Below is your **comprehensive sentence-by-sentence breakdown** of the document **“Anti-Phishing Training Notes”** in a **professionally formatted structure** ready for pasting into Microsoft Word. This structure is minimal in spacing, cleanly aligned, and easy to study or print.

**📘 Anti-Phishing Training – Study Notes**

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

**1. Purpose of the Anti-Phishing Campaign**

* The lesson demonstrates how to **run a phishing simulation** to test users’ ability to identify phishing emails.
* The goal is to see who clicks on phishing links and provide **remedial training** if necessary.
* A **free tool** called **Phish Insight** from **Trend Micro** is used to carry out the campaign.

**2. Getting Started with Phish Insight**

* Visit **phishinsight.trendmicro.com** to access the tool.
* A free account must be created before using it.
* Once logged in, select **“Create a Campaign”** to begin setting up the phishing test.

**3. Creating the Test Campaign**

* For this demo, only one target user is used — Jason Dion.
* His information is inputted:
  + First name: Jason
  + Last name: Dion
  + Email: jason@diontraining.com
  + Department: Instructor
* After entering the details, continue to the next step.

**4. Selecting a Phishing Email Template**

* A **LinkedIn-themed template** is selected since it’s common and trusted by users.
* The email content mimics a real LinkedIn connection request.
* Phrases include:
  + “Hi Jason Dion, I’d like to join your LinkedIn network.”
  + Buttons like “Accept” or “View Profile” appear authentic.
* The template is pre-designed but can be customized for realism.

**5. Sender Email Customization**

* The fake sender address is **invitations@linkein.com** — note that both “LinkedIn” and “invitations” are misspelled.
* These typos are intentional red flags users should catch.
* However, the email can be made even more realistic by using a properly spelled address.

**6. Campaign Scheduling Options**

* The campaign can be run:
  + Over **a few days, weeks, or a month**
  + With **immediate or delayed** responses to link clicks
* Ideal for **large organizations** testing **hundreds or thousands** of users.

**7. What Happens When Users Click the Link**

* Clicking on the fake link can trigger:
  + An immediate **training alert**
  + A redirect to a webpage that says:

“You’ve been phished. You need some remedial training. Click here to begin.”

* This response educates users **in real time** after a mistake.

**8. Sending the Campaign**

* After all settings are configured, the campaign can be **scheduled or started immediately**.
* Organizers can receive **SMS confirmations** when it starts.
* After the campaign runs, you can **analyze results** to see who was fooled and assign training accordingly.

**9. Anatomy of the Phishing Email**

* The phishing email appears to come from LinkedIn:
  + Subject line: “Jason, please add me to your LinkedIn network”
  + Looks authentic with logos and branding
* But on closer inspection:
  + Links **do not go to linkedin.com**
  + They redirect to fake domains like **websitefun.club**

**10. Red Flags to Identify**

* **Misspelled domain names** (e.g., “linkein” instead of “linkedin”)
* **Incorrect sender names** (e.g., “Invitations” vs. “LinkedIn Invitations”)
* **Unusual links** that don’t match legitimate services

**11. Recommended Safe Behavior**

* Never click links directly in emails that request login info.
* Instead, **open a new browser** and manually type the URL (e.g., linkedin.com).
* This avoids falling for phishing traps that mimic login pages to steal credentials.

**12. What Happens After Clicking a Fake Link**

* The phishing page may:
  + Prompt for login details
  + Appear identical to the legitimate site
  + Collect credentials for later **credential stuffing attacks**
* Once attackers get your username and password, they can:
  + Access the original site
  + Attempt to use the same credentials across other platforms

**13. Final Training Objective**

* Teach users to be cautious with links in emails.
* Reinforce the importance of verifying **URLs**, **senders**, and **message intent**.
* Simulated phishing campaigns help reduce real-world vulnerabilities.