Task 3.B

Personal threat model
Introduction

The business Instagram account, with 2 million followers, is a valuable asset but also a potential target for cyber threats like credential theft and phishing. This project focuses on creating a personal threat model to find weaknesses, assess risks, and develop strategies to protect the account from attacks. By identifying key assets, threats, and security measures, this model aims to improve the account's security and protect its reputationAsset

- Instagram Account: The account has 2 million followers, which represents brand value and engagement. Reputation: The business's public image depends on the integrity of this account.
- Business Data: Includes private messages, potential client collaborations, and sensitive information shared through DMs.
- Mobile Phone: The main access point to manage the Instagram account.
- Phone Number: Used for receiving login notifications and recovery attempts.

Threats

- Credential Theft: Hackers attempt to steal the account's login credentials through phishing or brute-force attacks.
- SIM Swapping: Attackers could hijack the phone number linked to the account to bypass two-factor authentication (2FA).
- Phishing: Fake emails or websites tricking the user into revealing their password.
- Malware: Malicious software that could infect your phone and compromise account access.
- Social Engineering: Attackers may trick you or Instagram support into giving them access.

Vulnerabilities

- SMS-based 2FA: Vulnerable to SIM-swapping attacks.
- Phishing Susceptibility: Lack of caution when interacting with unknown links or emails.
- Weak Phone Security: The phone might not have anti-malware protection or a strong passcode.
- Password Exposure: Risk of using the same password for other accounts, which could be compromised.