A close up of a logo

AI-generated content may be incorrect.

**Name: Shafiullah Anik**

**Student id: 30454295**

**ITECH-1502 Cyber security Fundamentals**

**Final project report**

**1. Project Summary**

This project focused on applying the cybersecurity concepts learned in class to a real-world scenario. I selected and completed the “Phishing Emails in Action” room on the TryHackMe platform, which provides practical, guided environments for learning through simulations. The main aim was to identify the indicators of phishing attempts by analyzing genuine phishing emails. Through this challenge, I learned how attackers use social engineering, visual deception, and technical manipulation to trick users into clicking malicious links or sharing sensitive information. I completed all eight tasks within the room, covering multiple phishing scenarios such as fake PayPal payments, package delivery updates, and document-sharing scams. Evidence of my work, including screenshots of progress, completion, and my TryHackMe account, has been attached to this report. Overall, this project strengthened my understanding of phishing analysis and demonstrated my ability to apply the NIST Cybersecurity Framework (CSF) concepts particularly Detect and Respond in a practical setting.

**2. Introduction**

Phishing attacks continue to be one of the most effective and dangerous cybersecurity threats. Attackers constantly create fake emails and websites that imitate trusted organizations to deceive victims into sharing credentials or financial information. This project provided a safe, guided environment for exploring how phishing works and how to detect such attacks in real-world settings. The **TryHackMe “Phishing Emails in Action”** room is designed to teach security students how to recognize phishing indicators, analyze malicious content, and connect theoretical knowledge to hands-on investigation techniques.

My project directly aligns with the **ITECH1502 unit learning outcomes**, which focus on building fundamental cybersecurity skills, developing analytical investigation techniques, and understanding defensive measures.  
**My professional portfolio link:** [Insert LinkedIn or GitHub link].

**3. Problem / Challenge Description**

The **challenge** was to examine a set of real phishing emails inside TryHackMe and determine what characteristics made them suspicious or malicious.

Each email contained a unique trick, such as a fake shipping notice, document download request, or account update message. The lab simulated a real-world analyst workflow where the goal is to **investigate**, **confirm** phishing indicators, and **document findings**.

This challenge was particularly relevant to the **Detect** and **Respond** functions of the NIST CSF, as I was required to:

* Identify potential phishing indicators
* Validate whether they represented real threats
* Decide on mitigation or response actions

Through this, I practiced the same analytical process that a Security Operations Centre (SOC) analyst follows when reviewing suspicious email alerts.

**4. Project Goals and Objectives**

The project aimed to build both technical and analytical cybersecurity skills. My specific objectives were:

1. **Analyze real phishing email samples** using the TryHackMe platform.
2. **Identify and document indicators of compromise (IoCs)** such as malicious links, fake domains, and urgent messages.
3. **Apply NIST CSF principles** of detection, analysis, and response throughout the process.
4. **Provide evidence and reasoning** for classifying each email as phishing or legitimate.
5. **Reflect on personal and professional learning outcomes** related to email analysis and security awareness.

**5. Methodology**

To complete the project, I followed a structured and logical process like what would occur in a real incident response investigation.

**Step 1 – Accessing the TryHackMe Environment**

I logged into my TryHackMe account and launched the “Phishing Emails in Action” room.  
The room overview displayed the learning objectives and list of tasks.

A screenshot of a computer

AI-generated content may be incorrect.

**Step 2 – Understanding the Phishing Scenarios**

I reviewed each of the eight simulated emails. Each one represented a different real-world phishing attempt:

* *Cancel your PayPal order*

A screenshot of a computer

AI-generated content may be incorrect.

* *Track your package*

A screenshot of a computer

AI-generated content may be incorrect.

* *Update payment details*

**A screenshot of a computer

AI-generated content may be incorrect.**

* *Select your email provider to view documents*, etc.

**A screenshot of a computer

AI-generated content may be incorrect.**

These scenarios helped me understand how attackers mimic trusted brands and use emotional triggers like fear or urgency.

**Step 3 – Technical Analysis of the Emails**

I analyzed each email by:

* Checking sender address and reply-to headers
* Hovering over embedded URLs to check for domain mismatches
* Inspecting message tone for urgency (“your order will be cancelled”)
* Identifying links that are redirected to credential-stealing pages

This process revealed several suspicious indicators including **spoofed domains**, **spelling variations**, and **impersonated brand logos**.

**Step 4 – Mapping to Cybersecurity Frameworks**

I mapped my approach to the **NIST Cybersecurity Framework (CSF)**:

* **Identify:** Recognizing phishing indicators (headers, links, behavior).
* **Detect:** Confirming malicious elements using URL and WHOIS checks.
* **Respond:** Recommending mitigation (block domain, warn users, awareness).

This approach helped connect practical actions to theoretical models discussed in class.

**Step 5 – Verifying Completion and Collecting Evidence**

After successfully completing all eight tasks, I earned 56 points and achieved 100 % completion in my TryHackMe profile.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

These screenshots serve as verification that the challenge was completed under my own account.

**6. Results and Outcomes**

**Key Findings:**

| **Observation** | **Indicator** | **Explanation** |
| --- | --- | --- |
| Suspicious sender address | Spoofed domain names | Domains slightly misspelled (e.g., paypa1.com). |
| Embedded links | Redirected to phishing login pages | Imitated login screens to collect credentials. |
| Message tone | Urgent language or threats | “Account will be suspended” or “verify now”. |
| Content structure | Branding and logo imitation | False sense of legitimacy and urgency. |

All eight emails were confirmed as phishing, using at least one of the above indicators.

This experience demonstrated that **effective phishing detection requires both technical verification and psychological awareness** of attacker tactics.

**Final Outcome:**

* **Platform:** TryHackMe
* **Room:** *Phishing Emails in Action*
* **Difficulty:** Easy
* **Tasks Completed:** 8
* **Score Earned:** 56 points
* **Completion:** 100 %

**7. Reflection and Learning**

**What I Learned**

This project taught me how to systematically analyse phishing emails using both technical and behavioural cues. I learned to inspect headers, check URL patterns, and assess sender credibility. More importantly, I developed a stronger understanding of **how social engineering exploits human trust**.

The TryHackMe lab made theoretical concepts like phishing lifecycle and NIST CSF functions practical. I realised that email analysis isn’t only about identifying a fake link but about understanding how an attacker thinks and how a victim might respond.

**How This Helped My Professional Growth**

Working through a realistic SOC-like environment helped me gain confidence in incident triage and digital investigation. It strengthened my attention to detail, analytical thinking, and decision-making under simulated pressure.

It also reinforced the importance of maintaining documentation, using evidence, and linking findings to frameworks which are critical for real cybersecurity jobs. I now feel more prepared for entry-level roles such as **Cybersecurity Analyst** or **SOC Tier 1 Technician**, where such analysis is part of daily responsibilities.

**What I Would Do Differently Next Time**

If I repeated this project, I would:

1. **Use automated tools** like Python scripts or VirusTotal APIs to analyse email headers and URLs faster.
2. **Test more advanced phishing rooms** to improve technical skills like sandboxing and malware detection.
3. **Simulate reporting processes** such as creating SOC-style tickets and recommending preventive controls.

By enhancing automation and reporting, I could make my analysis faster and more professional, mirroring how real SOC teams operate.

**8. Conclusion**

Completing this project gave me a deep understanding of phishing detection, analysis, and response. I was able to connect theoretical cybersecurity principles with a practical investigation in a safe online lab.

The project not only satisfied all assessment requirements but also helped me build tangible experience that can be presented in my cybersecurity portfolio. I am now more confident in my ability to identify phishing patterns, assess threats, and document findings professionally.

This activity represents a significant step in my journey to becoming a cybersecurity professional.

**9. References**

* TryHackMe. (2025). *Phishing Emails in Action* [Online Lab]. Retrieved from https://tryhackme.com
* National Institute of Standards and Technology (NIST). (2023). *Cybersecurity Framework (CSF) 2.0 Draft.*
* VirusTotal. (2025). *URL and File Reputation Checking Tool.*
* MxToolbox. (2025). *Email Header Analysis and DNS Tools.*
* OWASP Foundation. (2024). *Phishing Awareness and Mitigation Best Practices.*

**10. Appendix – Evidence Screenshots**

| **Figure** | **Description** | **Screenshot to Insert** |
| --- | --- | --- |
| **1** | TryHackMe “Phishing Emails in Action” – Room overview | Screenshot 1 |
| **2** | Tasks showing progress (around 68%) | Screenshot 2 |
| **3** | Dashboard showing username/profile and streaks | Screenshot 3 |
| **4** | Final completion badge – 100% complete | Screenshot 4 |
| **5** | Task list – all eight tasks completed | Screenshot 5 |