CYBERDEFENSES

2020 ELECTION MISINFORMATION

HOW SOCIAL MEDIA AND SEARCH ENGINES HELPED FUEL MISINFORMATION AND DISINFORMATION CYBER ATTACKS

The 2020 Presidential Election was unique for its intensity and controversy, and a contributing factor was the constant stream of election misinformation and disinformation on the internet, social media platforms and mobile messaging apps.

Leading up to, during and after the Presidential Election, our cyber intelligence team tracked cybercriminal and election cyberthreat actor darknet activity from both known cybercrime groups and new adversaries with election tampering agendas. One of the most prevalent attacks the team observed was planned misinformation and disinformation campaigns on the internet and social media channels. These campaigns were fueled by the swift propagation of facts and false information enabled by widespread social media sharing and high search engine rankings.

While election officials were using the internet and social media to inform voters about voter registration, how and where to vote and tabulation results, cyber attackers were simultaneously using the same platforms and marketing communication tactics, including social posts and search engine optimization (SEO), to amplify false or slightly false information. The result was an environment in which it was difficult for voters to sift through the streams of information and discern the facts.

In this way, digital channels became a platform that adversaries and cybercriminals could exploit to influence social behavior and election results.

Misinformation and disinformation attacks can be difficult for election officials and state offices to combat. Countering this requires voting officials to thoroughly control their message and consistently guide voters to trusted, legitimate sources of information. Fighting this form of election attack goes beyond the purview of state and local election officials. It requires the full support of internet and social media platforms to help legitimate information sources have a strong presence

THE IMPACT OF SOCIAL MEDIA ON ELECTIONS

It is well established that specific terms in social messaging can impact elections. The results of a study published by Nature in 2012, showed that terms and images that reflected election and voting topics directly influenced the information-seeking and real-world voting behavior of millions of people. Equally, this transmission of thought not only influenced the individuals who viewed them but also influenced the direct and indirect circles of social connections.

In the Nature study, 611,000 Facebook users received a social message at the top of their news feed encouraging them to vote and to share the fact that they voted with their Facebook friends. The researchers estimate that the message directly increased voter turnout by 60,000 votes. But a further 280,000 people were indirectly nudged to the polls by news feed posts informing them that their friends had clicked an “I voted” button.

Social media adds another layer to an already crowded and diverse media environment by blurring the lines between information producers, news media, and citizens, and by providing a space that serves both social and entertainment purposes, as well as fulfilling political and informational purposes.

Social media has fundamentally changed how election information is consumed. It allows people to maintain large social networks, which primarily comprise loose ties formed by friends, associates, acquaintances, and colleagues from different stages in life. The information sharing aspect of social media means individuals can be influenced by a broad swath of misinformation or disinformation that is being spread inadvertently and extensively through their personal networks.

Social media posts inherently contain little context which means they may not include some of the visual and contextual cues that have been shown to help users decipher the credibility of online news, such as links to a source, or independent fact-checks.

THE POWERFUL ROLE SEO PLAYS IN ELECTIONS

Internet search services join social media platforms in their ability not only to influence voter behavior, but also to amplify this influence exponentially. Search engines help voters find information on political candidates, polling times, and how and where to vote. Users scanning search query results click on links in predictable patterns, giving special emphasis to results at the top of the list and on the first page.

Companies spend billions of dollars on SEO to capitalize on these user behavior patterns and push their website pages to the top of query results. They are not alone, either. Criminal organizations, nation-states, and external influencers expend significant resources to perform the same function, driving an increase in the consumption of malicious or erroneous information, and in some cases, even malware. As a result, criminals can influence which links a user is most likely to click, which in turn affects user beliefs and behaviors around products, topics, and issues.

In a 2015 study titled the Search Engine Manipulation Effect and its Possible Impact on the Outcomes of Elections, researchers from the American Institute for Behavioral Research and Technology found that voter preferences can be altered by 20 percent or more by manipulating search engine results to favor one candidate over another. Additionally, when search engines favor certain results over others, the results “might interact synergistically with the process by which voter preferences affect search rankings, thus creating a sort of digital bandwagon effect.” A simple conclusion to this study is that “unregulated election-related search rankings could pose a significant threat to the democratic system of government.”

ESTABLISHING AND MAINTAINING AN AUTHORITATIVE VOICE OF TRUTH

It would seem at first glance that election officials hold the primary burden of combatting election misinformation and disinformation attacks; however, the complexity of the issue requires the help of search engine companies and social platforms. Motivated cybercriminals and election cyber-threat actors are using increasingly sophisticated methods and resources. Additionally, election communication departments have only a few owned media channels through which to share facts. But the internet and social media landscape where people consume information, both factual and false, is vast.

There are many things that internet and social media platform companies can do to effectively

fight election misinformation attacks. Social media platforms can help users determine if information is factual even if it is not possible for the platforms to perform fact checking because of privacy concerns that properly prevent the exposure of identity data. Social media channels can adjust their interfaces to enable more contextual information that would help users determine whether or not information is from a credible source before they share it.

Additionally, online platforms can help election officials maintain an authoritative position by supporting paid search engine content placement leading up to, during and after an election. This would help election communications teams gain a foothold in their offensive against organizations, including cyber threat actors, that use advanced organic SEO tactics to gain a larger influence on search engine rankings.

There are also significant things that election officials can do to curb the impact of misinformation and disinformation campaigns.

- **Make Election Information a Year-Round Focus**
  Focus on election information campaigns as much during non-election years as during election years so there is a consistent effort to establish your channels as the authority.
- **Devote Staff and Financial Resources to Election Information**
  Dedicate resources to SEO efforts to ensure high visibility during election cycles.
- **Direct Voters to a Single Source of Truth**
  No matter what channel voters are using to engage with you, link them to your website as the single source of all legitimate information.
- **Enlist Darknet Investigation Services**
  Hire a cybersecurity intelligence company to search the internet for copycat do mains and the darknet for misinformation and disinformation campaigns that could impact your jurisdiction.

Election security is multi-faceted. Protecting your technology and election equipment against attacks and tampering is just one element. There is a growing need and urgency to protect election information, and it requires vigilance and action from all of us, election officials, digital platform providers, and citizens.

1 Nature, 61-Million person experiment in social influence political mobilization, Robert M. Bond, Christopher J. Fariss, Jason J. Jones, Adam D I Kramer, Cameron Marlow, Jaime E Settle and James H Folwer. https://www.nature.com/articles/nature11421
2 Epstein, Robert, & Robertson, Ronald E. (2015). The Search Engine Manipulation Effect (SEME) and its Possible Impact on the Outcomes of Elections, https://aibrt.org/downloads/EPSTEIN_&_ROBERTSON_2015-The_Search_Engine_Manipulation_Effect-SEME-PNAS-w_SUPPLEMENTS.pdf

CyberDefenses is an award-winning Top 100 Managed Security services Provider (MSSP) and a leader in election security. Leading up to the 2020 Presidential Election, we worked with more than 400 counties and multiple states throughout the country to help increase election security. CyberDefenses provided Election Security Assessments, Best Practice Guides, Incident Response Plans, Policies, Training, and Election Threat Darknet Intelligence services.