TOOLS OF DISINFORMATION:

Inauthentic Content

Disinformation actors use a variety of tools to influence their victims, stir them to action, and create consequences. CISA created this fact sheet to illustrate deepfakes, forgeries, proxy sites, and other tools of disinformation actors.

Knowing these techniques can increase preparedness and promote resilience when faced with disinformation.

Key Terms

Misinformation misleads. It is false information that is communicated and spread, regardless of intent to deceive.

Malinformation sabotages. It is factual information that is taken out of context and presented to cause harm.

Disinformation deceives. It is false information that is intentionally crafted and spread to deceive.

Examples of Inauthentic Content

MANIPULATED AUDIO/VIDEO

Often times, audio/video content goes viral because it grabs the attention of the audience and is repeatedly shared. But what if this content is a cheapfake or deepfake? Manipulated audio/video content is dangerously effective at spreading false information.

- Cheapfakes are real audio clips and videos that have been sped up, slowed down, or shown out of context to mislead.
- Deepfakes are fake, but very believable, audio clips and videos, crafted and spread to deceive. They can convince you that people have said or done things that did not happen. Visual deepfakes can generate fake-but-plausible faces or full-body video. An audio deepfake can be a voice clone that produces new sentences from one person or multiple people on its own or with a fake video.

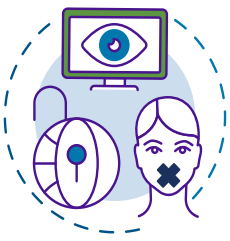
The quality of manipulated audio/video varies. Some fakes are detectable on closer examination, while uncovering others will require special software.

On its own, this content can be convincing. Check with multiple sources to confirm its authenticity.

FORGERIES

Forged artifacts typically feature fake letterheads, copied and pasted signatures, made-up social media posts, and maliciously edited emails. Such forgeries are made and distributed for various malign purposes. To make them more credible, forgeries are often presented as obtained from a hack, theft or other interception of documents—they purport to be "leaked" materials.

Stay vigilant. Forgeries can be packaged with authentic content to lend it credibility. If the forgery appears to be groundbreaking news, check reputable news sites to see if they are covering the event.



PROXY/FAKE WEBSITES

Proxy websites are fronts for malicious actors, designed to launder their disinformation and divisive content or use that content to drive website visits. These sites are not developed to provide authentic information.

Following high-visibility events, these sites will crop up to take advantage of the public's legitimate desire for information. Be cautious of sites that have unclear origins. Both the information and its sources should be trustworthy.

Clues like misspellings in a URL can indicate before even visiting a website that it may not be a trustworthy source.