that the majority (70%) were at high risk of this attack under the proposed metric.

Third, we present a novel cross-site browser framing vulnerability in Section 4 that could allow an attacker to misdirect a voter into casting a ballot for an unintended can-

didate. We highlight additional aggravating factors that increased the attack's severity beyond the general case. Finally, we describe our coordinated vulnerability disclosure effort with the affected vendor (Scytl) during the live election period. They promptly issued a mitigation, affecting as many as one million voters, and issued an advisory to their municipal clients acknowledging our findings.

2 BACKGROUND AND METHODOLOGY

The election was held on October 14th, 2022, although early voting began in some municipalities at least as early as October 9th. 417 separate municipal elections served a total of 10.7 million eligible voters [1]. While many voting methods were offered, this work focuses on the 219 municipalities offering online voting to a combined 3.8 million eligible voters. Of these, 154 municipalities eliminated paper ballots altogether, offering only a remote electronic voting method (either online or by telephone) to their combined total of 1.7 million eligible voters.

2.1 Data Collection Methodology

Comprehensive information about Ontario's online voting landscape is not readily available. Federal or provincial governments do not track the marketplace. Vendors typically decline to volunteer this information and in past instances have even refused our requests for it. The AMO publishes election results and tracks voting methods used by municipalities, but does not track vendor information [1]. The AMO also does not provide this information as a single usable dataset; instead, it provides data about the 444 Ontario municipalities across 444 separate web pages. An AMO representative told us that our request for a dataset could not be fulfilled, so we wrote a script to collect, extract and aggregate this data from their multitude of individual web pages.

To determine which municipalities worked with which vendor, we began with the observation from previous work [7] that vendors tended to follow a consistent URL format for each city's voting portal. For instance, Simply Voting used the URL convention `https://{municipality}.simplyvoting.com`, while Dominion used `https://intvoting.com/{municipality}`. We used this method to create an initial list during the early voting period in October. To validate this list and to determine the types of login credentials used by each city, we undertook an intensive process in the months following the election, manually locating and examining a wide range of online sources, including council meeting minutes, municipal staff reports, social media pages, YouTube videos, and the Internet Archive Wayback Machine. This approach allowed us to identify and validate all city/vendor pairs with high confidence.

Year	Dominion	Intelivote	Neuvote	Scytl	Simply Voting	Voatz	Total
				Eligible Voters by Vendor			
2018	1,323,194	860,985	n/a	253,437	304,479	n/a	2,742,095
2022	996,965	679,910	1,049	1,037,635	714,360	402,385	3,832,304
Change	(326,229)	(181,075)	1,049	784,198	409,881	402,385	1,090,209
				Municipal Clients by Vendor			
2018	49	98	0	2	28	0	177
2022	23	96	1	36	49	14	219
Change	(26)	(2)	1	34	21	14	42

Table 1: Summary of our Ontario online voting vendor census: 2018 to 2022.

2.2 Vendor Census Results and Dataset

The election results dataset and census form the basis of our analysis of voter authentication vulnerabilities in Section 3. Table 1 shows a summary of our vendor census. Our full dataset is available online.[1] In addition to presenting information about which vendors ran online elections for which cities, we combine this information with previous work from the 2018 election [7] showing the growth of online voting adoption in the province.

As the data shows, online voting adoption grew by 25% between the 2018 and 2024 election cycles, with over 50% of municipalities (representing over 3.8 million voters) now offering an online voting option.[2] One interesting finding was that the market share of Dominion Voting Systems declined considerably in 2022. Of Dominion's 49 municipal clients in 2018, 34 switched to a new vendor in 2022, and 8 discontinued online voting altogether. We conjecture this outcome is in large part due to their 2018 election night service disruption due to insufficient bandwidth provisioning [7]. Scytl's market share increased partly because they partnered with Intelivote in 2018, but operated as a separate provider in 2022. Neuvote and Voatz were newcomers to the market, and we anticipate additional new vendors will enter the market in 2026.

[1] 2022 Ontario Municipal Election Vendor Census. https://github.com/eklass3/ONElectionData_2022

[2] 219 municipalities represent over 50% since not all 444 municipalities run elections (mainly in the upper-tier/regional municipalities).

2.3 Observed Credential Mechanisms

Based on our findings from our vendor census, we found that credentials were overwhelmingly distributed to voters by postal mail. Voters receive a voter information letter (VIL) in their mailbox, which contains a login credential (typically an 8-16 digit PIN) [7] and the URL of the voting site. Voters authenticate to the website by providing the PIN from the VIL along with their date of birth. The risks of insecurely discarded credentials under this approach are explored in Section 3. The VIL instructs voters to connect to the voting site on their device by typing a partial URL into their browser's address bar (see Figure 1).[3] This, along with an additionally observed server configuration vulnerability, provides the basis for the cross-site browser framing attack discussed in Section 4.

Figure 1: Example Voter Information Letter (VIL) directing user to type a partial URL.[3]

3 RISK ANALYSIS OF INSECURELY DISCARDED CREDENTIALS

In this section, we examine the feasibility of harvesting discarded login credentials as an attack to maliciously alter an election outcome. Two observations are at the core of the proposed attack. First, harvesting a discarded credential offers a low-detectability way to cast a fraudulent ballot in cities that only offer online voting. Second is the observation that each of the 1.7 million eligible voters across the 154 online voting-only cities automatically received a Voter Information Letter (VIL) by postal mail contain-

[3] How to Vote Online - 2022 Ontario Municipal and School Board Election. Town of the Blue Mountains. Available: https://www.youtube.com/watch?v=RgJobco9cxs

ing a login credential (typically an 8-16 digit PIN). Since voter turnout in 2022 averaged 36.3% [1] across the province, we can infer that over a million credentials went unused. Based on the expectation that most credentials were insecurely discarded (as discussed below), this section attempts to quantify the risk of this attack across each city by examining the number of unused credentials relative to the declared victory margins in combination with the secondary date-of-birth credential used (if any).

The impetus to study this issue comes from an observation communicated to us by an Ontario election official (from an unpublished study currently in progress), who was made aware of discarded, unopened VILs in recycling bins at one of their community mailbox locations. Although this example is specific to one municipality, the conditions that facilitate such occurrences—centralized mail delivery and low voter engagement—are shared by most municipalities, suggesting that this issue is likely widespread. Our goal is to provide a simple metric that election officials can apply to their unique cases based on overt risk factors such as the widespread availability of unused VILs and the relative strength of secondary credentials like date of birth (DOB). We note our analysis is based on the reported login credential methods and voter turnout in each city only. Gathering data about the actual prevalence of discarded VILs would have raised complex legal issues and was beyond the scope of this work. We recommend that municipalities explore this question directly themselves.

Attack complexity

Our proposed credential harvesting attack is both manual and labor-intensive, so we begin by defining an upper bound on the effort required for this attack to be reasonably considered feasible. Supposing that a legitimate election campaign could knock on one thousand doors during an election period,[4] we define a malicious effort to collect up to 1,000 discarded VILs as the upper bound of feasibility for the purposes of this metric. We limited our analysis, therefore, to contests with victory margins of fewer than 1,000 votes. We further subdivide the attack complexity across three orders of magnitude: hard (up to 1,000 VILs), medium (up to 100 VILs), and easy (up to 10 VILs). Using this classification, we found that 700 races across approximately 70% of the 154 municipalities met one of these criteria. Table 2 shows the distribution.

[4] E.g., a recent federal candidate claims to have knocked on 5,000 doors. See: https://thetyee.ca/News/2024/03/04/One-Man-March-Beat-Poilievre-Own-Riding/

Attack Complexity	Victory Margin	Number of Races
Easy	1-10	24
Medium	11-100	148
Hard	101-1000	528

Table 2: Number of races in the 2022 election at risk of the proposed credential-stealing attack.

Combination Type	Municipalities (#)	Municipalities (%)
DOB (D-M-Y)	87	38.7%
DOB (M-Y)	6	2.7%
DOB (Y)	22	9.8%
Combination unknown	33	14.7%
DOB use unknown	75	33.3%
Does not use DOB	2	0.9%

Table 3: Survey of date of birth used as a secondary credential in the 2022 election.

3.1 Secondary Authentication Practices in Ontario Municipal Elections

Obtaining discarded VILs alone is typically not sufficient to cast a fraudulent vote. Many (but not all) municipalities require a secondary login credential to vote based on the voter's date of birth. We observed various combinations of year (Y), month (M), and day (D). Importantly, these combinations were often set by the municipality, not the vendor, so we had to confirm the specific configuration used in each municipality by referencing public-facing documents. In some instances, information about DOB combination or even if the municipality required a DOB was not publicly available (i.e., unknown). The analysis results are summarized in Table 3.

As has been previously observed [7], date of birth is a weak login credential: It is inherently low-entropy; It cannot be changed; and, although it is treated as private, it is not inherently *secret*. However, unlike many US states, which publish voter lists with full DOB information, Ontario does not make this information widely available—not even to candidates, so a successful attack would require an adversary to obtain this information by other means.

3.2 Options for Obtaining Voter DoB Information

Several entities in the election ecosystem have full access to voter DOB information, including Ontario's Municipal Property Assessment Corporation (MPAC), which curates the preliminary voter lists, as well as the e-pollbook service provider (as do many other companies and agencies in Ontario). Notwithstanding these potential insider threats, we consider potential options for an attacker to obtain Ontario voter DOB information through publicly available sources.

Data breaches

Large-scale data breaches involving dates of birth are a regular occurrence [8–10]. As part of our effort to explore data breach availability, we solicited legal advice from a firm in our jurisdiction specializing in cybercrime law. We were advised that downloading and analyzing freely available datasets represented low legal risk, as long as passwords or credit card numbers were not part of the data. We accordingly restricted our search to datasets where we could confirm these conditions were met prior to accessing them.

As a proof of concept, we downloaded and analyzed the 2019 Facebook data breach, which confirmed the existence of exposed Ontario voter DOBs online. Our analysis found that this dataset contained the first name, last name, city, and full dates of birth of 22,308 Ontario residents. We found an additional 28,276 Ontario residents with partial dates of birth (month and day) in this breach. Legal considerations prevented us from examining several larger data breaches as they contained password information, however it was apparent that the totality of exposure greatly exceeds what we were able to directly observe, given our constraints.

Online DOB Oracles

The login page of the voting site represents a kind of date of birth oracle with a limited number of guesses. Using a harvested PIN, the attacker can make a guess the voter's DOB. If the guess is correct, the login will be successful. However, several additional online DOB oracles exist in the form of Elections Canada's, Elections Ontario's, and MPAC's voter registration directories. All three services allow voters to check their registration status by entering their name, address, and date of birth (with the first two revealed to the attacker by the VIL). Using a oracle, the number of guesses expected to confirm a DOB varies by the specific year/month/day combination required by the municipality. We did not attempt to determine how many incorrect guesses could be made to each website before triggering a lockout period. To quantify DOB entropy, we

Authentication Level	Entropy (Bits)
Year-Month-Day	14.6
Year-Month	9.7
Year	6.1

Table 4: DOB entropy for differing combinations.

used the Ohio voter registry as a proxy [11], which contains complete DOB information. Ohio is demographically similar to Ontario and comparable in population size (approximately 8 million registered voters). The results of our analysis are shown in Table 4.

Of the 22 Ontario municipalities using year of birth as a secondary credential, our results indicate an attacker can find the correct date of birth in approximately 64 guesses on average, and possibly fewer in instances where a voter's name is correlated with their age. Ontario publishes a dataset of baby names for the past hundred years, listing each name and the number of newborns registered with that name (for $k \geq 5$).[5] As an illustrative example, consider an attacker-recovered VIL addressed to a voter named 'Ryszard'. This name only appears in the list between 1950-60, suggesting the voter's DOB could be recovered using an oracle in closer to 10 guesses. Of course, in municipalities using no DOB credential, such as the Town of Atikokan [12], the VIL alone is sufficient to cast a ballot.

3.3 Credential Attack Risk Metric

To quantify credential attack risks to municipalities, and similar to the parameterization methodology of the Common Vulnerability Scoring System (CVSS), we developed out risk metric by subjectively ranking cases toward identifying constituent risk factors. Our proposed risk metric is as follows:

$$R_{\text{credential\_attack}} = r_{EV} + r_{AV} + r_{VT} + r_{CC} + r_{HCC} + r_{SF}$$

where:

1. **Eligible Voters Risk (r_{EV})**: Scored 0–10 based on the size of the eligible voter population. Each point represents a 10th percentile decrease in population, with larger voting populations reducing the likelihood of close elections.

2. **Alternate Vote Risk (r_{AV})**: A binary score (0 or 10) based on the availability of voting methods. Municipalities offering additional voting methods score 0, as

[5] https://data.ontario.ca/dataset/ontario-top-baby-names-male

a discarded VIL could mean a voter intends to cast their ballot through other means. This would raise suspicion if the voter is logged as having already voted. Municipalities with only internet and telephone voting score 10, as this ensures that unopened and discarded VILs could be used to cast a fraudulent vote.

3. **Voter Turnout Risk (r_{VT})**: Scored 0–10, based on the percentage of eligible voters participating in the election. Each point denotes a 10th percentile decrease in voter turnout, with higher turnout decreasing the availability of discarded VILs.

4. **Councillor Closeness Risk (r_{CC})**: Scored 0–3 for each elected councillor based on their victory margin for that race. Margins of 1–10 votes score 3, 11–100 votes score 2, 101–1000 votes score 1. Greater than 1000 votes score 0. Smaller margins score higher, indicating past elections could have been more easily influenced, assuming this is an approximate predictor of future risk.

5. **Head of Council Closeness Risk (r_{HCC})**: Scored 0–3, the same as councillor closeness risk (r_{CC}) but based on the elected head of council's (typically, mayoral) victory margins.

6. **Secondary Factor Risk (r_{SF})**: Scored according to the difficulty of guessing the secondary credential (i.e., date of birth) based on our entropy calculations in Table 4. The scores are as follows: 5 for unknown credential level or unknown date-of-birth format; 2 for day-month-year format; 5 for month-year format; 8 for year-only format; and 10 for no date of birth used. Higher scores indicate greater risk.

We applied our risk metric to each municipality and categorized them into quartiles based on their point distributions. The highest observed score indicated the most extreme risk, with 69% of municipalities in the 2022 election classified as either high or extreme risk.

As one worked example, the Municipality of Sioux Lookout had the highest risk, scoring 40 points: $r_{EV} = 8$ (3,185 eligible voters), $r_{AV} = 10$ (online and telephone voting offered), $r_{VT} = 6$ (33% voter turnout), $r_{CC} = 11$ (one race with 1-10 margin, three with 11-100 margin, and two with 101-1000 margin gives 3+3(2)+2(1)=11), $r_{HCC} = 0$ (the mayor was acclaimed), $r_{SF} = 5$ (unknown DOB configuration). The summary of risk ratings for all the municipalities is given in Table 5. Our full dataset is available online (see supra note 1).

Risk Category	Municipalities (#)	Municipalities (%)
Low (0–9 pts)	12	5.5
Medium (10–19 pts)	54	24.7
High (20–29 pts)	78	35.6
Extreme (30–40 pts)	75	34.2
Total	219	100

Table 5: Distribution of municipalities based on risk scores.

3.4 Assumptions about Prevalence of Discarded Credentials

Our risk metric presumes an abundance of credentials thrown out, unused and intact. One question is how the incidence rate of secure destruction of unused VILs should affect the risk score. Let n_e, n_v represent the number of eligible and actual voters in a given city. Let $n_u = n_e - n_v$ be the total number of unused VILs in a given city. Let $0 \leq \sigma \leq 1$ represent the proportion of unused VILs that are securely destroyed. The number of unused VILs available for a credential attack, therefore, is $n_a = n_u(1 - \sigma)$. As a loose upper bound, we argue the risk rating should not be adjusted downward for cities where $n_a > n_v$, i.e., where more VILs were thrown out than cast in the election itself. Making a conservative assumption that half of the unused VILs were securely destroyed (i.e., $\sigma = 0.5$), we found 86 cities (39%) still met this criterion (i.e., more credentials were insecurely discarded than used). However, if we assume only one in 5 VILs were securely destroyed (i.e., $\sigma = 0.2$), then 184 (84%) still meet this criterion.

This demonstrates the difficulty municipalities would face to ensure insecurely discarded VILs were scarce enough to make this attack infeasible. Although determining actual values of σ was beyond the scope of this study, we suspect it was low across most cities. None of the sample VILs we found online contained instructions to securely destroy an unused VIL,[6] although any such instruction would go unseen by a voter who did not open their letter. We also found no evidence of a plan by any city to offer secure document destruction to voters.

4 CROSS-SITE BROWSER FRAMING ATTACK

This section presents findings relating to a cross-site framing vulnerability that we discovered in the 2022 Ontario Municipal Election and the ensuing coordinated disclosure with the affected vendor (Scytl). We performed a coordinated disclosure during

[6] See, e.g., Sample Voter Information Letter. City of Markham. https://www.electionsmarkham.ca/media/lnbhp4iq/voter-information-letter-sample-english.pdf

the live election and worked with them to correct the issue. Scytl acknowledged the vulnerability and sent an advisory to their 37 municipal clients, improving the security posture of the voting service for over one million eligible voters.

A *cross-site framing attack* involves a malicious website embedding another website inside an HTML `iframe` to misdirect users into performing unintended actions. Typically, the attack is structured around the expectation that the user is aware that they are visiting the outer (malicious) site, but unaware they are performing actions in the inner (framed) site. In the election context, we consider the reverse, where the voter believes they are interacting with the legitimate voting site, and are unaware it is being framed inside a malicious site to misdirect the voter to cast a vote for an unintended candidate.

4.1 Attack Assumptions

Although our proposed attack exploits voter authentication gaps at login time, it does not exploit the credentials directly. It does not exploit the Transport Layer Security (TLS) protocol or modify the voting website's underlying logic or network communications. It assumes the voter follows the instructions *as given* in the Voter Information Letter, which directs them to manually type a partial URL into their browser address bar.

The attack only requires the voter not to notice being redirected to a malicious URL. Generally, this is a strong (i.e., unrealistic) assumption. However, Ontario's online voting context presents at least one context-specific aggravating usability factor that makes this outcome more reasonable in practice: voters (and their browsers) encounter the genuine election site URL for the first time when voting.

Our analysis found that most cities offering online services used a new or different URL than in prior years. We identified three causes: Either the city was offering online voting for the first time (e.g., the City of Barrie), the town changed vendors between election cycles (e.g., the City of Belleville), or the vendor changed the election domain name between election cycles (e.g., Intelivote). Of the 1.39 million eligible voters in municipalities that offered online voting as the only voting method, 134 (87%) cities used a new URL compared to the 2018 election. Although a formal user study was outside the scope of this work, we hypothesize that without a prior history of engaging with the genuine voting site's URL, voters are less likely to notice a domain redirection at login.

4.2 Additional Aggravating Factors

Our analysis of municipal websites and associated social media found that cities rarely share the URL except in the VIL. We found no examples of VILs containing QR codes. Therefore, we generally expect voters to access the voting website by manually typing the URL into their browser's address bar. Two of the four sample VILs we examined in our study did not include the protocol (`https://`) as part of the URL. Neither of the two municipalities that included a complete URL on the VIL provided explicit instructions to voters to ensure they type "`https://`". For these reasons, we expect most voters would type a partial URL (e.g., `voting-site.com`) into their browser address bar. Browsers generally interpret this to mean the user is requesting an insecure HTTP resource, i.e., `http://voting-site.com`.

HTTP Strict Transport Security (HSTS) is a policy mechanism preventing the browser from making insecure HTTP requests. However, it is not strictly enforced on first use because the policy is communicated to the browser via an HTTP response header only after the site is accessed. Because the browser is seeing the voting site's URL for the first time, it has no previously cached site security settings to apply. Some browsers may attempt to upgrade the request to secure HTTPS automatically. A network-based attacker in a machine-in-the-middle (MitM) position blocking this request will often result in the browser downgrading to an insecure HTTP to maintain compatibility with legacy HTTP-only websites. Major browsers try to address this gap by maintaining a preloaded list of domains enforcing an HSTS policy, upgrading insecure HTTP connections for any domain on this list. Previous work has noted the relatively widespread prevalence of this gap in the online voting context [13].

4.3 Server-side Attack Detectability

Based on the factors described above, an attacker has a window of opportunity to hijack the voting session during the browser's initial insecure HTTP request. At this point, the attacker could redirect the voter to a malicious site (made to look and function like the genuine voting website) and harvest the login credentials the voter (unwittingly) types in. However, in this basic approach, the attacker has to cast the malicious vote on the voter's behalf using the voter's harvested credentials. However, in our conversation with one of the vendors, they pointed out that if numerous ballots were cast from a single attacker-controlled IP or were cast from IPs outside expected IP address ranges, suspicion would be raised on the server's side. A more sophisticated version of this attack could reduce its forensic footprint by maintaining the direct interaction between the voter's device (and hence IP) and the voting server. A cross-site browser framing attack, which frames the legitimate voting website inside an outer attacker-

Vendor	Insecure Redirects	Site Framing
Dominion	Yes	No
Intelivote	Yes	No
Neuvote	Yes	Yes
Scytl	Yes	Yes (Fixed)
Simply Voting	No	No
Voatz	Yes	No

Table 6: Vulnerability Analysis of Voting Services

controlled domain, would preserve the apparent browser-server interaction.

4.4 Vulnerability Discovery

In late September 2022, many of the Ontario municipal voting websites started to go live. We began examining the login pages of the six vendors for any publicly observable issues. In particular, we visited each login page and examined the security headers in the response. Our analysis found that five of the six vendors were vulnerable to insecure redirects when the voter types an incomplete URL for the first time, because they were not on the HSTS preload list. However, in Scytl's case, we observed that their primary domain (`secured.vote`) did not set any security headers.[7] In particular, we observed Scytl did not set the `Strict-Transport-Security` header (requiring HSTS), and consequently, it was not on the HSTS preload list, allowing the attacker to capture and redirect the voter's initial request for the login page. Additionally, the server did not set the `X-Frame-Options` to deny cross-site framing. We also observed Neuvote did not deny cross-site framing. Our findings are shown in Table 6.

4.5 Exploit and Payload Testing

We tested our attack by deploying two web servers—one legitimate, one malicious. The sites had differing domain names, and TLS was enabled in both. We used a web proxy on a local device to simulate the attacker's MitM position and behavior. We then tested typing the partial URL of the legitimate site in Google Chrome and had the proxy block any HTTPS requests to the legitimate site. We observed the browser sending an insecure HTTP request, and configured the proxy to respond with an `HTTP 301` redirect to the malicious site. We confirmed no browser warnings appeared on the voter's end

[7] `securityheaders.com` gave `secured.vote` a grade of F.

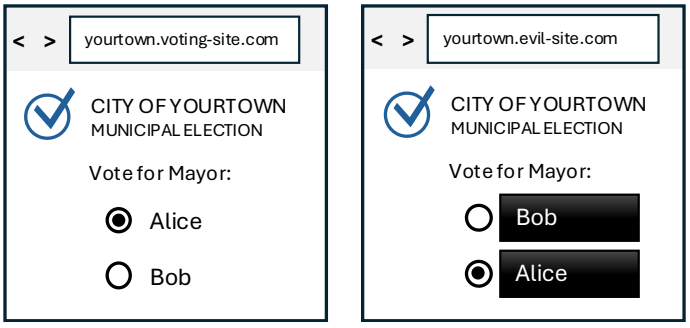

Figure 2: A cross-site framing attack in the election context. **Left**: Legitimate voting website depicting a vote for Alice. **Right**: Voting website framed inside a malicious site applying cross-site overlays (black) to misdirect a voter into voting for Bob instead.

at any point in this process.[8] We then tested and confirmed the ability to frame the legitimate site inside the malicious site, establishing the basic feasibility of the exploit.

The next step was to develop a payload to modify the voter's selections. In the cross-site framing setting, an attacker's options are fortunately limited: The malicious server cannot observe the messages exchanged between the browser and voting server, and cannot directly observe or control the voter's ballot selections in the inner framed site. Based on these limitations, our idea was to apply iframe-based overlays in the malicious outer frame to switch the apparent ordering of candidate names toward misdirecting the voter into casting a ballot for the wrong person. This approach is depicted in Figure 2. However, the attacker does not directly know which page of the inner-framed voting website the voter is currently accessing, and therefore does not know when to activate the name-swapping iframe overlays. We then considered a simple workaround: The malicious outer site provides the voter with explicit instructions to *double*-click all fields and buttons. We then used additional iframe overlays placed on the page-forward buttons to detect when the voter had advanced to the ballot page. This allowed the malicious site to activate the name-swapping overlays only on the intended page. Future work could improve on this approach. Since the adversary is already in a MitM position between the voter and the voting website, a length-based analysis of the TLS-encrypted traffic could be used to infer which page the voter is currently accessing. Previous work has demonstrated the basic feasibility of this approach in the online voting setting [14]. Putting it all together, the protocol-level view of the attack is given in Figure 3.

[8] This was tested on Chrome 128.0.6613.114 and Firefox 129.0.2 with default settings on Windows 10

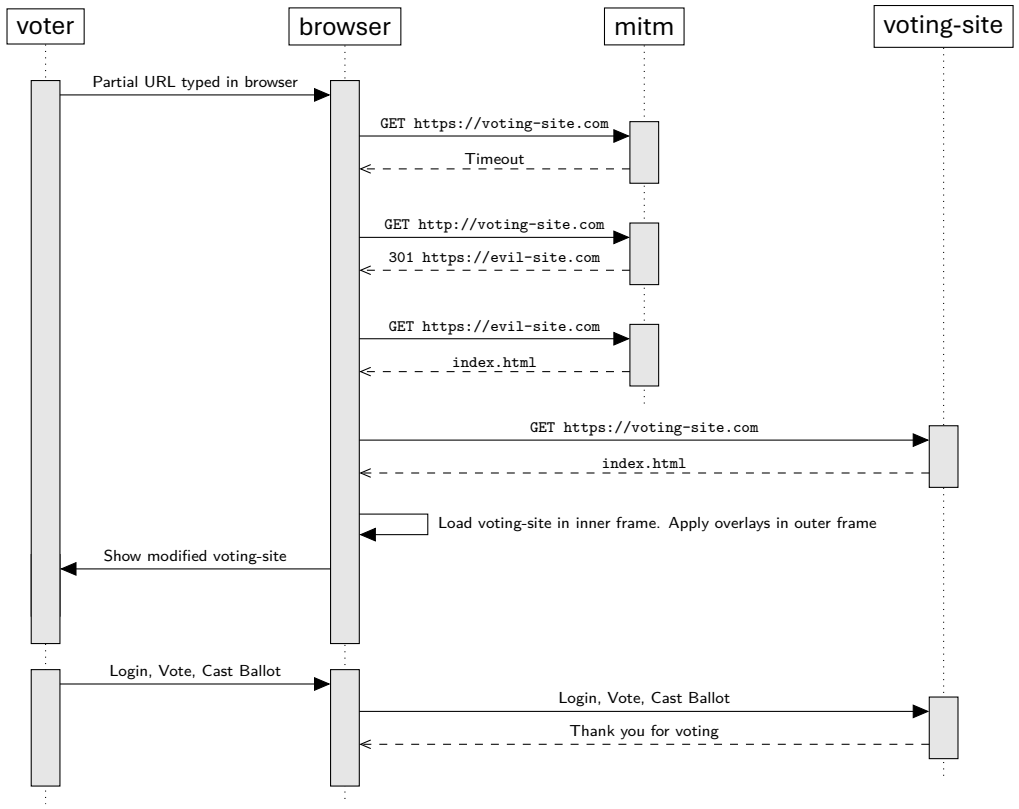

Figure 3: Cross-site framing attack showing a normal voting session (from the voting-site's point of view) despite the site's presentation having been maliciously modified in the voter's browser.

4.6 Coordinated Disclosure and Acknowledgement

After confirming our findings, we initiated a coordinated vulnerability disclosure with Scytl. They promptly responded, and we met on October 14th to discuss the attack and possible mitigation strategies. The following day (October 15th), they enabled their server's `X-Frame-Options` headers, preventing future cross-origin framing. The same day, they sent out an advisory to their municipal clients acknowledging our findings and describing the issue and their mitigation efforts and provided us written permission to publish our results. In Neuvote's case, unfortunately we observed the behavior too late to correct it before the election. This is the first time we have presented these findings publicly, and we are unaware of any ongoing litigation efforts in Ontario pertaining to the 2022 election that would be affected by the publication of this work.

5 DISCUSSION AND CONCLUSION

We provide several recommendations to Ontario municipalities to reduce the future risk of these attacks. However, these findings may be useful to other jurisdictions as well: Most ballots cast in the 2022 municipal election were processed by companies currently running elections in the US, Europe, and elsewhere.

Challenges to Secure Web Sessions in the Election Context

Although the cross-site browser framing vulnerability in Section 4 was mitigated by the vendor enabling a single server security header, the overall attack was due to a combination of multiple security and usability gaps. It was aggravated further by the ephemeral, one-time nature of the voting URL. A standard penetration test would likely have caught the missing security header before the voting period began. Penetration tests are generally not made available to the public. Unfortunately, we do not know if the root cause of the oversight rests with the municipal client, vendor, or pentesting company (if one occurred). The independence of these tests is also an obstacle: Small municipal clients may not have the budget to commission such a test on their own, relying on the vendor to commission their own prior to the procurement process. A recent voluntary national standard for municipal online voting provides guidance on this matter: "In addition to contracted penetration testing, terms and conditions for open-ended adversarial testing of the online voting service should be offered" (see §6.1.7, [15]). The risk of this attack can be further reduced if governments develop a unified and persistent voting portal. Future work should study whether a voter is more likely to notice a URL redirection attack against a domain they have previously used and whether this effect increases over time. At a minimum, reusing domains across election cycles could narrow the attacker's window of opportunity by allowing the voter's browser to enforce previously cached security settings.

Challenges to Secure Voter Credentials

The credential harvesting attack presented in Section 3 is inherent to the approach of automatically mailing every voter a PIN, and full mitigation will likely require a fundamental redesign of the voter authentication method. Ontario municipalities, however, are constrained in how they communicate with voters. Voter lists only contain a voter's name, address and date of birth, making the latter the sole shared 'secret' between the voter and the city. Unfortunately, there appears to be no clear pathway forward at this time. Both Canada and Ontario have no digital identity infrastructure (like in Estonia). As a near-term mitigation strategy, however, the presence of a creden-

tial harvesting attack could be made detectable if municipalities followed up with voters through an independent communication channel, acknowledging when a vote was cast in their name. For example, municipalities could mail a post-election "thank you for voting" letter and instruct the voter to contact the municipality if no such vote was cast by them. Another mitigation option is to require a secondary email-based registration step. In the meantime, we recommend cities apply the metric in Section 3 to determine their risk level and identify any aggravating factors in their context. Second, cities should consider ways to reduce the number of unused discarded VILs, starting with estimating the rate of insecurely discarded VILs and integrating the possibility of credential attacks into their overall election security strategy.

6 ACKNOWLEDGEMENTS

The authors thank Scytl and the anonymous reviewers. This work was supported by NSERC Discovery, SSHRC Grant No. 430-2022-01059, and Brock University's Chancellor's Chair for Research Excellence.

REFERENCES

[1] Association of Municipalities of Ontario, "2022 Municipal Election Results Website," Accessed August 30, 2024. url: elections2022.amo.on.ca.

[2] A. Juels, D. Catalano, and M. Jakobsson, "Coercion-resistant electronic elections," in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society*, pp. 61–70, 2005.

[3] R. Kusters and T. Truderung, "An epistemic approach to coercion-resistance for electronic voting protocols," in *2009 30th IEEE Symposium on Security and Privacy*, pp. 251–266, IEEE, 2009.

[4] S. Delaune, S. Kremer, and M. Ryan, "Coercion-resistance and receipt-freeness in electronic voting," in *19th IEEE Computer Security Foundations Workshop (CSFW'06)*, pp. 12–pp, IEEE, 2006.

[5] J. Clark and U. Hengartner, "Selections: Internet voting with over-the-shoulder coercion-resistance," in *International Conference on Financial Cryptography and Data Security*, pp. 47–61, Springer, 2011.

[6] Tyler Kula, "Challenge to Lambton Shores election dismissed," *The Observer (Sarnia)*, October 6, 2019. url: https://www.theobserver.ca/news/local-news/challenge-to-lambton-shores-election-dismissed.

[7] A. Cardillo, N. Akinyokun, and A. Essex, "Online Voting in Ontario Municipal Elections: A Conflict of Legal Principles and Technology?," in *Electronic Voting: International Joint Conference (E-Vote-ID)*, vol. 11759 of *Lecture Notes in Computer Science*, pp. 67–82, 2019.

[8] Mary Vallis, "So you gave personal info to a company caught in a data breach. Now what?," *CBC News*, July 8, 2023. url: https://www.cbc.ca/news/canada/cybersecurity-consumer-protection-tips-1.6900450.

[9] Tyler Griffin, "Data breach exposed health info on pregnancies and births of 3 million Ontarians," *National Post*, Sep 26, 2023. url: https://nationalpost.com/news/canada/perinatal-child-registry-data-breach-affects-3-million-ontarians.

[10] Maham Abedi , "LifeLabs hack: What Canadians need to know about the health data breach," *Global News*, December 18, 2019. url: https://globalnews.ca/news/6311853/lifelabs-data-hack-what-to-know/.

[11] Ohio Secretary of State, "Statewide voter files download page," 2024. url: https://www6.ohiosos.gov/ords/f?p=VOTERFTP.

[12] Town of Atikokan, "HOW TO VOTE ONLINE in the 2022 Election," 2022. url: https://www.facebook.com/atikokantown/videos/1265289370957760/.

[13] A. Cardillo and A. Essex, "The Threat of SSL/TLS Stripping to Online Voting," in *Electronic Voting: International Joint Conference (E-Vote-ID)*, vol. 11143 of *Lecture Notes in Computer Science*, pp. 35–50, 2018.

[14] J. Brunet, A. D. Pananos, and A. Essex, "Review your choices: When confirmation pages break ballot secrecy in online elections," in *Electronic Voting: 7th International Joint Conference (E-Vote-ID)*, vol. 13553 of *Lecture Notes in Computer Science*, pp. 36–52, 2022.

[15] *Online Voting – Part 1: Implementation of Online Voting in Canadian Municipal Election (CAN/DGSI 111-1)*. Digital Governance Standards Institute, 2024.

7 2022 CITY/VENDOR ONLINE VOTING CENSUS

For the full dataset, including risk score calculations, see our 2022 Ontario Municipal Election Vendor Census: https://github.com/eklass3/ONElectionData_2022

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
Addington Highlands, Township of	4,549	Intelivote	Intelivote	36	TRUE	No suggestion of DOB
Adelaide Metcalfe, Township of	2,464	Intelivote	Intelivote	35	TRUE	No suggestion of DOB
Adjala-Tosorontio, Township of	8,965	N/A	Scytl	32	TRUE	Uses DOB
Ajax, Town of	85,443	Simply Voting	Simply Voting	26	TRUE	No suggestion of DOB
Alfred and Plantagenet, Township of	8,435	Intelivote	Intelivote	24	TRUE	Uses DOB
Algonquin Highlands, Township of	7,923	N/A	Scytl	30	TRUE	No suggestion of DOB
Alnwick/Haldimand, Township of	6,973	Intelivote	Intelivote	30	TRUE	Uses DOB
Amaranth, Township of	3,463	Intelivote	Intelivote	19	FALSE	No suggestion of DOB
Arnprior, Town of	7,504	Intelivote	Voatz	24	TRUE	Uses DOB (d-m-y)
Arran-Elderslie, Municipality of	5,247	N/A	Simply Voting	26	TRUE	Uses DOB (d-m-y)
Ashfield-Colborne-Wawanosh, Township of	5,861	Simply Voting	Simply Voting	30	TRUE	Uses DOB
Asphodel-Norwood, Township of	3,940	Simply Voting	Simply Voting	26	TRUE	Uses DOB (d-m-y)
Atikokan, Town of	2,029	N/A	Scytl	37	TRUE	Does not use DOB
Augusta, Township of	6,133	Intelivote	Intelivote	12	FALSE	Uses DOB (d-m-y)
Aurora, Town of	43,032	Dominion	Dominion	16	FALSE	Uses DOB (y)
Aylmer, Town of	5,455	Intelivote	Intelivote	30	TRUE	No suggestion of DOB
Bancroft, Town of	3,817	N/A	Intelivote	36	TRUE	No suggestion of DOB
Barrie, City of	102,379	N/A	Scytl	28	TRUE	Uses DOB
Belleville, City of	39,602	Dominion	Simply Voting	19	TRUE	Uses DOB (d-m-y)
Black River-Matheson, Township of	2,605	N/A	Intelivote	34	TRUE	No suggestion of DOB
Bluewater, Municipality of	9,060	Simply Voting	Simply Voting	29	TRUE	Uses DOB (d-m-y)
Bradford West Gwillimbury, Town of	27,833	Dominion	Simply Voting	32	TRUE	No suggestion of DOB
Brant, County of	31,038	N/A	Dominion	17	FALSE	Uses DOB (y)
Bracebridge, Town of	16,626	Dominion	Simply Voting	30	TRUE	Uses DOB
Brantford, City of	75,305	Dominion	Dominion	16	FALSE	Uses DOB (y)
Brighton, Municipality of	10,373	N/A	Simply Voting	22	TRUE	Uses DOB (d-m-y)

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
Brockton, Municipality of	8,012	Dominion	Simply Voting	25	TRUE	No suggestion of DOB
Brockville, City of	16,785	Intelivote	Intelivote	25	TRUE	Uses DOB (d-m-y)
Burlington, City of	142,218	Dominion	Voatz	10	FALSE	Uses DOB (d-m-y) + Pre-registration
Calvin, Municipality of	652	N/A	Intelivote	33	TRUE	Uses DOB
Cambridge, City of	95,921	Dominion	Dominion	15	FALSE	Uses DOB (y)
Carleton Place, Town of	9,537	Intelivote	Intelivote	28	TRUE	No suggestion of DOB
Carling, Township of	3,166	Intelivote	Intelivote	31	TRUE	Uses DOB
Carlow/Mayo, Township of	1,371	Intelivote	Intelivote	32	TRUE	No suggestion of DOB
Casselman, Municipality of	3,224	Intelivote	Intelivote	25	TRUE	Uses DOB (d-m-y)
Cavan Monaghan, Township of	8,117	Simply Voting	Simply Voting	23	TRUE	Uses DOB (d-m-y)
Central Frontenac, Township of	7,872	Intelivote	Intelivote	38	TRUE	No suggestion of DOB
Central Huron, Municipality of	6,863	Simply Voting	Simply Voting	27	TRUE	Uses DOB (d-m-y)
Centre Hastings, Municipality of	4,443	Intelivote	Intelivote	32	TRUE	No suggestion of DOB
Centre Wellington, Township of	23,329	Intelivote	Scytl	25	TRUE	Uses DOB
Champlain, Township of	7,491	Intelivote	Intelivote	30	TRUE	Uses DOB (d-m-y)
Chatham-Kent, Municipality of	80,332	Dominion	Dominion	15	FALSE	Uses DOB (y)
Clarence-Rockland, City of	19,997	Intelivote	Intelivote	27	TRUE	Uses DOB
Clarington, Municipality of	73,471	N/A	Simply Voting	26	TRUE	Uses DOB
Clearview, Township of	12,993	Intelivote	Dominion	17	FALSE	Uses DOB (y)
Cobourg, Town of	16,737	Intelivote	Intelivote	20	TRUE	Uses DOB (d-m-y)
Cochrane, Town of	4,184	N/A	Intelivote	9	FALSE	Uses DOB (d-m-y)
Collingwood, Town of	22,189	Dominion	Dominion	12	FALSE	Uses DOB (y)
Cramahe, Township of	5,627	N/A	Intelivote	33	TRUE	Uses DOB (d-m-y)
Deep River, Town of	3,282	Simply Voting	Simply Voting	29	TRUE	Uses DOB (d-m-y)
Douro-Dummer, Township of	7,230	Simply Voting	Simply Voting	28	TRUE	Uses DOB
Dryden, City of	5,422	Simply Voting	Simply Voting	29	TRUE	Uses DOB
Dysart Et Al, Municipality of	9,588	N/A	Scytl	29	TRUE	No suggestion of DOB
Ear Falls, Township of	685	N/A	Simply Voting	34	TRUE	No suggestion of DOB
East Gwillimbury, Town of	25,300	N/A	Scytl	14	FALSE	No suggestion of DOB
East Hawkesbury, Township of	2,905	N/A	Intelivote	32	TRUE	No suggestion of DOB
East Zorra-Tavistock, Township of	5,900	Intelivote	Intelivote	26	TRUE	Uses DOB (d-m-y)
Edwardsburgh/Cardinal, Township of	5,503	Intelivote	Intelivote	8	FALSE	Uses DOB (d-m-y)
Elizabethtown-Kitley, Township of	8,242	Intelivote	Intelivote	12	FALSE	Uses DOB (d-m-y)
Espanola, Town of	4,075	N/A	Scytl	35	TRUE	Uses DOB

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
Fort Frances, Town of	5,317	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)
French River, Municipality of	4,054	N/A	Intelivote	34	TRUE	No suggestion of DOB
Frontenac Islands, Township of	2,319	Intelivote	Intelivote	14	FALSE	No suggestion of DOB
Gananoque, Separated Town of	4,429	Intelivote	Intelivote	33	TRUE	No suggestion of DOB
Georgian Bay, Township of	9,252	Dominion	Simply Voting	30	TRUE	No suggestion of DOB
Georgian Bluffs, Township of	10,638	Dominion	Scytl	13	FALSE	Uses DOB
Georgina, Town of	36,970	N/A	Scytl	14	FALSE	Uses DOB
Goderich, Town of	6,552	Simply Voting	Simply Voting	27	TRUE	Uses DOB
Grand Valley, Town of	2,866	Intelivote	Intelivote	34	TRUE	Uses DOB (d-m-y)
Gravenhurst, Town of	14,704	Dominion	Simply Voting	30	TRUE	No suggestion of DOB
Greater Madawaska, Township of	5,232	Simply Voting	Voatz	32	TRUE	Uses DOB
Greater Napanee, Town of	12,718	Intelivote	Intelivote	31	TRUE	No suggestion of DOB
Greenstone, Municipality of	2,951	Intelivote	Intelivote	35	TRUE	Uses DOB (d-m-y)
Grey Highlands, Municipality of	10,465	Dominion	Dominion	16	FALSE	Uses DOB (y)
Grimsby, Town of	23,920	Simply Voting	Voatz	7	FALSE	Uses DOB (d-m-y)
Haldimand County	40,868	N/A	Dominion	12	FALSE	Uses DOB (y)
Halton Hills, Town of	46,980	N/A	Dominion	16	FALSE	Uses DOB (y)
Hamilton, Township of	9,567	Intelivote	Intelivote	29	TRUE	Uses DOB (d-m-y)
Hanover, Town of	6,115	Dominion	Scytl	29	TRUE	No suggestion of DOB
Hastings Highlands, Municipality of	6,689	Intelivote	Intelivote	32	TRUE	Uses DOB
Havelock-Belmont-Methuen, Township of	7,498	Simply Voting	Simply Voting	14	FALSE	Uses DOB (d-m-y)
Highlands East, Municipality of	9,099	N/A	Scytl	30	TRUE	No suggestion of DOB
Huntsville, Town of	20,837	Dominion	Simply Voting	26	TRUE	No suggestion of DOB
Huron East, Municipality of	7,562	Simply Voting	Simply Voting	27	TRUE	Uses DOB (d-m-y)
Huron Shores, Municipality of	2,351	N/A	Scytl	37	TRUE	Uses DOB
Huron-Kinloss, Township of	7,407	Dominion	Simply Voting	31	TRUE	No suggestion of DOB
Ignace, Township of	1,049	N/A	Neuvote	26	TRUE	Uses DOB (d-m-y)
Innisfil, Town of	32,770	Dominion	Scytl	37	TRUE	No suggestion of DOB
Kawartha Lakes, City of	71,517	Dominion	Scytl	24	TRUE	Uses DOB (d-m-y)
Kenora, City of	11,143	Simply Voting	Simply Voting	18	TRUE	Uses DOB (d-m-y)
Killarney, Municipality of	1,373	Intelivote	Intelivote	38	TRUE	No suggestion of DOB
Kincardine, Municipality of	10,884	Dominion	Simply Voting	20	TRUE	Uses DOB (d-m-y)

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
Kingston, City of	96,204	Dominion	Voatz	9	FALSE	Uses DOB (d-m-y) + Pre-registration
Lake of Bays, Township of	8,265	Dominion	Simply Voting	25	TRUE	Uses DOB (d-m-y)
Lambton Shores, Municipality of	12,199	Intelivote	Scytl	30	TRUE	No suggestion of DOB
Lanark Highlands, Township of	7,116	Intelivote	Intelivote	16	FALSE	No suggestion of DOB
LaSalle, Town of	25,702	Intelivote	Scytl	24	TRUE	No Suggestion of DOB
Leeds and the Thousand Islands, Township of	10,221	Intelivote	Intelivote	13	FALSE	Uses DOB (d-m-y)
Limerick, Township of	1,075	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)
Lincoln, Town of	20,087	Dominion	Dominion	17	FALSE	Uses DOB (y)
Loyalist Township	13,665	Intelivote	Intelivote	11	FALSE	Uses DOB (d-m-y)
Lucan Biddulph, Township of	4,199	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)
Madoc, Township of	2,069	N/A	Intelivote	30	TRUE	Uses DOB (d-m-y)
Magnetawan, Municipality of	3,689	N/A	Intelivote	16	FALSE	Uses DOB (d-m-y)
Malahide, Township of	6,542	N/A	Intelivote	37	TRUE	No suggestion of DOB
Manitouwadge, Township of	1,527	N/A	Scytl	30	TRUE	No Suggestion of DOB
Mapleton, Township of	7,034	N/A	Dominion	21	FALSE	Uses DOB (y)
Marathon, Town of	2,468	N/A	Scytl	31	TRUE	No Suggestion of DOB
Markham, City of	220,234	Scytl	Scytl	12	FALSE	No Suggestion of DOB
Marmora and Lake, Municipality of	4,844	Intelivote	Intelivote	29	TRUE	Uses DOB (d-m-y)
McDougall, Municipality of	3,826	Intelivote	Intelivote	28	TRUE	Uses DOB (d-m-y)
McKellar, Township of	3,213	Intelivote	Intelivote	27	TRUE	Uses DOB (d-m-y)
McNab/Braeside, Township of	6,831	Intelivote	Voatz	27	TRUE	Uses DOB (m-y)
Melancthon, Township of	2,545	Intelivote	Intelivote	32	TRUE	Uses DOB (d-m-y)
Merrickville-Wolford, Village of	2,889	Intelivote	Intelivote	10	FALSE	Uses DOB (d-m-y)
Middlesex Centre, Municipality of	14,313	Intelivote	Intelivote	27	TRUE	Uses DOB (d-m-y)
Midland, Town of	14,301	N/A	Intelivote	29	TRUE	No suggestion of DOB
Minden Hills, Township of	12,019	Intelivote	Scytl	16	FALSE	No Suggestion of DOB
Mississippi Mills, Municipality of	12,365	Intelivote	Intelivote	22	TRUE	Uses DOB (d-m-y)
Mono, Town of	7,486	Intelivote	Intelivote	30	TRUE	Uses DOB (d-m-y)
Montague, Township of	3,458	Intelivote	Intelivote	26	TRUE	Uses DOB (d-m-y)
Morris-Turnberry, Municipality of	2,978	Simply Voting	Simply Voting	36	TRUE	No suggestion of DOB
Mulmur, Township of	3,626	Intelivote	Intelivote	30	TRUE	Uses DOB (d-m-y)
Muskoka Lakes, Township of	17,174	Dominion	Simply Voting	22	TRUE	Uses DOB (d-m-y)
New Tecumseth, Town of	31,731	N/A	Dominion	15	FALSE	Uses DOB (y)
Newmarket, Town of	61,370	Scytl	Voatz	13	FALSE	No suggestion of DOB

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
North Bay, City of	41,418	N/A	Simply Voting	6	FALSE	Uses DOB (d-m-y)
North Dumfries, Township of	8,419	Intelivote	Dominion	21	FALSE	Uses DOB (y)
North Dundas, Township of	8,716	Intelivote	Intelivote	24	TRUE	Uses DOB (d-m-y)
North Frontenac, Township of	6,195	N/A	Intelivote	35	TRUE	Uses DOB
North Glengarry, Township of	8,316	Intelivote	Intelivote	15	FALSE	Uses DOB (d-m-y)
North Grenville, Municipality of	14,378	Intelivote	Intelivote	7	FALSE	Uses DOB (d-m-y)
North Huron, Township of	4,016	Simply Voting	Simply Voting	32	TRUE	Uses DOB
North Kawartha, Township of	6,774	Simply Voting	Simply Voting	31	TRUE	No suggestion of DOB
North Middlesex, Municipality of	4,361	Intelivote	Intelivote	30	TRUE	Uses DOB (d-m-y)
North Stormont, Township of	4,987	Intelivote	Intelivote	24	TRUE	Uses DOB (d-m-y)
Northern Bruce Peninsula, Municipality of	9,682	Dominion	Simply Voting	28	TRUE	No suggestion of DOB
Oliver Paipoonge, Municipality of	5,212	N/A	Intelivote	25	TRUE	Uses DOB (d-m-y)
Otonabee-South Monaghan, Township of	6,356	Simply Voting	Simply Voting	32	TRUE	No suggestion of DOB
Owen Sound, City of	15,690	Dominion	Simply Voting	26	TRUE	No suggestion of DOB
Parry Sound, Town of	5,257	Intelivote	Intelivote	32	TRUE	No suggestion of DOB
Pembroke, City of	10,375	Dominion	Voatz	13	FALSE	Uses DOB (m-y)
Penetanguishene, Town of	7,725	Dominion	Scytl	36	TRUE	No suggestion of DOB
Perth East, Township of	8,727	Simply Voting	Simply Voting	32	TRUE	Uses DOB
Perth, Town of	5,407	Intelivote	Intelivote	30	TRUE	Uses DOB
Petawawa, Town of	12,440	Dominion	Voatz	16	FALSE	Uses DOB (m-y)
Peterborough, City of	65,703	Dominion	Dominion	11	FALSE	Uses DOB (y)
Petrolia, Town of	4,567	Intelivote	Scytl	13	FALSE	No Suggestion of DOB
Pickering, City of	76,021	Dominion	Dominion	16	FALSE	Uses DOB (y)
Plympton-Wyoming, Town of	7,247	Intelivote	Scytl	31	TRUE	No suggestion of DOB
Point Edward, Village of	1,668	Intelivote	Scytl	31	TRUE	No Suggestion of DOB
Port Hope, Municipality of	14,420	Intelivote	Intelivote	26	TRUE	Uses DOB
Prescott, Town of	3,374	Intelivote	Intelivote	15	FALSE	Uses DOB (d-m-y)
Prince Edward, County of	23,935	Dominion	Dominion	10	FALSE	Uses DOB (y)
Quinte West, City of	35,607	Dominion	Simply Voting	39	TRUE	Uses DOB
Ramara, Township of	11,869	Intelivote	Intelivote	10	FALSE	Uses DOB (d-m-y)
Red Lake, Municipality of	2,807	Simply Voting	Simply Voting	26	TRUE	Uses DOB (d-m-y)
Renfrew, Town of	6,459	Dominion	Voatz	12	FALSE	Uses DOB (m-y)
Richmond Hill, City of	130,714	N/A	Dominion	14	FALSE	Uses DOB (y)
Rideau Lakes, Township of	12,876	Intelivote	Intelivote	36	TRUE	Uses DOB
Russell, Township of	15,272	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
Sables-Spanish Rivers, Township of	3,302	N/A	Scytl	39	TRUE	Uses DOB
Sarnia, City of	54,148	Intelivote	Scytl	19	TRUE	No Suggestion of DOB
Saugeen Shores, Town of	13,883	Dominion	Simply Voting	29	TRUE	Uses DOB
Scugog, Township of	18,318	N/A	Dominion	18	FALSE	Uses DOB (y)
Seguin, Township of	9,032	Intelivote	Intelivote	28	TRUE	Uses DOB (d-m-y)
Selwyn, Township of	16,903	Simply Voting	Simply Voting	26	TRUE	Uses DOB (d-m-y)
Severn, Township of	14,147	N/A	Intelivote	14	FALSE	Uses DOB
Shelburne, Town of	5,823	Intelivote	Intelivote	33	TRUE	No suggestion of DOB
Shuniah, Municipality of	3,965	Intelivote	Intelivote	30	TRUE	Uses DOB (d-m-y)
Sioux Lookout, Municipality of	3,185	Simply Voting	Simply Voting	40	TRUE	Uses DOB
Smiths Falls, Town of	6,840	Intelivote	Intelivote	30	TRUE	No suggestion of DOB
South Bruce Peninsula, Town of	13,160	N/A	Simply Voting	22	TRUE	Uses DOB (d-m-y)
South Bruce, Municipality of	4,893	Dominion	Simply Voting	27	TRUE	No suggestion of DOB
South Dundas, Municipality of	8,510	Intelivote	Intelivote	7	FALSE	Uses DOB (d-m-y)
South Frontenac, Township of	18,116	Intelivote	Intelivote	31	TRUE	Uses DOB
South Glengarry, Township of	10,757	Intelivote	Intelivote	20	TRUE	Uses DOB (d-m-y)
South Huron, Municipality of	8,200	Simply Voting	Simply Voting	27	TRUE	No suggestion of DOB
South Stormont, Township of	10,782	Intelivote	Intelivote	7	FALSE	Uses DOB (d-m-y)
South-West Oxford, Township of	5,661	Intelivote	Intelivote	28	TRUE	Uses DOB (d-m-y)
Southgate, Township of	6,568	Dominion	Scytl	38	TRUE	No suggestion of DOB
Southwest Middlesex, Municipality of	4,552	Intelivote	Intelivote	26	TRUE	Uses DOB (d-m-y)
Springwater, Township of	17,504	Dominion	Scytl	30	TRUE	No suggestion of DOB
St. Thomas, City of	31,103	Simply Voting	Simply Voting	25	TRUE	Uses DOB (d-m-y)
Stirling-Rawdon, Township of	4,259	N/A	Intelivote	28	TRUE	Uses DOB (d-m-y)
Stone Mills, Township of	7,407	Intelivote	Intelivote	14	FALSE	Uses DOB (d-m-y)
Stratford, City of	26,554	Simply Voting	Simply Voting	24	TRUE	Uses DOB
Strathroy-Caradoc, Municipality of	18,111	Intelivote	Intelivote	28	TRUE	No suggestion of DOB
Tay Valley Township	6,224	Intelivote	Intelivote	31	TRUE	Uses DOB (d-m-y)
Tecumseh, Town of	19,689	Intelivote	Scytl	27	TRUE	No Suggestion of DOB
Temiskaming Shores, City of	8,113	N/A	Intelivote	9	FALSE	Uses DOB (d-m-y)
Thames Centre, Municipality of	11,166	Intelivote	Intelivote	20	TRUE	Uses DOB (d-m-y)
The Blue Mountains, Town of	13,903	Dominion	Scytl	26	TRUE	No Suggestion of DOB
The Nation Municipality	10,288	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)

Municipality	Eligible Voters (2022)	2018 Online Voting Vendor	2022 Online Voting Vendor	Credential Risk Score	High Risk (≥ 20)	2022 DOB credential
The North Shore, Township of	669	N/A	Simply Voting	34	TRUE	No suggestion of DOB
Thorold, City of	18,269	N/A	Dominion	19	FALSE	Uses DOB (y)
Thunder Bay, City of	83,010	Intelivote	Dominion	10	FALSE	Uses DOB (y)
Tillsonburg, Town of	14,287	Intelivote	Intelivote	23	TRUE	Uses DOB (d-m-y)
Timmins, City of	30,765	Dominion	Dominion	14	FALSE	Does not use DOB
Trent Hills, Municipality of	12,672	Intelivote	Intelivote	33	TRUE	No suggestion of DOB
Trent Lakes, Municipality of	11,743	Simply Voting	Simply Voting	16	FALSE	No suggestion of DOB
Tudor and Cashel, Township of	1,728	Intelivote	Intelivote	34	TRUE	No suggestion of DOB
Tweed, Municipality of	6,199	Intelivote	Intelivote	26	TRUE	Uses DOB (d-m-y)
Tyendinaga, Township of	3,798	N/A	Voatz	31	TRUE	Uses DOB (m-y)
Vaughan, City of	225,983	N/A	Scytl	13	FALSE	No Suggestion of DOB
Warwick, Township of	2,737	Intelivote	Scytl	33	TRUE	No suggestion of DOB
Wasaga Beach, Town of	23,836	Intelivote	Dominion	9	FALSE	Uses DOB (y)
Wawa, Municipality of	2,067	Intelivote	Intelivote	36	TRUE	No suggestion of DOB
Wellesley, Township of	8,402	Dominion	Scytl	30	TRUE	No Suggestion of DOB
West Elgin, Municipality of	4,401	Intelivote	Intelivote	29	TRUE	Uses DOB (d-m-y)
West Grey, Municipality of	11,667	Dominion	Simply Voting	29	TRUE	No suggestion of DOB
West Lincoln, Township of	12,727	N/A	Voatz	9	FALSE	No suggestion of DOB
West Perth, Municipality of	6,963	Dominion	Voatz	32	TRUE	No suggestion of DOB
Whitestone, Municipality of	3,721	Intelivote	Intelivote	13	FALSE	Uses DOB (d-m-y)
Whitewater Region, Township of	6,344	Dominion	Voatz	13	FALSE	Uses DOB (m-y)
Wilmot, Township of	17,110	N/A	Scytl	9	FALSE	No Suggestion of DOB
Wollaston, Township of	2,555	N/A	Intelivote	29	TRUE	Uses DOB (d-m-y)
Woolwich, Township of	19,885	Dominion	Scytl	11	FALSE	No Suggestion of DOB
Zorra, Township of	6,632	N/A	Intelivote	29	TRUE	Uses DOB (d-m-y)