# Internship Task Report – Email Analysis

## 📌 File Analyzed

* **Filename:** sample-100.eml
* **Type:** Email Message File (.eml)
* **Source:** Provided for internship analysis task

## 1. Email Metadata

* **From:** Zonnepanelen installateur <zonnepaneel@appjj.serenitepure.fr>
* **Reply-To:** news@aichakandisha.com
* **To:** phishing@pot
* **Subject:** *“Zonnepanelen voor een goede prijs”* (Translation: *Solar panels for a good price*)
* **Date:** Thu, 3 Nov 2022 04:56:15 +0000
* **Sender IP:** 57.128.69.202
* **Message-ID:** <0.0.0.0.1D8EF409A5C12CE.37AA@dturm.de>

## 2. Authentication Results

* **SPF:** None (domain dturm.de does not designate permitted senders)
* **DKIM:** None (message not signed)
* **DMARC:** None
* **CompAuth:** Fail

🔴 **Conclusion:** Authentication checks failed → Suspicious message.

## 3. Email Content

The email is a **promotional offer for solar panels** (in Dutch).  
Key highlights from the message body:

* Discusses **rising electricity & gas costs** due to inflation.
* Claims **millions of Dutch consumers already bought solar panels**.
* Promises:
  + Installation within **one day**
  + Cost savings of **hundreds of euros yearly**
  + Free quotes from **multiple providers**

It includes multiple links redirecting to **http://go.nltrck.com/...**, which is **not the same domain as the sender**. This is a potential **phishing/malicious redirect**.

## 4. Indicators of Phishing/Spam

1. **Suspicious sender domain**: appjj.serenitepure.fr vs links leading to nltrck.com.
2. **Failed SPF, DKIM, and DMARC**.
3. **Generic marketing-style HTML template** with tracking links and call-to-action buttons.
4. **Urgency & financial bait**: “Save hundreds of euros, act now!”

## 5. Conclusion

This email is likely a **phishing or spam campaign** disguised as a solar panel promotion.  
It attempts to lure recipients into clicking suspicious links under the promise of cost savings.

✅ **Action Taken for Report:**  
- Extracted metadata  
- Analyzed authentication results  
- Summarized email body & intent  
- Highlighted phishing indicators

## 6. Recommendations

* **Do not click** on embedded links.
* Report to **security/IT team** if received internally.
* Block the sender’s domain/IP.
* Educate users to recognize **failed authentication + suspicious links** as red flags.