

AMANI J. DWORKIN

Chicago, IL • 734-646-2113 • amanijaise07@gmail.com • amanidworkin.com • linkedin.com/in/amanidworkin

EDUCATION

DePaul University — B.S. Cybersecurity

Class of 2028

Presidential Scholar | Dean's List

SKILLS & CERTIFICATIONS

HARDWARE – Custom PC Building & Repair | Cisco Switching & Routing (VLAN, ACL, Static Routing) | BadUSB | Flipper Zero | HackRF One (SDR)

OFFENSIVE & TESTING – Kali Linux / NetHunter | Metasploit | Nmap | k6 (load & availability testing) | Self-built phishing framework

DEFENSIVE & ANALYSIS – Wireshark | Microsoft Defender | Firewall policy configuration | Endpoint hardening

INFRASTRUCTURE – Proxmox virtualization | Isolated VM environments | Network segmentation

FRAMEWORKS – MITRE ATT&CK (Enterprise & ICS) | NIST CSF 2.0 | NIST AI RMF

LANGUAGES – Python | Java | PowerShell | Bash

CERTIFICATIONS – Cybersecurity (UofM Nexus) | AI Essentials (Google)

EXPERIENCE

The Obsidia Project — Co-Founder & Lead Technical Author/Editor

2026–Present

Independent 501(c)(3) nonprofit producing cited public case studies of major cybersecurity incidents.

- Authored the inaugural case study on the Colonial Pipeline ransomware attack: a ten-section public-record analysis built on 34 numbered citations and an 11-technique MITRE ATT&CK for ICS mapping.
- Produced the companion four-round tabletop exercise mapped to NIST CSF 2.0, with defined participant roles, a severity reference table, and readiness scoring.
- Own the organization's evidence standard: source weighting, per-sentence citation, and boundary language separating what the public record establishes from what it does not.
- Administer the formal review and assent process for a ten-member advisory board that includes the founding leader of the UK's National Cyber Security Centre and a co-creator of CVE.
- Authored the internal methodology governing AI-assisted public-record collection and drafting, defining where machine-assembled evidence ends and author judgment begins.

Independent Security Research — AI Phishing Defense Architectures

2026–Present

Comparative evaluation of three AI defense architectures under adaptive attack.

- Designing a controlled head-to-head evaluation of three defense architectures, holding the underlying model constant so architecture is the only variable.
- Architected ICC (Isolated Criteria Code), an original design in which static code extracts signals and the model reasons only over structured signals and trusted context, never attacker-controlled text; benchmarked against a dual-LLM privilege-separation pattern and a single-model baseline. Testing in progress.
- Stress-testing each architecture against attack families tailored to its specific weaknesses: prompt injection, AI-personalized phishing, business email compromise, compromised-inbox attacks, and architecture-specific attacks such as evidence-field injection.
- Measuring attack success rate alongside false-positive rate on legitimate business email — a detector that blocks real operations is unusable regardless of catch rate.
- Built and administer the supporting lab: Proxmox virtualization with isolated offensive and defensive VMs, plus mobile and physical-access testing with Kali NetHunter, BadUSB, and rogue-device payloads.

GhostGuard — Creator & Developer

2026

- Built and published an AI-powered phishing detection app (5-star App Store rating, 10+ reviews) that flags suspicious emails and messages and returns plain-language threat verdicts.
- Integrated a large language model with Python to analyze message content, sender reputation, and known-bad-sender patterns.
- Developed a "Check a Link" feature that detonates suspicious URLs in a sandboxed VM and cross-references third-party threat-intelligence and reputation APIs.
- Now serves as the single-model baseline in ongoing adversarial research, where its architecture is being tested for structural susceptibility to prompt injection.

Sphinx Organization — Security Contractor

2025

- Designed and executed an authorized phishing simulation against ~15 employees including full executive leadership, using a self-built phishing simulation framework.
- Conducted authorized load and availability testing with k6, finding that the site could not sustain elevated request rates — a denial-of-service exposure from absent rate limiting.
- Evaluated endpoint, physical, and third-party vendor security posture, including Microsoft Defender configuration and firewall policy.
- Delivered findings and remediation recommendations that were adopted by executive leadership.

ACCOMPLISHMENTS

BIG EAST Rugby Freshman of the Year (2025) | Division I Student-Athlete (2025–Present) | Youngest-Ever Recipient, UofM Nexus Cybersecurity Certification (2023) | DEF CON NIRUBI Competition Winner (Duo) | National African American Academic Recognition (2024)