THIEN QUY PHAM

Toledo, OH | ThienQuy.Pham@rockets.utoledo.edu | 419-250-9437
https://www.linkedin.com/in/thienquypham/ | https://github.com/thienquy05 | https://thienquypham.vercel.app/

SUMMARY

Computer Science student focused on cybersecurity and AI security, with 15+ security incidents remediated in four months and 1,000+ endpoints managed through Active Directory and Microsoft Intune. Red-teamed an LLM phishing detector against 41 payloads. Seeking a **Summer 2027 cybersecurity internship**.

EDUCATION

The University of Toledo *Toledo, OH*
Bachelor of Science in Computer Science | GPA: 3.6 | Expected Dec 2027

CERTIFICATIONS

- Google Cybersecurity Professional Certificate (Coursera, Oct 2025)
- CompTIA Security+ (in progress)

PROJECTS

AI Phishing Detection Platform — *Cybersecurity Analyst & Developer, 4-person team*
https://github.com/Phishing-Detection-Team/fraudify

- Designed a regex pre-flight filter modeled on known jailbreak and prompt-injection patterns (DAN, ChatML tokens, instruction-override phrasing) that blocks attacks before they reach the LLM.
- Red-teamed the filter against 41 real attack payloads, found the most common jailbreak phrase slipping through, and patched the gap to lift the block rate 10 percentage points with zero false positives.
- Cut response time on blocked attempts from a 15-20 second model inference call to under 5 milliseconds by short-circuiting the LLM entirely.
- Closed a hidden-content injection vector in the Gmail/Outlook extension by parsing email bodies with innerText rather than textContent, keeping CSS-hidden payloads out of the analyzer.
- Applied NIST CSF data-integrity practices to the PostgreSQL layer: bcrypt password hashing, 20 check constraints, and 15 field validators enforced at both the database and ORM layers across 5 models.

EXPERIENCE

University of Toledo *Toledo, OH*

IT System Administrator *Jan 2026 – Present*

- Responded to 15+ security incidents in four months: identified and remediated unpatched Windows 10 endpoints carrying open vulnerabilities, and isolated 2 malware-infected devices from the network.
- Triage security alerts and enforce device compliance policies across 1,000+ Windows and macOS endpoints managed through Active Directory and Microsoft Intune.
- Own endpoint lifecycle management: imaging, deployment, OS and application patching, and hardware refresh cycles that keep the fleet in compliance.
- Provide Tier 2 support for 250+ classrooms and offices, resolving desktop, network, printer, and peripheral failures and documenting root cause for the Tier 1 queue.

Undergraduate Research Assistant *Dec 2025 – Present*

- Develop Python/OpenCV video tracking and behavior-state analysis to extract zebrafish motion features from Novel Tank Test footage.
- Prepare labeled trial data and training workflows that estimate compound-family probabilities, evaluate models, and flag novel responses.

IT Support Technician *Dec 2025 – May 2026*

- Triaged 10-15 tickets per week through UToledoHelp, the university's in-house ticketing platform, spanning same-day fixes to multi-day network and hardware escalations.
- Escalated each case through a structured process, writing resolution notes clear enough for the next technician to reproduce the fix.

SKILLS

Cybersecurity: Incident Response, Threat Analysis, Malware Containment, Vulnerability & Patch Management, Endpoint Security, NIST CSF, OSINT, Network Segmentation
AI Security: Prompt Injection Defense, Jailbreak Red-Teaming, Model Evaluation, Input Validation, OpenCV
Systems Administration: Active Directory, Microsoft Intune, PowerShell, Windows, macOS, Linux, VMware, Endpoint Imaging, Tier 2 Support
Languages & Tools: Python, SQL, C, C++, Java, JavaScript, HTML/CSS, Git, Flask, PostgreSQL/SQLite3
Lab & Coursework: Splunk, TryHackMe, HackTheBox