**Social Engineering Project: Understanding Digital Footprints**

**Subject: Ansley Jean**

**Phase 1: Ethical Considerations and Methodology**

The ethical considerations for this project are of utmost importance. The research was conducted with the full consent of all participants, ensuring that privacy was respected throughout the process. Sensitive details have been anonymized or generalized to uphold ethical standards. Only publicly available information was used, maintaining an ethical approach that prevents any form of privacy invasion. The methodology for this research involved gathering publicly accessible data from social media platforms, public databases, and online searches. Google searches were conducted using Ansley Jean’s name and related keywords to compile relevant information. The research strictly adhered to ethical guidelines, ensuring that no private or unauthorized data was accessed.

**Phase 2: Collected Data**

The research gathered various data points that contribute to understanding the digital footprint of Ansley Jean. His full name, birthdate, address, email, and phone number were all publicly available. His professional background includes current employment at BJ’s Wholesale Club as a Front-End Associate since July 2023. He previously worked at TJ Maxx as a Cashier/Sales Associate from July 2020 to March 2022 and also held a Student Ambassador position at Adobe between June 2022 and 2023. His educational background indicates that he attended Bowie State University from 2019 to 2023, majoring in Computer Technology. Regarding social media presence, his LinkedIn profile is accessible, along with two Instagram accounts, 'aj.uno' and 'vitamin.ayisyen', and two Twitter accounts, 'ajuno\_' and 'LaMVPJacks0n'. His online activities suggest engagement in professional discussions and technology-related content. He has shared posts on LinkedIn related to his field, including his role as an Adobe Student Ambassador, where he promoted Adobe software and organized workshops. His job-seeking status is publicly visible, highlighting his openness to work in Java Software Engineering, HTML Development, and Computer Engineering. Additionally, his interests and affiliations indicate participation in online forums, professional networking, and involvement with groups related to his field. His engagement on social media provides insights into his professional aspirations and personal interests.

**Phase 3: Risk Analysis and Threats**

The findings from the research reveal several potential security risks associated with Ansley Jean’s digital footprint. The public availability of personal information, including his full name, birthdate, address, email, and phone number, poses a significant risk. This data can be used to craft personalized phishing attacks, identity theft schemes, or fraudulent attempts to exploit his personal details. Another vulnerability arises from his professional and job-seeking information on LinkedIn. Cybercriminals or malicious actors could use this information to impersonate recruiters or offer fraudulent job opportunities, potentially leading to social engineering attacks. Additionally, his open sharing of work history, education, and skills provides attackers with contextual data that could be exploited in deception schemes. His social media presence further exposes him to risks. The visibility of his accounts, along with posted content and interactions, allows malicious individuals to analyze his habits, preferences, and personal affiliations. Location-based tags and event participation further contribute to his exposure, making him a potential target for impersonation or location-based attacks.

**Recommendations for Security Improvement**

* Restrict Personal Information Access: Ansley should limit the public visibility of his birthdate, address, phone number, and email. Adjusting privacy settings to ensure that only trusted connections can view this information is advisable.
* Enhance Social Media Privacy Settings: Setting social media accounts to private where possible would help reduce exposure. He should be cautious about accepting friend or follow requests from unknown users.
* Reduce Online Footprint: It is recommended that he removes or limits old public posts that contain personal or professional details. Avoiding oversharing on platforms that do not require professional visibility will enhance his security.
* Be Wary of Phishing and Scams: Ansley should be cautious when receiving unsolicited job offers or messages that seem suspicious. Verifying the legitimacy of recruiters before engaging can help protect against fraudulent schemes.

**Phase 4: Presentation & Reflection**

This project has provided valuable insight into the significance of managing one’s digital footprint. The research demonstrated how easy it is to compile detailed personal profiles using publicly available information. This underscores the importance of privacy settings, controlled sharing of personal data, and awareness of cyber threats. A key takeaway from this exercise is the realization that digital footprints can expose individuals to risks such as identity theft, phishing attacks, and impersonation scams. By implementing security best practices, such as limiting the visibility of personal details and being vigilant about online interactions, individuals can reduce their susceptibility to social engineering attacks. Through this research, it became evident that the online presence of an individual requires careful monitoring and proactive security measures. The findings reinforce the necessity of digital security awareness, not only for professionals but for anyone who actively engages in online activities. Ultimately, the project highlights the need for individuals to take control of their digital identities and safeguard their personal information against potential threats.