Phishing - Phishmas Greetings

Day 12

Learn how to spot phishing emails from Malhare's Eggsploit Bunnies sent to TBFC users.

- Spotting Phishing Emails

Spotting Phishing Emails

Overview

Room URL: https://tryhackme.com/room/spottingphishing-aoc2025-r2g4f6s8l0

Difficulty: Medium

Category: Phishing

Date Completed: 12/12/2025

Objectives

- Spotting phishing emails
- learn trending phishing techniques
- Understand the differences between spam and phishing

Table of Contents

Introduction

As TBFC's defenses crumble under King Malhare's assault, the Eggsploit Bunnies launch a coordinated phishing campaign designed to exploit the chaos of the Christmas crisis. With McSkidy kidnapped and Wareville's email protections down, attackers have a critical window to compromise employees and deepen their infiltration. The challenge isn't just spotting obvious red flags—it's understanding attacker psychology: how they impersonate trusted contacts, manufacture urgency, and weaponize legitimate tools to steal credentials and access. In this triage operation, you'll learn to separate harmless spam from precision-crafted phishing attacks, identifying the telltale signals

that reveal each attacker's true intent.

Phishing Indicators

- SPF/DKIM/DMARC authentication results
- Sender domain vs. Return-Path discrepancies
- Free email domains for corporate impersonation
- Punycode and typosquatting in domain names
- Social engineering language (urgency, authority, legitimacy)

Walk Through

1. Email 1
    1. Email 1 is a invoice from paypal
        1. Not all of the links direct to paypal.com
        2. It is an invoice for $699.89
        3. the "From" email is `service@paypal.com`
        4. The SPF record failed as `Danielle378.onmicrosoft.com` sent the email
    2. This is a phishing email
        1. Spoofing
        2. Fake Invoice
        3. Sense of Urgency
2. Email 2
    1. Missed Voice message from McSkidy
        1. The from address is `calls@tbfc.com`
        2. Has an attachment of `Play-Now.mp3`
        3. SPF Failed `smpt.mailfrom=tbfc.com`
            1. recieved from `gw3097.weakmail.com`
    2. Email is phishing
        1. Spoofing
        2. Impersonation
        3. Malicious Attachmet
3. Email 3

1. Email from Mcskidy indicating needs a new vpn, will be unreachable by phone and needs to use personal email
    1. From `mcskiddy202512@gmail.com`
    2. SPF Pass
2. Phishing
    1. Impersonation
    2. Sense of Ugency
    3. Social Engineering Text
4. Email 4
    1. Email from TBFC HR about Annual Salary Raise
        1. from `no-reply@dropbox.com`
        2. Drop box indicates from `hr.tbfc@outlook.com`
        3. SPF Pass
    2. Email is Phishing
        1. Impersonation
        2. Social Engineering Text
        3. External Sender Domain
5. Email 5
    1. Email bout improving event logistics
        1. from `laura@candycane-co.wv`
        2. No external links
        3. Advertising their platform
        4. SPF Pass
    2. Spam Email
6. Email 6
    1. TBFC-IT shared a file with you
        1. From `tbfc-it@tb(f)c.com` the f is a Latin character, not English
        2. Christmas Flattop Upgrade Agreement
            1. Link goes to `microsoftooline.co`
        3. SPF Pass
    2. Email is Social Engineering
        1. Impersonation
        2. Typosquatting/Punnycodes
        3. Social Engineering Text

Lessons Learned

- **Learned how to identify and distinguish phishing attacks from spam by analyzing sender authentication (SPF/DKIM/DMARC failures), domain legitimacy, and attacker intent.** The key is recognizing that phishing targets specific users with precision deception (credential theft, malware delivery, financial fraud), while spam targets quantity for promotion or data harvesting. Authentication failures, spoofed `From:` fields, and mismatched `Return-Path` headers are critical indicators.
- **Mastered the recognition of modern phishing techniques including impersonation, social engineering, typosquatting, punycode exploitation, malicious attachments, and the weaponization of legitimate platforms (Dropbox, OneDrive) to bypass security filters and steal credentials.** The evolution of phishing now focuses on moving users out of secure email environments into fake login pages and cloud-sharing platforms, making threat detection dependent on understanding attacker psychology and context rather than technical filtering alone.

Resources

TryHackMe