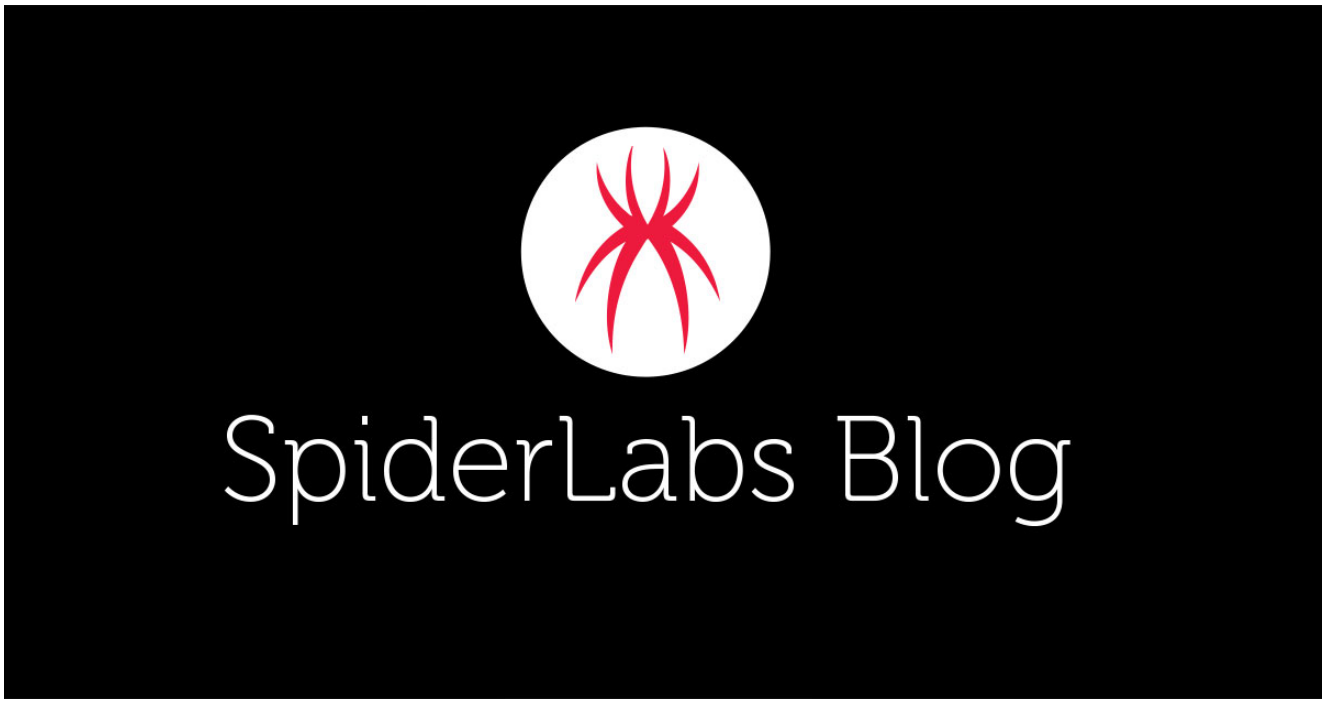
Interactive Phishing: Using Chatbot-like Web Applications to Harvest Information



Blogs & Stories

SpiderLabs Blog

Attracting more than a half-million annual readers, this is the security community's go-to destination for technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

Phishing website links are commonly delivered via email to their respective targets. Once clicked, these websites often show a single webpage that outright asks for sensitive information like account login credentials, credit card details, and other personally identifiable information (PII).

Recently, we have encountered an interesting phishing website containing an interactive component in it: a *chatbot*. Unlike a lot of phishing websites, this one establishes a conversation first, and bit-by-bit guides the victim to the actual phishing pages.

Although the phishing method is quite unique, it still uses email as the delivery channel. A deeper inspection of the email header shows that the "*From*" header is missing the email address component, which is a red flag already.

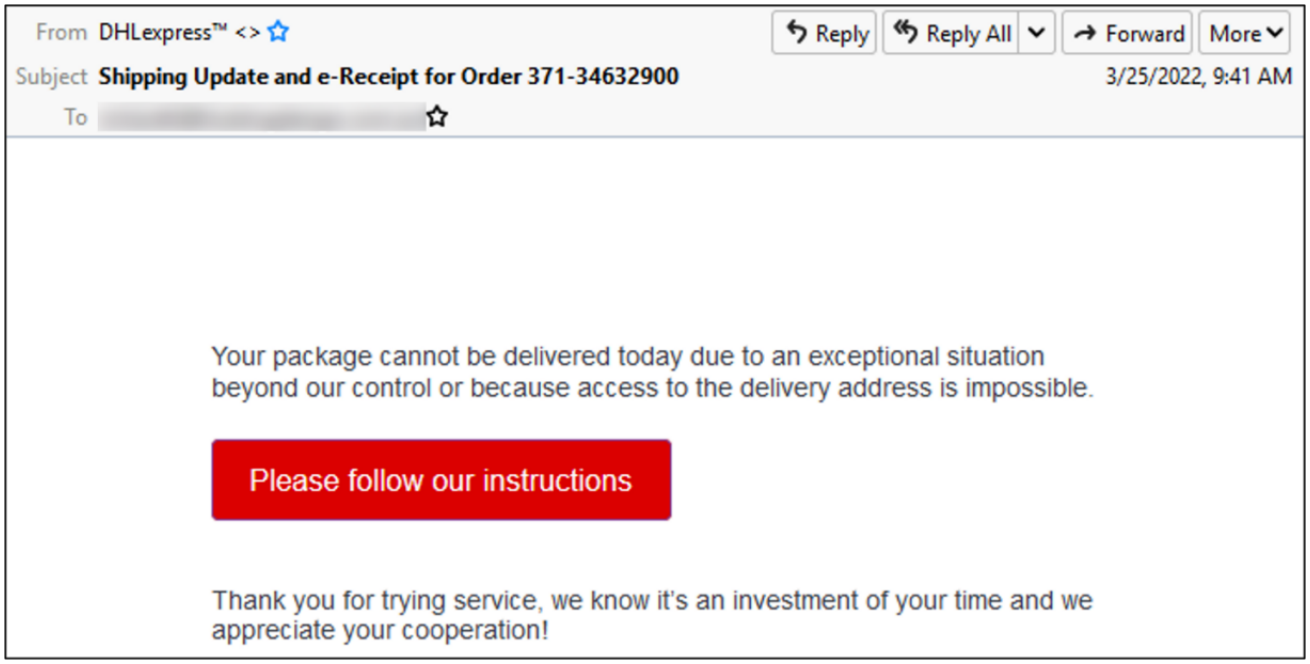


Figure 1. Phishing email with spoofed "From" header (DHLexpress).

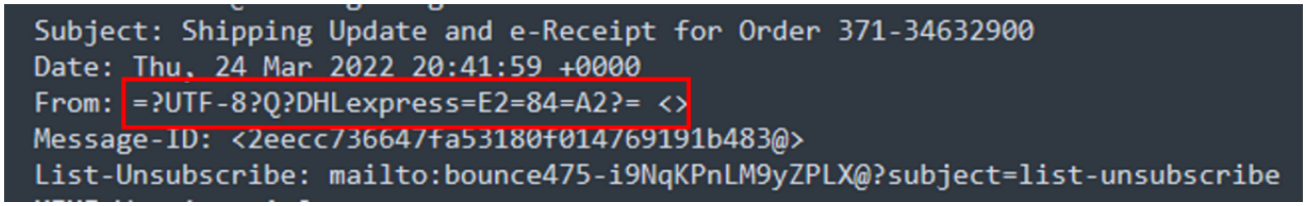


Figure 2. The spoofed "From" header does not have an email component.

Clicking the "*Please follow our instructions*" will open a browser and direct the recipient to a downloadable PDF file. There are two ways that this file will redirect the recipient to the actual phishing site. The first is through the "*Fix delivery*" button, and the second one is by copying an alternative URL from the file.

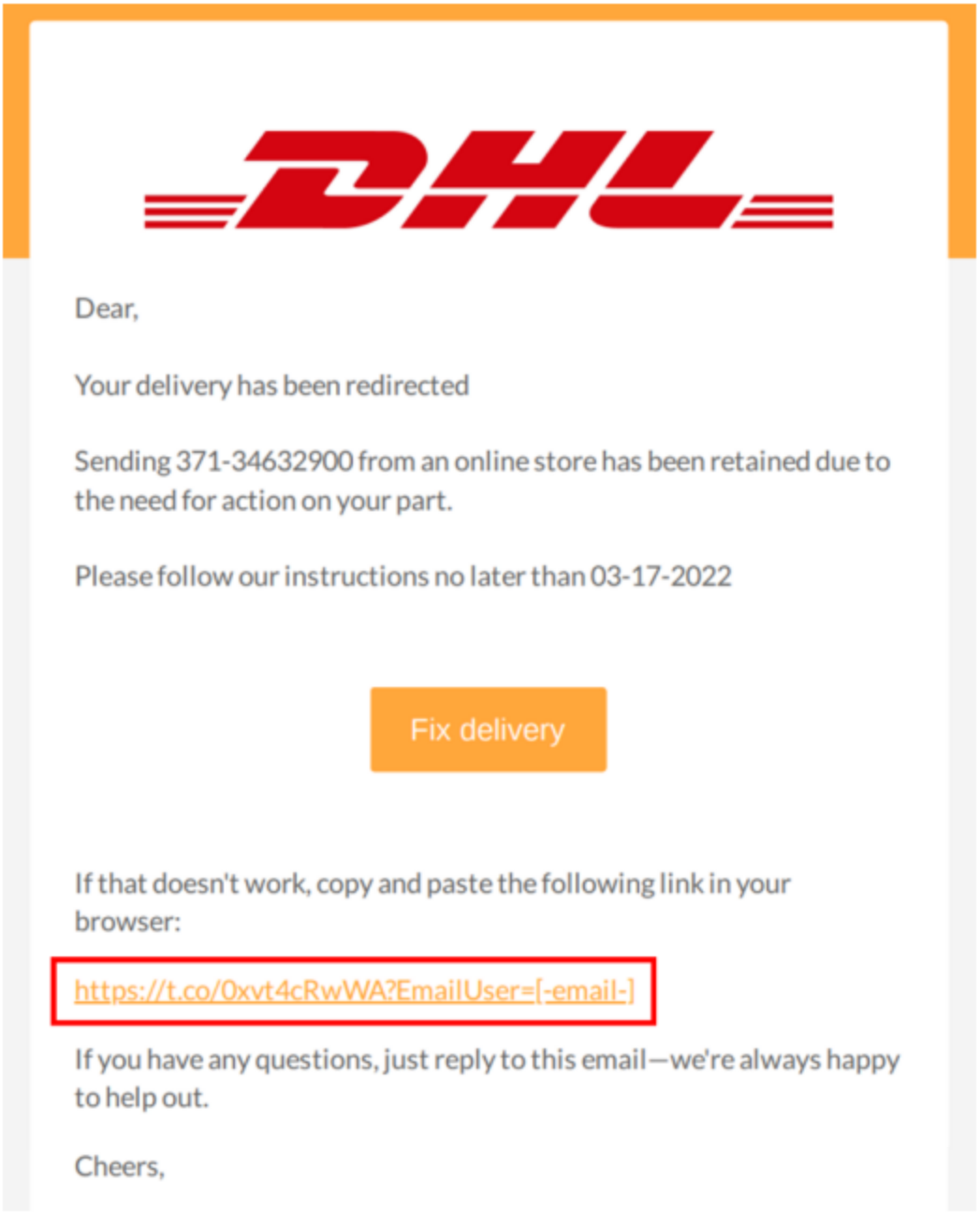


Figure 3. Downloadable PDF file carrying the DHL brand that contains the link to the phishing site.

Either of the two methods will redirect the user to the same website, and this is where the actual phishing starts.

The Phishing Link Chain

The first stop is the chatbot-like page that tries to engage and establish trust with the victim. We say “chatbot-like” because it is not an actual chatbot. The application already has predefined responses based on the limited options given.

```
var chatConfig = {
    "messageStart" : {
        "message" : [
            "Hello !",
            "Welcome to the Interactive Parcel Management System.",
            "I am your virtual guide Suzy and I will help you today.",
            "Please confirm this is your tracking number: <strong>371-34632900</strong>"
        ],
        "choices" : [
            {
                "q1" : "Yes that is correct !"
            },
            {
                "q2" : "No"
            }
        ]
    },


    "q1" : {
Response"message" : [
            "Thanks for confirming, #371-34632900 !",
            "We have a package with you as the recipient, but the label was damaged - attached is a photo of your package.",
            "Please indicate whether we should deliver this package to a home or business address."
        ],
```

Figure 4. The portion of the JavaScript containing the predefined responses of the "chatbot".

The first part of the engagement simply confirms the tracking number of the supposedly ordered item.

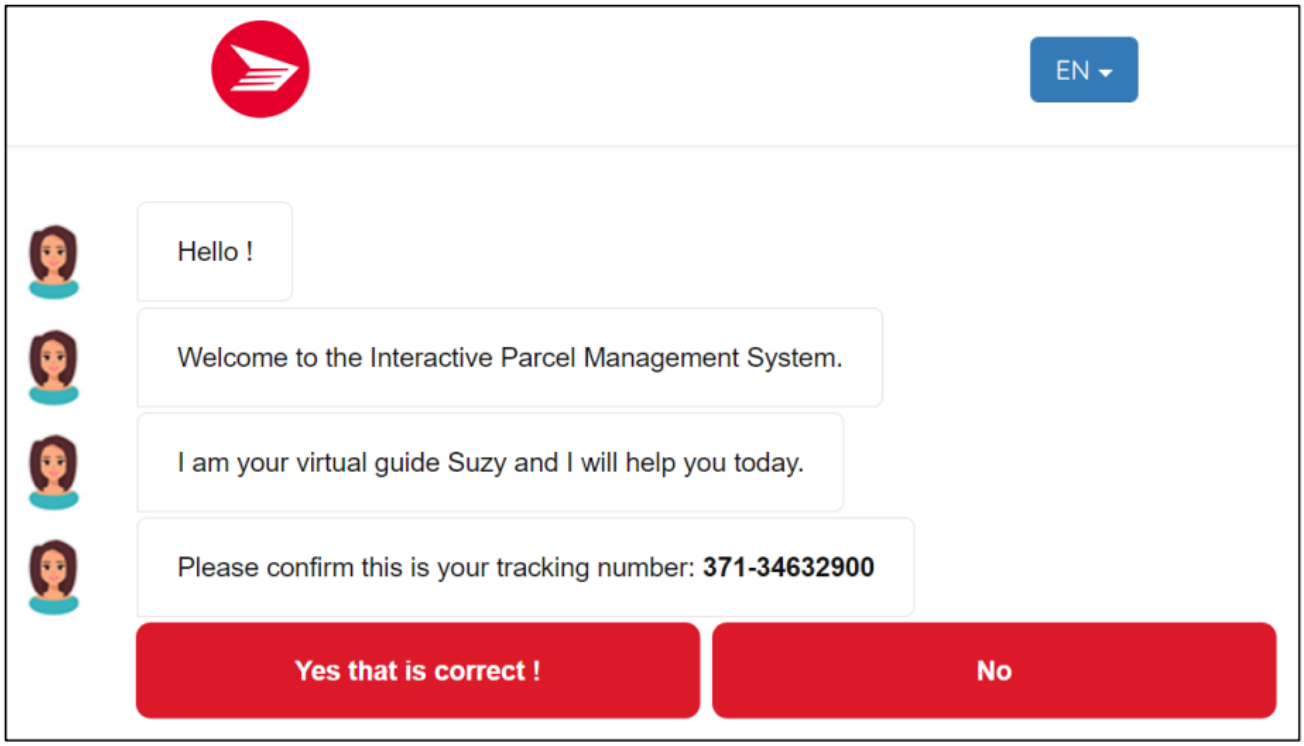


Figure 5. Chatbot-like page confirming the order tracking number.

By clicking the "*yes*" option, the program will try to engage at a higher level with the victim by showing the picture of the item and asking for the preferred delivery address (i.e., home or office address).

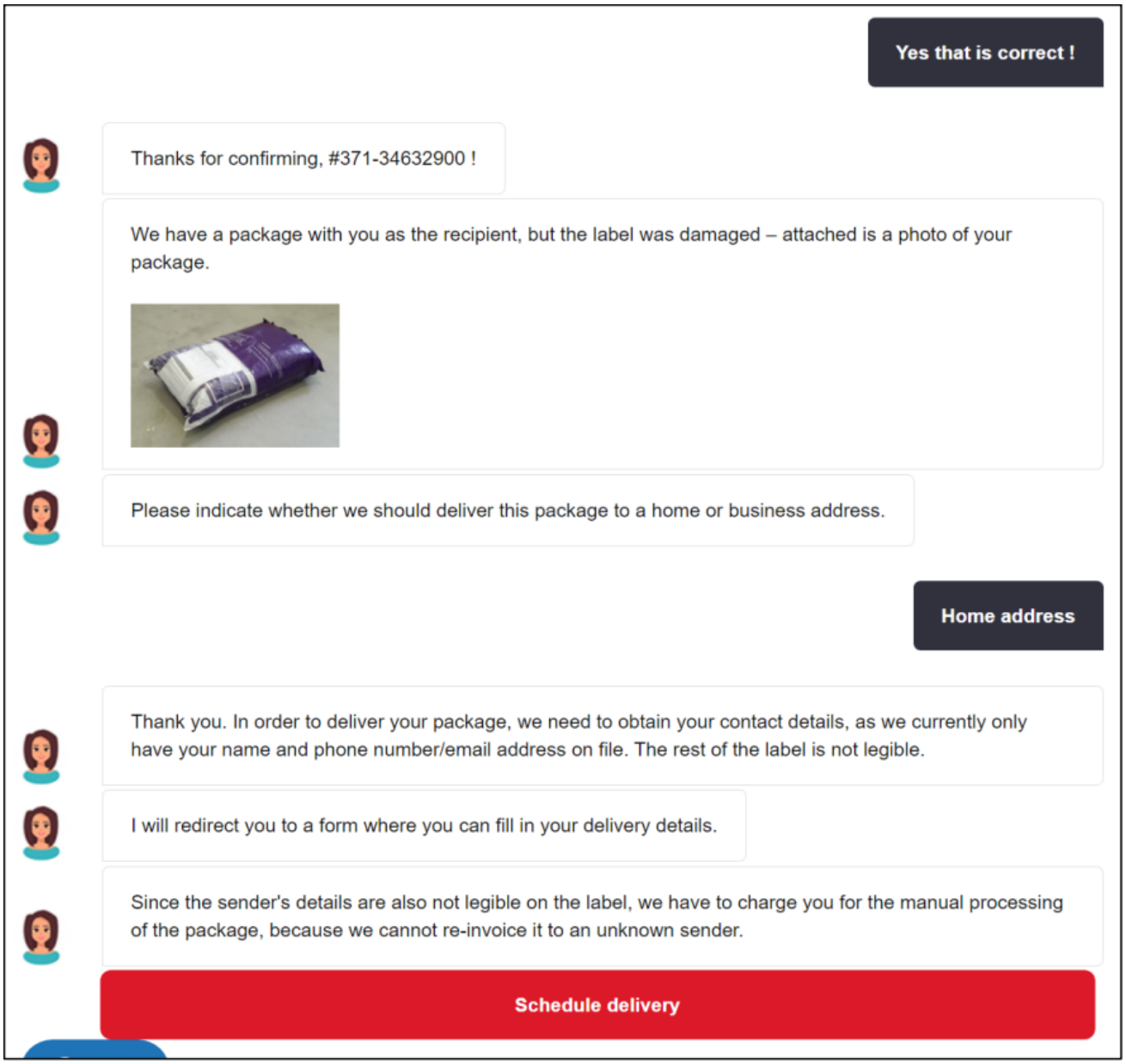


Figure 6. The "chatbot" giving more details and instructions to the recipient.

To gain even more confidence and trust from the target, a CAPTCHA is presented right after the victim clicks the "*Schedule delivery*" button. However, something is odd here – nothing else is clickable except for the confirm and close button.

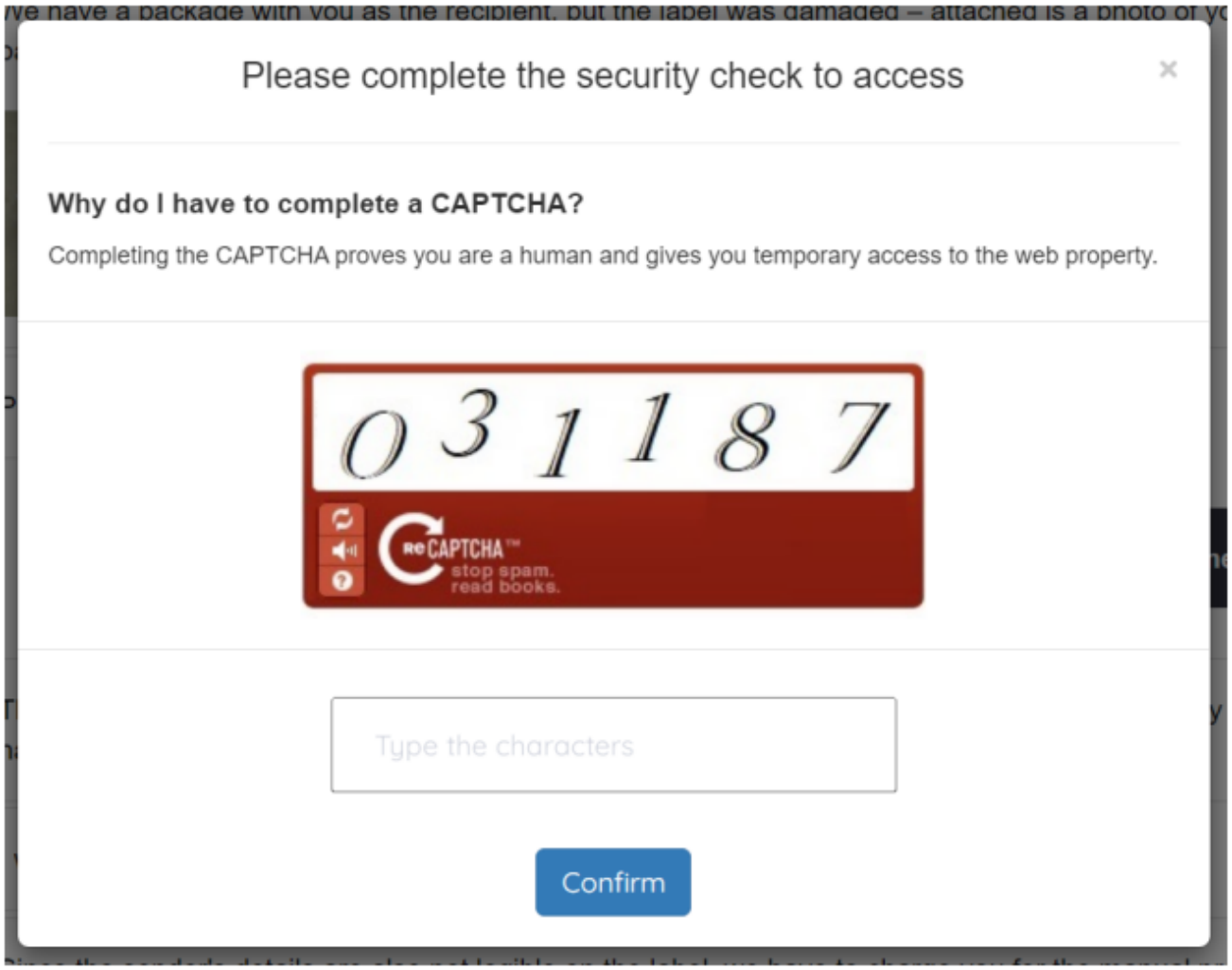


Figure 7. Fake CAPTCHA requiring the victim to type the exact numbers presented.

By checking the page source, it can be confirmed that the CAPTCHA is nothing more than an embedded JPEG image file.

```
</div>
<div class="modal-body">
  <center><img src="./POST Support EN _ 202.89.42.242 _ [redacted]files/captcha.jpg"></center>
</div>
<div class="modal-footer">
```

Figure 8. The CAPTCHA is simply an image embedded in the HTML.

By clicking "*Confirm*", the victim will now be redirected to another page where the "*chatbot*" asks for login credentials (i.e., email address and password) as well as the delivery address.

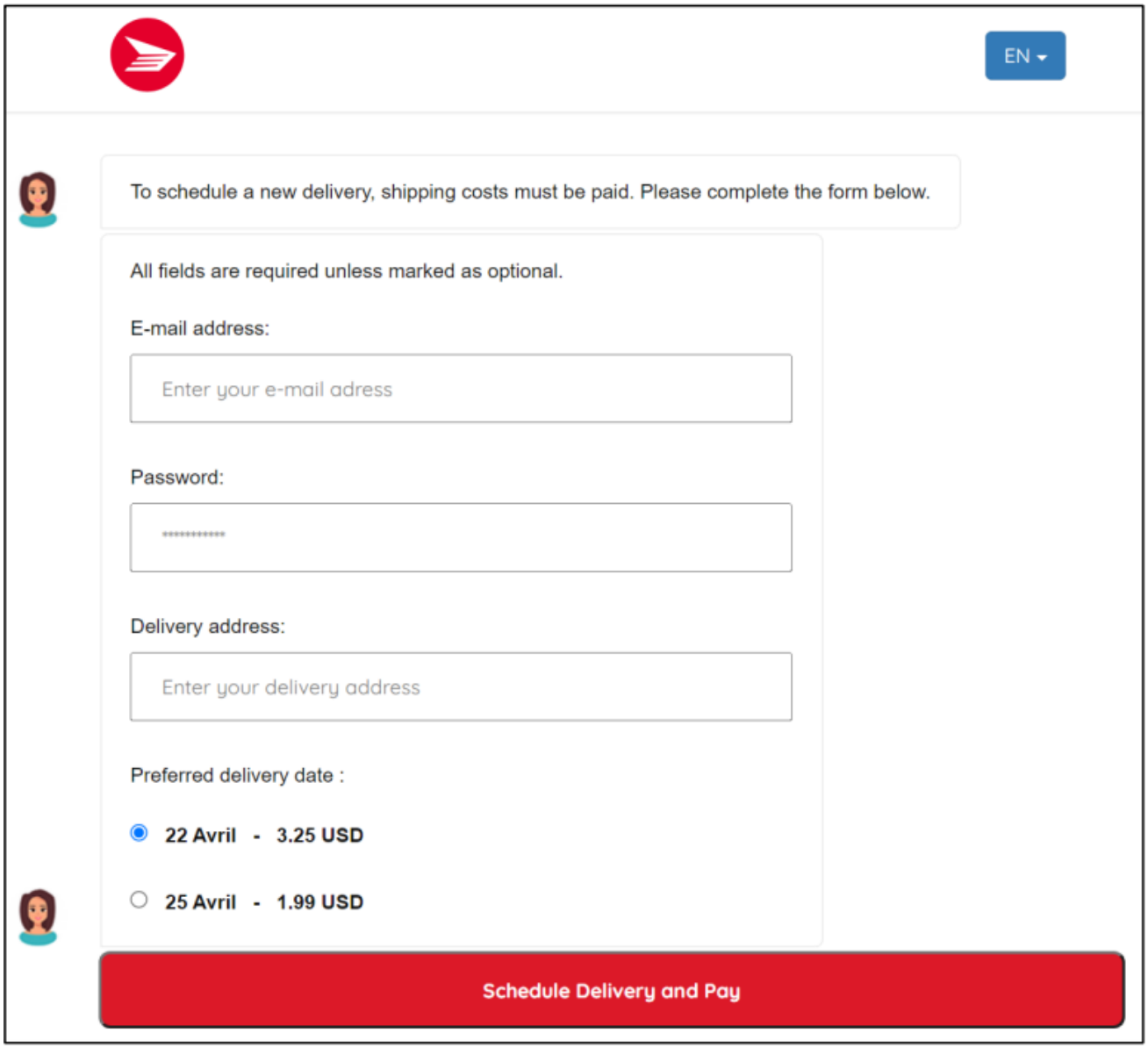


Figure 9. The "chatbot" asking for the victim's email, password, and delivery address.

At this point you might think that the perpetrators have taken what they want, but you would be wrong. The phishing does not stop on this page. Clicking the "*Schedule Delivery and Pay*" button will redirect the victim again to another phishing page. This time, trying to steal credit card information.

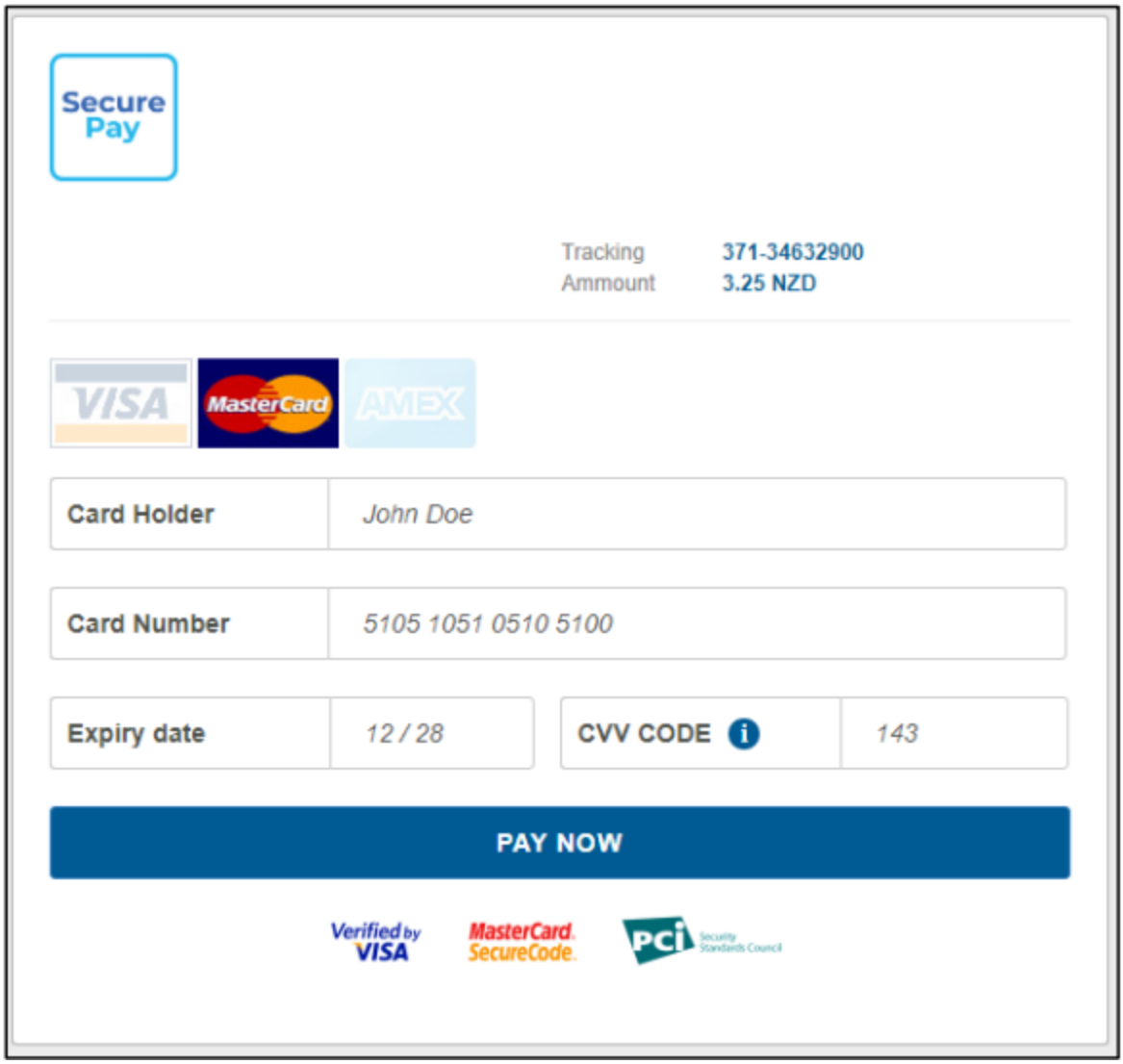


Figure 10. Credit card details harvester.

The credit card page has some input validation methods. One is card number validation, wherein it tries to not only check the validity of the card number but also determine the type of card the victim has inputed.

Once the victim fills out the form,clicking the "*PAY NOW*" button will redirect the victim to a loading page, which after a few seconds will then redirect to an OTP (One-Time Password) page. The OTP is an automatically generates characters (numeric or alphanumeric) which are usually sent to the user's registered mobile number. This serves as another layer of user authentication for a single transaction or session.

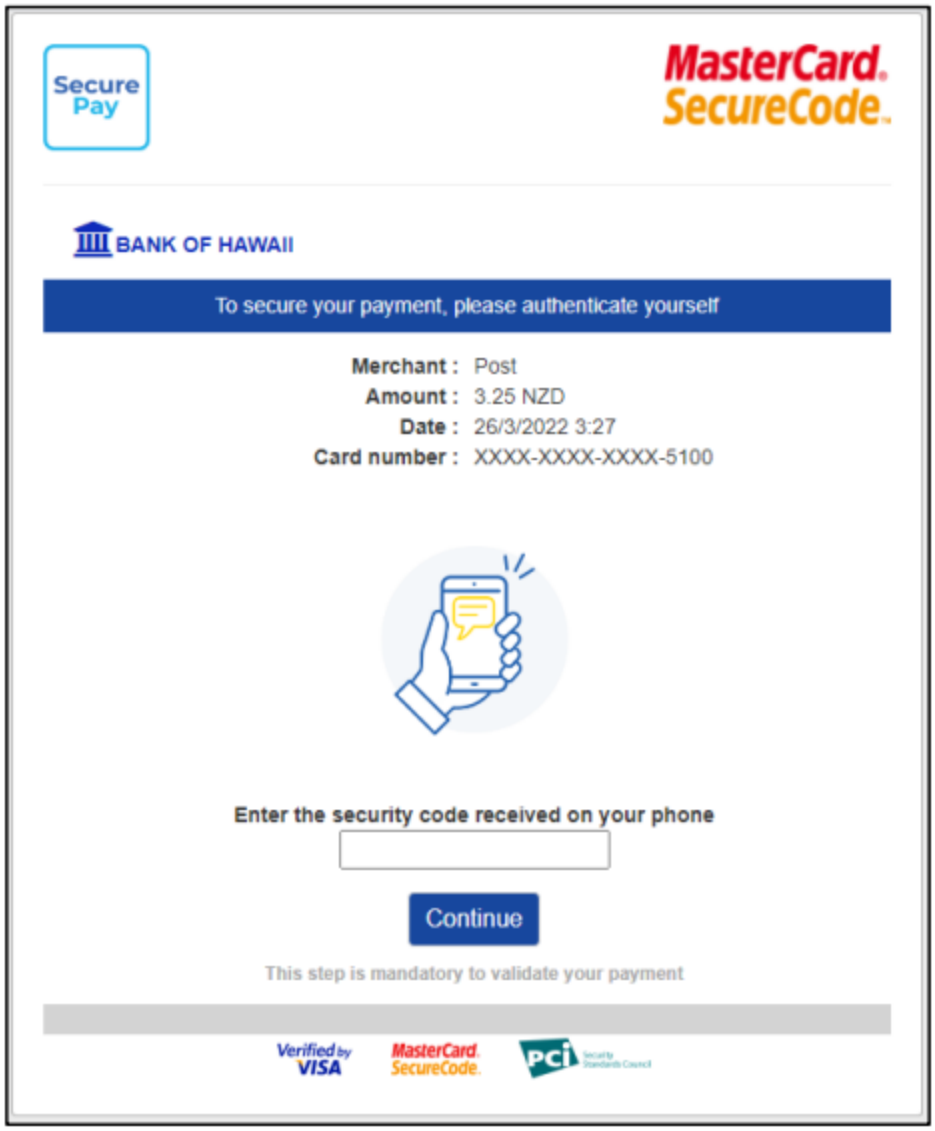


Figure 11. The program asking for OTP that was sent to the victim's phone number.

The fact that the web page asks for OTP is quite surprising because the previous pages did not ask for any mobile number information. Putting in random characters will just redirect you to the same page stating that the security code is no longer valid. On the fifth try, however, the page redirects to another page saying that the submission was successfully received. This marks the end of the perpetrator’s phishing chain.

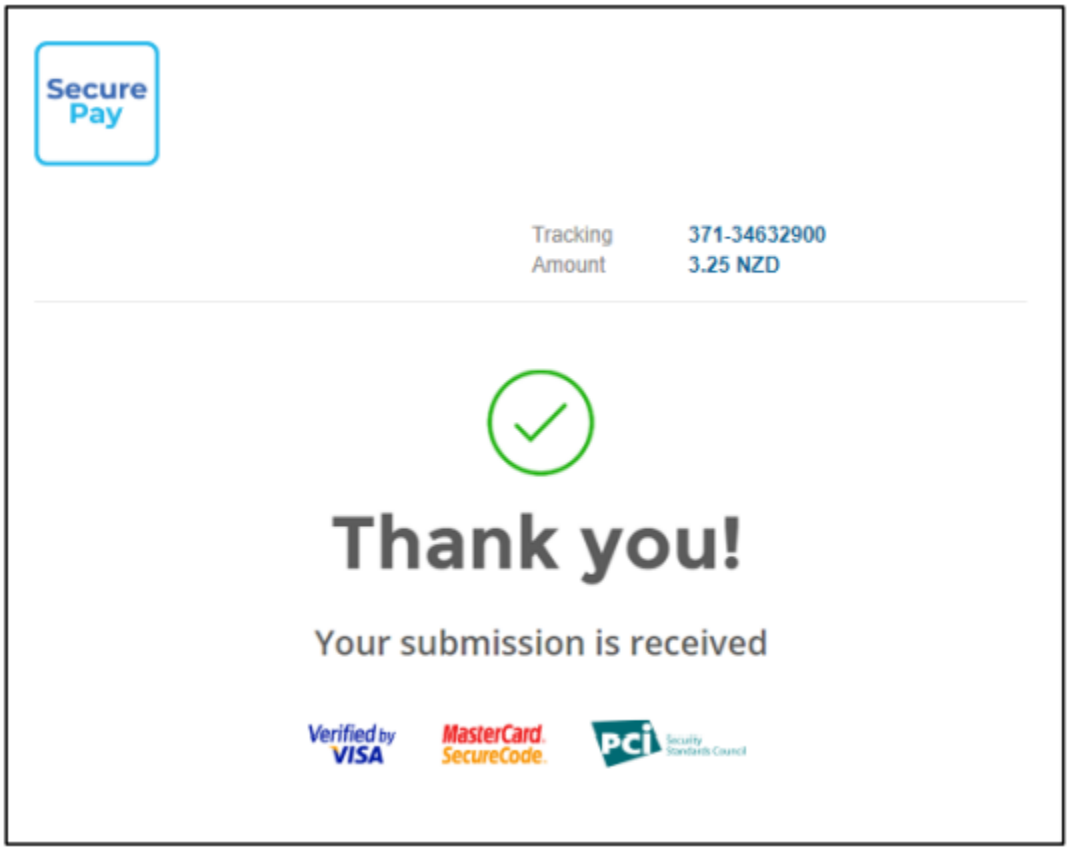


Figure 12. A submission success status after several OTP attempts.

Summary of the Phishing Link Chain:

Step	Description	URL
1	Chatbot Engagement	hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/1_Chi_Chat[.]php
2	Credential Phishing	hxxps://dhiparcel-management[.]support[1]livechat[.]24mhd[.]com/2_Chi_Contact[.]php
3	Credit Card Phishing	hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/3_Chi_Pay[.]php
4	Loading Page	hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/4_Chi_Load[.]php
5	OTP Page	hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/5_Chi_3D[.]php

6	Submission Successful Status	https://dhiparcel-management.support-livechat.24mhd.com/6_Chi_Confirm.php

It is worth noting that the URLs start with “dhi”, a misspelled version of the brand name “dhl” or “DHL”, which is clearly a spoofing technique.

The sample of this phishing email was detected by Trustwave Mailmarshal last March 25, 2022. As of this writing, the actual phishing application is still active, but now using a newly registered domain.

Conclusion

In general, using chatbots adds an interactive component to a website. This often results in a higher conversion rate because it makes the site more interesting and engaging for the users. This is what the perpetrators of this phishing campaign are trying to capitalize on. Aside from spoofing the target brand on the phishing email and website, the chatbot-like component slowly lures the victim to the actual phishing pages. Also, the addition of fake OTP and CAPTCHA pages makes the phishing website makes it seem more legitimate.

Chatbot, OTP, and CAPTCHA technologies are already common and widely used by big brands in their online systems. Therefore, customers are advised to be really careful on what they are clicking online and be aware of sophisticated phishing campaigns such as this.

Indicators of Compromise

hxxps://a0b6de4b-5060-4360-9623-8bbb76e5b670[.]usrfiles[.]com/ugd/a0b6de_47258ffcd6a14a949917fe100118be1c[.]pdf

hxxps://noticecenters[.]org/Home/?Activation=##az-AZ-09-{99}##

hxxps://t[.]co/0xvt4cRwWA?EmailUser=[-email-]

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/1_Chi_Chat[.]php

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/2_Chi_Contact[.]php

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/3_Chi_Pay[.]php

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/4_Chi_Load[.]php

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/5_Chi_3D[.]php

hxxps://dhiparcel-management[.]support-livechat[.]24mhd[.]com/6_Chi_Confirm[.]php

hxxps://www[.]live-support[.]net/1_Chi_Chat[.]php

hxxps://www[.]live-support[.]net/2_Chi_Contact[.]php

hxxps://www[.]live-support[.]net/3_Chi_Pay[.]php

hxxps://www[.]live-support[.]net/4_Chi_Load[.]php

hxxps://www[.]live-support[.]net/5_Chi_3D[.]php

hxxps://www[.]live-support[.]net/6_Chi_Confirm[.]php