**>>Mail:**

**Subject: Urgent Security Alert: Your Apple Account Has Been Suspended**

**From: Apple Support [support@apple-updates.co](mailto:support@apple-updates.co)**

**Date : XX/XX/XXXX**

**Body:**

**Dear Customer,**

**We have noticed some unusual activity on your Apple ID. For your safety, we have temporarily suspended your account access.**

**To restore full access to your account and prevent permanent suspension, you must verify your identity immediately. Please click on the link below to update your information:**

**[Verify Your Account Now](https://www.google.com/url?sa=E&source=gmail&q=http://www.appIe.com-verify.us/login?id=23894723908)**

**Failure to comply within 24 hours will result in the permanent closure of your Apple ID and all associated services, including iCloud, iTunes, and App Store.**

**Thank you for your cooperation.**

**Sincerely,**

**Apple Security Department**

**>>Analyze the "From" address.**

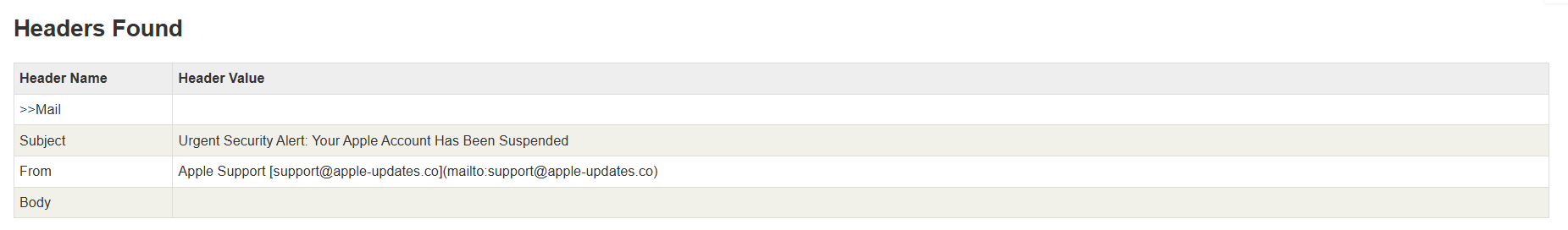
**Look at the address provided in the sample: `support@apple-updates.co`.**

**What is the sender's name? "Apple Support" - This looks legitimate at first glance.**

**What is the actual email domain? The domain is the part after the "@" symbol: `apple-updates.co`.**

**Analysis: Does `apple-updates.co` match the official domain for Apple, which is `apple.com`? No, it does not. This is a classic sign of spoofing or impersonation. The attacker has chosen a domain that looks similar to the real one to deceive you.**

**Check Email Headers for Discrepancies\*\***

****

**>>Identify Suspicious Links or Attachments**

**Locate and analyze any links. Do NOT click them.**

**In our sample email, the link is "Verify Your Account Now."**

* **The attacker has hidden the real link behind friendly-looking anchor text. If this were a real email, you would hover your mouse over the text "Verify Your Account Now" to see the actual URL.**

**>> Look for Urgent or Threatening Language**

**Read the body of the email and identify the tone and emotional triggers.**

* **Urgency: "To restore full access..." and "...must verify your identity immediately."**
* **"...prevent permanent suspension." and "Failure to comply...will result in the permanent closure of your Apple ID..."**
* **This language is designed to create a sense of panic and pressure the recipient into acting without thinking. Legitimate companies rarely use such aggressive or threatening tones to communicate security issues.**

**>> Note Any Mismatched URLs (The Real Link vs. The Display Link)**

**Compare the text of the link to the actual URL it points to.**

**Let's look at the sample:**

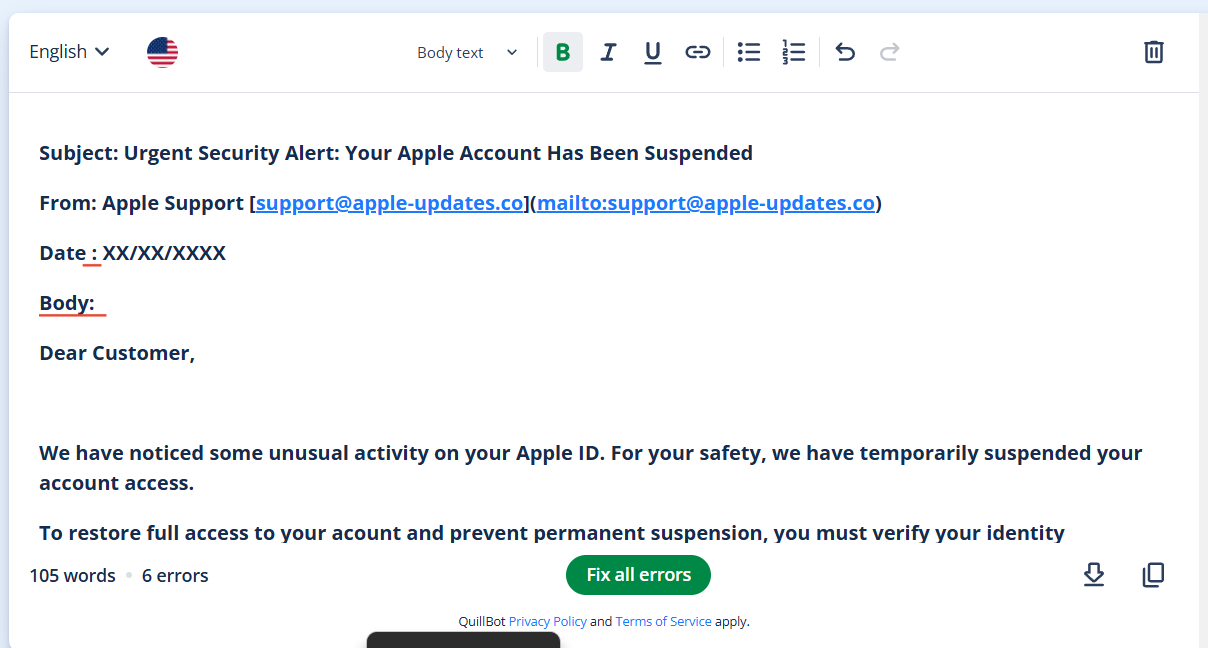
* **[Verify Your Account Now]**
* **http://www.appIe.com-verify.us/login?id=23894723908`**
* **The URL itself is suspicious. It uses a capital "i" (`I`) instead of a lowercase "L" (`l`) in `appIe`, a common trick called "typosquatting."**

**\* The domain is `com-verify.us`, not `apple.com`. The attacker has used "apple.com" as a subdomain to trick you into thinking it's legitimate. This is a very clear red flag.**

**>> Verify Presence of Spelling or Grammar Errors\*\***

* **Carefully read the entire email text.**
* **Scan the text for misspellings. In our example, `appIe.com` is a good example of this, even though it's a URL.**
* **Look for awkward phrasing or grammatical errors. Our sample is relatively clean, but many phishing emails have mistakes like "Dear Customer" (a generic greeting), or sentences that don't flow naturally.**

**The generic greeting "Dear Customer" instead of your actual name is a significant indicator that the sender does not know who you are.**

****



**This is the steps to identifying the fishing attack basically.**