

Konfydence for Universities

Defending Academic Integrity, Research, and Student Trust

Universities are no longer just centers of learning — they are high-value digital environments.

Student credentials, research data, grant information, and institutional access are increasingly targeted through **human-focused attacks**, not technical exploits.

Konfydence helps universities address the **human layer of cyber risk** through practical, behavior-based training that works under real pressure.

The Problem: Human Risk on Campus

Most campus security incidents do not begin with malware.

They begin with a **single moment of pressure**:

- A fake library login
- A “peer review” request
- An urgent message from “IT”
- A finance request to a student treasurer
- A compromised collaboration tool

These attacks don’t test technical skill — they exploit **urgency, authority, familiarity, and emotion**.

Beyond Finances: Protecting Academic Integrity

On campus, being “HACKed” isn’t just about money.

It can mean:

- Lost or leaked thesis data
- Stolen research or IP
- Compromised academic credentials
- Grant or publication interference
- Reputational damage to the institution

Konfydence trains students and staff to recognize manipulation **before credentials, research, or access are lost.**

The H.A.C.K. Framework (Behavior, Not Awareness)

Konfydence is built around the H.A.C.K. framework — a simple diagnostic model students can apply **in real time**:

- **H — Hurry:** Artificial urgency that blocks thinking
- **A — Authority:** Titles or institutions used to force compliance
- **C — Comfort:** Familiar names, tools, or tone that lower skepticism
- **K — Kill-Switch Emotions:** Fear, excitement, shame, or pressure

When one or more H.A.C.K. signals appear, students are trained to **pause before acting.**

The 5-Second Defense: A Trainable Skill

Konfydence does not ask students to memorize threats.
It trains a **repeatable behavioral response.**

The 5-Second Defense

When pressure appears:

1. **Pause** — do not click, reply, or act immediately
2. **Verify** — use a second channel (not the message itself)
3. **Apply the Easy-Money Test** — if it feels too easy or too urgent, stop
4. **Report, Don't Hide** — escalation is strength, not failure

This turns awareness into **habitual behavior.**

Learning by Doing: Scenario-Based Training

Students don't read about scams — they **experience realistic scenarios** in a safe environment.

- 80+ real-world scenarios
- Short, high-stakes decisions
- Group discussion and reflection

- No fear tactics, no shaming

The result: practiced responses under pressure, not theoretical knowledge.

For Student Leaders & Organizations

Student unions, clubs, and societies manage:

- Real budgets
- Events and vendors
- Member data
- Shared credentials

Konfydence provides a **plug-and-play safety toolkit** for:

- Student unions
- Clubs & societies
- Fraternities & residences
- Student councils

Turn a 20-minute meeting into a practical safety workshop — no IT expertise required.

Evidence That Institutions Can Use

Konfydence supports **documentation and accountability**, not just participation.

Universities receive:

- Participation logs
- Observational summaries
- Behavioral insight templates
- Audit-ready narrative summaries

This allows institutions to demonstrate **human risk management**, not just awareness completion.

One Kit. One Campus Impact.

Through our Buy-One-Give-One model:

- Each physical Konfydence kit activates a **1-year digital license for a school or university**
 - Institutions gain access without procurement friction
 - Training reaches students who need it most
-

Start With a Pilot

Most universities begin with:

- One faculty or department
- Orientation programs
- Student leadership groups
- International or first-year cohorts

Konfydence scales from pilot to campus-wide adoption without re-engineering.