Author: Tyrell Fowler

Senior Business Administration Student | Cybersecurity Enthusiast | Security+ Candidate

Austin, TX | tyrell607@gmail.com | (832) 918-8242

🛠️ Project Overview

This simulated threat analysis explores a phishing campaign targeting university students with a fake financial aid alert. The goal was to evaluate red flags, assess risk, and recommend countermeasures. This project demonstrates my ability to identify social engineering tactics and communicate technical findings clearly — a valuable skill for both civilian and military cyber roles.

📧 Phishing Email Breakdown

- **Subject Line:** Urgent: Your Financial Aid Has Been Revoked
- **Sender:** htustudentaid@gmail.com
- **Tactic:** Fear-based urgency + impersonation of authority

- **Fake Link:** Redirects to a phishing login portal mimicking the university site

---

🔍 Red Flags Identified

- Domain mismatch (gmail.com vs .edu)
- Grammatical and spelling errors
- Emotional manipulation language
- URL does not match legitimate portal

💥 Potential Impact

- Student login credentials compromised

- Unauthorized portal access
- Financial data theft
- Further phishing or lateral movement using compromised accounts

---

✅ **Recommended Defenses**

- Enable email domain authentication (SPF, DKIM, DMARC)
- Require Multi-Factor Authentication (MFA) on student portals
- Launch anti-phishing awareness campaigns
- Monitor failed logins from suspicious IP addresses

🧠 **Reflection**

This project taught me how threat actors exploit human emotion and urgency. I learned how to think like an attacker — and defend like a cybersecurity analyst. It also helped me realize that

my overthinking tendencies are a strength when applied to cyber defense, risk assessment, and intelligence work.