

ARTIFICIAL INTELLIGENCE AND **ELECTIONS**

NAVIGATING A NEW TECHNOLOGICAL AND CIVIC LANDSCAPE





THE FIRST AI-INFLUENCED ELECTION

Artificial intelligence brings many new possibilities, both positive and negative, to our election systems.

2024 is set to be the first US election in which AI tools will be widely available. As such, it is imperative that governments, institutions, and individuals have the tools necessary to identify AI-generated information, whether it is AI-voice fake robocalls, AI-generated political images, or AI-run pages that push disinformation.



WHAT IS ARTIFICIAL INTELLEGENCE

Artificial intelligence is a field of science concerned with building computers and machines that can reason, learn, and act in such a way that would normally require human intelligence or that involves data whose scale exceeds what humans can analyze. This includes recent work in processing and understanding language and images, making recommendations, and more.



There are multiple sub-categories of Artificial intelligence; the categories this presentation will focus on are Deepfakes, generative AI images, and Ai chatbots.







ARTIFICIAL INTELLIGENCE HAS MANY BENEFITS TO SOCIETY



Helps Streamline Processes

Al can automate repetitive tasks, allowing employees to focus on more complex tasks that require critical thinking and problem-solving.

Al-powered machines can also perform tasks faster and more accurately than humans.



Supports information Gathering

With the assistance of AI, research and data scientists are able to better analyze patterns, predict outcomes, and make adjustments in half the time. Information that would have taken months to collect now can be done in minutes, if not seconds.



ARTIFICIAL INTELLIGENCE HAS SOME CONCERNS

Artificial intelligence has many positive aspects, but those positives do not come with real concerns. Artificial intelligence can be a source of misinformation and disinformation based on who is deploying the technology. To an untrained eye, Al-generated materials could seem real.





Hi Quality Creation

High-level Al-generated content can often be indistinguishable from human-created content, which could spread misinformation.



Widely Available

Al tools are widely available, meaning anyone can leverage Al for their own means.



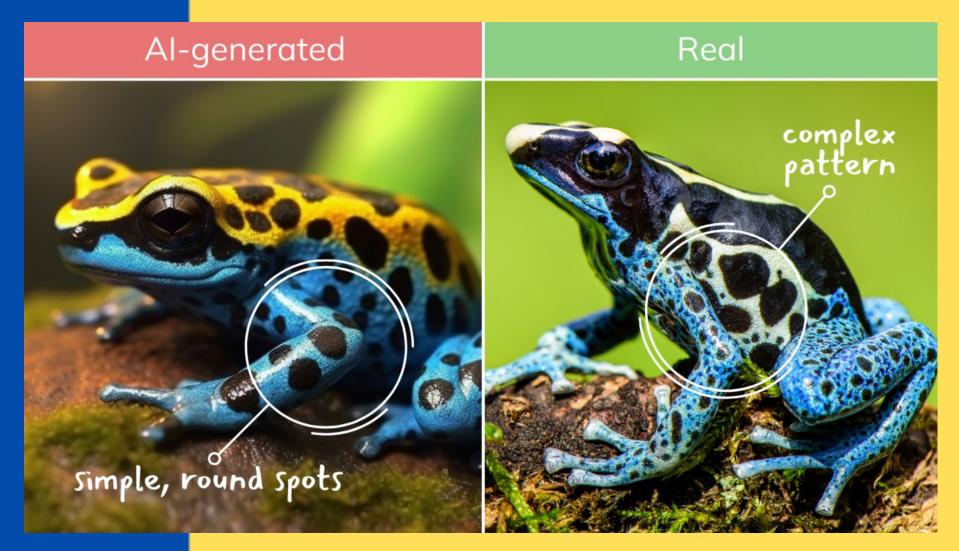
ACTIVITY: WHICH IS AI AND WHICH IS NOT?







ANSWER





WHICH IS AI AND WHICH IS NOT?







ANSWER





Real





WHICH IS AI AND WHICH IS NOT?







ANSWER

Al-generated

Real









TIPS & TRICKS TO DETERMINING AI

- Unusual or Inconsistent Details: Al-generated images often contain minor, noticeable detail errors. Encourage students to look for abnormalities like asymmetrical facial features, odd finger placement, or objects with strange proportions.
- Texture and Pattern Repetition: Al sometimes struggles with complex textures or patterns, leading to noticeable repetition or awkward transitions. Students should look for unnatural patterns in textures like hair, skin, clothing, or background elements.
- Lighting and Shadows: Al-generated images can have inconsistent or unrealistic lighting and shadows. Students should check if the lighting on different objects in the image matches and if the shadows are consistent with the light sources.



AI AND ELECTIONS

In the 2024 election season, Al has already been used by bad actors to spread disinformation, reduce faith in our electoral system, and cripple the election system. These are a few examples and scenarios.

Chatbots' inaccurate, misleading responses about US elections threaten to keep voters from polls

New Hampshire investigating fake Biden robocall meant to discourage voters ahead of primary





2024 ELECTIONS

America's election chiefs are worried AI is coming for them

Election officials are important enough to fake — and public enough to make it easy to do — but anonymous enough that voters may easily be tricked.



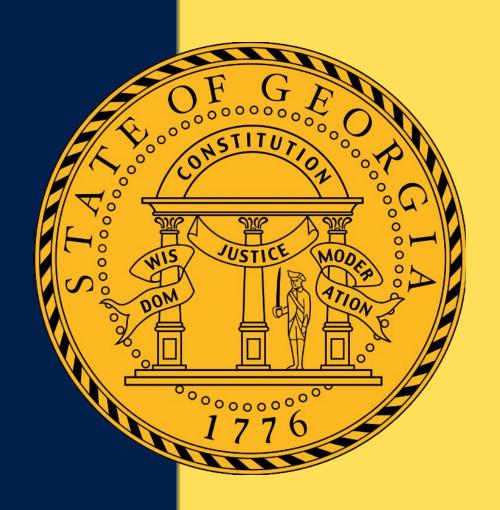
FAKE SECRETARY OF STATE ROBOCALL SENT TO POLL WORKERS ON ELECTION DAY.

Secretary of State is worried about the use of deep fakes targeting poll workers and government officials telling them misinformation about the upcoming November 5, 2024 election. One scenario is a false call from a secretary of state telling poll workers they aren't needed on Election Day.



What Type of Tech?

This election attack employed an Audio deep fake. An audio deep fake (also known as voice cloning or deepfake audio) is a product of artificial intelligence used to create convincing speech sentences that sound like specific people saying things they did not say. This technology was initially developed for various applications to improve human life. For example, it can be used to produce audiobooks, and also to help people who have lost their voices (due to throat disease or other medical problems) to get them back. Commercially, it has opened the door to several opportunities. This technology can also create more personalized digital assistants and natural-sounding text-to-speech as well as speech translation services.



FAKE SOCIAL MEDIA VIDEOS RELEASED OF ELECTED OFFICIALS AND COMMUNITY LEADERS SPREADING DISINFORMATION.

Generative Ai creates new opportunities for spreading misinformation throughout social media websites. (Instagram, Tik-Tock, Twitter, etc) Believable fake videos of community members saying untrue things are expected to be spread widely during the election season.





FAKE BIDEN ROBOCALL SENT TO DISCOURAGE VOTERS AHEAD OF THE 2024 PRIMARY.

During the New Hampshire primary in January of 2024, a robocall of a deepfake of President Joe Biden which used artificial intelligence to mimic President Joe Biden's voice and discourage voters in the state from coming to the polls during the primary election. It is currently unknown how many voters received these deep fakes and the origin of the deepfake robocall.

"I didn't think about it at the time that it wasn't his real voice. That's how convincing it was," - Gail Huntley, a 73-year-old Democrat in Hancock, New Hampshire.

—

Guiding Questions

- Why was this attack effective?
- If you and your team woke up on election day with widespread reports of an audio deep fake telling people not to vote, how would you respond?
- How could we tell the public about this technology in order to prepare them?
- If you know this attack is coming how would you respond?
- What populations and communities are most vulnerable to this type of disinformation?
- What sources can we spread to counter these fake sources?

POLITIC

New Hampshire investigating fake Biden robocall meant to discourage voters ahead of primary



E - President Joe Biden speaks in the East Room, Jan. 19, 2024, in Washington. Authorities issued cease-and-desist orders Tuesday against two Texas companies they believe were connected to robocalls that us

FAKE ACCOUNTS AND CHATBOTS

Social media is a breeding ground for misinformation. The ease and ability to create fake profiles and use artificial intelligence to spread misinformation through direct messages. These chatbots are trained to engage in conversation with people to scam and trick them into giving out personal information. The chatbots leverage high levels of distrust in Institutions and authority (Gov, Justice, Edu) to spread disinformation.

Peer to Peer

Catfishing

Fake accounts of loved ones and peers sending communications authored by malicious entities to spread disinformation.

Fake Institutional

Accounts

Fake news and government accounts give the illusion of authenticity. Often times, these accounts use the same graphics and bios to create these accounts and use similar user names.



FAKE CULTURAL GROUPS AND PAGES

On social media sites like YouTube and Facebook, fake private groups and run content channels give the illusion of community but are often traps for stealing information, spreading disinformation, and creating conflict. Many people join these pages because they appeal to an affinity or fandom they align with and seek like-minded individuals. These methods are effective because they are exploiting low literacy & barriers to access information to fill the gaps with misinformation.

Leveraging Cultural

Cues

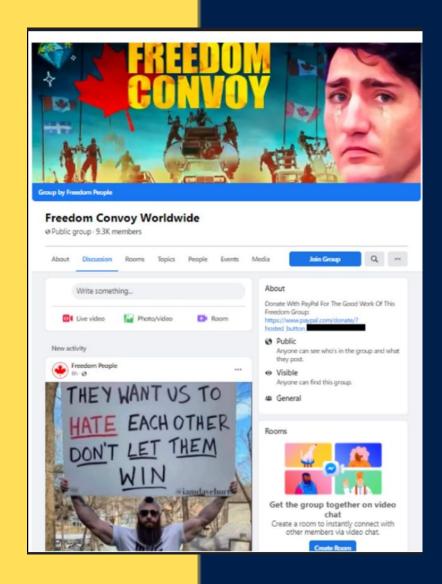
Fake accounts use cultural cues to attempt to trick members of affinity groups (Black, Queer, Migrant, etc). These groups serve as misinformation eco-chambers.

Psychological

Manipulation

Fake groups and pages often serve the goal of making users angry to farm engagement.

Fearmongering on issues like Jobs, Immigration, and Crime and spreading fake statistics.



WHAT CAN WE DO?





Confirm Your Source

Make sure the information you are receiving is from a trusted source and look into it. Do not just take things on face value.



Follow Up on Messages

Do not share personal information in social media DM's. If you know the person, text them or call them to ensure you are talking to a real person.



Be a source of real info

Do not be afraid to share real information to your followers. If you almost get caught in a scam, share it and let your community know.

