Case Study: The Google Sign-in phishing simulation

An Analysis of Social Engineering Susceptibility on Mobile Messaging Platforms

Mr K Molotsi
Cybersecurity Researcher / Enthusiast

November 24, 2025

ETHICAL DISCLAIMER

This study was conducted in a controlled environment for educational purposes. All participants were known associates of the researcher. Following the simulation, all participants were immediately debriefed, and any harvested credentials were permanently destroyed without access or misuse. The goal of this project is to analyze human behavior in relation to cybersecurity awareness.

Abstract

This report details the findings of a social engineering simulation targeting mobile users via WhatsApp. By leveraging the ”Trusted Contact” vector and a pretext of urgency, the simulation achieved a high click-through rate. The study highlights the vulnerability of mobile interfaces (which often hide URLs) and the psychological impact of social pressure on security hygiene.

1 Introduction

Phishing remains the primary entry point for 90% of cyberattacks. While corporate email filters are becoming more sophisticated, mobile messaging platforms (WhatsApp, Signal, Telegram) act as a ”high-trust” environment where users are less likely to expect malicious activity. This study aimed to test the resilience of users against a targeted ”Smishing” (SMS/Mobile Phishing) attack delivered by a known contact.

2 Methodology

2.1 The Pretext

The simulation utilized a classic ”Urgent Assistance” pretext. The attacker (myself) posed as a friend in need of a favor.

- **Vector:** WhatsApp (Mobile)
- **Scenario:** ”Bro please review this website portfolio for me, I need to submit a review tonight.”
- **The Hook:** A spoofed Google Sign-In page hosted on a deceptive domain.

2.2 The Psychological Triggers

The attack relied on three core principles of influence (Cialdini’s Principles):

1. **Liking/Friendship:** The target knows the sender, bypassing initial skepticism.
2. **Urgency:** The phrase ”submit tonight” creates a time constraint that discourages critical analysis.
3. **Commitment/Consistency:** Friends generally want to be helpful (Altruism).

3 Findings & Analysis

Following the simulation, participants completed a structured survey. The data revealed significant gaps in mobile security awareness.

3.1 Quantitative Results

- **Trust Factor:** 85.7% of participants stated they clicked the link purely because they trusted the sender.
- **URL Inspection:** A surprising 0% of users checked the URL bar before entering credentials.
- **Visual Deception:** 57.1% of users were convinced by the visual accuracy of the Google logo, ignoring the URL mismatch.

3.2 Qualitative Analysis: The "Mobile Blind Spot"

A key finding was the limitations of the mobile UI. On desktop browsers, the URL bar is prominent. On mobile devices, screen real estate is limited, and app-based browsers often hide the full URL structure.

> *"I didn't even look at the link; I just saw the message came from you and clicked."* – Anonymous Participant

This highlights that **Trust** is the most dangerous vulnerability in social engineering. Technical controls (firewalls, filters) are rendered useless when the user voluntarily opens the door.

4 Recommendations

To mitigate risks associated with Trusted Contact Vectors, the following behaviors are recommended:

4.1 For Individuals

- **Out-of-Band Verification:** If a friend sends a link asking for credentials or money, call them to verify.
- **URL Expansion:** Be wary of shortened links. Long-press the link to preview the actual destination.
- **MFA (Multi-Factor Authentication):** Even if credentials are harvested, MFA provides a secondary layer of defense.

4.2 For Organizations

- **Mobile Security Training:** Awareness programs must specifically address "Smishing" and mobile-specific threats, not just email phishing.
- **Zero Trust Mindset:** Adopt a "Trust but Verify" approach, even with known contacts.

5 Conclusion

This simulation demonstrates that familiarity breeds complacency. The participants were not "tech-illiterate"; they were simply socially engineered. Effective cybersecurity requires a holistic approach that includes hardening the "Human Firewall" against psychological manipulation.