ELECTION CENTRAL

Volume 1, Issue 12 Sept. 18, 2024

Threats of AI Against Elections: How Our Office is Preparing for AI technology.

In the past year, artificial intelligence, or AI technology has become more visible in our daily lives. The search bar on Instagram and Facebook has been changed to Meta AI, Bing, and Canva offer AI generated images, and Google shows an AI generated overview of the topic searched for.

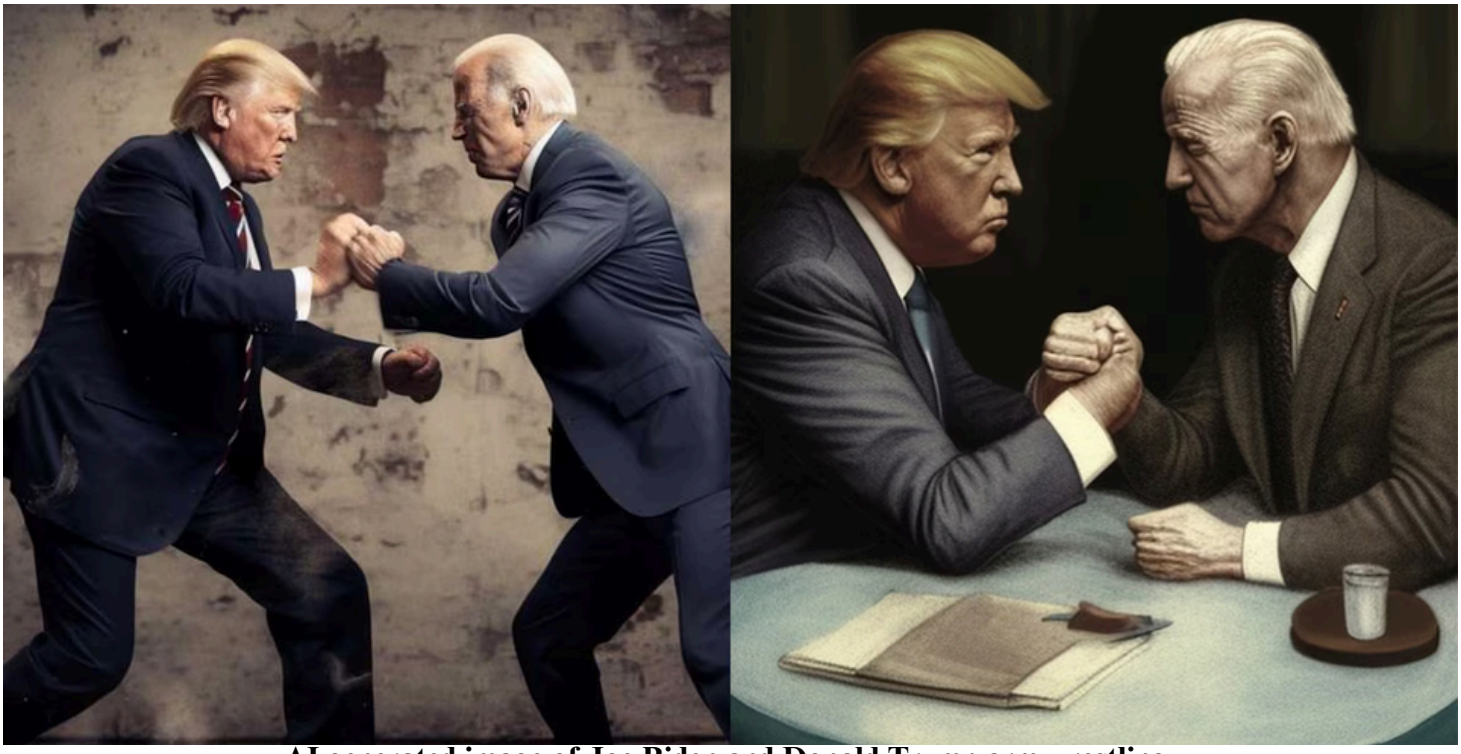
While consuming AI generated media might be interesting and fun, the threat is AI's potential to spread disinformation and misinformation.

The November General election is fast approaching and as election officials, we are preparing for the possible risks of AI impacting the election cycle. In order to do so, we must understand how AI can disrupt our electoral process.

First, knowing the difference between disinformation and misinformation is important.

Disinformation is when someone spreads false or inaccurate information as fact, with an intention to deliberately mislead others. The person spreading the disinformation knows the information is false. For example, a political candidate could use AI generated videos, or also known as deep fakes videos, to mischaracterize their opponent in order to sabotage their campaign.

Misinformation is when someone *unintentionally* spreads false or inaccurate information usually on social media. Essentially, people who spread misinformation are they themselves victims of disinformation.



AI generated image of Joe Biden and Donald Trump arm wrestling.

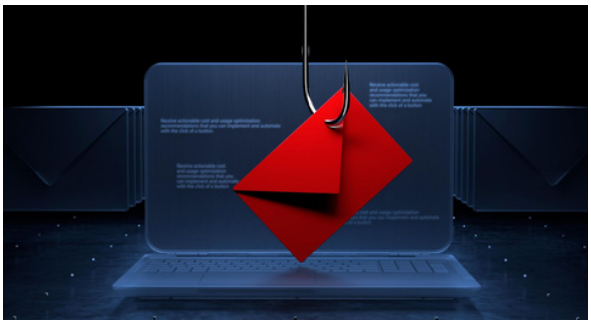
Information made by generative AI can be text, images, code, or other types of content in response to a prompt entered by a user (i.e. ChatGPT). The technology uses a computing process called deep learning to learn sets of data and then replicates to create new data that appears human-generated. The more data generative AI is trained on, the more human-like the end product becomes.

The most common way generative AI is used against cyber security against election officials is through social engineering. Social engineering are techniques aimed at tricking a target into revealing specific information or performing a specific action for illegitimate reasons. For example, victims of social engineering could've downloaded software or websites with viruses, or been scammed of money.

Over 69 percent of breaches were due to social engineering with phishing emails being the most prominent vector, according to the 2021 Data Breach Investigation Report (DBIR).

Phishing is a form of social engineering that uses email or malicious websites to solicit personal information by posing as a trustworthy organization. Other forms of social engineering are vishing (voice phishing) and smishing (SMS phishing).

In recent years, scammers have used AI to make it easier to mass execute scams through phishing.



The phishing techniques are also generated within a short amount of time with the scams being more convincing and are personalized to potential victims.

While some states are pushing bills to address AI's threat on democracy, legislation alone will not be enough to protect the electoral process. This is why we are training election officials and election officers to identify AI generated election disinformation and address the claims in a timely manner.

For voters, it is important to understand social media literacy in order to analyze messages and content in a thoughtful and responsible way.

We highly encourage voters to double check any City of Richmond election related information with our office. Official information regarding elections will be communicated directly from our office, website, and social media platforms.

As AI technology becomes more sophisticated, we need to better prepare ourselves for potential threats and to uphold the standards of our democracy.

5 Key Concepts of Social Media Literacy:

1. **All media messages are “constructed.”**
2. **Media messages shape our perceptions of reality.**
3. **Different audience, different understanding of the same message.**
4. **Media messages have commercial implications.**
5. **Media messages embed points of view.**

SIFT Method

STOP - Ask yourself what the reputation of the claim and the source is. Don’t read or share media until you know what it is.

INVESTIGATE - Do your research and look into the source before engaging with its content. Understanding the expertise and agenda of the source is crucial in order to interpret what they say.

FIND ANOTHER SOURCE - Find another trusted source to confirm the claims before coming to any conclusions.

TRACE CLAIMS - By the time a video, image, or text reaches you, it has generally been stripped of context. Do your due diligence and trace the claim back to the source to identify the context and get a better interpretation of the information you came across.