

CYBERSECURITY AWARENESS MONTH

FAKE NEWS & DEEPPFAKES

October 2022



THE TRUTH ABOUT FAKE NEWS

THE FACTS...

- Fake News is a false narrative published and promoted as fact.
- Anyone with a Social Media account can 'publish' falsehoods as if they were truths.
- Often people are paid to post fake news.
- Automated programs, called bots, rapidly spread fake news.

BUT WHY?

- Fake news is created to change people's beliefs, attitudes, or perceptions, so they will ultimately change their behavior.
- Agenda driven propaganda can quickly influence politics, markets, and reputation.



8 WAYS TO VERIFY FACTS

Consider the Source: A local blog will not be as trustworthy as a major academic journal.

Supporting Sources: Look at the cited sources cited. Do they even exist?

Multiple Perspectives: Don't just rely on a single article. Consider diverse sources, such as news from different countries or authors with different backgrounds.

Credible Author: Research their reputation in the community, whether they have a specific agenda, or if the person posting is a real person.

Date Check: Make sure that the date is recent.

Comments: Quite often comments posted in response can be auto-generated by bots or by people hired to promote confusing, or false information.

Check Your Biases: Be objective. Could your own biases influence your response to the article? Challenge yourself by reading other sources you normally would not review.

Paid Advertising: Check to see if the article is funded, and if so by whom.



THINK BEFORE YOU SHARE

Fake news relies on believers to repost, retweet, or otherwise forward false information. If you're uncertain as to the authenticity of an article, think twice or hold off on sharing it with others.

Workplace Tip: If it's news relating to your company, and it seems suspicious, be sure to verify it with your team lead, supervisor, or manager.



THE TRUTH ABOUT DEEPPAKES

THE FACTS...

- Deepfakes are artificial images and sounds put together with machine-learning algorithms. A deepfake creator uses deepfake technology to manipulate media and replace a real person's image, voice, or both with similar artificial likenesses or voices.
- The purpose is to deceive viewers that something was said or happened that never occurred, often to spread misinformation and for other malicious purposes.

TOP METHODS FOR SHARING:

- Scams and hoaxes.
- Celebrity pornography.
- Election manipulation.
- Social engineering.
- Automated disinformation attacks.
- Identity theft and financial fraud.



DID YOU KNOW?

43%
increase in
malicious
deepfake
attacks since
2019

85,000+
deepfake
videos were
identified in
2020 with a
prediction to
double in 2021


7%
of deepfake
videos are
made for
comedic
purposes

DEEPFAKE IN BUSINESS

Many companies are concerned about several scams that rely on deepfake technology. Here's a few examples of how deepfakes are being used.

- Supercharging scams where deepfake audio is used to pretend the person on the other line is a higher-up such as a CEO asking an employee to send money.
- Extortion scams.
- Identity theft where deepfake technology is used to commit crimes like financial fraud.
- Many of these scams rely on an audio deepfake. Audio deepfakes create what are known as “voice skins” or “clones” that enable them to pose as a prominent figure. If you believe that voice on the other line is a partner or client asking for money, it's a good idea to do your due diligence. It could be a scam.

SPOT THE FAKE

- 
- ✓ Unnatural eye movement and lack of blinking.
 - ✓ Unnatural facial expressions. Facial morphing.
 - ✓ Unnatural hair.
 - ✓ Abnormal skin colors. Face tone vs. body tones.
 - ✓ Unnatural body shape.
 - ✓ Awkward head and body positioning.
 - ✓ Odd lighting or discoloration.
 - ✓ Bad lip-syncing. Robotic-sounding voices.
 - ✓ Digital background noise.
 - ✓ Blurry or misaligned visuals.

MR. BEAN VS. STALLONE



FAKE TAKE: CHALLENGE

Watch this video and identifying as many deepfake clues as you can.
HINT: You can use the previous slide to guide you.



THANK YOU



Stay Cyber Safe.