# Phishing Investigation Workflow by Victor Mumo

1. **Identifying the Threat**
    - Extracted a suspicious URL (api[.]yu3[.]io/5ctkkw) from a phishing email.
2. **Initial Analysis**
    - Opened the URL in a secure environment (isolated VM or sandbox).
    - Observed that it mimicked **Absa Bank's login page**.
3. **Technical Investigation**
    - Used **Burp Suite** to capture HTTP requests & responses.
    - Identified exfiltration endpoint (loranto[.]com/wp-content/update/send_login.php.).
    - Noted redirection to eu2[.]contabostorage[.]com/0f057bf4d91340d3ae18d5f31372fa7e[:]mygo/abs/loading[.]html on **Contabo Storage** after submission.
4. **Infrastructure Analysis**
    - Performed **WHOIS lookups** on involved domains.
    - Checked hosting providers and IP addresses.
    - Used **VirusTotal** & threat intel tools to see if domains/IPs were flagged.
5. **Compiling Evidence**
    - Captured screenshots of the phishing page.
    - Documented HTTP traffic & error messages (403, 421).
    - Mapped attack flow from initial phishing attempt to credential exfiltration.
6. **Reporting & Mitigation**
    - Structured findings into a detailed phishing campaign report.