

### CYBERSECURITY AWARENESS DAY 13

Let's talk about **Deepfakes** 

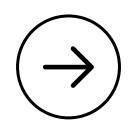


## Deepfakes: The New Face of Online Deception

We've entered an era where seeing is no longer believing.

Al can fake your boss, your pastor, even your spouse.

Your best defense isn't technology It's awareness, skepticism, and discernment



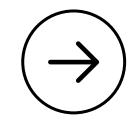
#### What are Deepfakes?



Deepfakes are AI-generated videos, audio, or images that make people appear to say or do things they never did.

They use deep learning (AI) to replace real faces or voices with fake ones and the results can look shockingly real.

For example: imagine seeing a video of your CEO announcing mass layoffs, or a politician admitting to a crime only to find out none of it was real.



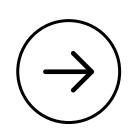
#### Why it matters



Deepfakes aren't just about celebrities or politics.

They're now used in:

- Job scams fake interviews with HR managers using stolen videos.
- Romance scams Al-generated partners who never exist.
- Corporate fraud fake video calls tricking employees to send money or data.
- Defamation fake videos destroying reputations in seconds.



#### How to Spot a Deepfake



- Look closely at the eyes and mouth they often blink strangely or move unnaturally.
- Listen carefully the voice may sound flat, emotionless, or mismatched with facial expressions.
- Cross-check sources, don't believe viral videos until confirmed by credible outlets.
- Be skeptical of urgency —
  Scammers use emergency tones to make you act fast.

#### **How to Stay Safe Online**



- Always verify requests through another channel (e.g., call the person).
- Be cautious when accepting video calls from unknown contacts.
- Train your mind to pause before reacting emotionally that pause can save your reputation, your data, or your money.
- Train your team regularly on AIdriven scams.
- Follow updates from reliable cybersecurity sources



# Share, like and follow for more Cybersecurity awareness tips