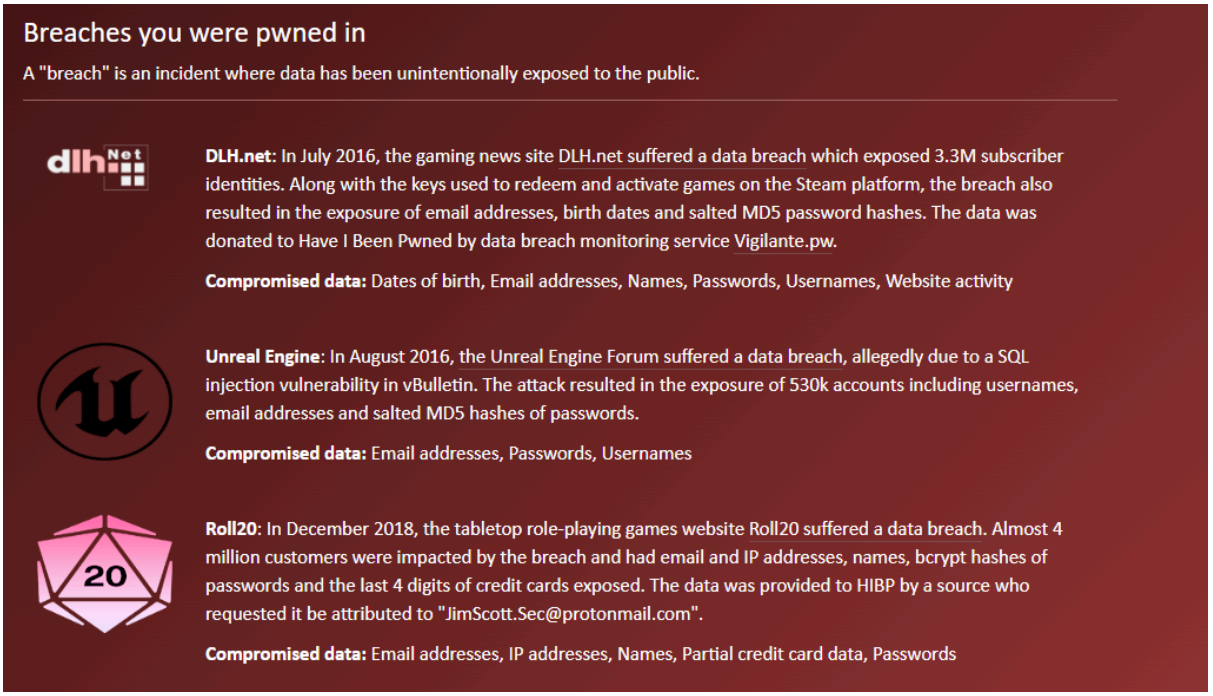
Email Threat Analysis

This report was written on the 1st of April 2025 for my Cyber Security portfolio. It deals with common Email Threats, how to verify the alleged threat and how to take measures against it.
Please note that all malicious links have been broken up by square brackets to prevent accidental access through misclicks.

My oldest Gmail account, created in the early 2010s, has been part of a grand total of 6 data breaches, weirdly enough, half of them being in the same year, 2016.
Though I have repeatedly secured it and no longer use it for anything more important than to register on unimportant websites, it is still part of actively shared combo-lists and thus receives some alerts and spam emails from time to time.



Being into video games in 2016 was a mistake, apparently.

One such spam email I received recently was from an “alleged” DHL automatic email sender, “warning” me of a missed delivery and urging me to take action to avoid having “my” package taken back to its source.
We’ll proceed to analyze the email, first starting from its actual contents, then moving on to the header, and finally bringing all information together to verify its origin through third party applications.

Part 1 - Why Phishing?

According to the IBM X-Force Threat Intelligence Indexes of the last few years, Phishing is the most common initial attack vector attackers perform on targets. Though the adoption of phishing mitigation techniques in the last few years has managed to drop the total share from 41% in 2021, to 30% in 2023, phishing still represents the single most common type of attack.
The following gives an insight on the reasons why:

- It is easy to acquire a list of target victim users' email addresses through basic reconnaissance in social media platforms (like LinkedIn) and leaked third-party subscriptions data.
- It is not hard to weaponize an email by including malicious links or attachments.
- The average user lacks security awareness and training.
- It is easy to automate massive phishing campaigns.
- It is easy to come up with new ways to evade email security detection.

Usually, we recognise three types of Email threats:

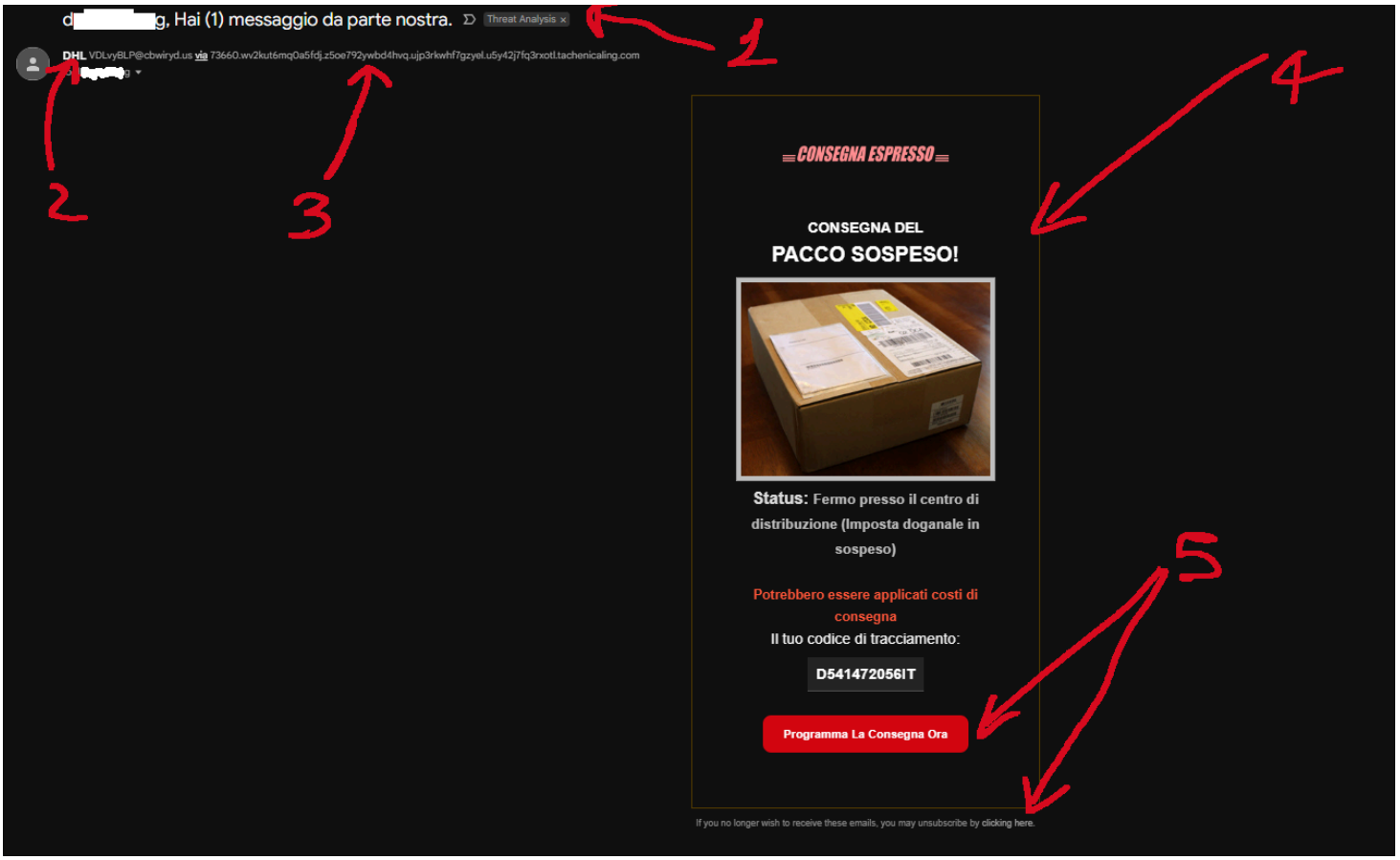
1. **(Spear)Phishing emails:** Phishing and spearphishing are both types of email attacks that aim to steal sensitive information and compromise a target's computer system. The difference between them stands in the intended target audience: Spearphishing are much more personalized and aimed specifically at known individuals, rather than regular Phishing campaigns which are generalized and aimed at the broader public.

   These types of email threats can either weaponize the body of the email, through malicious links, or the attachments, through malicious software masking as legitimate files.

2. **Blackmail emails:** Email scams where attackers claim to possess sensitive data about their target, most often of a sexual nature. It is particularly effective as it preys on the common fear of having one's private life exposed to the public. The attackers propose to exchange the deletion of this information for money, through cryptocurrency transfers. Most often an easy callable bluff.

3. **Business Email Compromise:** In which the attackers target specific individuals within a company – generally those with access to financial information – to trick them into making fraudulent transactions. It's the most complex of the three to perform, as it relies deeply on social engineering and spoofing techniques.

Part 2 - Email Contents



Actual screenshot of the email content. It reads: "Package delivery SUSPENDED! Stuck at the distribution center [Awaiting payment for customs duties]. Delivery charges may apply. Your tracking code: XXX. Reprogram Your Delivery Now."

We'll begin by taking a look at how the email looks.

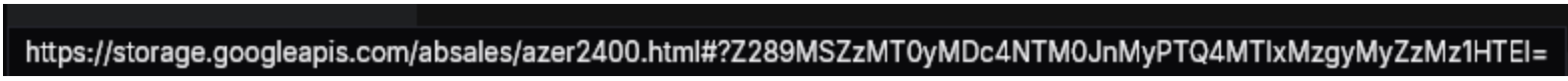
A common indicator that a message is from a phishing campaign – and thus malicious – is in its language: Phishing emails depend heavily on the emotional manipulation of their targets in order to trigger a response. Phishing language urges the user who reads it to take action immediately or be faced with unpleasant scenarios.
In the example shown, the attackers are urging me to reschedule the supposed delivery of my package or be faced with increased delivery costs. We could all see how this would be annoying if it were really happening.

Let's analyze it step by step, following the numbers I've used to highlight the different parts of the email to take into consideration:

1. The subject. It reads: "[email name], you have (1) message from us." Generic enough to avoid spoiling its contents in the preview, and likely to prompt the

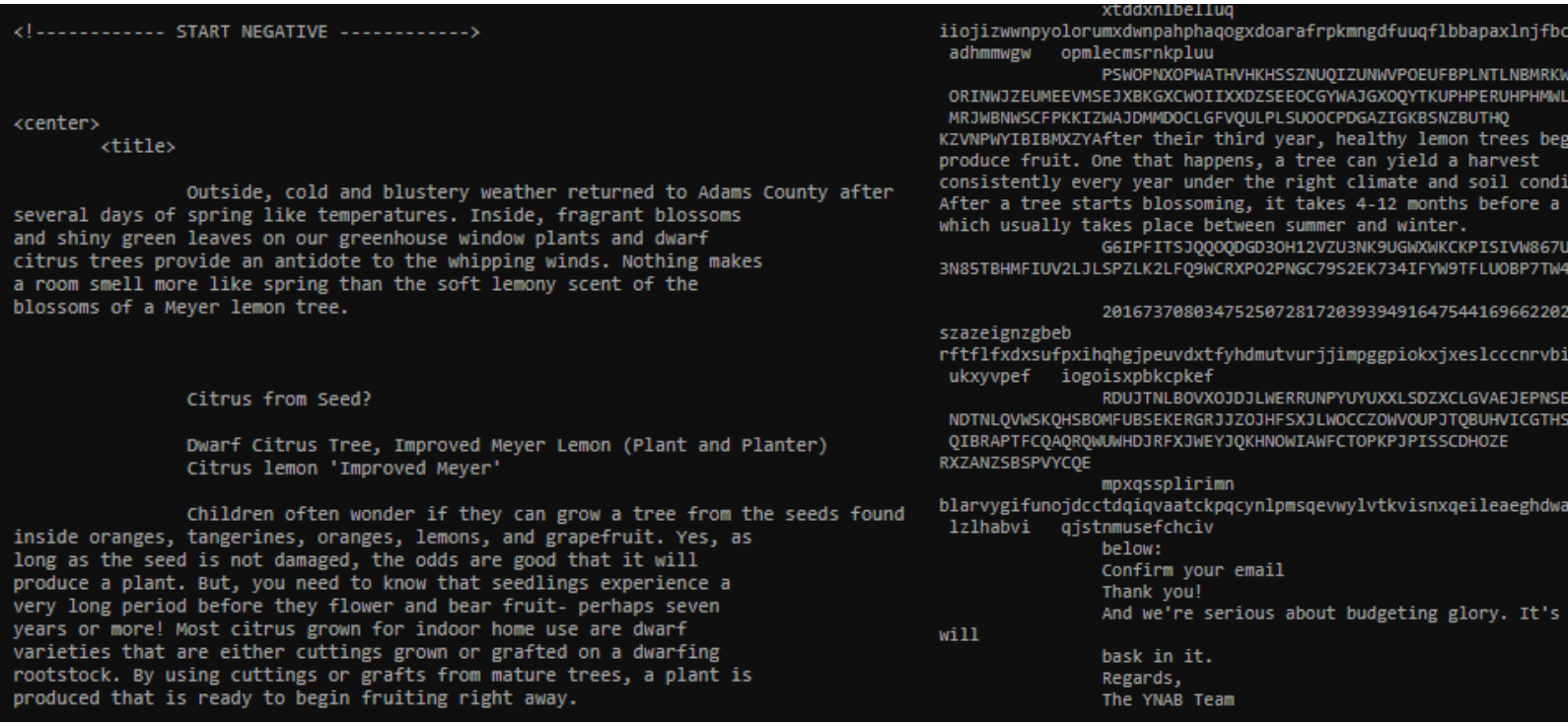
user into action by pairing it with number 2. It is also one of the most common email subjects used in such attacks.

2. The email username reads “DHL” and is trying to give a (false) sense of security to the user by reassuring the inattentive of the email’s origin.
3. The actual email sender address is “VDLvyBLP[@]cbwiryd[.]us”, so not an actual DHL address. It is also sent through another intermediate domain with a really long name.
4. The actual email body, as already discussed. Refer to the image’s caption for a translation of its contents.
5. The two (malicious) links given to us by the attackers are actually just one masquerading as two different functions. In case a non-expert user may believe that the email is legit, but they’re aware that no package is awaiting for them at DHL, the attackers have provided a handy “unsubscribe” button.



The actual link behind both buttons, as shown by the browser’s preview, is hardly a legitimate DHL link.

For some reason also, the email also contains a large invisible text about growing Citrus trees, in between large sections of seemingly random character codes.



This bit is 20,686 characters long. They seem really committed to it.

The sources of these in-depth essays about growing citrus seem to come from two different websites: The Master Gardeners and How to Provide for your family, plus

what seems to be a previous phishing campaign impersonating the online budgeting application, “You Need a Budget”.
As for the reasons why this text is present in the email, I cannot say.

Part 3 - Email Analysis

Truth be told, the contents would already be enough to class this email as a phishing attempt and thus marking it for deletion, but we wanna go the extra mile in here to make sure we’re not wasting the (precious) time of underpaid logistics workers.

Thus, we proceed into the technical analysis of this message through its headers.

```
Message-ID: <67df9e1c.050a0220.1cb6dc.5cd4SMTPIN_ADDED_MISSING@mx.google.com>
From: DHL <VDLvyBLP@cbwiryd.us>
Subject: d[redacted]g, Hai (1) messaggio da parte nostra.
To: d[redacted]g@gmail.com
Date: Sun, 23 Mar 2025 06:37:31 +0100 . 481213823
MIME-Version: 1.0
Content-Type: text/html; charset="UTF-8"
```

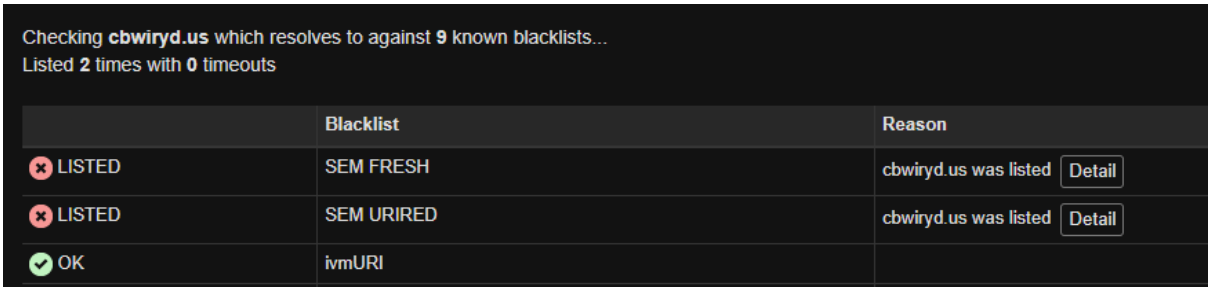
First, the metadata. It includes the timestamp of its sending to my email, generic info about the content type and MIME version.

It also tells us, in the Message-ID field that the sender agent didn’t generate a proper Message-ID and this had to be filled in by Google. This suggests a misconfigured SMTP server, or the Mail User Agent neglecting to add its own header to the email.

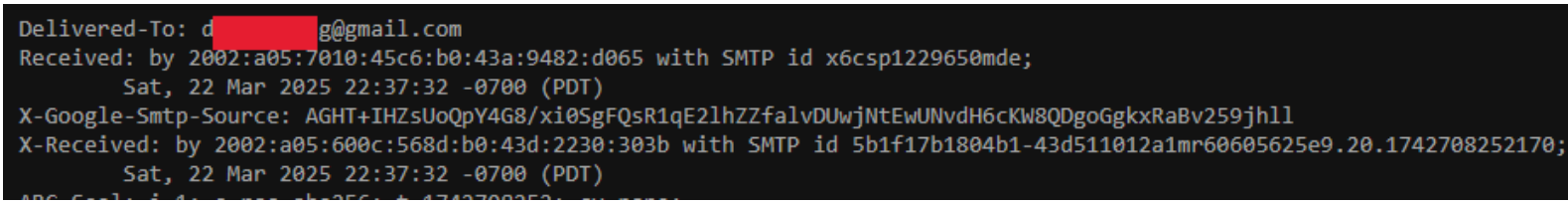
A passage into MXToolBox reveals to us that the whole domain lacks any sort of standard configuration and authentication:

Category	Host	Result
spf	cbwiryd.us	No SPF Record found
http	cbwiryd.us	The remote name could not be resolved: 'cbwiryd.us' (http://cbwiryd.us)
dmarc	cbwiryd.us	No DMARC Record found
mx	cbwiryd.us	No DMARC Record found
mx	cbwiryd.us	DNS Record not found
dns	cbwiryd.us	DNS Record not found
blacklist	cbwiryd.us	Blacklisted by SEM FRESH
blacklist	cbwiryd.us	Blacklisted by SEM URIRED
mx	cbwiryd.us	DMARC Quarantine/Reject policy not enabled

At the time of writing, this domain has been added to two blacklists:



Which would already be reason enough to discard the email as malicious.



The X-headers provide us with information about the sender's ip, which appears to be an IPv6 tunneled into an IPv6, as it is common with IPv6 in the 2002::/16 CIDR range. The SMTP server in which this email passed through is configured in Pacific Daylight Time.

The information we're actually looking for is contained in the above image, and it gives us an insight of the actual source of this message.
The Sender Policy Framework pass gives us an authorized sender domain of: "return101862[@]73660.wv2kut6mq0a5fdj.z5oe792ywbd4hvq.ujp3rkwhf7gzyel.u5y42j7fq3rxotl.tachenicaling[.][com]" with an IP address of 51.75.79.222, which is also highlighted as the return-path email.
The domain exposed in the received field for the revealed IP address is from OVHcloud, a French domain provider. According to Shodan, the actual location of the IP is in Frankfurt.

Analyzing the intermediate sender domain through urlscan.io, we get an interesting picture. There is an actual website related to it, htt]p://tachenicaling.co]m/, which has the front of a website template for a law firm.

Love the phone number.

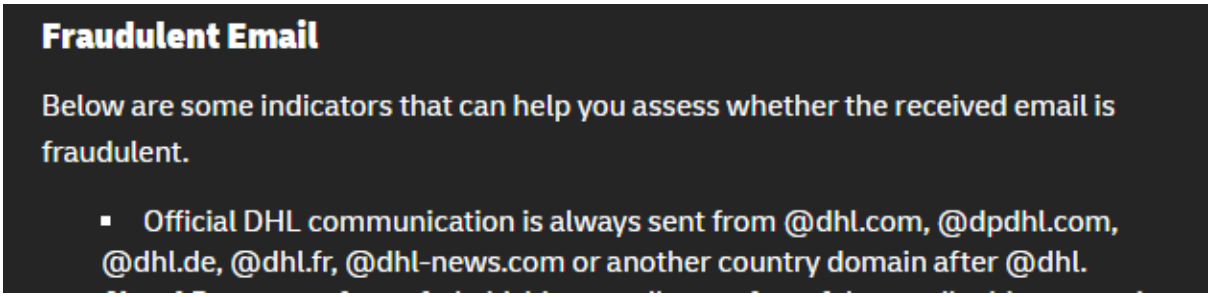
So yeah, totally a DHL website.

For comparison, here's what an actual DHL email header should look like:

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@dhl.com header.s=20140901 header.b=Kl4nVCBM;
       spf=pass (google.com: domain of noreply.odd@dhl.com designates 165.72.200.105 as permit
smtp.mailfrom=NoReply.ODD@dhl.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=dhl.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
```

Where both the domain "dhl.com" and the ip address "165.72.200.105" can be easily verified as legitimate.

The DHL website also provides a list of original domains every email should come from.



Finally, we'll look at the link included in the email, using again urlscan.io
It is a (currently) blank page, with an IP address of 185.80.130.183, which as verified through Shodan and IPInfo, links us back to a small Lithuanian internet service provider named UAB Esnet. And if we go and look at the redirects…

There's a whole link dedicated entirely to my email account. If we take it apart:

- **nav=unsuboffre::tracker:** This likely indicates the action to be taken. It is unclear what the real intention of this "unsuboffre" was, but it sure wasn't to unsubscribe to the spearphishing campaign.
- **deploy=2078534:** This could be an identifier for the specific email campaign or deployment.
- **user=d g%40gmail.com:** This is the URL-encoded (where %40 stands for @) representation of my email account, demonstrating this was a targeted effort.
- **email_id=481213823:** This is likely a unique identifier for the email sent to me.

The final verdict can easily declare this email as malicious.