Here's your **comprehensive sentence-by-sentence breakdown** of the document **“Impersonation Notes”**, formatted professionally for **clean pasting into Microsoft Word**. It includes detailed explanations, no excessive spacing, and numbered topics for alignment and memorization.

**📘 Impersonation & Elicitation – Study Notes**

**CompTIA A+ 220-1102 | Objective 2.4 – Social Engineering Techniques**

**1. Definition and Nature of Impersonation**

* Impersonation is a **social engineering attack** where the attacker **pretends to be someone or something else** to gain trust or access.
* It's highly effective because it **exploits trust and authority**.

**2. Examples of Impersonation**

* **Physical Penetration Testing**:
  + Attackers pretend to be employees, delivery personnel, or contractors to **gain access to restricted facilities**.
* **Phishing + Pretexting**:
  + Pretexting helps establish a backstory or scenario that supports impersonation.
  + Example: Call someone pretending to be from IT support after learning about their systems via phishing.

**3. Business Email Compromise (BEC)**

* A common example of impersonation via email.
* The attacker **compromises or spoofs an executive's email address** to trick another employee.
* The message often involves **urgent requests**, such as transferring funds or sending sensitive info.

**4. Physical Entry via Disguise**

* Attackers may dress up to look like **delivery drivers (e.g., UPS)** or **technicians (e.g., ISP employees)**.
* These disguises often lead to **being let in without question**.
* People often **escort attackers directly** to sensitive locations like the **telecom closet** or **server rooms**.

**5. Ease of Acquiring Uniforms**

* Uniforms (like UPS or Xfinity shirts) can easily be purchased online, e.g., **on eBay** for under $35.
* Wearing a recognizable uniform significantly increases trust and reduces suspicion.

**6. Psychological Principle: “Dress for the Job You Want”**

* People assume that someone **in uniform must be legitimate**.
* Example: Walking in with a box, pretending to deliver it to “Greg in Accounting,” can lead to unrestricted access.

**7. Utility of the Disguise**

* Attackers can bring tools and hacking equipment inside a building **inside the disguise box**, including:
  + Lock pick sets
  + Wireless sniffers
  + Rubber duckies (USB payload devices)
  + Kali Linux laptops
* Because it appears they’re “on the job,” people are unlikely to question them.

**8. Purpose and Strategy Behind Impersonation**

* Impersonation **exploits the natural tendency to trust authority figures** or service providers.
* It's commonly used in **social engineering assessments** and **red team engagements**.

**9. What Can Be Done After Entry?**

* Once inside, attackers can begin **elicitation** to gain further info or prompt actions.

**10. What Is Elicitation?**

* Elicitation is the act of **drawing out information from a target**.
* It can happen in person, by phone, or via email/chat.
* Essentially, it’s about **asking questions in a casual or helpful way** to get useful intel.

**11. Examples of Elicitation in Action**

* Asking someone to help make a copy at the copier could expose:
  + **Access codes**
  + **Printer configurations**
  + **Internal IP addresses**
* This info reveals the **internal network structure** of the organization.

**12. Human Nature and Risk**

* Most people **want to be helpful** and **don’t question minor requests**, especially from those who look official.
* This makes impersonation and elicitation **powerful low-tech attack methods**.

**13. Why This Matters for the Exam**

* This content directly aligns with **CompTIA A+ 220-1102 Objective 2.4**, which focuses on:
  + Social engineering tactics (e.g., impersonation, elicitation)
  + Common methods of deception
  + Human vulnerabilities and trust exploitation