Worksheet: Deepfake Detective — Spotting Video Manipulations

Objective: Build awareness of deepfake warning signs and the underlying technology.

1. Crash-Course Sidebar

A one-page primer on how deep learning generates deepfakes: - **GANs (Generative Adversarial Networks):** A Generator creates fake frames while a Discriminator learns to spot them. - **Pipeline Steps:** Data collection — Model training on facial mappings — Frame-by-frame synthesis — Post-processing. - **Common Artifacts:** Unnatural blinking, blurred edges, inconsistent lighting.

2. Frame-by-Frame Analysis

Watch the provided video clip. Pause on four key frames and annotate potential tampering signs:

| Frame # | Timestamp | Warning Signs (e.g., blinking, shadows, lip-sync issues) | | |
|---------|-----------|--|--|--|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| | | | | |

3. Tech Comparison Chart

Match each deepfake detection tool with its pros and cons:

| Detection Tool | Pros | Cons |
|-------------------------------|------|------|
| FaceForensics | | |
| Microsoft Video Authenticator | | |
| Deepware Scanner | | |
| | | |

4. Creative Exercise

Imagine you need to warn your social media followers about a trending deepfake. Draft a 140-character alert tweet highlighting key red flags:

| Tweet: | | | |
|--------|--|--|--|
| | | | |
| | | | |

Instructions for Teachers/Facilitators: - Provide a short deepfake video link for analysis. - Allow 20–30 minutes for students to complete all sections. - Conclude with a discussion comparing which warning signs were most reliable.

Adapt sample clip links and tool list to the latest available resources.