Title: Phishing Awareness Simulation Project

Date: 3/09/2024

Author: Yonase Kidane

1. Introduction:

- **Objective:** To assess the phishing awareness of family members (Arsema and Lubona) through a controlled phishing simulation.
- **Methodology:** A fake Uber Eats voucher offer was sent via text message to evaluate how easily they would recognize the scam.

2. Methodology:

- **Participants:** Arsema (sister), Lubona (sister)
- **Scenario:** A text message from an unknown number offered a $15 Uber Eats voucher, with a shortened link leading to a page revealing the phishing test.
- **Tools Used:** Google Sites for the phishing test page and Bitly for URL shortening.

3. Results:

- **Arsema:** Identified the phishing attempt as fake because she assumes all offers like that are scams.
- **Lubona:** Recognized the text as suspicious since she doesn't typically receive messages like that.

4. Analysis:

- **Strengths:** Both demonstrated strong instincts in recognizing phishing attempts based on their personal awareness.
- **Areas for Improvement:** A need for deeper knowledge of more sophisticated phishing tactics that may not align with their current expectations.

5. Recommendations:

- **Phishing Quiz:** Both participants should take the Google Phishing Quiz to further solidify their phishing detection skills.

- **Ongoing Awareness:** They should remain vigilant and continue educating themselves about evolving phishing strategies.

6. Conclusion:

- The simulation successfully demonstrated that Arsema and Lubona possess strong cybersecurity instincts. However, continued education and awareness are essential for maintaining and improving their ability to detect increasingly complex phishing attempts.