Below is the full sentence-by-sentence breakdown of your document **“Social Engineering Attacks Notes”** formatted as **high-yield, professionally aligned study notes**. It is structured for clear pasting into Microsoft Word and follows CompTIA A+ 220-1102 exam Objective **2.4 (Common Social Engineering Attacks)**. All information is extracted and expanded in a logical, exam-prep-friendly format.

**📘 Social Engineering Attacks – Study Notes**

**CompTIA A+ 220-1102 | Objective 2.4 – Security Awareness**

**1. Definition of Social Engineering**

* Social engineering is an attempt to **manipulate individuals** into revealing confidential information or performing actions that compromise security.
* Instead of attacking systems or software, it targets **human behavior** and **trust**.
* These attacks are designed to **bypass technical controls** by tricking the person behind the system, often the **weakest link** in an organization’s security.

**2. Example: Social Engineering vs. Brute Force**

* If an attacker finds a **strong WPA2 AES Wi-Fi password**, it may take **years to brute force**.
* However, through **social engineering**, the attacker might trick someone into **giving them the password**, accessing the network the same day.
* This shows why **hacking the human** can be far easier than hacking technology.

**3. The Human Factor**

* Most successful cyberattacks exploit **employee error or human trust**.
* Regular **cybersecurity training** is essential to raise awareness and teach staff how to identify and resist these techniques.

**4. Tailgating**

* **Tailgating** occurs when an attacker follows an **authorized person into a secure area** **without their knowledge or consent**.
* Example: An attacker waits until someone swipes their badge and enters a secure door, then slips in **before the door shuts**.
* **Prevention tip**: Train employees to **pull doors shut** behind them and not rely on automatic closing.

**5. Piggybacking**

* Similar to tailgating but with **consent or awareness** of the employee.
* Example: An attacker carries boxes and asks someone to open the door for them, pretending to be burdened or in a rush.
* If the employee helps by swiping their badge and letting the attacker in, this is **piggybacking**.
* Key risk: The attacker uses **one person’s credentials to enter** alongside them.

**6. Shoulder Surfing**

* **Shoulder surfing** is the act of **visually observing** someone entering sensitive data, like a password or PIN.
* Example: Watching over someone’s shoulder as they type "P-A-S-S-W-O-R-D".
* Doesn’t have to be obvious—can also occur when someone sitting nearby **glances at your screen** to see personal data.
* Even **indirect observation** qualifies as shoulder surfing.

**7. Eavesdropping**

* **Eavesdropping** is similar to shoulder surfing but involves **using ears** instead of eyes.
* Example: An attacker overhears a conversation between you and your boss about **financial projections**.
* This technique **harvests sensitive spoken information** without permission or awareness.

**8. Dumpster Diving**

* Involves **searching through trash or recycling** to find sensitive information.
* Despite being unsanitary, attackers use this method because it’s **highly effective**.
* Example: An attacker might find **phone lists, emails, org charts, or account numbers** in discarded papers.
* Often used as a **preliminary recon technique** before conducting deeper attacks like phishing or impersonation.

**9. Dumpster Diving Prevention**

* Use **crosscut shredders** to destroy documents before disposal.
* Store discarded materials in **locked bins** accessible only to **authorized personnel or waste management services**.
* Never discard printed confidential info without **proper destruction**.

**10. Summary of Techniques**

| **Technique** | **Key Characteristic** | **Attack Vector** | **Example Scenario** |
| --- | --- | --- | --- |
| Tailgating | Unauthorized entry without consent | Physical access | Sneaking in behind someone at a door |
| Piggybacking | Unauthorized entry **with consent** | Physical access | Carrying boxes and being let in |
| Shoulder Surfing | Visual observation of sensitive info | Human visibility | Watching someone type a password |
| Eavesdropping | Audio capture of sensitive conversations | Human proximity (audio) | Overhearing business discussions |
| Dumpster Diving | Retrieving info from discarded items | Physical environment | Finding old records in a trash bin |