# LEVEL TWO

This week's cyber villain, **Dr. Deepfake**, uses the power of artificial intelligence (AI) to supercharge phishing attacks making them **trickier, faster, and more realistic** than ever! You need to be well-versed in these threats to stay one move ahead as you navigate work and home life.

**Your mission:**

Complete these mobile-friendly, interactive exercises on AI, phishing, and cyber safety to upgrade your skills and reach **Level 2** in your quest to become a **cyber superhero**.

**You'll learn:**

- Warning signs of AI-generated social engineering attacks
- Why AI-powered phishing is on the rise
- How to stay secure using AI programs

***To start SCAN or CLICK the QR codes***


**VILLAIN**: Dr. Deepfake

**ATTRIBUTES**: Tricky, Convincing

**ATTACK MODES**: Impersonation, Fraudulent activity:

- Posing as coworkers/contacts
- Faked faces
- Voice Simulators

## Online Safety Tips

- Be wary of unexpected attachments or urgent requests for information.
- Ensure communication is through known contacts and secure channels.
- Verify the requester's identity before sharing sensitive information
- Never share any personal or company information with AI chatbots.
- Set strict privacy settings on social media and don't share your location.

## Protect Your Digital Identity

DIGITAL IDENTITY: Online profile, digital records, all other data representing you.

DATA PRIVACY: Your right to control your personal (or company) information.

1. Choose what to share
2. Know how your data is used
3. Control who has access
4. Protect against unauthorized use

Artificial Intelligence (AI) is reshaping how digital identities are created, interpreted, and used. With the ability to gather and process large amounts of data quickly, recognize patterns, and make predictions, AI poses new challenges for privacy.