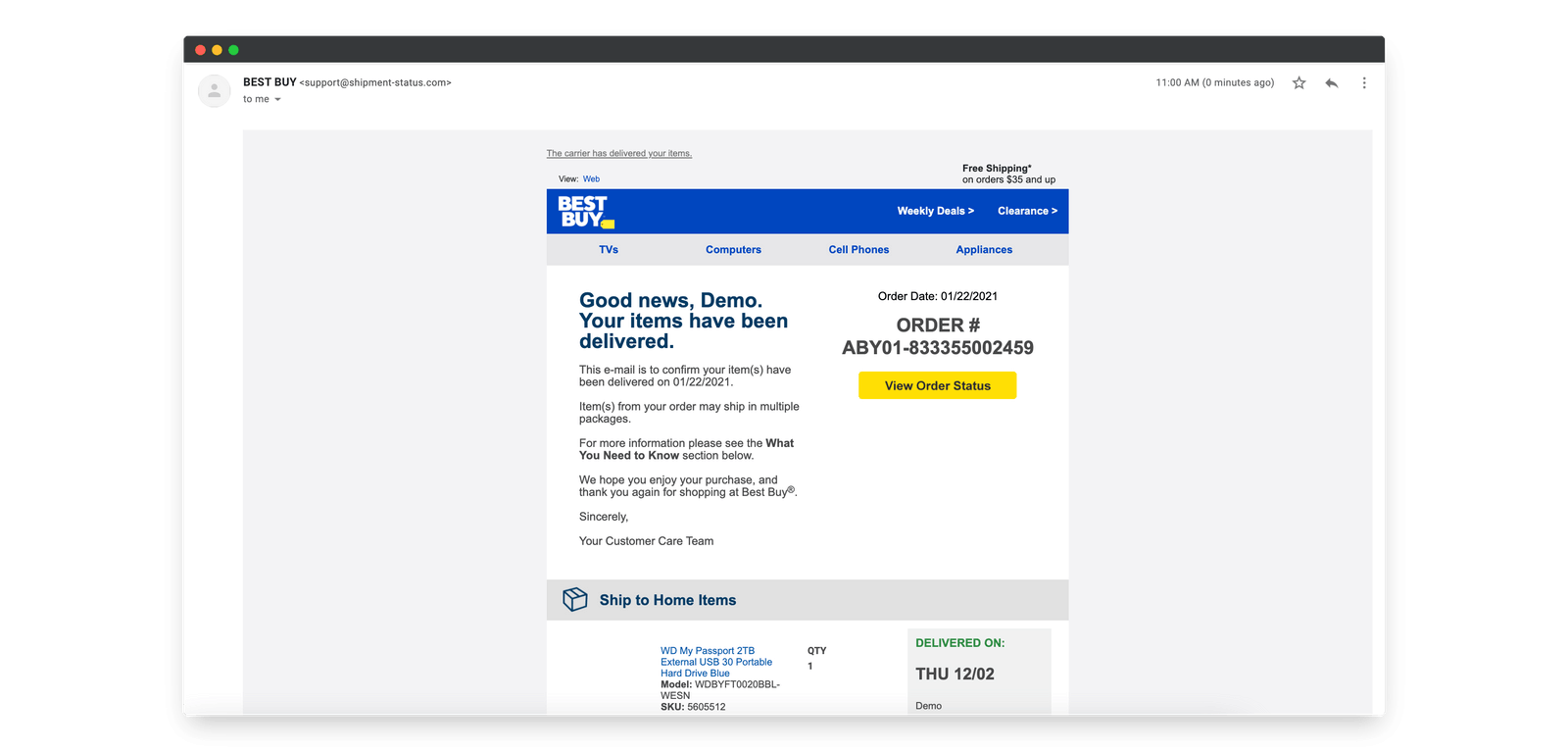
**TASK-2**

**ANALYZING A PHISHING EMAIL SAMPLE**

**(IDENTIFYING CHARACTERISTICS)**

1. **Obtaining a sample phishing email :**

****

* I have selected this sample email because this email have all the characteristics that are possible to determine this as a phishing email. ( those mentioned in hints ).
* I searched many websites but found this in a website called – **Hook Security**.

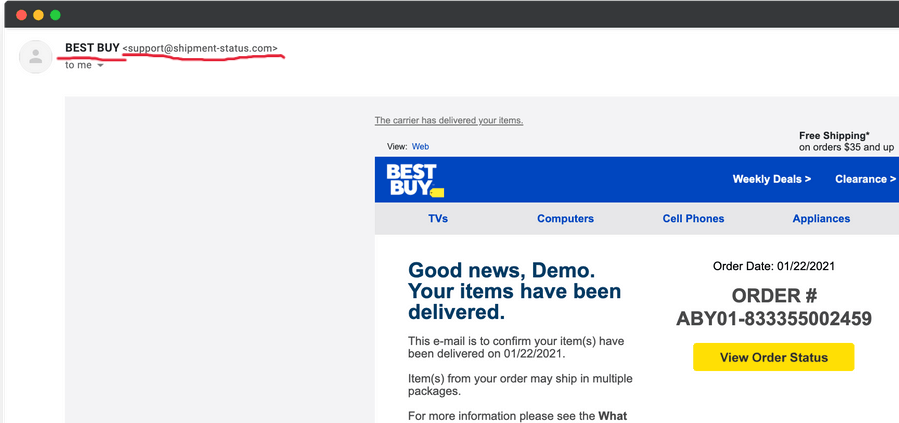
1. **Examining sender’s email address for spoofing :**

**Spoofing :** Spoofing is the act of pretending to be someone or something else to trick people or systems into trusting you.

Even though the email looks like it’s from a trusted source (like a bank or company), the actual sender is a fraud.

**Let’s analyse our sample phishing email for such kind of spoofing in sender’s email address :**

We can find 2 proofs to suspect the email as phishing email. Those are mentioned below the image.

****

* Here, we can clearly see that the “Actual email address” and the “Display name” are different in sender’s information section.

DISPLAY NAME = **BEST BUY**

ACTUAL EMAIL = [**support@shipment-status.com**](mailto:support@shipment-status.com)

* We can say that the email address is suspicious as the extension is not common and legitimate – [support@shipment-status.com](mailto:support@shipment-status.com).

1. **Checking email headers for discrepancies:**

* I have extracted the header of my sample phishing email :

Return-Path: <bounce@shipment-status.com>

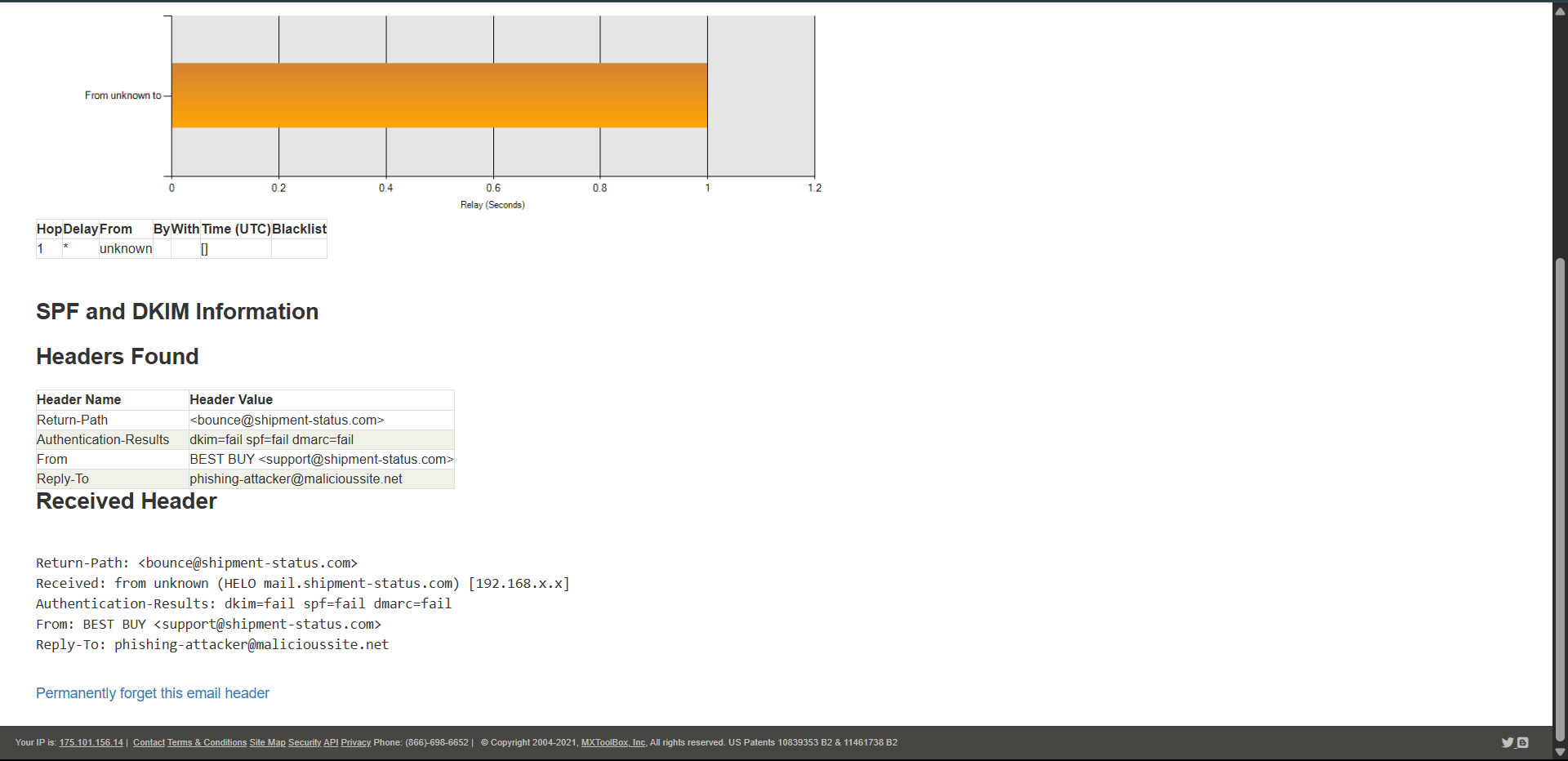
Received: from unknown (HELO mail.shipment-status.com) [192.168.x.x]

Authentication-Results: dkim=fail spf=fail dmarc=fail

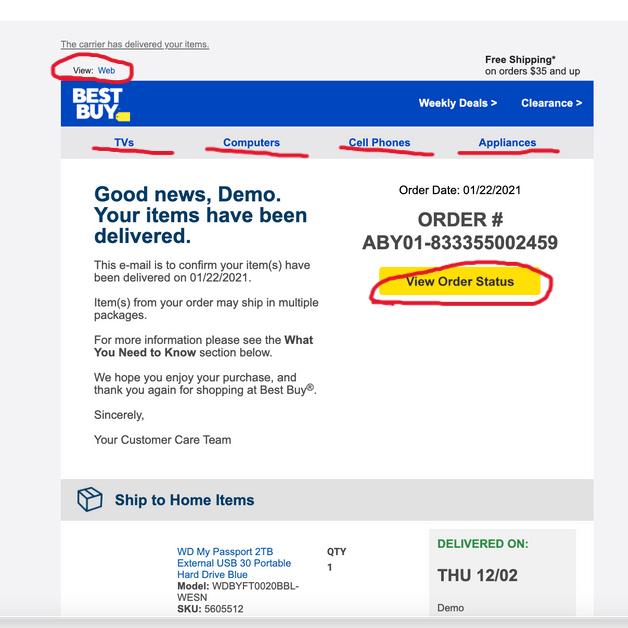
From: BEST BUY <support@shipment-status.com>

Reply-To: [phishing-attacker@malicioussite.net](mailto:phishing-attacker@malicioussite.net)

* I have entered this header and analyzed that through an online header analyzer.
* Online header analyzer website : **MxToolbox.**

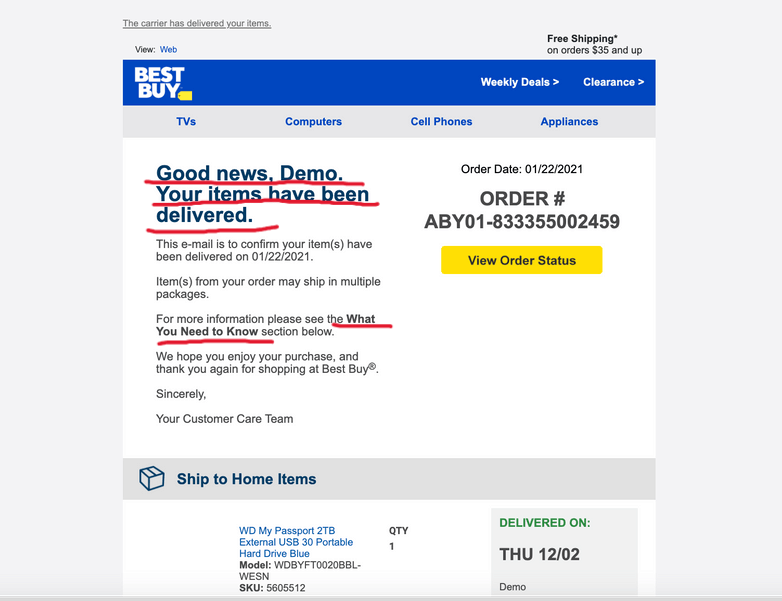


1. **Identifying suspicious links or attachments :**

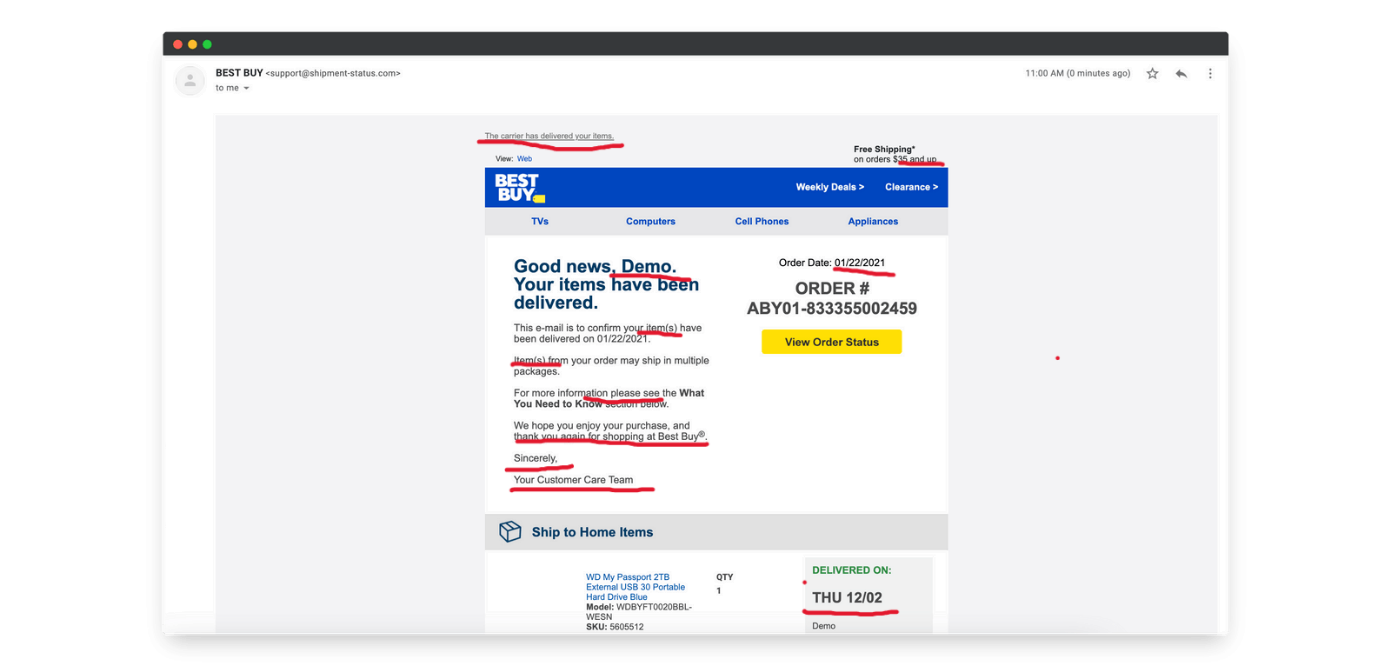
****

* These all could be click baits. But specially – **“web(top left)”** and **“view order status”** are baits for the victims.

1. **Looking for urgent or threatening language in the email body.**



1. **Verifying presence of spelling or grammar errors.**

****

1. **Summary of all the phishing traits :**

 **Spoofed Sender Name & Fake Domain:**  
The email claims to be from **“BEST BUY”**, but the sender address is support@shipment-status.com, which is not associated with the official Best Buy domain (bestbuy.com). This is a classic spoofing tactic.

 **Unusual or Generic Phrases:**  
The message uses unprofessional phrases such as:

* *“Your customer care team”* –
* *“The carrier has delivered your items”* –
* *“For more information please see the What You Need to Know section”* –
* *“We hope you enjoy your purchase”* –

 **Fake Order Information:**  
The email gives a random **order number (ABY01-833355002459)** and claims delivery of a product the user never purchased. This is meant to provoke curiosity or concern.

 **Suspicious Link/Button:**  
The **“View Order Status”** button is meant to lure users into clicking. It likely redirects to a fake login or malicious website.

 **Lack of Personalization:**  
It addresses the user as *“Demo”*, which clearly shows it is not targeted or genuine. Legitimate companies use your real name.

 **Overly Polished Layout to Mask Fraud:**  
While the email tries to mimic Best Buy’s branding, the **content and tone are not professional**. It feels robotic and oddly generic for a major company.