DEFEND YOUR DEGREE

The University Student Guide to Digital Resilience

The Reality Check

You worked hard to get here. Scammers know it. They don’t hack your laptop; they hack your stress, your ambition, and your bank account. In a university setting, the biggest threats aren't "viruses"—they are fake opportunities designed to exploit your need for income and academic success.

The Top 4 University Scams

1. The "Money Mule" Trap (High Risk) A "job offer" or "social media contact" asks you to receive money into your personal bank account and then transfer it to another account, allowing you to keep a 10% commission for your "trouble."

- **Reality:** This is **Money Laundering**. You are being used to move stolen or criminal funds. Even if you didn't know the money was "dirty," you can face criminal charges, bank account closure, and expulsion.
- **HACK Signal: Comfort** (It looks like a simple task) and **Kill-switch** (Extreme excitement over "easy" money).

2. The "Ghost" Internship / Remote Job You receive a high-paying, remote job offer for a "Personal Assistant" or "Data Entry" role. They send you a digital check to buy equipment and ask you to wire the "excess" back to their supplier.

- **Reality:** The check is fake and will bounce in 3 days. The money you wired back is your own real cash—and it’s gone.
- **HACK Signal: Hurry** (They need the equipment ordered "today") and **Authority** (The recruiter seems professional).

3. The "Tuition Discount" Fraud An email or WhatsApp message offers a 10–20% discount on your tuition if you pay via an "international payment agent" or a specific cryptocurrency link.

- **Reality:** Universities **never** offer tuition discounts through third-party agents or crypto. They are simply stealing your tuition money.
- **HACK Signal: Hurry** (Limited time offer) and **Kill-switch** (The relief of saving thousands of dollars).

4. The "Department Dean" Gift Card Scam An urgent text or email from someone claiming to be your Professor or a Dean. They claim they are in a meeting and need you to buy gift cards for a departmental event immediately.

- **Reality:** No faculty member will ever ask a student to fund an event with gift cards.
- **HACK Signal: Authority** (Using a leader's name) and **Hurry** (The "meeting" is happening now).

Don’t Get HACKed: Your 5-Second Defense

- **H — HURRY:** Are they rushing you? "Pay within 2 hours" or "Only 1 spot left!"
- **A — AUTHORITY:** Are they using the University logo or a Dean’s name to stop you from double-checking?
- **C — COMFORT:** Does it look like a campus portal? Remember: scammers can spoof ".edu" addresses.
- **K — KILL-SWITCH:** Are you feeling a rush of fear about your grades or intense excitement about a "dream" job? **If your heart is racing, your logic is off.**

The "Permission to Pause" Rule

1. **Verify via a Second Channel:** Never click the link provided. Go to the official University portal, call the Financial Aid office, or walk into the department in person.
2. **The "Easy Money" Test:** If a job pays $500 for an hour of work, or asks you to move money through your personal account, **it is a scam.**
3. **Report, Don't Hide:** If you have been targeted or if you clicked a link, tell **Campus IT or Student Security** immediately. They are there to help, not to judge.

Master the Skill

Don't wait for a real threat to hit your bank account. Use the **Konfydence Scam Survival Kit**—a 15-minute tabletop training tool designed to build the "Pause Habit" you need to protect your finances throughout your academic career.

Learn more at: www.konfydence.com