



FIA Brand Guide

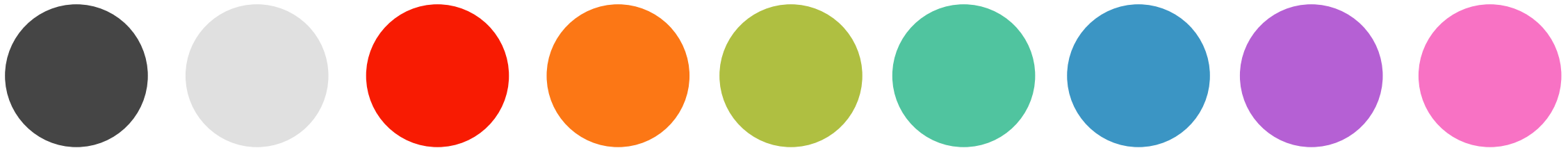
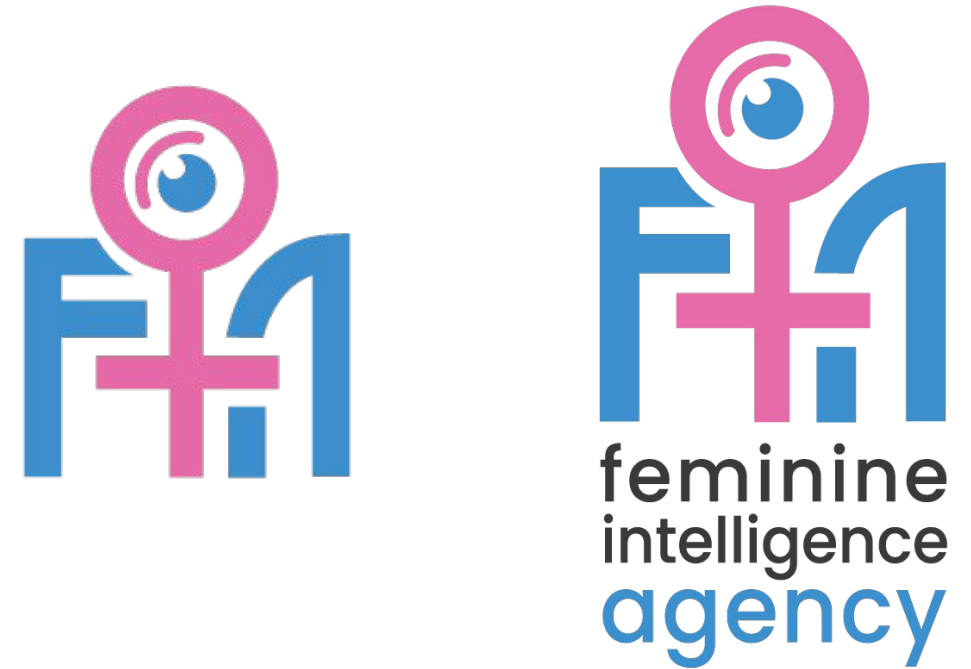
Headlines: Poppins Medium

Body text Lato Light

FIA icon library

[AI-images](#)

[Photos](#)





THE PROBLEM

As AI-driven threats escalate, the tools to protect women haven't kept pace. Most remain unaware of how digital coercion, social engineering, and psychological manipulation work—let alone how to defend against them.

Common Social Engineering Tactics

How the Attacks Happen



Deep-fake sextortion – AI-generated nudes used for blackmail



Voice-clone emergency scam – fake call from a friend in distress



AI-crafted phishing DM – customized messages with class/professor details



AI romance catfish – chatbots posing as romantic partners



Stalkerware installs – covert GPS/message tracking

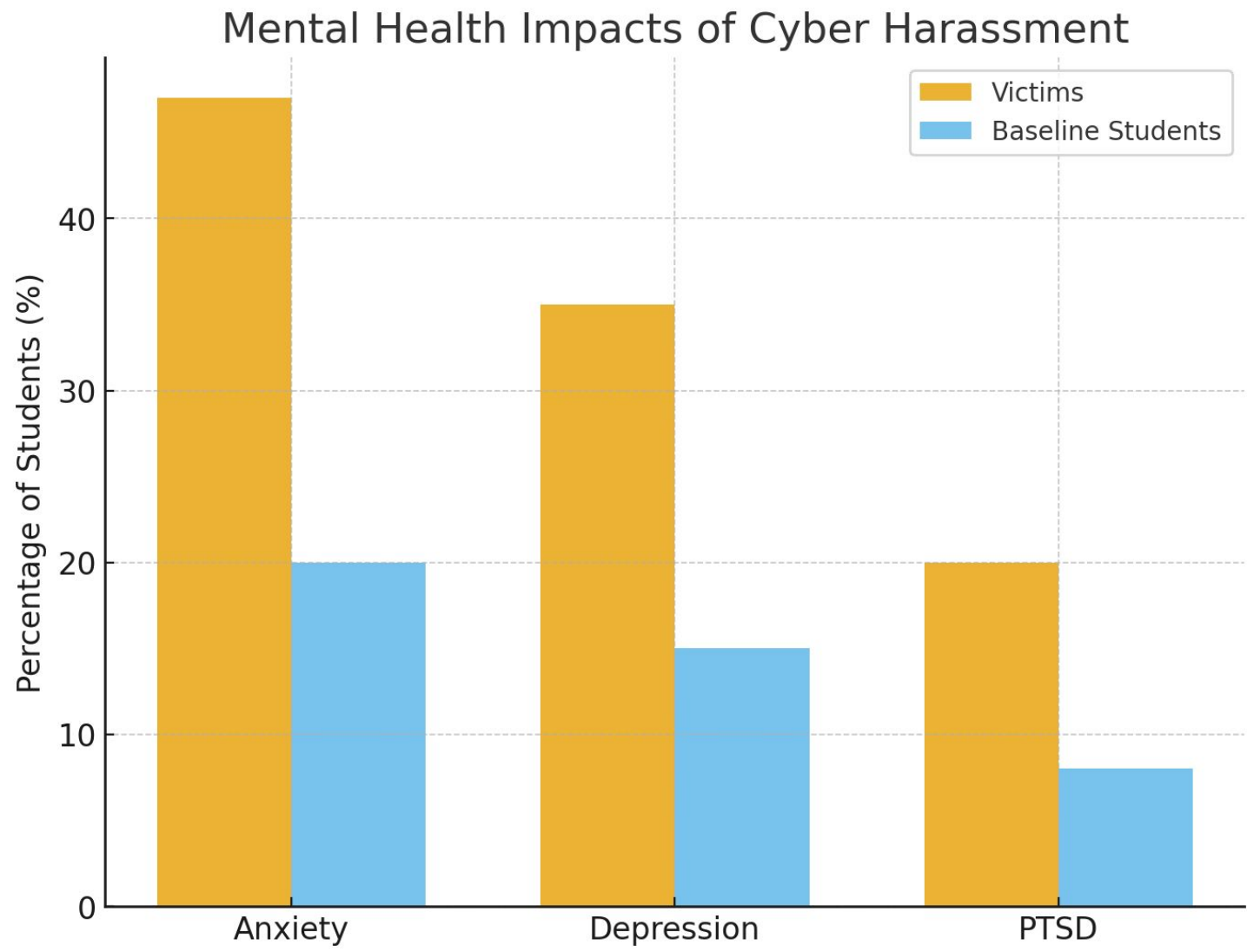
Source: Thorn (2024); The Guardian (2023); Palo Alto Networks Unit42 (2025); Secureframe (2025); UN Women (2024)

Health Consequences

The Human Toll

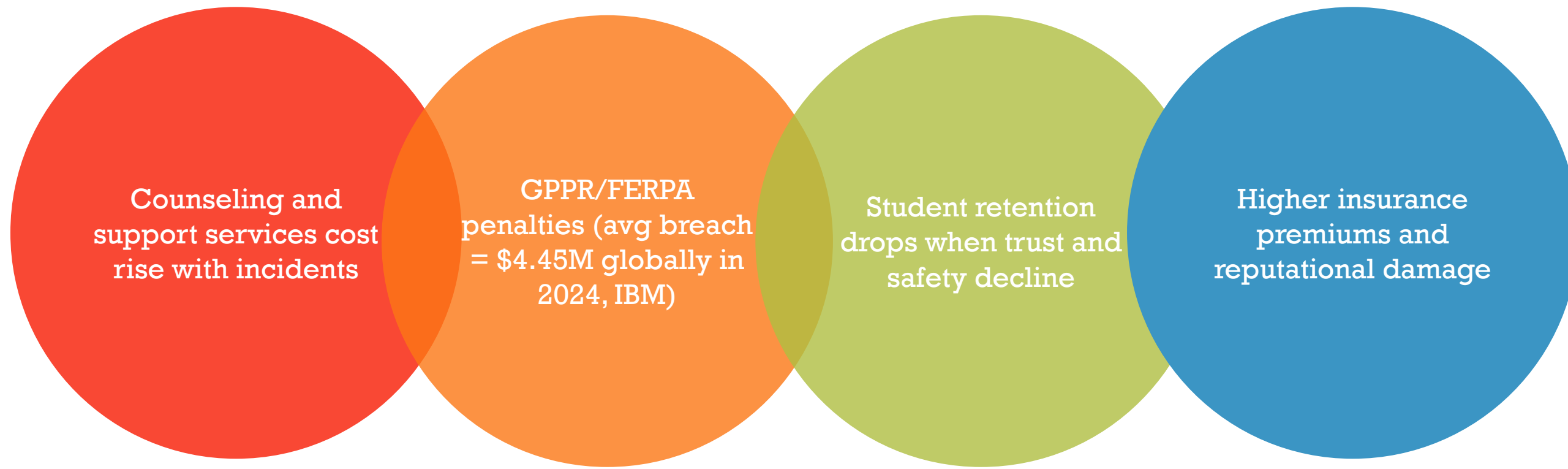
- 47% report anxiety after cyber harassment
- 20% report PTSD
- 35% report depression

Source: SafeHome.org, Cyberstalking Statistics (2024)



Institutional Costs

Why Universities Should Care



Counseling and
support services cost
rise with incidents

GPPR/FERPA
penalties (avg breach
= \$4.45M globally in
2024, IBM)

Student retention
drops when trust and
safety decline

Higher insurance
premiums and
reputational damage

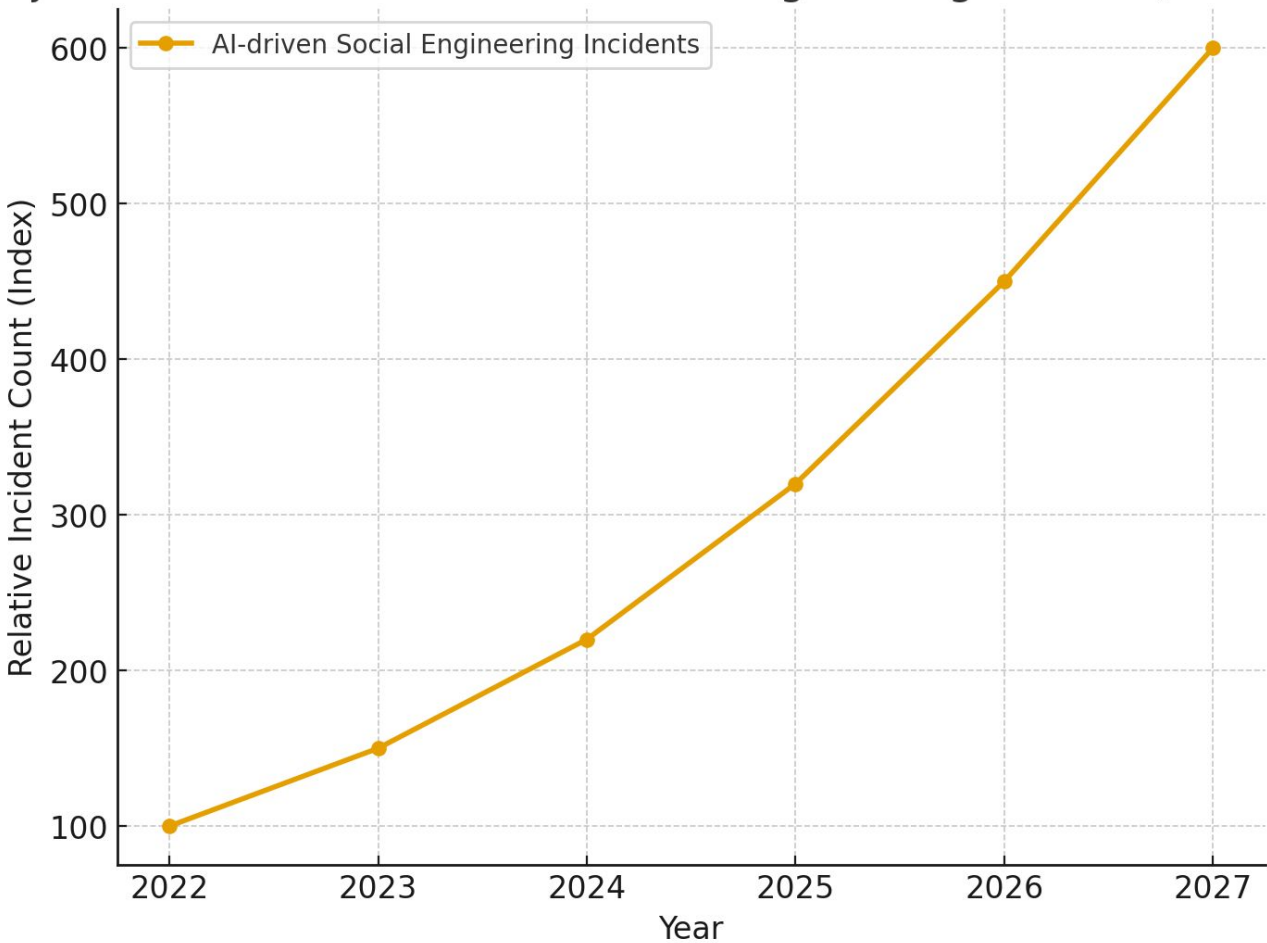
Source: IBM, Cost of a Data Breach
Report (2024); EDUCAUSE Review
(2023)

Projected Threat Growth

If No Action Is Taken...

- 📈 AI-driven social engineering attacks are increasing sharply year-over-year (2022 → 2027).
- 🤖 Attackers now use automation, deepfakes, and generative AI to scale faster than defenses.
- 🔍 Students are especially vulnerable to personalized, AI-crafted phishing and scams.
- ⚠️ *“87 % of organizations faced AI-powered cyberattacks in 2025”* – the threat is already mainstream.
- 💣 Without intervention, incidents are projected to double again by 2027, driving higher costs and risks for universities.

Projected Growth of AI-Driven Social Engineering Attacks (2022-2027)



Why Current Training Fails

The Status Quo Isn't Working



Time-heavy and expert led ->
not scalable for students

Generic, one-size fits all ->
low engagement

Minimal long-term behavior
change

Risks of Waiting / Call to Action

Act Now



Financial

Rising breach costs and penalties



Reputational

Loss of trust in the institutions



Duty of Care

Failing to protect students



FIA Micro-Training Works

-> Example: Set Instagram privacy in 3 steps



Peer-to-peer

Relatable, student
driven training



Cost-effective

No expensive
experts required



Scalable

Works across
entire campuses



Actionable

students leave
safer after every
session