4-2024

Guardians of the Ballot Box: Addressing Cybersecurity Vulnerabilities and Privacy Concerns for Local Election Officials in Digital Spaces

Steven Windisch

Adrienne Brookstein

Steven Chen

Adan Vela

National Counterterrorism Innovation, Technology, and Education Center

Guardians of the Ballot Box

Addressing Cybersecurity Vulnerabilities and Privacy Concerns for Local Election Officials in Digital Spaces

Research Team

- Steven Windisch, Assistant Professor, Department of Criminal Justice, Temple University
- Adrienne Brookstein, Doctoral Student, Department of Criminal Justice, Temple University
- Steven Chen, Doctoral Student, Department of Criminal Justice, Temple University
- Adan Vela, Associate Professor, Department of Industrial Engineering and Management Systems, University of Central Florida

Overview

Throughout the 2020 U.S. election, nefarious actors sought to discover "the truth" about "irregularities" from mail-in balloting and the perceived "clandestine" vote certification process. In many cases, the line between political activism and political extremism dissolved, whereby local election officials (LEOs) reported being followed, threatened with violence, and falsely accused of "stealing" the election via phone, mail, email, and social media platforms. Ultimately, numerous LEOs would require protection from law enforcement and, in some cases, choose to resign.

Online platforms have revolutionized the way LEOs interact with citizens, offering unprecedented opportunities for engagement and dialogue. However, among the benefits lie inherent risks, particularly concerning safety and privacy. One primary concern is the inadvertent disclosure of sensitive personal information by users themselves. Despite privacy settings and platform features aimed at safeguarding personal data, users may unknowingly expose details such as their whereabouts, daily routines, or connections, which could be exploited by individuals with malicious intent. Such information can serve as a blueprint for verbal or physical harassment, posing significant threats to the safety and well-being of elected officials. The ubiquity of social media usage opens avenues for unintentional disclosure of personal information, which malicious actors can leverage for nefarious purposes.

Our study delves into the intricate landscape of cybersecurity vulnerabilities, with a specific focus on LEOs. Through the lens of Open-Source Intelligence (OSINT), we aim to identify and dissect potential weaknesses that adversaries could exploit to target politicians. By meticulously analyzing the nuances of social media usage within the political sphere, our study endeavors to highlight vulnerabilities and propose mitigation strategies. This includes advocating for enhanced user education and awareness, platform-level security enhancements, and proactive monitoring and response mechanisms to swiftly identify and neutralize potential threats.

Interim Findings

Findings from the OSINT trials highlight the abundance of personal information online. Most participants had nine or more variables exposed, revealing the extensive digital footprints people leave. The study unveils alarming trends, with sensitive information like work addresses and phone numbers found rapidly. Sources varied, with mainstream websites and governmental platforms being vulnerable. These findings stress the importance of cybersecurity measures and user education to protect privacy and security in the evolving digital landscape.

Key Findings:

- In total, 91% (n = 100) of OSINT variables were discovered across the ten red-teaming trials.
- We discovered nine or more OSINT variables for eight participants.
- We discovered every (n = 10; 100%) participant's: (1) work phone number, (2) work address, (3) home phone number, (4) home address (5) marital status, (6) date of birth, and (7) political affiliation.
- In 80% of the trials, we found participants' work addresses and work phone numbers in less than three minutes.
- In 70% of the trials, we found participants' home addresses and home phone numbers in less than fifteen minutes.
- In 55% of trials, we found participants' marital status and date of birth in less than twenty minutes.
- The majority (n = 63; 57%) of OSINT variables were discovered on "mainstream" websites such as Wikipedia, LinkedIn, and Instagram.
- Over a third (n = 37; 34%) of OSINT variables were discovered on "governmental or official websites" such as "house.gov," "census.gov," or "USA.gov."
- Over half (60%) of the samples' personal social media accounts were "public" and over three-quarters (90%) of the samples' work social media accounts were "public."

Policy Implications

- These findings carry significant policy implications. **First, the ease with which sensitive personal information can be obtained underscores the need for robust data privacy regulations.** Governments may need to reassess and strengthen existing laws to ensure individuals' privacy rights are adequately protected in the digital age.
- **Second, governments should prioritize investments in cybersecurity measures to safeguard against unauthorized access to personal information.** This includes enhancing encryption standards, implementing multi-factor authentication, and improving cybersecurity training for individuals and organizations.
- **Third, there is a need for greater transparency and accountability from both public and private entities that collect and handle personal data.** Clear guidelines and standards should be established for the responsible handling of sensitive information, with mechanisms in place to hold accountable those who fail to comply.
- **Fourth, there is a necessity for widespread educational initiatives to raise awareness about online privacy risks and best practices for protecting personal information.** This includes integrating digital literacy and cybersecurity education into school curricula and providing resources for ongoing public awareness campaigns.
- **Finally, given that a significant portion of OSINT variables were found on mainstream and social media platforms, policymakers may consider implementing stricter regulations on these platforms to prevent the misuse of personal data and ensure users have greater control over their privacy settings**.

Methodology

We conducted ten red-teaming trials on Google's Incognito browser, ensuring private browsing to prevent the retention of browsing history, cookies, and site data. At the onset of each trial, the PI provided the red teamers with the participant's first and last name and the state of service. Each trial was initiated using only this information. Beyond the initial search query, red teamers then integrated systematic search strategies with an iterative approach to facilitate comprehensive and dynamic information gathering aligned with our research objectives.

The red-teaming trials were structured into phases, each targeting specific information, including workplace information, personal addresses and information, and social media accounts, and determining if they had received threats or been targeted. Predefined objectives and potential websites guided search queries within each phase. Concurrently, the process was iterative, with newly discovered information incorporated into subsequent search queries to refine and expand the scope.

In adherence to Institutional Review Board protocols, non-personal computers in the department's computer lab were utilized to ensure subject privacy, guaranteeing that the research team had no access granted to personal accounts. Throughout the trials, the red team was not authorized to log into social media or people finder websites to gather information. This ensured that everyone could access the data collected, maintaining transparency and accountability in the research process. Finally, data was recorded and timestamped on paper, ensuring an auditable record of each trial.

Future Directions

Future research directions in light of these findings could include:

1. Investigating the real-world implications of the ease of access to personal information, such as instances of identity theft, stalking, or political manipulation;
2. Developing and evaluating technological solutions to enhance online privacy protection, such as advanced encryption methods and privacy-preserving algorithms. Research could focus on the feasibility, usability, and effectiveness of these solutions in mitigating privacy risks; and
3. Investigating factors influencing individuals' decisions to share personal information online and their awareness of privacy risks. Understanding user behavior can inform the design of more effective privacy controls, awareness campaigns, and educational interventions. By pursuing these research directions, scholars can contribute to a deeper understanding of the challenges associated with online privacy, ultimately informing the development of more effective policies, technologies, and interventions to protect individuals' privacy rights.

Grant Acknowledgement and Disclaimer: This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 20STTPC00001-04-00. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security or the University of Nebraska at Omaha.