SPOT THE SIGNS OF DEEPFAKES

Deepfakes are artificially created or edited **photo, video, or audio** content that mimic people of considerable influence! They can be used by cybercriminals to create convincing and realistic content to conduct scams or phishing attacks.

SPOT A DEEPFAKE WITH THESE 2 STEPS:

ASSESS

- Check the content against official sources
- Take note of any urgent or threatening language
- Be wary of attractive deals or invites to download third-party apps
- Refrain from giving away your personal information like NRIC, date of birth
- Do not share the content with others

ANALYSE

Spot the signs of deepfake:

- Unnatural facial expressions
- Inconsistent content resolution or lighting
- Blurring on the edges of the speaker's face
- Audio-video inconsistencies

HOW CAN WE RESPOND?

- Guard your **digital identity** (e.g. photos, videos)
- Set your social media accounts to **private**
- **Report** deepfakes to your service provider or call the National Crime Prevention Hotline
- **Educate** your family and friends about deepfakes

CSA SINGAPORE
Cyber Security Agency of Singapore

Want to know more?

Scan the QR code to read CSA's advisory:

GO.gov.sg