TryHackMe Advent of Cyber 2025 Day 12 Challenge Report

Phishing Email Analysis & Detection

1. Executive Summary

This report documents the completion of Day 12 of the TryHackMe Advent of Cyber 2025 event. Successfully triaged and classified 6 emails, distinguishing 5 phishing attempts from 1 spam message. Identified multiple malicious indicators including impersonation, spoofing, typosquatting/punycode exploitation, social engineering, malicious attachments, and side-channel communication attempts. Collected all 6 flags demonstrating comprehensive phishing detection capabilities.

2. Challenge Overview

Objective: Triage incoming emails, classify each as spam or phishing, identify three clear phishing signals per malicious email, and collect flags upon successful classification.

Threat Actor: Malhare's Eggsploit Bunnies targeting TBFC employees

Results: 6/6 emails correctly classified, all flags collected

3. Email Classification Summary

Email #	Classification	Subject/Sender	Primary Signals
1	**PHISHING**	Monika (Side channel)	Spoofing, Urgency, Fake Invoice
2	**PHISHING**	New Audio Message	Impersonation, Spoofing, Malicious Attachment
3	**PHISHING**	URGENT: McSkidy VPN	Impersonation, Social Engineering, Urgency
4	**PHISHING**	External Sender	Impersonation, External Domain, Social Engineering
5	**SPAM**	Marketing/Logistics	Legitimate marketing (no malicious intent)
6	**PHISHING**	TBFC-IT Laptop Upgrade	Impersonation, Typosquatting/Punycode, Social Engineering

4. Detailed Email Analysis

4.1 Email 1: Side Channel Communication Attempt

Subject/Sender: Monika - Side channel to WhatsApp

Classification: PHISHING

Identified Signals:

- **Spoofing:** Email authentication failures
- **Sense of Urgency:** Pressuring immediate action
- **Fake Invoice:** Attempting financial fraud

Analysis: Attacker attempts to move conversation to WhatsApp (side channel) to continue social engineering outside company monitoring. Classic technique to bypass security controls.

Flag: THM{yougotanumber,i-keep-it-going}

4.2 Email 2: Malicious Attachment with Spoofing

Subject: New Audio Message from McSkidy

From: McSkidy Missed Call Notifier <calls@tbfc.com>

Classification: PHISHING

Identified Signals:

- **Impersonation:** Pretending to be McSkidy
- **Spoofing:** SPF and DMARC authentication failures
- **Malicious Attachment:** .html file disguised as voice message

Technical Evidence:

- **Authentication-Results:** SPF=fail, DKIM=fail, DMARC=fail
- **Return-Path:** zxwsedr@easterbb.com (not tbfc.com)
- **Attachment:** Play-Now-mp3-29a-ojqew-war3-20.html (17 KB)

Analysis: Domain appears legitimate (tbfc.com) but authentication completely fails. Return-Path reveals real sender from easterbb.com. HTML attachment runs JavaScript without browser sandboxing, providing full endpoint access.

Flag: THM{number2-was-not-the-hardl}

4.3 Email 3: VPN Credential Harvesting

Subject: URGENT: McSkidy VPN access for incident response

From: McSkidy <mcskiddy20251203521@gmail.com>

Classification: PHISHING

Identified Signals:

- **Impersonation:** Free Gmail domain pretending to be McSkidy
- **Social Engineering Text:** Fabricated incident to create urgency
- **Sense of Urgency:** "URGENT," "immediately," pressure tactics

Social Engineering Tactics:

- **Authority:** Impersonating respected team member
- **Urgency:** "Currently unreachable," "ongoing incident"
- **Side Channel:** Requests credentials sent to personal Gmail
- **Malicious Intent:** Harvesting VPN credentials for network access

Analysis: Classic impersonation using free email domain. Real TBFC employee McSkidy would use company domain. Multiple red flags including urgent language, side-channel communication request, and credential harvesting attempt.

Flag: THM{impersonation-is-a-real-thing-keep!}

4.4 Email 4: External Domain Impersonation

Subject: External sender domain communication

Classification: PHISHING

Identified Signals:

- **Impersonation:** External sender pretending to be internal
- **External Sender Domain:** Non-TBFC domain claiming internal status
- **Social Engineering Text:** Manipulative content to deceive recipient

Analysis: Sender domain does not match TBFC's internal domain structure. Email attempts to appear as internal communication while originating externally.

Flag: THM{not-back-SOC-mas!!!}

4.5 Email 5: Legitimate Marketing (SPAM)

Subject: Improve your event logistics this SOC-mas season

From: Lara <lara@candycane.co.wv>

Classification: SPAM

Characteristics:

- **Intention:** Pure marketing - promoting logistics services
- **Content:** Professional business proposal
- **Sender:** Legitimate business domain (candycane.co.wv)
- **No Malicious Intent:** No credential theft, malware, or fraud attempts

Analysis: Unsolicited marketing email offering event logistics services. While annoying, it poses no security threat. No impersonation, no social engineering for malicious purposes, no dangerous attachments. Simply bulk marketing.

Flag: THM{it-was-just-a-sp4m!}

4.6 Email 6: Typosquatting with Legitimate Platform Abuse

Subject: TBFC-IT shared "Christmas Laptop Upgrade Agreement" with you

From: TBFC-IT <tbfc-it@tbfc.com> (fake with punycode ƒ)

Classification: PHISHING

Identified Signals:

- **Impersonation:** Pretending to be TBFC IT department
- **Typosquatting/Punycode:** Latin letter ƒ instead of normal f
- **Social Engineering Text:** Attractive proposal (laptop upgrade)

Technical Evidence:

- **Punycode Detection:** Return-Path shows ACE prefix (xn--) encoding
- **Visual Similarity:** ƒ looks like f but is Unicode character
- **Legitimate Platform:** Uses OneDrive to appear trustworthy

Attack Chain:

1. Fake domain using punycode to mimic TBFC
2. Shares document via legitimate OneDrive platform
3. Attractive subject (Christmas laptop upgrade)
4. Document likely contains fake login page or malicious content

Analysis: Sophisticated attack combining multiple techniques. Punycode makes domain look legitimate at first glance. OneDrive usage adds credibility and bypasses email filters. Attractive proposal (laptop upgrade) increases click likelihood. Header analysis reveals xn-- encoding confirming punycode exploitation.

Flag: THM{number6-is-the-last-one-OK!}

5. Phishing Techniques Summary

5.1 Impersonation

Detected in 5 of 6 emails. Attackers pretended to be trusted entities (McSkidy, TBFC-IT, internal staff) using free domains or fake domains to gain credibility.

5.2 Email Spoofing

Identified through authentication failures (SPF, DKIM, DMARC). Return-Path analysis revealed real sender addresses differing from displayed 'From' addresses.

5.3 Social Engineering

Present in all phishing emails. Tactics included urgency creation, authority exploitation, attractive proposals, side-channel communication requests, and fabricated scenarios.

5.4 Typosquatting & Punycode

Advanced technique using Unicode characters that visually resemble legitimate letters. Detected through Return-Path header analysis showing ACE prefix (xn--) encoding.

5.5 Malicious Attachments

HTML files disguised as voice messages. These run without browser sandboxing, providing full endpoint access for malware execution.

5.6 Legitimate Platform Abuse

Attackers leveraged OneDrive to appear trustworthy and bypass email filters. Links to legitimate platforms combined with fake domains create convincing lures.

6. Detection Methodology Applied

6.1 Sender Domain Analysis

- Verified sender domains match organizational structure
- Identified free domains (gmail.com) as impersonation indicators
- Detected punycode through character inspection and header analysis

6.2 Header Inspection

- Examined Authentication-Results for SPF, DKIM, DMARC status
- Compared Return-Path with displayed 'From' address
- Identified ACE prefix (xn--) indicating punycode encoding

6.3 Content Analysis

- Recognized social engineering tactics (urgency, authority, fear)
- Identified malicious intent (credential harvesting, side-channel requests)
- Distinguished marketing spam from malicious phishing

6.4 Attachment Review

- Scrutinized file types (HTML files disguised as voice messages)
- Recognized dangerous file extensions and social engineering disguises

7. Key Skills Developed

- Phishing vs spam differentiation
- Email header analysis (SPF, DKIM, DMARC, Return-Path)
- Impersonation detection (domain verification)
- Social engineering recognition (urgency, authority, fear tactics)
- Typosquatting and punycode identification
- Email spoofing detection (authentication failures)
- Malicious attachment identification
- Multi-signal correlation for accurate classification

8. Conclusion

Day 12 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in phishing email analysis and detection. Successfully triaged 6 emails with 100% accuracy, distinguishing 5 sophisticated phishing attempts from 1 legitimate spam message.

The challenge demonstrated the evolution of phishing attacks, from basic impersonation to advanced techniques including punycode exploitation and legitimate platform abuse. Modern phishing focuses on credential theft rather than direct malware delivery, requiring analysts to understand both technical indicators (header analysis, authentication checks) and behavioral patterns (social engineering tactics).

Key takeaway: Phishing remains the easiest path to initial access because it targets people rather than technology. Comprehensive email analysis combining sender verification, header inspection, content evaluation, and threat intelligence is essential for protecting organizations from these precision attacks.

Challenge Status: **COMPLETED ✓**