Election Security: How Information (and Misinformation) Play a Role

NCSL Capitol Forum
Executive Committee Task Force On Cybersecurity
December 9, 2019
Overview

CDT’s Election Privacy & Security Project
Priorities in 2020
Voter Confidence
Defining Misinformation
Understanding Misinformation
You Make The Call

Examples
Evaluating Content
Sources
What You Can Do
Resources
Introduction to CDT’s Election Privacy & Security Project

About CDT

At the Center of Democracy and Technology, we believe in the power of the internet. Whether it’s facilitating entrepreneurial endeavors, providing access to new markets and opportunities, or creating a platform for free speech, the internet empowers, emboldens, and equalizes people around the world.

Election Privacy & Security Project

The project addresses key election cybersecurity issues, such as election official training, technical volunteer capacity building, social media disinformation campaigns, and robust post-election auditing, by crafting resources for election officials. It is led by Maurice Turner, Deputy Director & Senior Technologist.
Priorities in 2020

Cybersecurity 101 & Risk-limiting Audit Training for Election Officials
Assess the level of cybersecurity awareness of election officials; Identify and adapt existing training materials to meet specific needs of election officials; Deliver adapted training.

Building Bridges between Election Officials, Stakeholders, Vendors, & Information Security Professionals
Assist officials in identifying civic-minded individuals or organizations (schools, associations, companies, State National Guard) with technical skills in the areas of security research and network or systems administration interested in acting as technical volunteers; Reduce tensions impeding progress on common values and issues across the community.

Modern Standards & Alternative Voting Systems
Advocate for a regulatory system that streamlines innovation allowing for rapid development by incumbents and newcomers, including the use of open-source software & commercial-off-the-shelf hardware.
Voter Confidence

VOTER CONFIDENCE

Misinformation
Changing votes
Disruption
## Defining Misinformation

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Intent to Cause Harm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mis-information</strong></td>
<td>False</td>
</tr>
<tr>
<td><strong>Dis-information</strong></td>
<td>False</td>
</tr>
<tr>
<td><strong>Mal-information</strong></td>
<td>True</td>
</tr>
</tbody>
</table>
Understanding Misinformation

AUTHENTICITY

Misinformation
Unintentional mistakes such as inaccurate photo captions, dates, statistics, translations, or when satire is taken seriously.

Disinformation
Fabricated or deliberately manipulated audio/visual content. Intentionally created conspiracy theories or rumours.

Malinformation
Deliberate publication of private information for personal or corporate gain rather than public interest, such as revenge porn. Deliberate change of context, date or time of genuine content.

Source: First Draft News
You Make The Call

*Political ads are complicated
Examples

- Florida candidates questioned results because election night reporting website malfunctioned (2019)
  - Misrepresenting accurate tabulation calls into question the entire election process

- **Thousands of bots** targeted Kentucky gubernatorial race (2019)
  - Account tweeting “Bye bye Bevin.” was retweeted at least 91 times before being suspended; bot accounts continued to tweet screenshots of the message

- Facebook announced the takedown of **50 Instagram accounts** with thousands of followers posting about US social and political issues and the 2020 election (2019)
  - Russian-based troll farms with links to Internet Research Agency (IRA) claimed to reach multiple politically active US communities, some based in swing states.
Evaluating Content

**Reputation.** Based on recognition and familiarity

**Endorsement.** Whether others find it credible

**Consistency.** Whether the message is echoed by multiple sites

**Expectancy violation.** Whether a website looks and behaves in an unexpected manner

**Self-confirmation.** Whether a message confirms one’s beliefs

**Persuasive intent.** The intent of the source in creating the message

Source: Shorenstein Center at HKS
Sources

Foreign Actors

Organized Criminal Groups

Pranksters

Political Activists

Unintentional Disruptors
What You Can Do

- Establish yourself as an **authentic** source of information
  - Join social networks (Twitter, Facebook, Snapchat) to broadcast your message using the same communication channels
  - Transition to DMARC for email and .gov for website to prevent impersonation

- **Protect access** to your communication channels
  - Enable two-factor authentication, password managers
  - Microsoft and Google offer advanced account protection to detect attacks to email

- Develop and **practice** media responses
  - Table top exercises (TTX) use realistic scenarios to build confidence and identify gaps in procedures
Resources

- Center for Democracy & Technology Election Privacy & Security Project
- Center for Technology & Civic Life Online Series: Cybersecurity for Election Officials
- DHS Cybersecurity & Infrastructure Security Agency Election Security Resource Center
- National Association of Secretaries of State TrustedInfo2020
- Harvard Shorenstein Center Information Disorder
- Unhack The Vote Uncovering Russian Twitter Bots
- Alliance for Securing Democracy Hamilton 2.0 dashboard
- Brookings Institution Fighting deepfakes when detection fails
- NATO STRATCOM COE How Social Media Companies are Failing to Combat In Online
3 Months

Until Presidential Primary Elections
Maurice Turner | Deputy Director
E: maurice@cdt.org | T: @TypeMRT