Below is a **comprehensive sentence-by-sentence analysis** of the document **“Spyware Notes.docx”**, converted into **professional study notes**. This version is aligned for **CompTIA A+ 220-1102 (Objective 2.4 – Security)**, formatted for **Word compatibility**, and structured with numbered topics and minimal spacing for easy pasting.

**🕵️ Spyware & Related Threats – Study Notes CompTIA A+ 220-1102 | Objective 2.4 – Security**

**1. Overview**

* This lesson covers **spyware** and related malicious software:
  + Spyware
  + Keyloggers
  + Stalkerware
  + Adware
  + Potentially Unwanted Programs (PUPs)
* These threats primarily aim to **compromise user privacy** and may disrupt system performance.

**2. Spyware**

* **Spyware** is software designed to **monitor user activity** and collect information **without consent**.
* Common infection methods include:
  + Compromised websites
  + Malicious downloads
  + Third-party software installations
* Once installed, spyware may:
  + Scan files, emails, browsing history, and calendar events
  + Operate silently in the background
  + Build a profile of user behavior and preferences
  + Sell or exploit the collected data

**3. Keyloggers**

* A **keylogger** is a specialized type of spyware.
* It records **every keystroke** typed on the system.
* Attackers can capture:
  + Usernames and passwords
  + Credit card numbers
  + Sensitive communications
* Some keyloggers also take **periodic screenshots**, transmitting them to the attacker.

**4. Stalkerware**

* **Stalkerware** is an invasive spyware variant often installed **intentionally** by someone with **physical access** to the victim’s device.
* Common users include controlling partners or employers.
* Capabilities include:
  + GPS tracking
  + Reading text messages
  + Monitoring phone calls
  + Accessing the device’s **microphone** and **camera**
* This software is often used for **personal abuse**, not financial gain.
* Stalkerware can facilitate **harassment**, **stalking**, or **domestic abuse**.
* Defense against stalkerware includes:
  + Strong passwords
  + Regular software updates
  + Checking for unfamiliar or suspicious applications

**5. Adware**

* **Adware** is a subtype of spyware focused on **displaying targeted advertisements**.
* It collects data such as:
  + Browsing history
  + Search queries
* Uses collected data to serve **interest-based ads**.
* Example: Searching for “wedding venues” may trigger ads related to weddings.
* Effects of adware include:
  + Disruption of user experience with pop-up ads
  + Slower device performance
  + Introduction of security vulnerabilities due to invasive tracking

**6. Potentially Unwanted Programs (PUPs)**

* **PUPs** are software applications users **did not intentionally install**.
* They often come bundled with legitimate software.
* Although not always malicious, PUPs are often:
  + Intrusive
  + Annoying
  + Resource-draining
* Common PUP behavior:
  + Changing browser settings
  + Displaying pop-ups
  + Installing toolbars
* PUPs often hide in **“custom” or “advanced” installation options**.
* Users can avoid PUPs by:
  + Carefully reviewing installation steps
  + Unchecking unnecessary add-ons or toolbars

**7. Summary and Best Practices**

* **Spyware and keyloggers**: Steal personal data.
* **Stalkerware**: Violates personal privacy and may facilitate abuse.
* **Adware**: Bombards users with ads and may impact performance.
* **PUPs**: Interfere with system settings and degrade usability.
* **Best Practices to Protect Yourself**:
  + Stay vigilant with software installations
  + Use strong device security (passwords, updates)
  + Routinely check for suspicious applications
  + Employ anti-malware and behavior-based detection tools