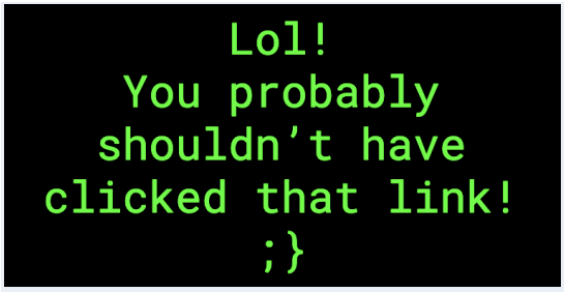
**Incident Response Plan: Suspicious Link Click – Potential Malware Infection**
**Company:** MedSecure Insurance
**Date:** 26/05/2025
**Prepared by:** Sandiso Mayekiso, Cyber Security Analyst

---

## 1. Detection

- **Initial Indicator:** Colleague's screen displays message: *"LOL YOU PROBABLY SHOULD-N'T HAVE CLICKED THAT LINK."*




- **Action:** Immediately isolate the personal device from all network access (Wi-Fi, LAN, VPN).
- Notify the IT Security Incident Response Team (IRT).
- Confirm the incident: Verify the compromise and assess the situation.

---

## 2. Analysis

- **Role: Security Analyst (*Sandiso Mayekiso*)**
    I. Perform a preliminary investigation: Determine if the link led to a malware download or phishing attempt.
    II. Check network logs for unusual activity (e.g., outbound connections, data ex-filtration).
    III. Scan the device using company-approved antivirus and malware analysis tools.
    IV. Gather information: Collect relevant logs, system data, and other evidence.
- **Role: Digital Forensics Specialist**
    I. Conduct full forensic imaging of the device.
    II. Analyze potential malware behavior and trace origin.

- **Role: Compliance Officer**
    I. Assess the breach against national data protection laws.
    II. Prepare for possible reporting to the Information Regulator.

---

**3. Containment**

- **Short-Term Measures:**
    I. Isolate or Keep the compromised device offline to prevent further spread.
    II. Immediately revoke credentials used on the device.
- **Long-Term Measures:**
    I. Implement Endpoint Detection and Response (EDR) monitoring across systems.
    II. Block any known malicious IP addresses or domains linked to the attack.

---

**4. Eradication**

- Completely remove any detected malware or backdoors.
- Patch system vulnerabilities and ensure OS and antivirus definitions are up to date.
- Reset affected accounts with new credentials and enforce multi-factor authentication (MFA).

---

**5. Recovery**

- Reimage or restore the device from a clean backup.
- Closely monitor for signs of lingering threats or unusual activity.
- Reconnect the device to the network only after formal clearance by the IRT.

---

**6. Lessons Learned**

- Conduct a post-incident review with all team members.
- Train staff/employees on phishing awareness and safe link practices.
- Update the company's incident response documentation and training programs.

---

**Incident Severity: HIGH**

The compromise poses a significant threat to the confidentiality and security of sensitive personal data, thereby jeopardizing compliance with pertinent regulatory requirements. Prompt intervention is essential to safeguard patient information and uphold the integrity of our regulatory framework, ensuring adherence to stringent data protection standards.