Slide 1 – Title / Cover

- “Hi everyone, today I’ll be sharing why women, particularly students, are at heightened risk from social engineering and AI-driven cyberattacks — and how the Feminine Intelligence Agency can help address this problem.”

Slide 2 – The Problem

- “Women face unique cyber risks — from catfishing and sextortion to intimate partner password theft. Generative AI is making these attacks more convincing, faster, and harder to detect. Our goal is to show why urgent action is needed.”

Slide 3 – Common Social Engineering Tactics

- “Here are some of the most common attack tactics we see targeting women: deepfake sextortion, AI-cloned emergency calls, personalized phishing DMs, romance chatbots, and stalkerware. Each of these exploits trust, emotion, or relationships to trick victims into giving away access.”

Slide 4 – Case Study

- “Let me give you a quick story: A student received what sounded like a real phone call from a friend begging for help. It was actually an AI-generated voice clone. She gave away her university login, and her account was hijacked within hours. This shows how realistic these scams have become.”

Slide 5 – Health Consequences

- “The impact goes beyond stolen data. Nearly half of women report anxiety after cyber harassment, with many also experiencing depression and even PTSD. These aren’t just technology issues — they’re mental health issues that universities are struggling to support.”

Slide 6 – Institutional Costs

- “These attacks also carry serious costs for schools: higher counseling demands, multimillion-dollar breach penalties, reduced student retention, and increased insurance premiums. This makes cybersecurity not only a student safety issue, but also a financial and reputational issue for universities.”

Slide 7 – Projected Threat Growth

- “And the threat is only accelerating. Incidents are rising year over year, powered by AI tools that attackers now use at scale. In fact, 87% of organizations faced AI-powered cyberattacks in 2025. Without intervention, these incidents are projected to double again by 2027.”

Slide 8 – Why Current Training Fails

- “Traditional cybersecurity training simply isn’t working for students. It’s too time-heavy, one-size-fits-all, and fails to create lasting behavior change. We need a new approach that meets students where they are.”

Slide 9 – FIA Micro-Training Works

- “Unlike generic cybersecurity training, FIA focuses on micro-trainings that students can actually use in their daily lives. They’re peer-to-peer, so the content feels relevant and relatable. They’re cost-effective and scalable, meaning universities can reach thousands of students without relying on expensive experts. And most importantly, they’re actionable — students walk away knowing exactly how to protect themselves, whether that’s tightening Instagram privacy settings or recognizing a phishing DM.”

Slide 10 – Risks of Waiting / Call to Action

- “The risks of waiting are clear: financial losses from breaches, reputational damage to institutions, and failing the duty of care to protect students. Now is the time to act — and FIA is ready with a solution that works.”