



How Hackers Are Using AI, and How to Stop Them

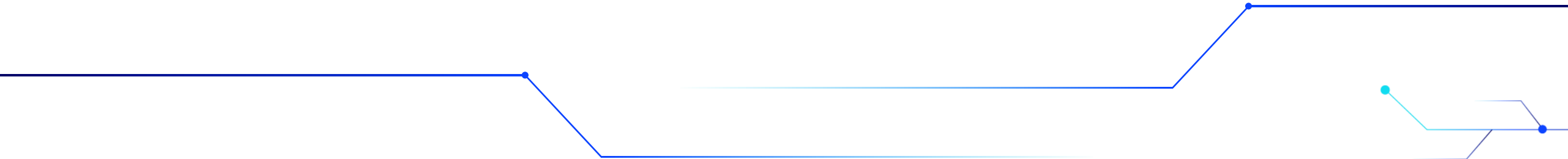
Will Bass

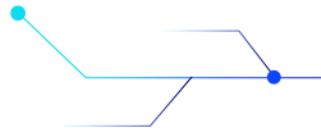
VP, Cybersecurity Services



Agenda

A decorative blue line graphic that starts as a horizontal line on the left, then angles upwards to the right, then continues as a horizontal line across the top of the slide.

- Introduction
 - AI Myths
 - How Hackers Leverage AI
 - What You Can Do About It
 - Q&A
- 
- A decorative blue line graphic that starts as a horizontal line on the left, then angles downwards to the right, then continues as a horizontal line across the bottom of the slide. In the bottom right corner, there is a small, stylized graphic consisting of several blue lines and dots, resembling a circuit or network diagram.



Introduction

Will Bass, VP of Cybersecurity Services

- Over 25 years of IS and IT Experience
- CISSP, CISA, QSA, CISM, CDPSE, and PMP
- Lead the Cybersecurity practice for Flexential Professional Services



[@WB_IT](https://twitter.com/WB_IT)



[linkedin.com/in/willbass](https://www.linkedin.com/in/willbass)



Will.Bass@Flexential.com

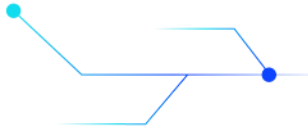


AI Myths



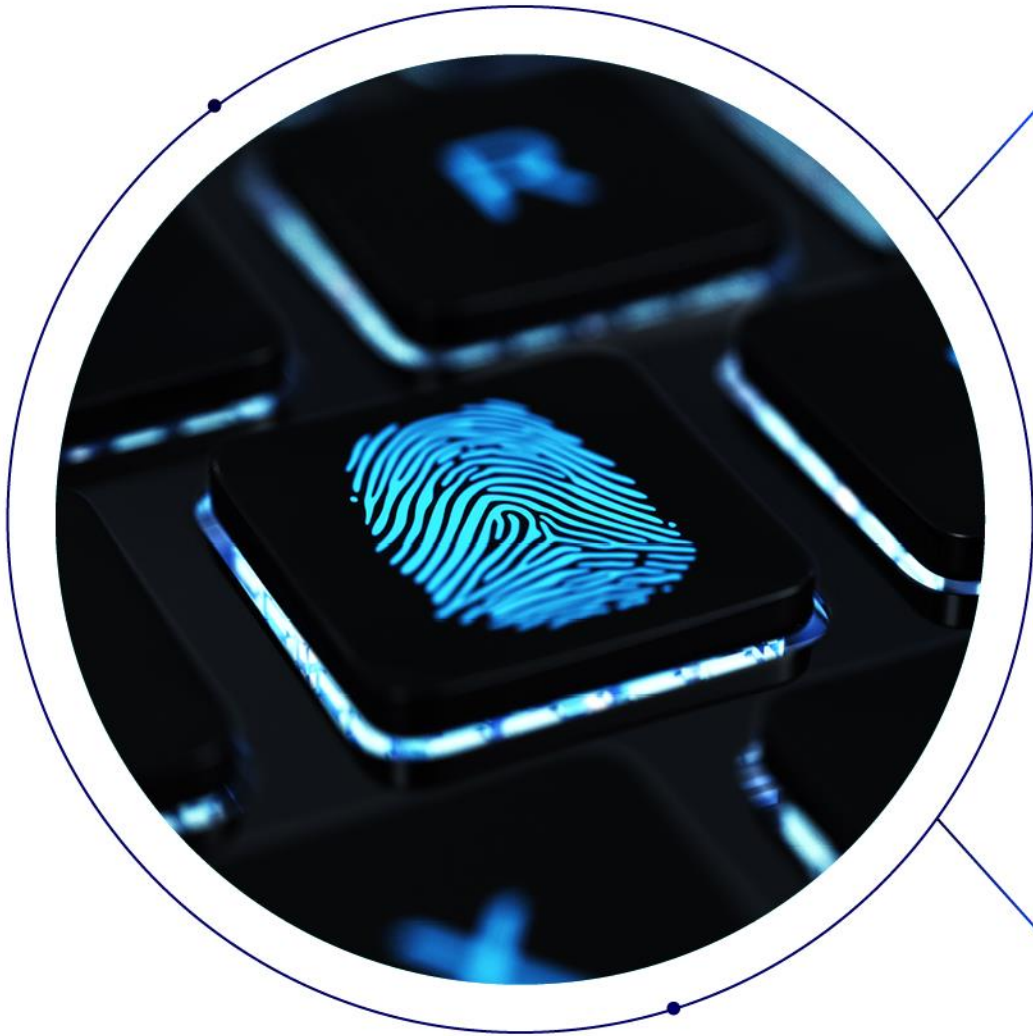
Artificial Intelligence Myths

Exposing the Hype



- Artificial Intelligence (AI) and Generative AI are the Same Thing
 - Generative AI is a subset of AI
 - Other AI technologies:
 - Machine Learning (ML)
 - Natural Language Processing (NLP)
- AI Replacing Hackers
 - 72% of hackers aren't worried about being replaced
- AI Taking Your Job
 - What you do and how you do it will change





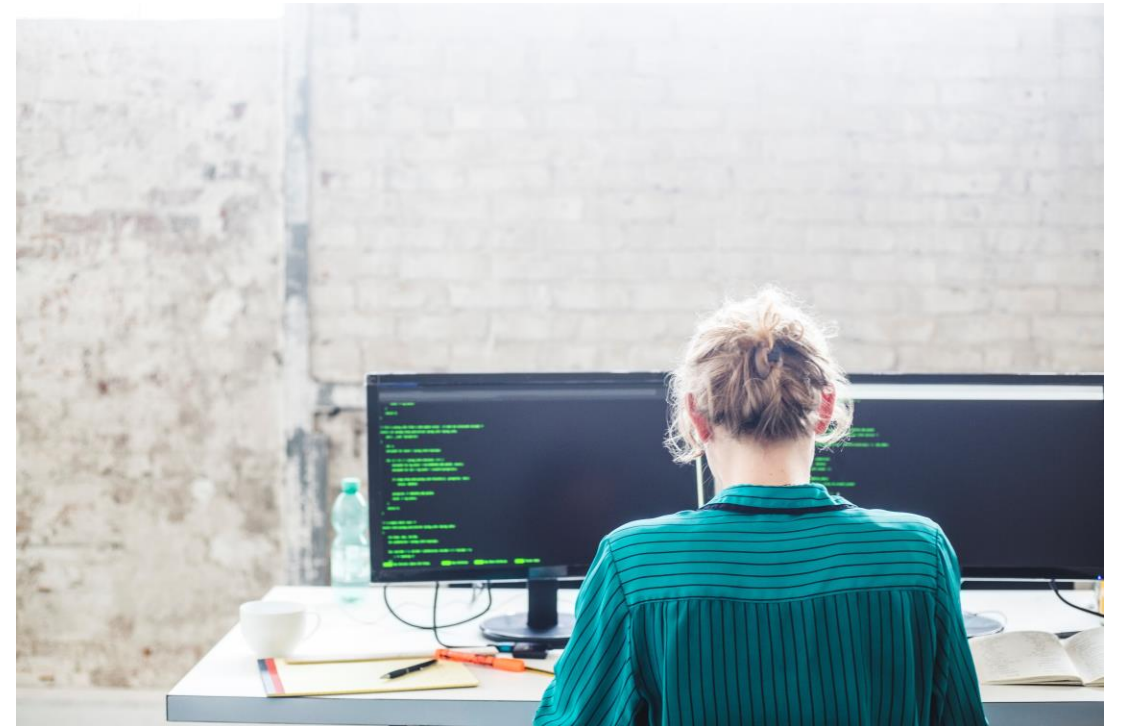
How Hackers Leverage AI



Social Engineering

Compromising People

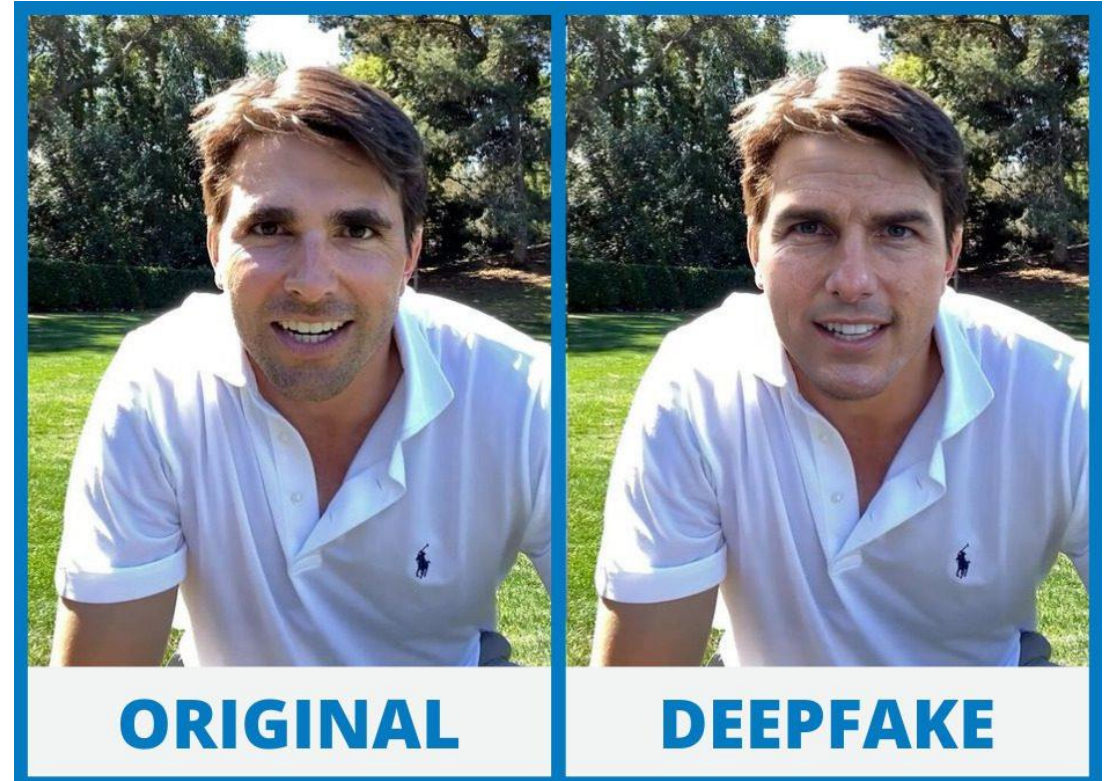
- Enhanced Phishing Tactics
 - Better phishing emails
- Personalized Attacks
 - Targeted based on publicly available information
- Chatbots
 - Illusion of genuine communication



Deep Fakes

What is Real?

- Video Deep Fakes
 - Evolution of deception
- Bypassing Biometrics
 - Authentication challenges
- Voice Deep Fakes
 - Who are you talking to?

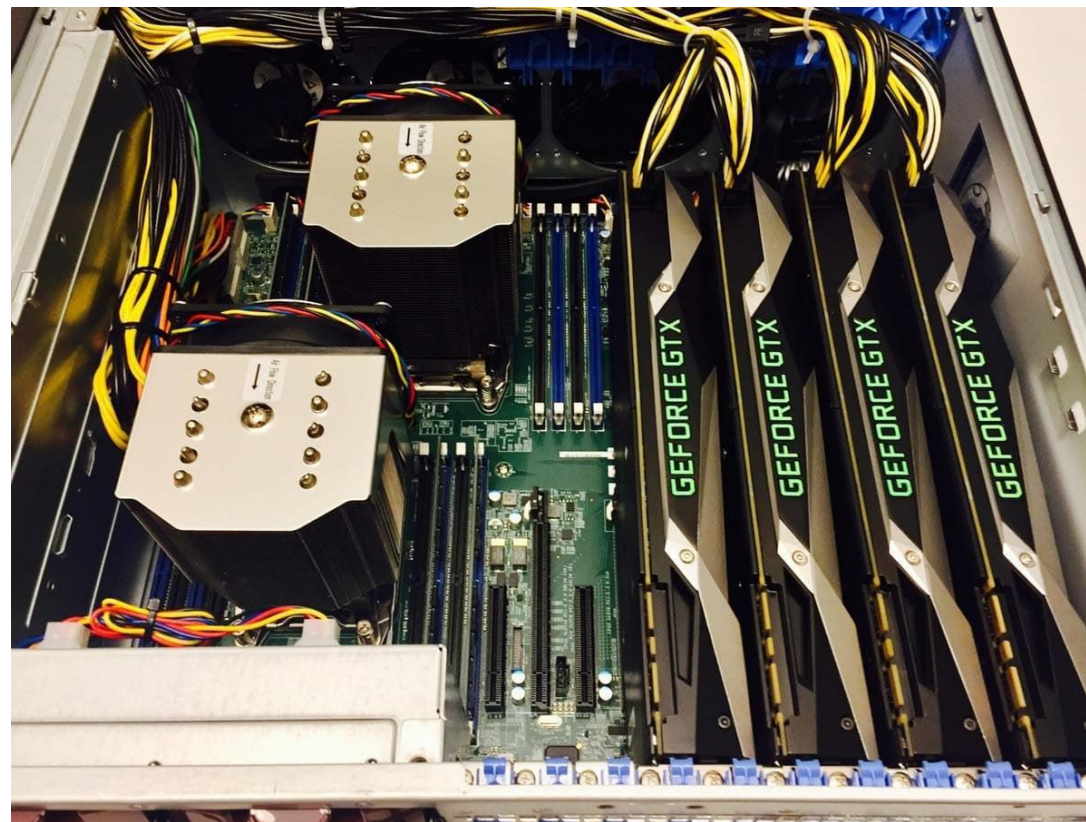




Password Guessing

Better Password Lists

- AI Enhanced Password Cracking
 - Social media
 - Previous compromises



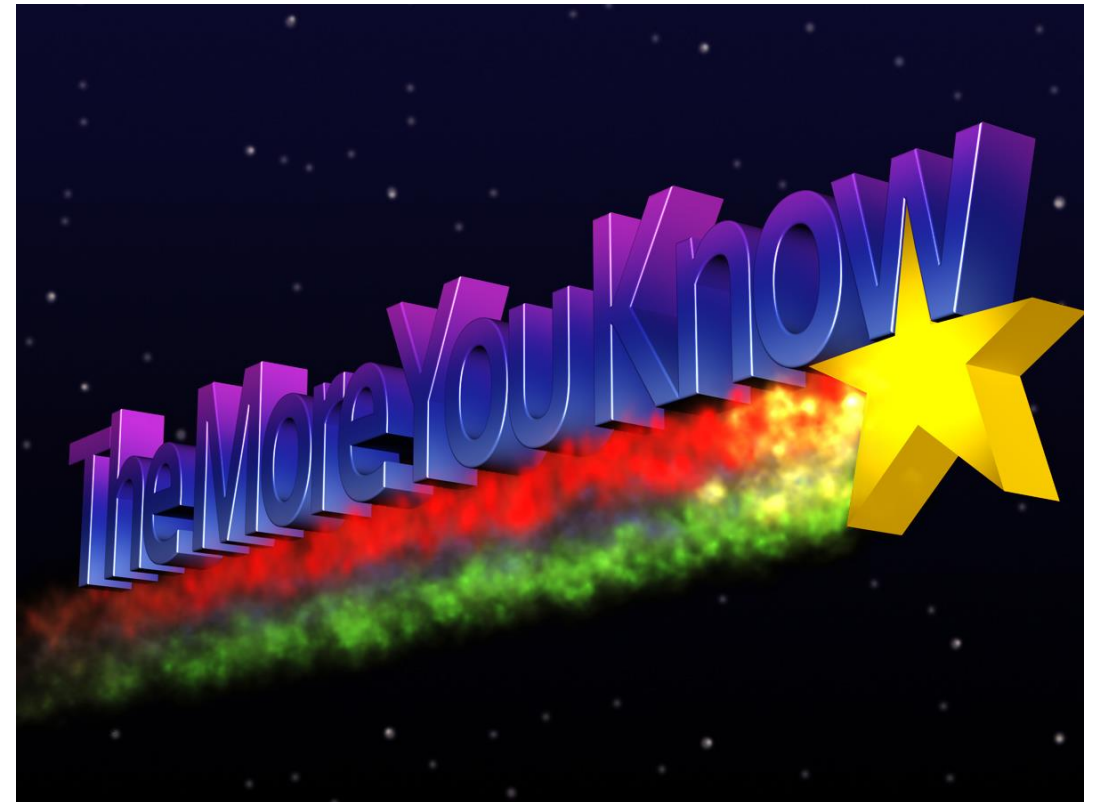


What You Can Do About It



User Education

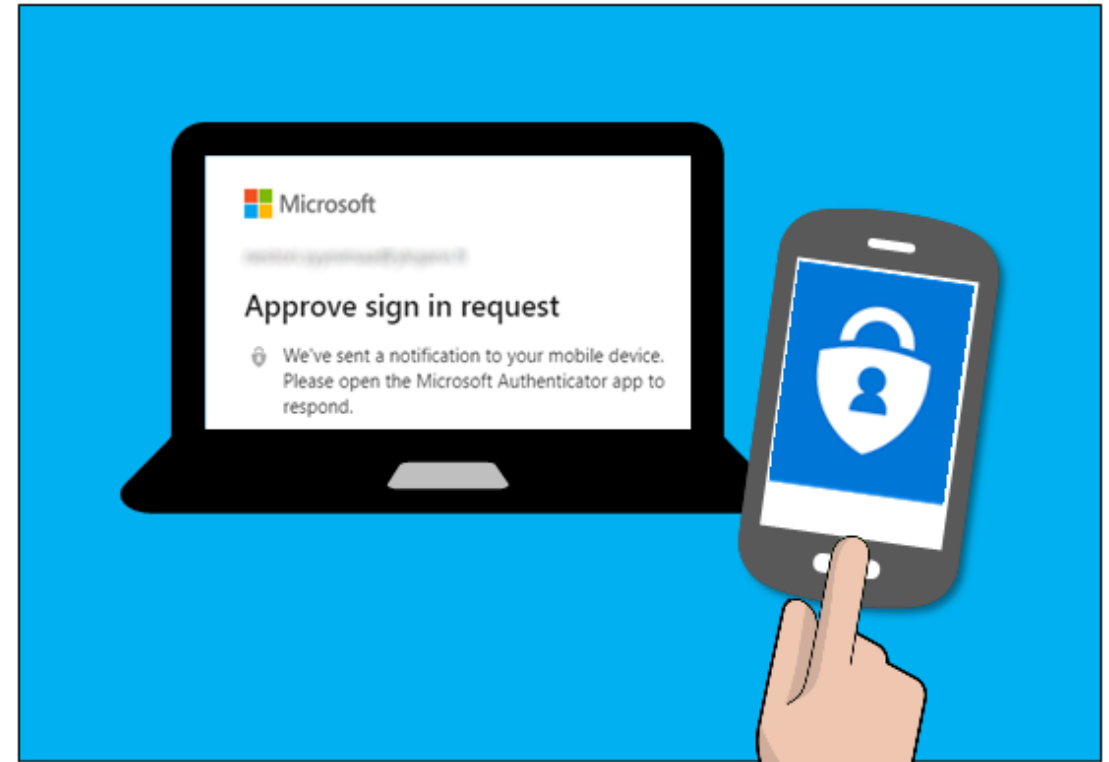
- Recognizing New Attack Vectors
 - Know the signs of an attack
- Phishing Awareness Training
 - Expand the tactics
 - Have a way to report



Multifactor Authentication and Beyond

Build Defenses

- Fortifying Security
 - Authenticator app
- Beyond Passwords
 - Public/Private keys
 - Offline knowledge



Defense-in-Depth

- Layered Defense Strategy
 - People
 - Process
 - Technology
- Use AI Defenses



Test Your Readiness

Do your defenses work?

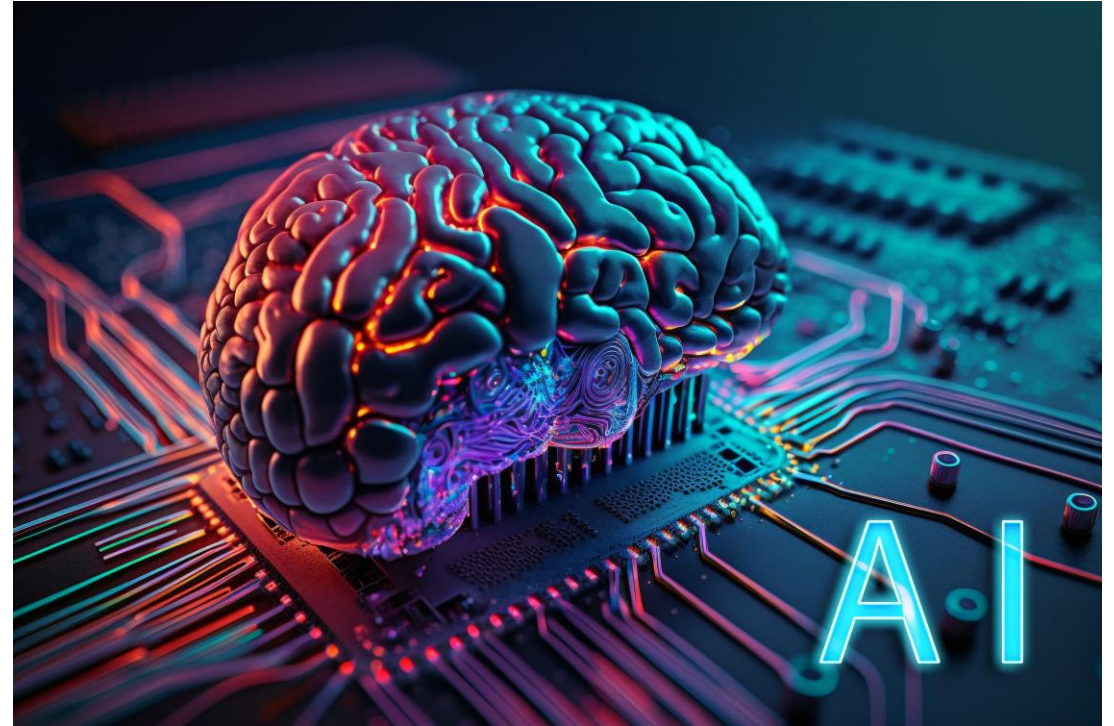
- Penetration Testing
 - Test defenses
- Tabletop Exercises
 - AI scenarios
- Social Engineering
 - AI attacks and techniques



Takeaways

Put AI to work for you

- Learn it, Love it
- Build it into your cybersecurity program
- Implement defenses before you need them





Questions?

