🛡 Project: Phishing Attack Investigation

Introduction

Phishing attacks remain one of the most common and dangerous cybersecurity threats. These attacks involve tricking individuals into revealing sensitive information by impersonating trusted entities. This project aims to develop the skills necessary to identify, investigate, and respond effectively to phishing attempts.

Phishing Analysis Report

1. Overview

Incident Title:

Phishing Attempt – *"Stanley Tumbler Customer Survey" Spoof*

Date Identified:

Saturday, 16 December 2023

Reported By:

User or automated system (e.g., phishing@pot)

2. Executive Summary

A phishing email impersonating the "Dick's Sporting Goods Department" was received, offering a free Stanley Tumbler as a reward for completing a customer satisfaction survey. The email encouraged recipients to click a malicious link under the pretense of confirming the offer. This is a typical example of a phishing scheme designed to harvest personal or financial information using marketing lures.

3. Indicators of Phishing

Indicator	Description

Suspicious Sender Name	"Dick's Sporting Goods Department" — lacks official branding and domain.
Generic Greeting	Addressed to "phishing@pot" — suggests bulk distribution rather than personalization.
Urgency & Reward Bait	Phrases like "Final notice", "Reward offer expires", and "Your Reward: Stanley Tumbler" indicate urgency-based manipulation.
Malformed Grammar	Unprofessional phrasing such as "Your Name Came Up For" and inconsistent punctuation.
Suspicious Links	Hyperlinks such as "Confirm-Here" and unsubscribe options may lead to malicious domains.
Unverified Address	Physical address (110 N Interstate 35, Round Rock, TX) appears potentially spoofed or irrelevant.

4. Technical Analysis

Tools Utilized:

- **Thunderbird** – Email client used for header inspection
- **VirusTotal** – Detected phishing flag from one vendor (Segasec)
- **MXToolbox.com** – Domain and mail server reputation checks
- **IPinfo.io** – Identified IP origin as Germany

URL/Link Analysis:

- The primary link ("Confirm-Here") was submitted to VirusTotal.
- **Result:** Identified as phishing by a reputable vendor.
- The domain was not associated with Dick's Sporting Goods, indicating clear deception.

5. Threat Objective

The phishing campaign appears designed to achieve one or more of the following:

- Harvest credentials through fake web forms
- Confirm active email addresses via user interaction
- Collect personal data for future targeted attacks
- Exploit brand reputation to build trust and increase click-through rates

6. Risk Assessment

Category	Assessment
Impact	Moderate to High
Likelihood	Medium to High
Severity	High (if user interaction occurs)