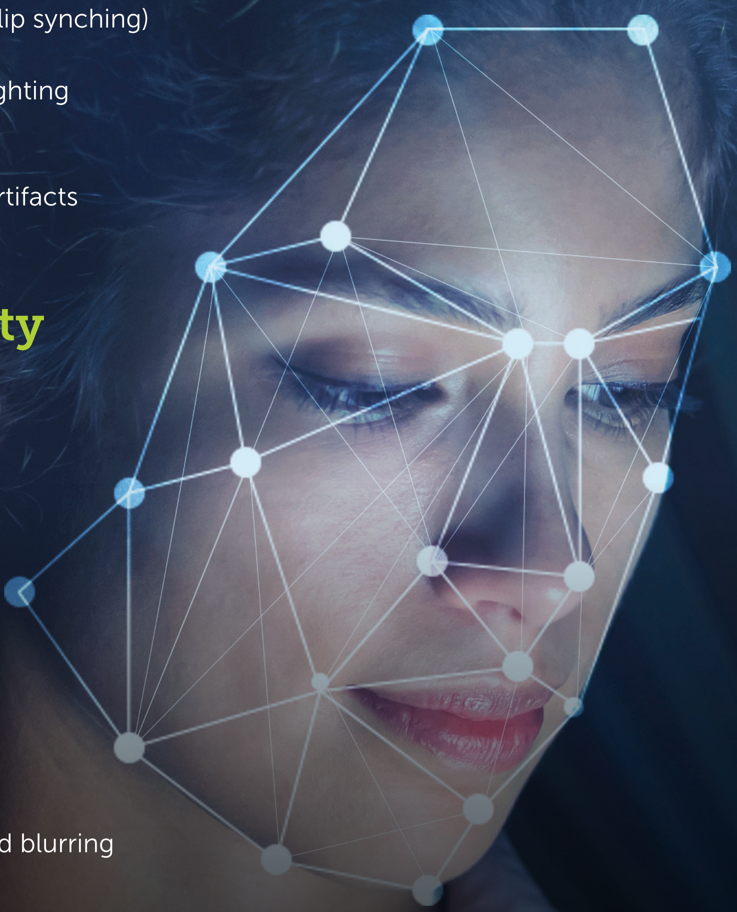
CYBERSECURITY AWARENESS

How to spot a deepfake

Bad actors are finding new ways to deceive and scam their targets, using artificial intelligence to create hyper-realistic videos, audio, and images known as deepfakes. Anyone can fall victim to these scams, resulting in significant financial losses and other harm to individuals and businesses. Help prevent the spread of misinformation by being skeptical, vigilant, and aware of telltale signs that what you see might not be what it seems.



Video Inconsistencies

- Unnatural facial movements (e.g., blinking, lip synching)
- Inconsistent lighting or reflections
- Glitches and artifacts

Audio Quality

- Robotic tone
- Mismatched emotion
- Unusual articulation

Photo Distortion

- Asymmetry and blurring
- Background errors
- Unrealistic skin texture or aging
- Unnatural facial hair

What to do if you suspect a deepfake

- **Verify the source.** Did it originate from a reputable organization?
- **Conduct a reverse image search.** Use a search engine to look for similar images and trace its origin.
- **Check metadata.** Does the embedded information within the digital file show inconsistencies or anomalies?
- **Use an AI deepfake detector.** While not foolproof, online detectors can help you determine if a digital media file is potentially fake.
- **Report suspicious content.** Follow your organization's IT security policies and procedures to report potential threats.
- **Engage a cybersecurity consultant.** Look for a team that can help you assess your risks, identify and respond to threats, and train employees for future risk mitigation.

KAUFMAN
ROSSIN

Learn more at kaufmanrossin.com