



Working Safely with AI

What Every Employee Needs to Know



wizer-training.com

AI Is Already In Your Life

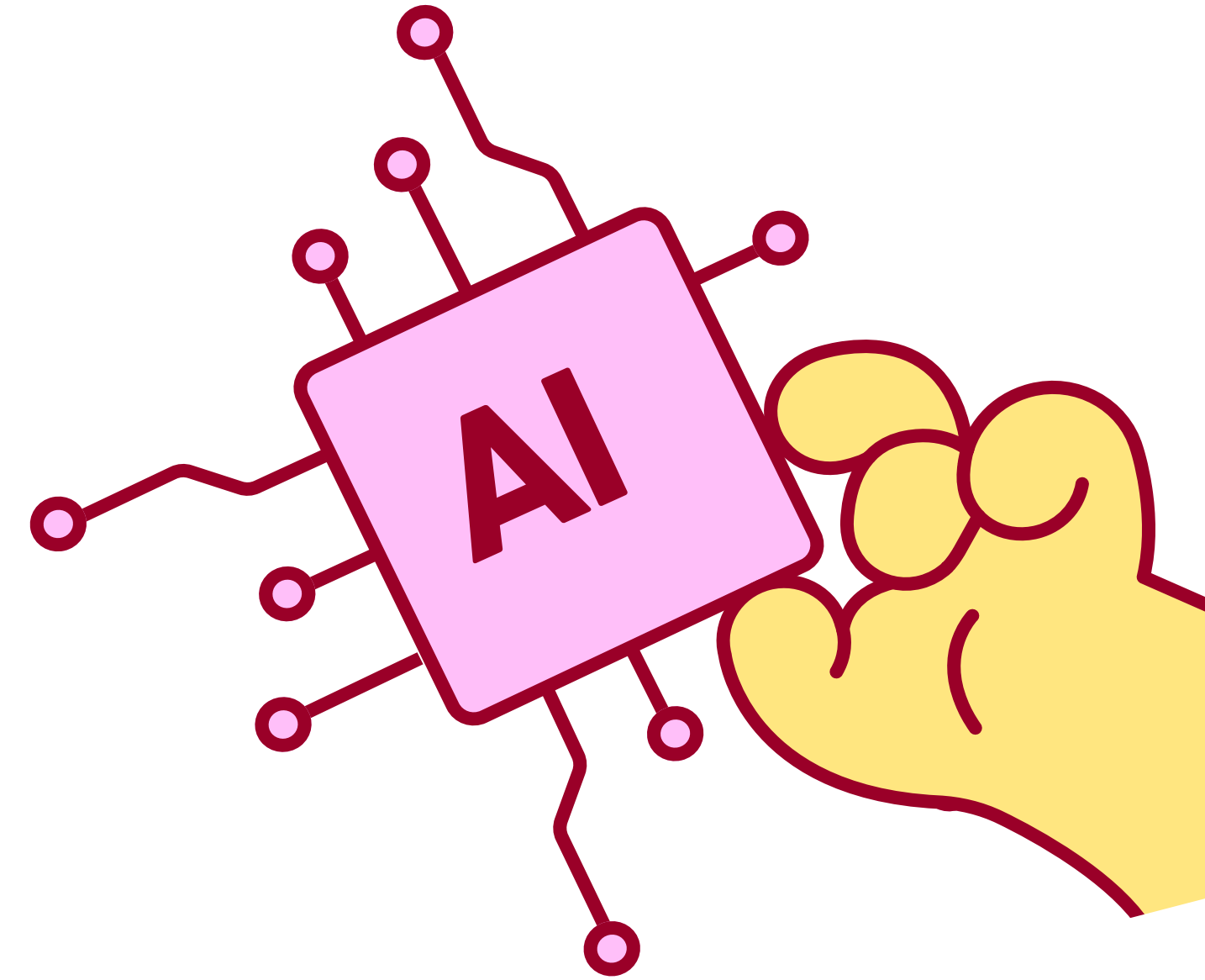
**Most people think AI is something they open.
It's not.**

It's already helping decide:

- What you search
- Which emails you see
- The route you drive
- The videos you watch
- The products you're shown

AI isn't the future.

It's already working beside you—whether you realize it or not.



The Problem With AI

AI sounds confident – even when it's wrong.
It can make up facts, sources, or details.

This is called an AI hallucination.
Because AI is often right, people tend to trust it too much.

What determines AI quality?

Biased data → Biased outputs

Low-quality data → Confident but incorrect answers

Remember: AI doesn't know the truth. It predicts what is most likely to come next based on what it has learned.





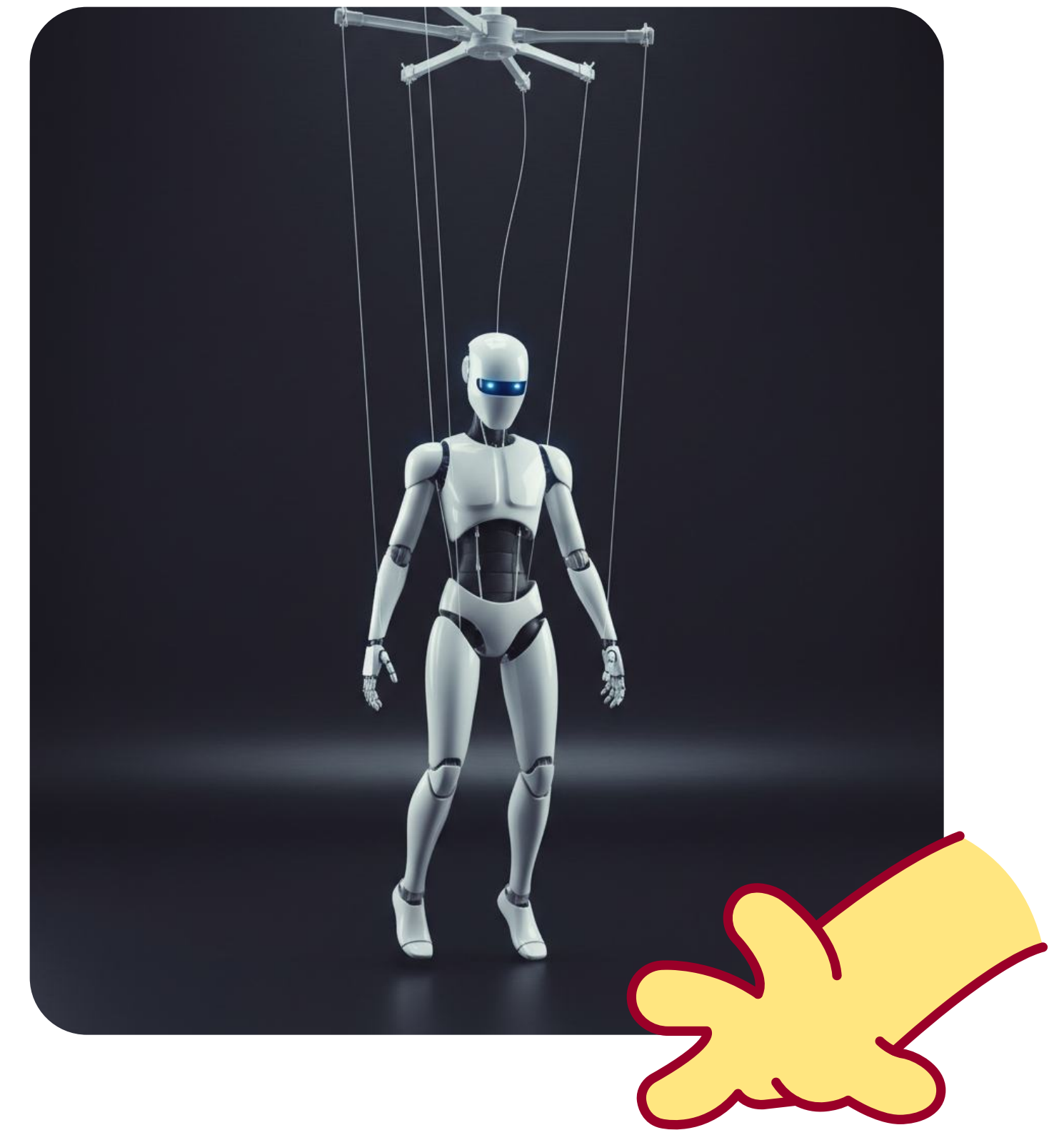
How Attackers Are Weaponizing AI – Examples

AI Account Takeovers

Instead of stealing Microsoft or Google accounts, attackers target AI accounts directly.

Why it works?

it's the new insider threat. Imagine having an employee inside the company who follows instructions without questioning them.



Deepfake Executive Fraud

scammers impersonated a CFO during a video meeting and convinced the finance team to wire \$25 million.

Why it works?

It feels real!

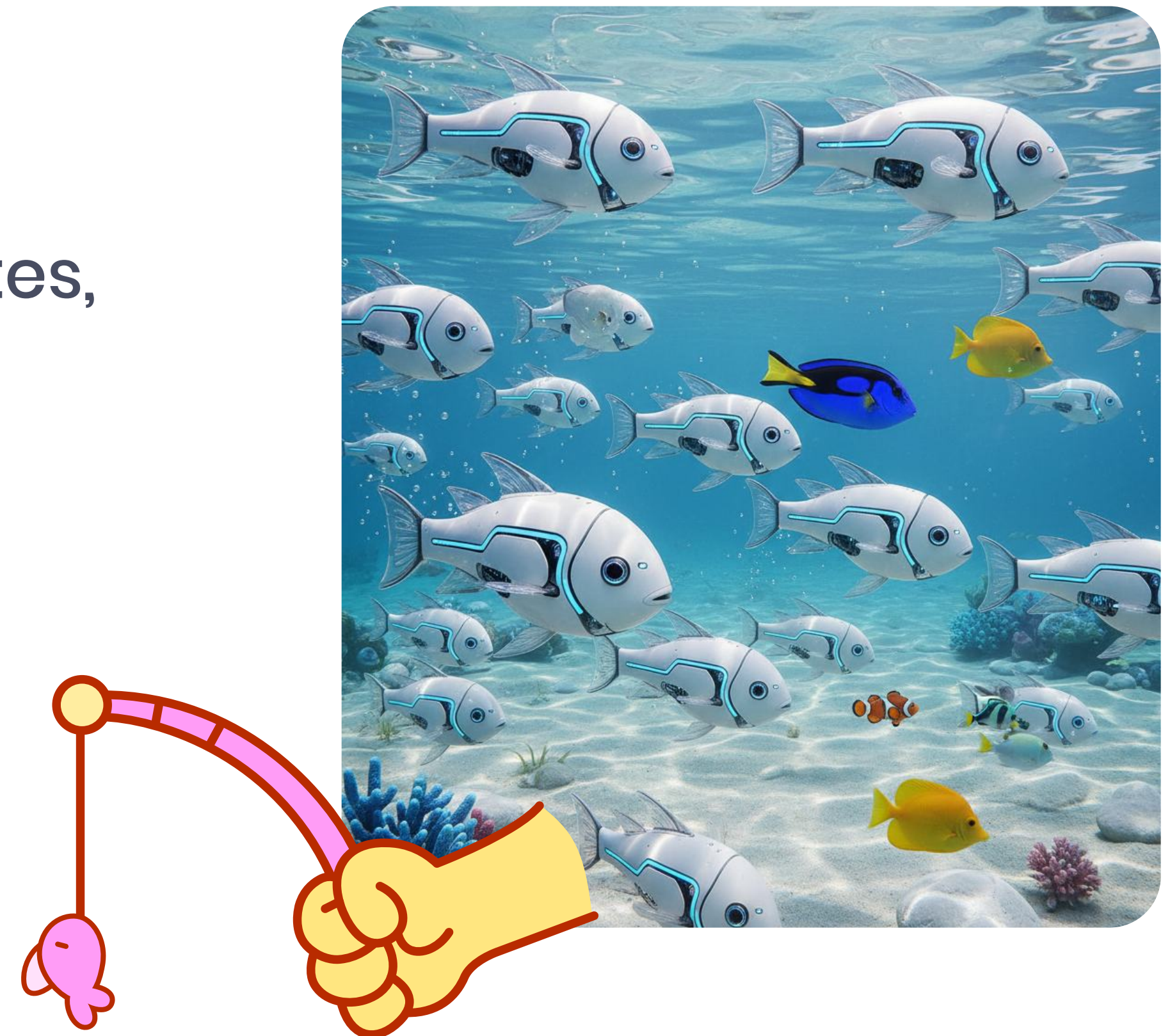


Prompt Injection Attacks

Hidden instructions embedded in emails, websites, PDFs, or documents used to trick AI.

Why it works?

Think of it as "social engineering for AI."

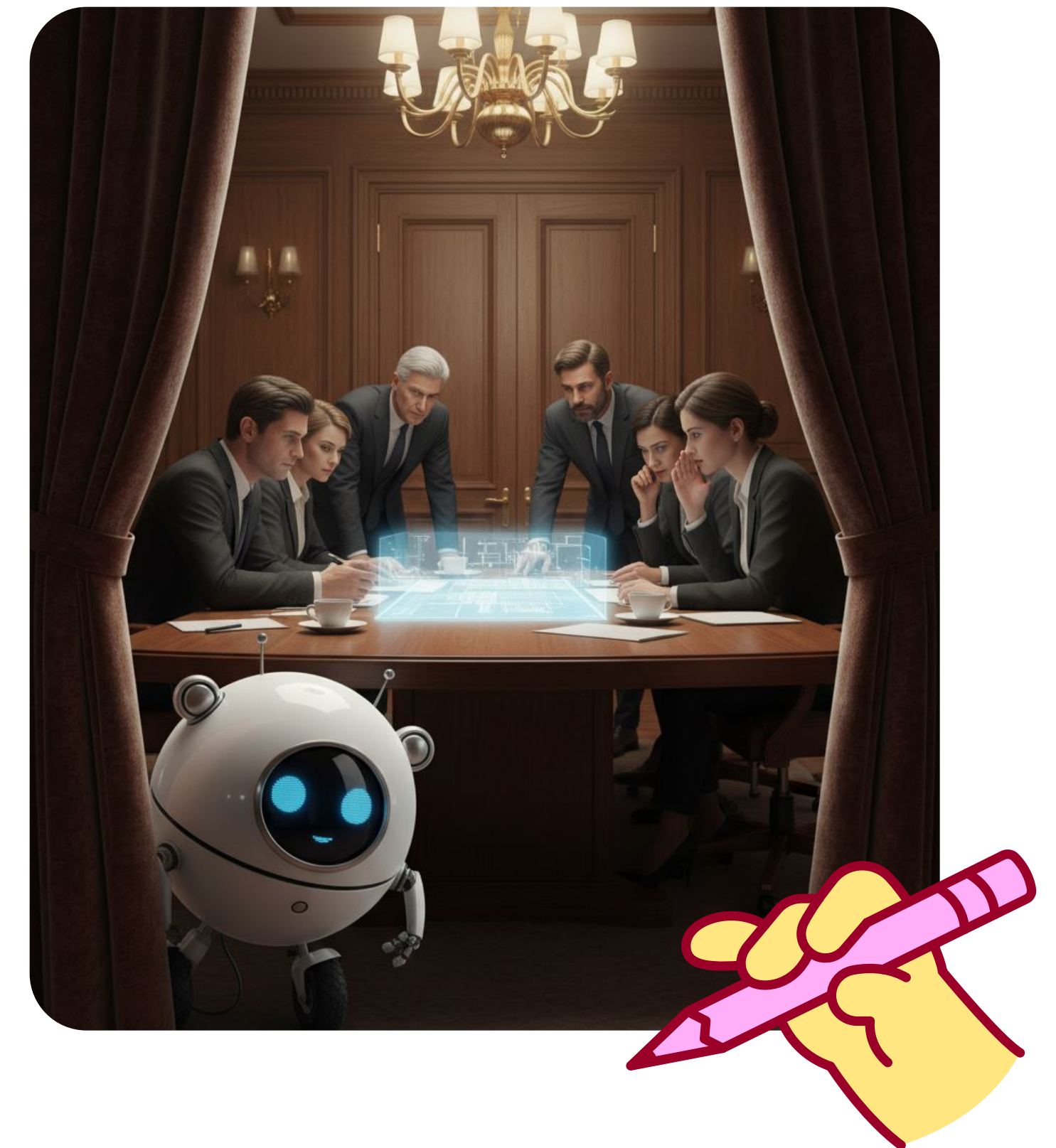


AI Meeting Note-Taker Attacks

Attackers send AI note-takers to join your meetings and capture everything that is said.

Why it works?

Employees are getting used to seeing bots from tools like Zoom, Teams, and Google Meet.



Shadow IT Became Shadow AI

Employees may be using:

- ✓ Personal Ai accounts
- ✓ Unapproved Ai Apps
- ✓ Connect Ai to company data without authorization

Why it works?

Companies are pushing employees to use AI to increase productivity. Without training and guardrails, it's a jungle out there





What can we do?

Keep A Human In The Loop

Ai can draft, summarize, classify and recommend

HOWEVER A person should approve decision that affect:



Customers



Legal



Money



Production System



Security

Human approval for critical actions Continuous monitoring and oversight
Only the access it needs Rules for what it can and cannot share



Ai Agents – Treat Them Like A New Hire

Before giving an AI agent access to company systems, make sure it has:



One clearly defined role



Only the access it needs



Rules for what it can and cannot share



Human approval for critical actions



Continuous monitoring and oversight

Do This Next

Write the AI job description before connecting it to Data

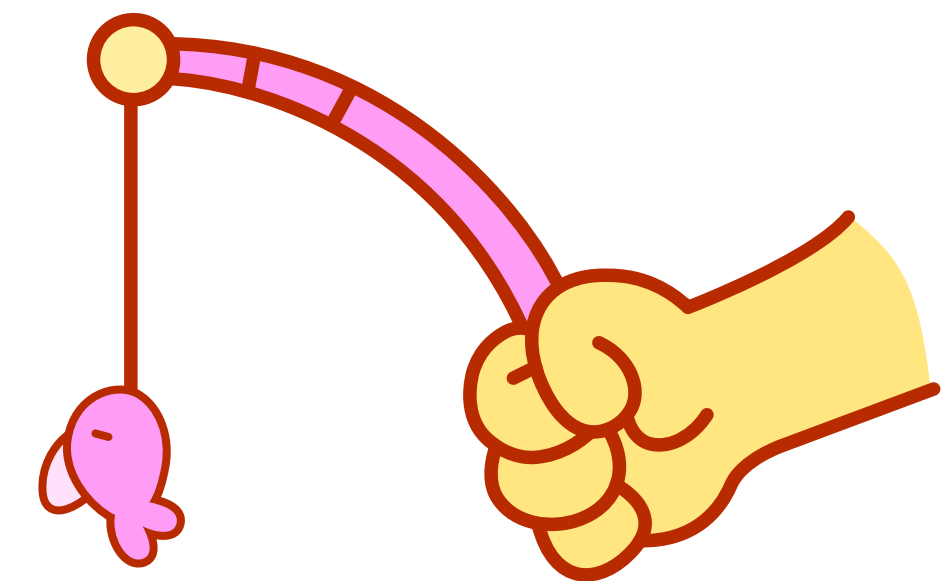


From Fake Emails To Fake Humans

- We used to ask: "Is this email real?"
- Now we must ask: "Is this person real?"
- You can no longer trust what you see or hear alone.
- Verify important requests using a trusted method (call back, Teams, known phone number, or another approved channel).
- Never skip approval or verification steps, even if the request appears to come from your CEO, a coworker, or a trusted partner.
- Policies matter more than ever. They protect you when your eyes and ears can't.

Remember:

In the age of AI, "Looks real" is no longer proof.
Verification is your new superpower.





Policies Only Work If People Know Them

Download Wizer's **AI Acceptable Use Policy** template and customize it for your organization today.

[**Download Policy Template**](#)

Download our **AI Usage Survey** to discover where AI is already being used.

[**Download Survey**](#)



Whew! You made it.

**Get started with Wizer for free
and train your team today...**

wizer-training.com 

