AI in Social Engineering and Phishing: An Overview

AI is transforming cyberattacks by making social engineering more effective. Social engineering manipulates people to gain access. Phishing tricks victims into revealing sensitive info.

This presentation explores how AI boosts attack sophistication and efficiency.

○ **Group members:-**
Omkar Bhambid
Prabhav Nerurkar
Nikhil Damse

The Problem: Social Engineering Vulnerabilities

Human Weakness

Humans remain the weakest security link in breaches (Verizon DBIR).

Detection Limits

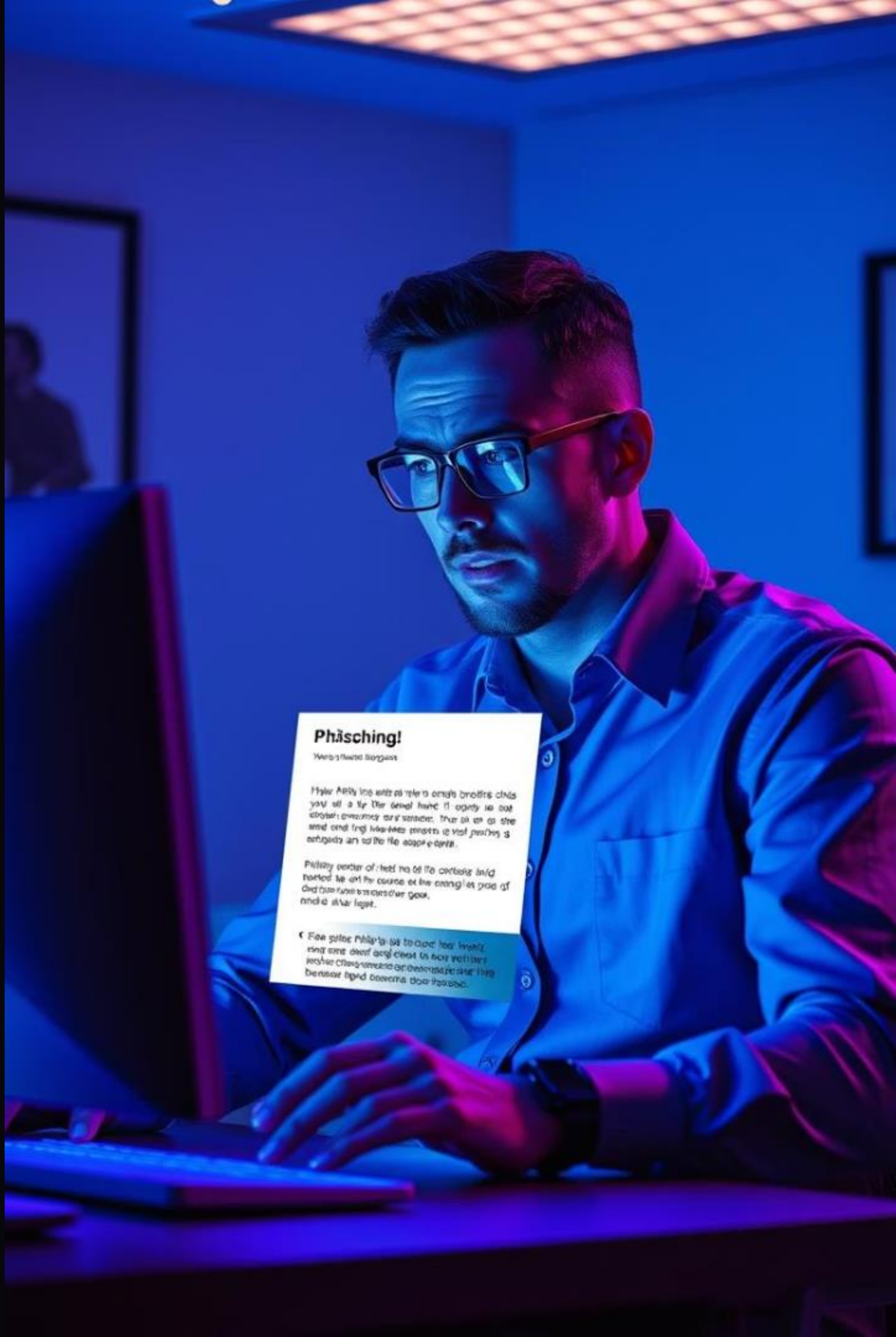
Current phishing detection tools often fail against evolving attacks (APWG).

Financial Impact

Phishing caused losses over $4.2 billion in 2020 alone.

Rising BEC Threats

Business Email Compromise attacks increased 24% last year (FBI IC3).



AI as the Solution... for Attackers

Email Automation

AI crafts highly personalized phishing emails at scale.

Fake Profiles

AI generates realistic social media profiles to build trust.

Voice Cloning

Voice AI imitates trusted voices to deceive victims.

Deepfakes

Convincing deepfake videos manipulate targets emotionally.

Code/Tool Breakdown: AI Phishing Toolkit

GPT-3

Generates convincing, personalized phishing emails.

DeepFaceLab

Creates realistic deepfake videos for social manipulation.

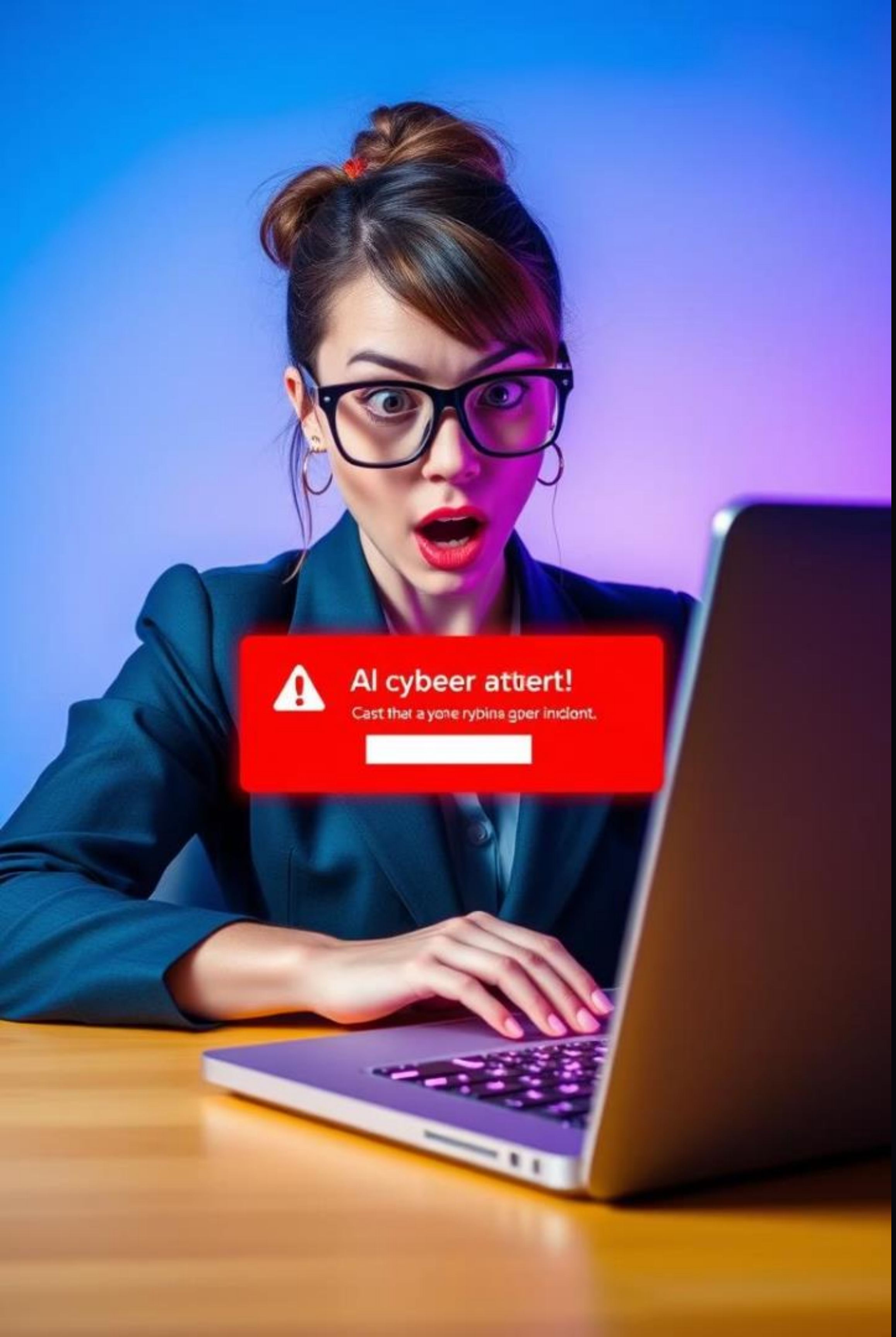
Wavenet

Clones voices with natural intonation for audio deception.

OpenPhish

Helps bypass phishing detection using known phishing data.

Example: Python scripts scrape data to personalize phishing emails automatically.



Real-World Use Cases: AI-Powered Attacks

1

CEO Deepfake Fraud

Cost company $35 million in a single scam (WSJ report).

2

Political Disinformation

AI-generated fake news campaigns sway public opinion (Oxford study).

3

Targeted Phishing

Customized AI phishing targets defense contractors (Mandiant report).

Countermeasures: Defending Against AI

AI Threat Detection

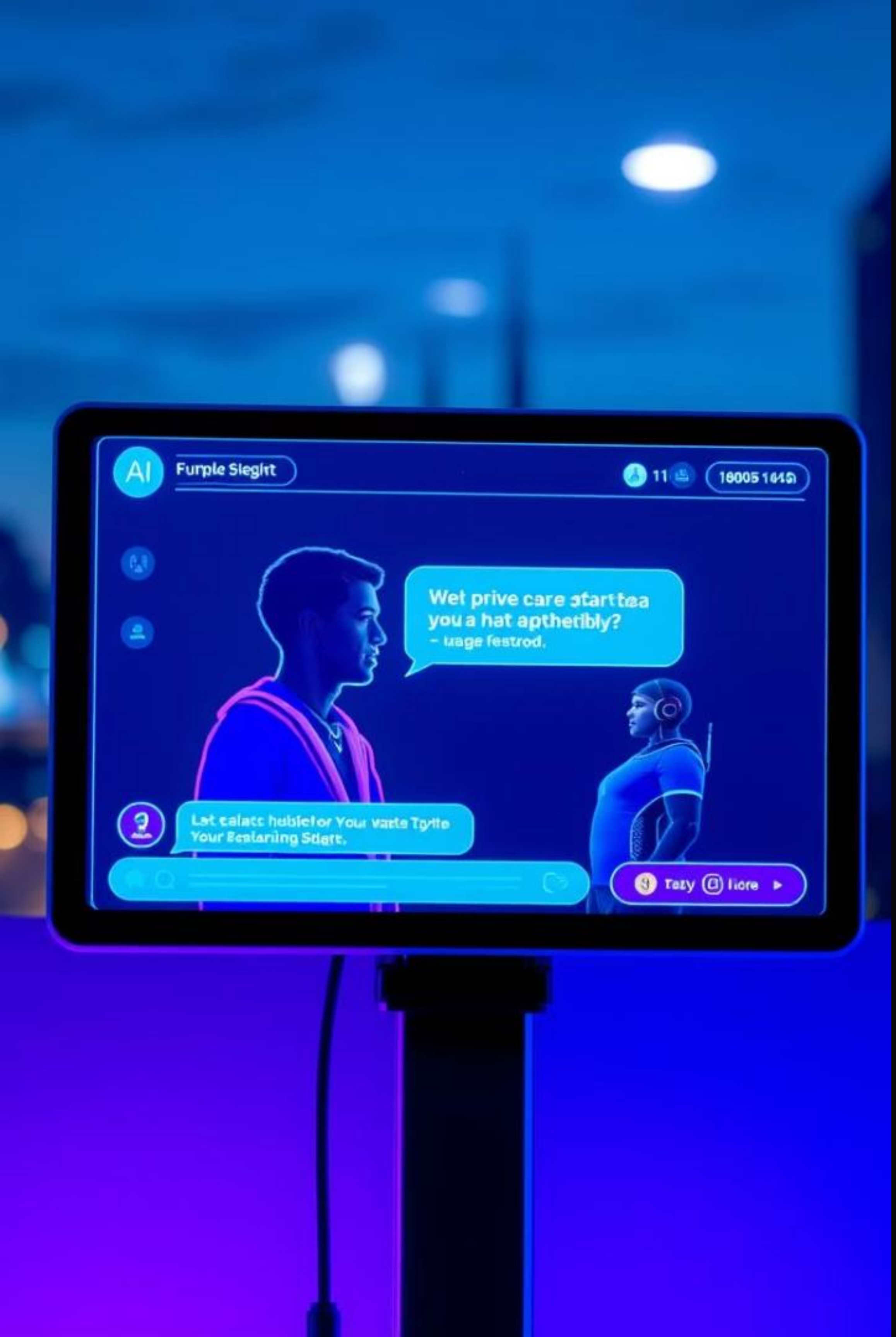
Systems like Darktrace proactively detect AI-driven threats.

Biometric Security

Multi-factor authentication strengthens access controls.

User Education

Training employees to spot AI-generated deepfakes and phishing.


AI
Furple Slegitt
Wet prive care starttea you a hat apthetibly? – uage festrod.
Lat calatc hublefor Your vazta Tgyite Your Eealaning Sdert.

Future Enhancements: The Escalating AI Arms Race

1 Real-Time AI Manipulation

Chatbots capable of manipulating victims instantly.

2 Predictive AI

AI forecasts victim behavior to increase success rates.

3 Adaptive Attacks

AI adjusts tactics to evade new security measures automatically.

Conclusion: The Future of Trust

Changing Trust

AI reshapes how we assess authenticity and trust online.

Stay Vigilant

Remain alert to evolving AI-driven social engineering.

Invest in Tools

Use AI-powered detection systems for defense.

Continuous Training

Educate employees regularly about new AI threats.

GitHub Links of Group Members =>

OMKAR BHAMBID:- https://github.com/dragon-omk/finalproject

PRABHAV NERURKAR:- https://github.com/prabhav1628/Prabhav-Pranay-Nerurkar

NIKHIL DAMSE:- https://github.com/NikhilDamse/finalproject

Demo link:- https://youtu.be/ewpUTYIMIkc?si=MgIxAUiMH34Vb43w