



Wyłudzenia danych od użytkowników kart za pośrednictwem fałszywych SMS oraz reklam/postów

Przekazujemy informację odnoszącą się do prób wyłudzenia danych od użytkowników kart za pośrednictwem fałszywych SMS oraz reklam/postów.

Opis działania cyberprzestępców

Fałszywe SMS-y

Schemat działania cyberoszustów opiera się na masowej wysyłce wiadomości SMS z informacją o rzekomych problemach z dostarczeniem przesyłki. Najczęściej przestępcy podszywają się pod wizerunki najbardziej rozpoznawalnych dostawców usług, np.: Poczty Polskiej, InPost, UPS, itp., aby wzbudzić w swoich potencjalnych ofiarach możliwie jak największe zaufanie. Starają się nakłonić odbiorców wiadomości do uzupełnienia danych karty na fałszywej stronie internetowej, do której prowadzi link zawarty w SMS-ie.

Umieszczony w wiadomości link, przenosi potencjalną ofiarę na fałszywą stronę, ładząco przypominającą prawdziwe strony firm kurierskich. Tam, pod pretekstem np. dopłaty za ponowną dostawę, znajduje się fałszywy formularz płatności. Cyberprzestępcy nakłaniają do wpisania danych karty płatniczej, które wykorzystują następnie do kradzieży pieniędzy z konta ofiary (Klienta).

Fałszywe reklamy/ posty

Posty mają na celu wzbudzić zainteresowanie, podejść do Klienta emocjonalnie lub zachęcić go świetną okazją inwestycyjną. Reklamy/posty wyłudzające dane do logowania na portale społecznościowe służą cyberprzestępcom do:

- 1) pozyskania danych zapisanych na tychże portalach (na przykład dane kart płatniczych);
- 2) wykorzystania profilu Klienta do oszustw z wykorzystaniem kodów BLIK oraz
- 3) pozyskania danych do logowania do bankowości elektronicznej.

W jaki sposób chronić się przed tego typu cyberatakami?

W przypadku jakichkolwiek wątpliwości co do autentyczności otrzymanego SMS-a, należy skontaktować się bezpośrednio z firmą lub instytucją, którą ma reprezentować nadawca. Należy użyć oficjalnego numeru telefonu lub adresu e-mail z oryginalnej strony internetowej, nie należy korzystać z danych podanych w SMS-ie.

Jeśli Klient podał dane kart płatniczych lub bankowości internetowej na portalu lub fałszywej stronie, powinien natychmiast skontaktować się ze swoim Bankiem.

Fałszywe inwestycje (w związku z trendem, jaki jest głoszony medialnie, że rok 2024 jest rokiem hossy na kryptowalutach) szczególną uwagę należy zwrócić na reklamy inwestycji w kryptowaluty.

Fałszywe domeny/ sklepy internetowe

Jak rozpoznać fikcyjną domenę?

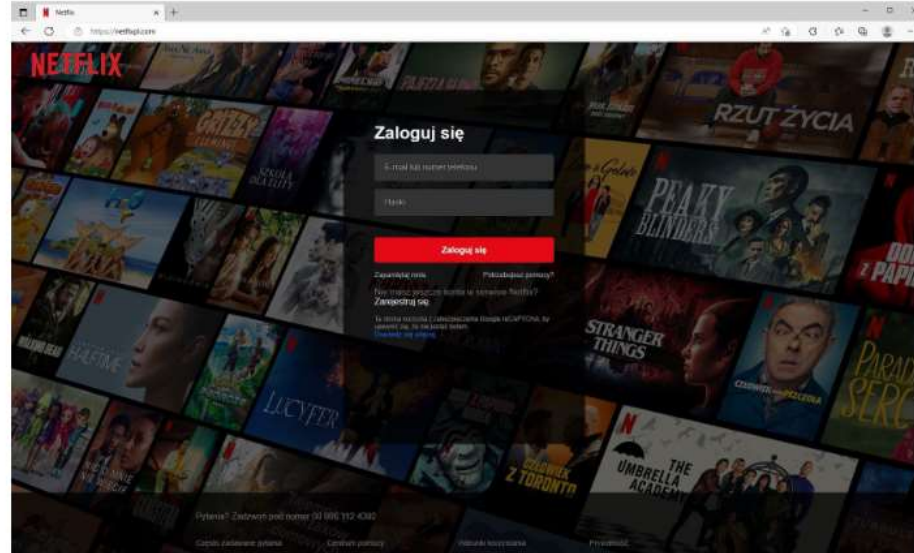
1. Adres domeny jest niewłaściwy np. com.pl/ .press.com.pl/ pl-xxx.top/ -pl. World;
2. Brak polskich znaków na stronie sklepu;
3. Oferta promocji np. -50 % na cały asortyment;
4. Ceny produktów są bardzo zaniżone;
5. Metody płatności są ograniczone, a czasami możliwa jest tylko płatność kartą.

Poniżej przedstawiamy Państwu wybrane metody oszustw:



Fałszywe wiadomości SMS – Netflix

NETFLIX: Twoja subskrypcja wygasła, prosimy o jej odnowienie poprzez potwierdzenie danych w ciągu 24 godzin.
<https://netflixpl.com/>

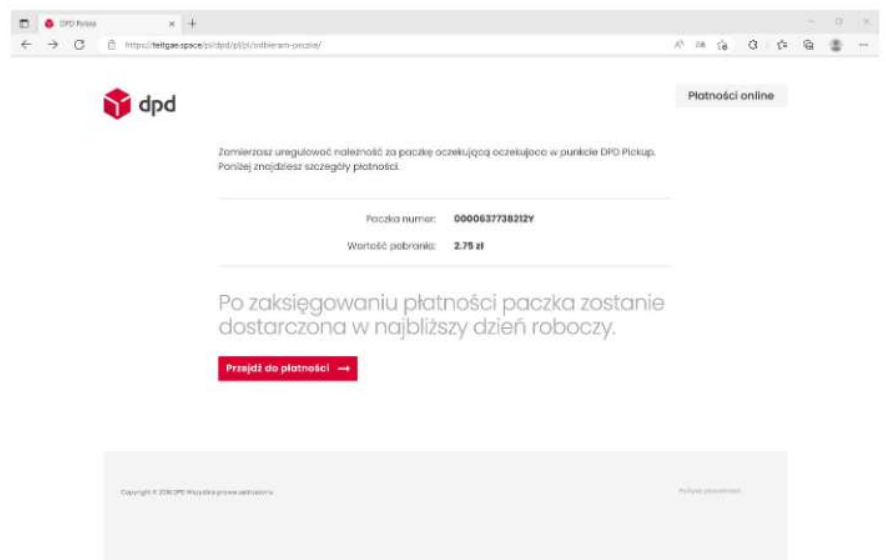


Fałszywe wiadomości SMS – DPD

niedziela, 4 grudnia 2022

DPD: Dostawa twojej przesyłki została wstrzymana z powodu nadwagi. Ureguluj należność 2.75 zł aby uniknąć zwrotu przesyłki:
<https://tiny.one/2p88auds>

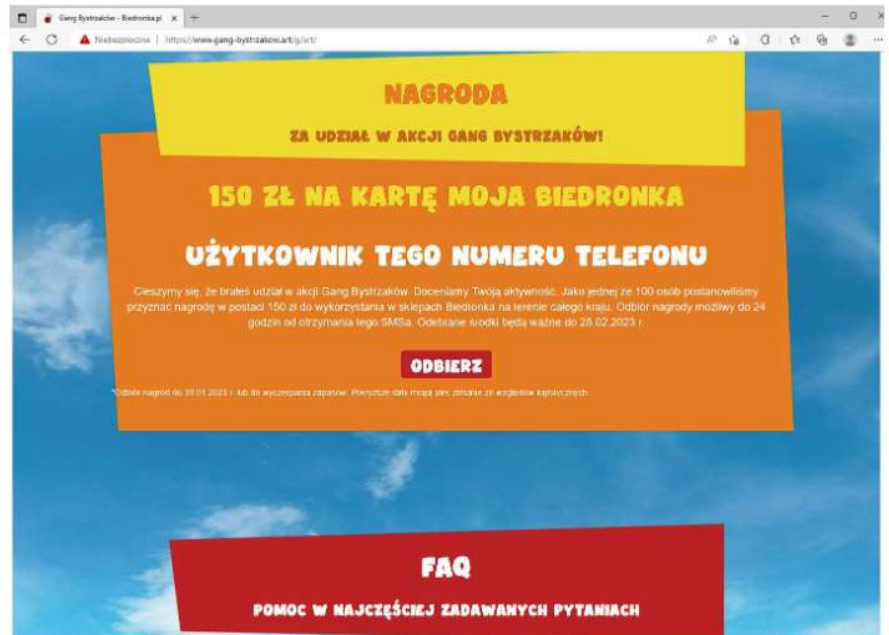
08:54





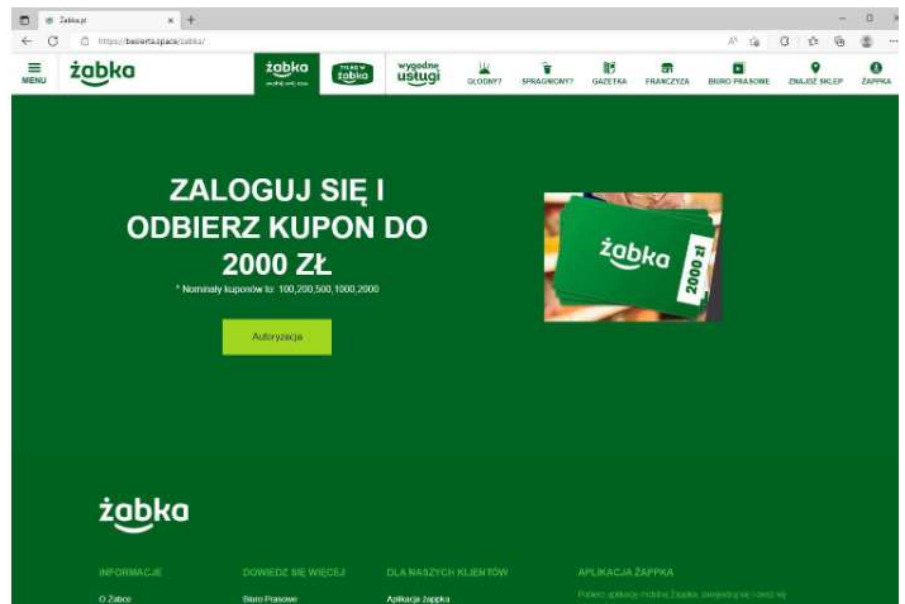
Fałszywe wiadomości SMS – Biedronka

Witaj Mirosław.
Otrzymujesz nagrodę w wysokości 150zł na karte Moja Biedronka. Odbierz: <https://www.gang-bystrzakow.art/g/ang?w=0bEeb> 14:18



Fałszywe wiadomości SMS – Żabka

Otrzymałeś kupon na zakupy od Żabka: <https://tinyurl.com/44w8hjsf>
Teraz





Fałszywe wiadomości SMS – InPost

Twoja paczka została wstrzymana z tytułu niedopłaty 2.50 PLN. Przepraszamy za utrudnienia. Prosimy uregulować należność: <https://tinyurl.com/4yj4zcfz>

14:59

The screenshot shows a browser window with the URL <https://vistoriahak.pl/paczka/98220579622357/>. The page features the InPost logo and a button for 'Płatności online'. The main text reads: 'Zamierzasz uregulować należność za paczkę oczekującą w Paczkomacie. Poniżej znajdziesz szczegóły płatności.' Below this, it displays 'Paczka numer: 346597203529738501357138' and 'Wartość pobrania: 2.50 zł'. A message states: 'Po uregulowaniu należności otrzymasz kod uprawniający Cię do zapłaty paczki z Paczkomatu.' At the bottom, there is a yellow button labeled 'Przejdź do płatności →'.

Fałszywe wiadomości SMS – Zapłać Mandat

W dniu 2.01.2023 twój mandat zostanie przekazany do komornika z tytułu zaległości 5.00 PLN. Oplac teraz: <https://tinyurl.com/4fb66pfj>

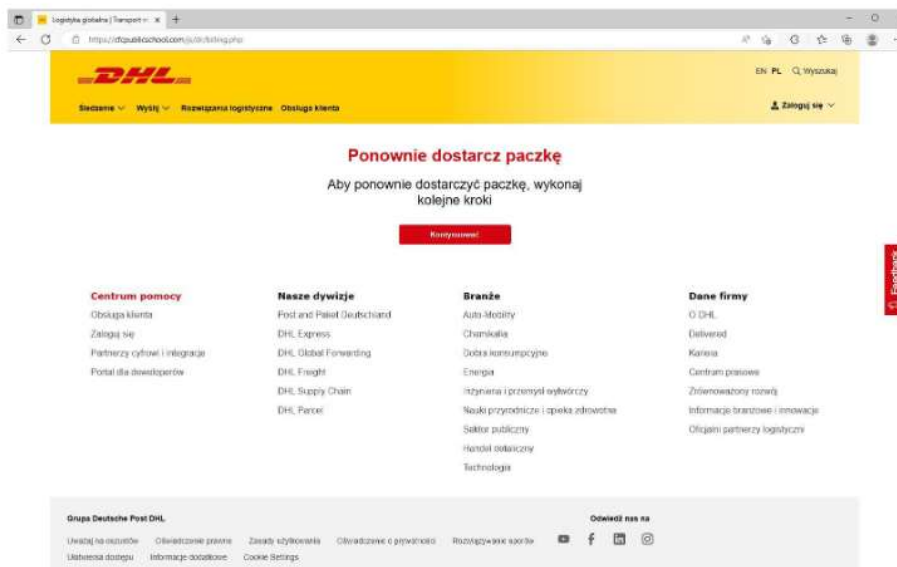
The screenshot shows a browser window with the URL <https://skarbik.mkp.pl/wszelamandat/wskaz/>. The page has a header with a logo and a main text block: 'Na tej stronie można zapłacić grzywnę należną w drodze mandatu karnego (np. przez Policję), startującą dochód budżetu państwa. Od 1 stycznia 2010 roku, poborem należności wynikających z tego rodzaju grzywn, na terenie całego kraju zajmuje się Pierwszy Urząd Skarbowy w Opolu.' Below this is a form titled 'Mandat karny:' with fields for 'Kwota' (5.00 zł PLN), 'Pełnił' (empty), 'Telefoni' (48), and 'Nr rachunku, na który zostanie przekazana wpłata' (47 1010 0005 0201 6090 0999 0000). The 'Odbiorca' is listed as 'Pierwszy Urząd Skarbowy w Opolu'. At the bottom, it says 'Wybierz jednorazową formę płatności:'.



Fałszywe wiadomości SMS – DHL



[DHL Polska]
Drogi Kliencie, Twoja przesyłka nie mogła zostać dostarczona z powodu nieuiszczenia opłat celnych :
<https://v.ht/post-dhl>

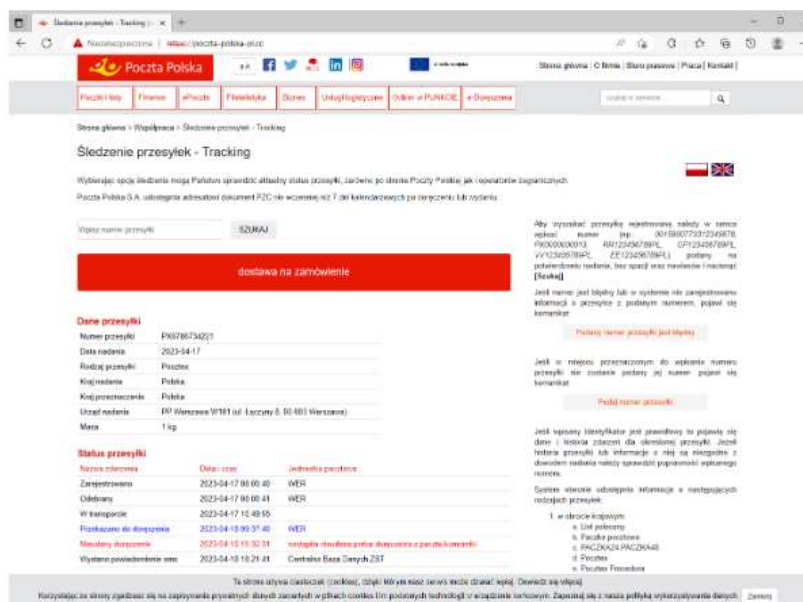


Fałszywe wiadomości SMS – Poczta Polska

09:46

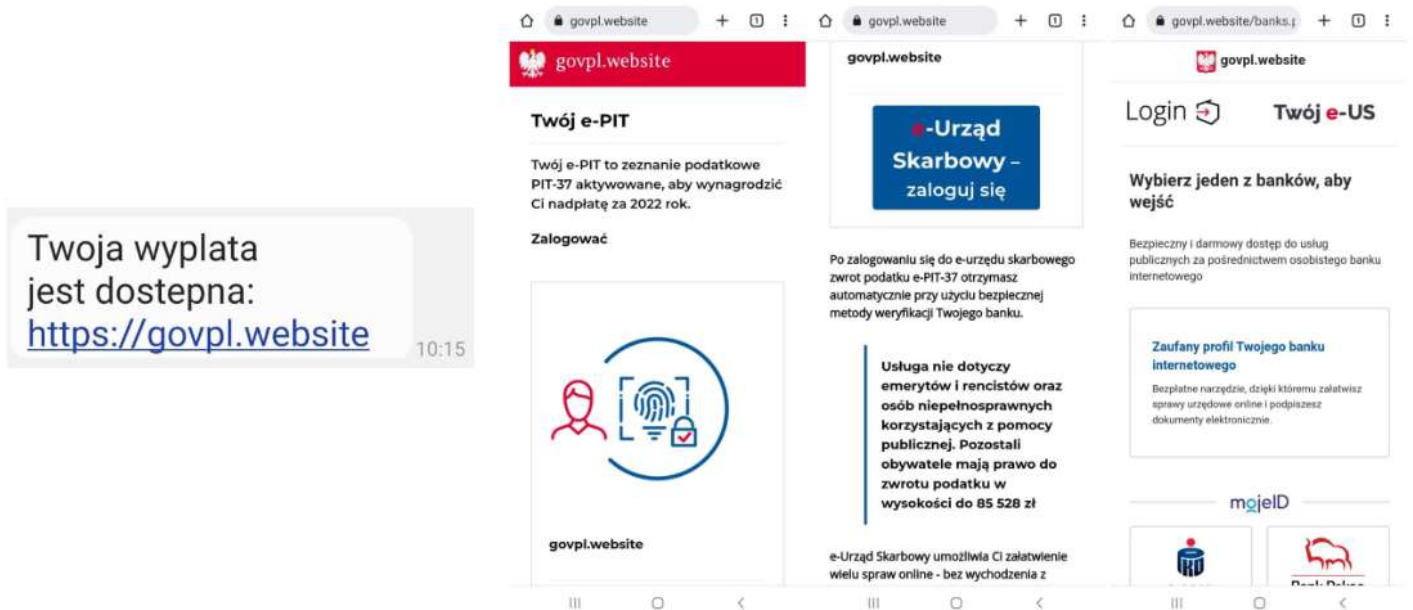


Witam, paczka nie może zostać dostarczona z powodu błędnego numeru domu, proszę o aktualizację:
https://s_id/poczta

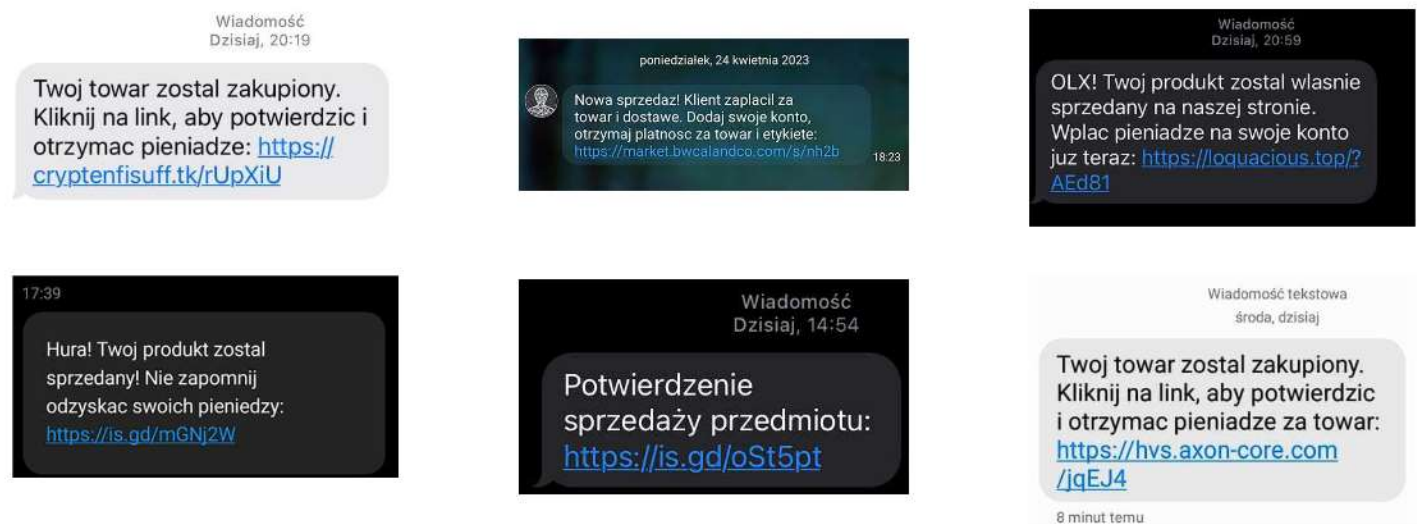




Fałszywe wiadomości SMS – e-PIT



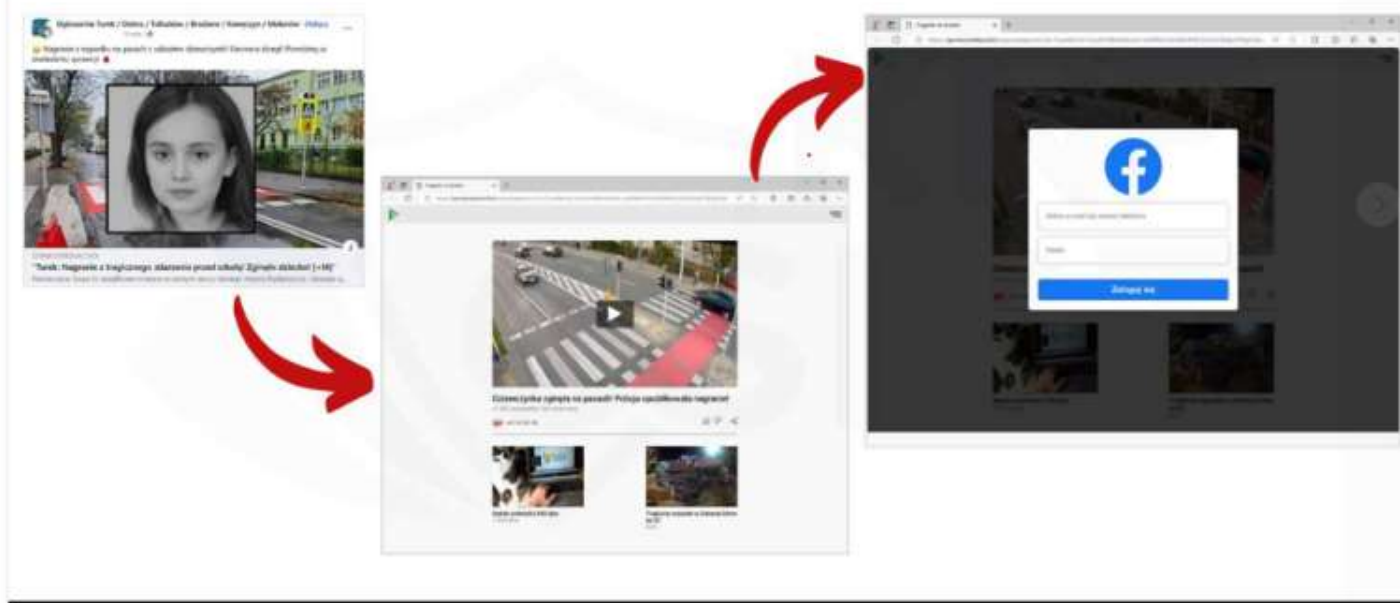
Fałszywe wiadomości SMS – Oszustwo na kupującego



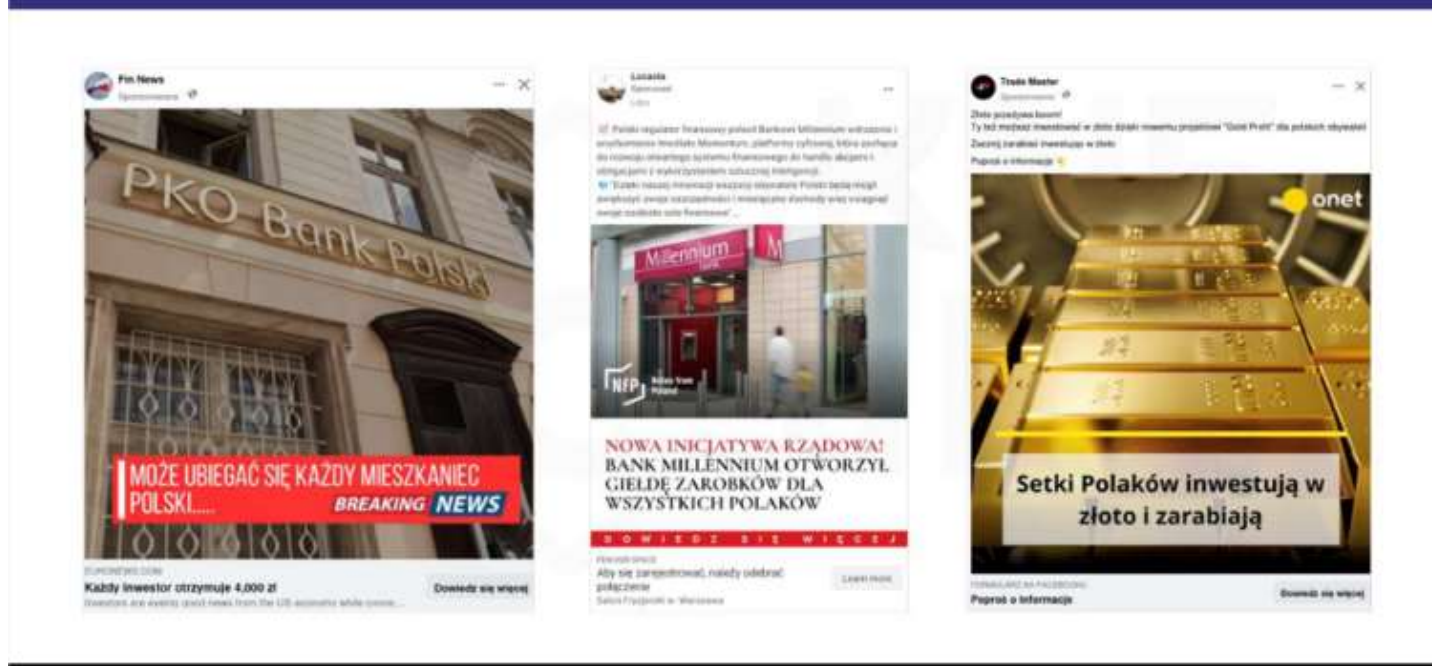


Przykładowe fałszywe reklamy/ posty i domeny

UWAGA NA OSZUSTWA!

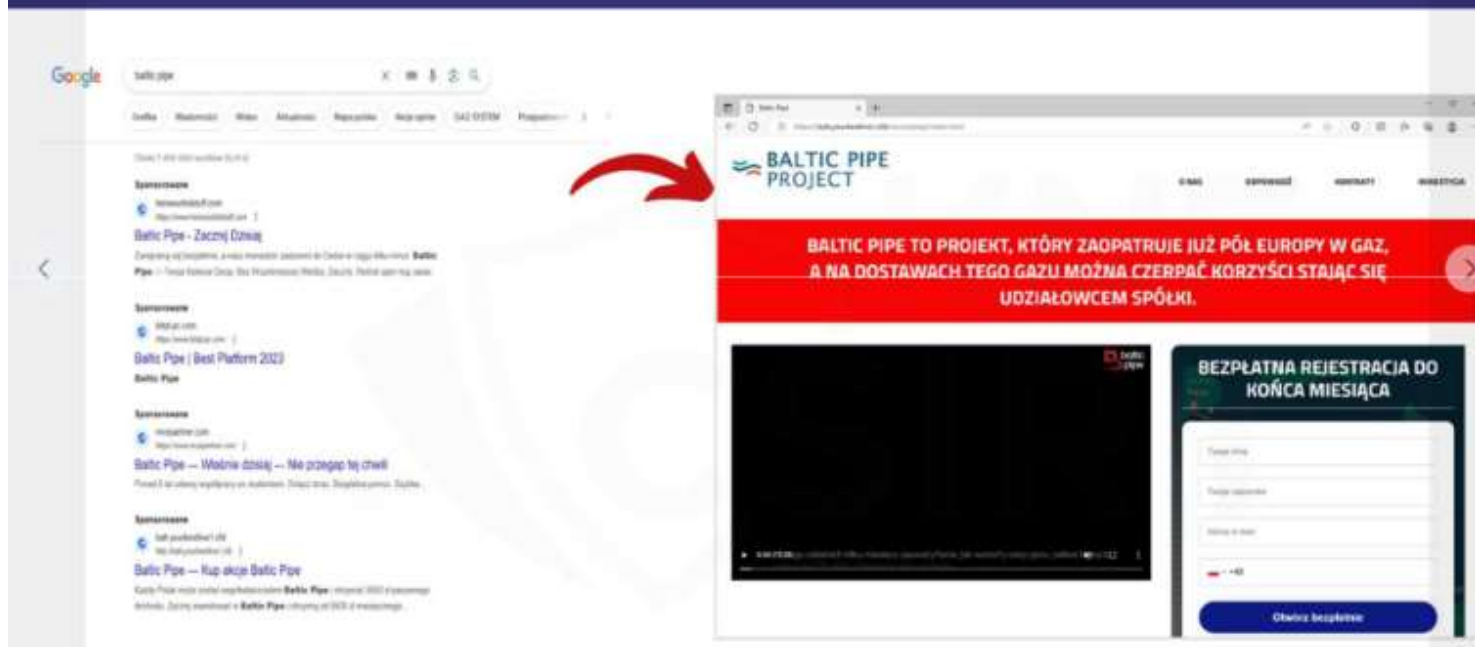


UWAGA NA FAŁSZYWE REKLAMY!





FAŁSZYWE INWESTYCJE!



UWAGA NA FAŁSZYWE STRONY FIRM KURIERSKICH!

Prawdziwe domeny

inpost.pl
emonitoring.poczta-polska.pl
dhl.com
ups.com
dpd.com

Fałszywe domeny

inpost.pl-logi.icu
poczta.polska.pl.world
dhlexpresss.top
trackingups.com.pl
dpdhupost.top

**Pamiętaj, aby zawsze dokładnie
sprawdzać nazwę domeny!**

