| Tomiwa Oladejo |
| --- |

Milton Keynes, Buckinghamshire | +44 7342897651 | tommdej@gmail.com

# Profile

A Cyber Security graduate with a robust academic foundation and hands-on expertise in information systems, network security, and advanced threat mitigation strategies. Demonstrates proficiency in diverse operating systems, state-of-the-art security tools, and sophisticated incident response protocols. Adept at identifying vulnerabilities and implementing strategic remediations, with a methodical and detail-oriented approach. Exceptional communication and collaborative skills which complement a commitment to continuous professional development and innovation in cybersecurity practices.

# Project Experience

## Email spam filter (Final year project) | 11th October 2022 – 21st April 2023

* Engineered a machine-learning-based spam detection system leveraging Python and TensorFlow frameworks.
* Applied sophisticated preprocessing techniques such as tokenization and stop-word elimination to optimise dataset accuracy.
* Evaluated algorithmic performance through rigorous testing, documenting results in an extensive technical report.

## Vulnerability assessment and penetration testing| 11th October 2022 – 16th March 2023

* Executed systematic vulnerability assessments of simulated enterprise networks to identify critical security weaknesses.
* Utilised industry-standard tools, including Nmap, Wireshark, and Metasploit, for network scanning, packet analysis, and exploit validation.
* Delivered comprehensive technical recommendations in a structured remediation plan, supported by empirical data.

## Information security management system portfolio | 29th September 2021 – 10th March 2022

* Security Issue Identification & Analysis: Identified the specific security incident and analysed the techniques used by attackers, the vulnerabilities exploited, and the affected assets (e.g., user data, company reputation).
* Impact & Threat Assessment: Evaluated the short- and long-term impacts of the breach on the organisation, including financial loss and reputational damage, and identified potential threat vectors and vulnerabilities.
* Risk Management & Proposed Controls: Developed a risk register with identified risks and implemented procedural, technical, and physical controls (e.g., firewalls, training programs, access controls) to mitigate future threats.

## Computer forensics and investigation | 19th January 2023 – 28th April 2023

* Conducted advanced forensic analysis utilising Cellebrite’s Physical Analyser to extract and parse digital data.
* Performed comprehensive evaluations of textual, multimedia, and application datasets to identify evidentiary artefacts.
* Synthesised findings into a detailed forensic report, adhering to rigorous methodological standards and evidentiary protocols.

# Education

## Nottingham trent university, Nottingham| September 2020 – July 2023

* BSc (Hons) Computer Systems (Cyber Security) – Graduated with a 2:1

# Relevant Modules

* Digital Investigations
* Security in Practice
* Advanced Networking
* Internet of Things
* Information Security
* Cyber Security
* Advanced Topics
* Final Year Project - Coded an Email Spam Filter

# Skills & Abilities

* Security Tools: Nmap, Firewalls, IDS/IPS.
* Networking: Advanced Network Protocol Analysis, Traffic Monitoring and Incident Response Coordination.
* Cybersecurity Expertise: Advanced Threat Detection, Comprehensive Vulnerability Management, Structured Incident Handling

# Additional Information

* Engaged in ongoing research to remain at the forefront of emerging cybersecurity threats and mitigation techniques.
* Working towards Certification in CompTIA Security+
* Programming & Scripting: Python and Java
* Tools and Platforms: Linux (Kali, Ubuntu), VMWare, Metasploit, Wireshark, Autopsy, Cellebrite.
* Professional Attributes: Exceptional communication, critical problem-solving, efficient time management, and meticulous attention to detail.