



# Ministerstwo Cyfryzacji

Sekretarz Stanu  
Paweł Olszewski

BM.WP.057.97.2025  
Warszawa, 30 czerwca 2025 r.

**Szanowny Pan  
Szymon Hołownia  
Marszałek Sejmu RP**

Dot. pisma z 27 maja br. Posłów na Sejm RP Pani Agnieszki Ścigaj, Pani Anny Dąbrowskiej – Banaszek oraz Pana Grzegorza Piechowiaka w sprawie oszustw związanych z kryptowalutami (interpelacja nr 9905)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłów pytania.

**Ad 1) Czy Ministerstwo Cyfryzacji monitoruje aktywność podmiotów prowadzących kampanie potencjalnie oszukańcze?**

W Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, nadzorowanym przez Ministra Cyfryzacji, funkcjonuje Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT NASK. W ramach swojej działalności CSIRT NASK monitoruje zjawisko związane z publikowaniem reklam oraz kampanii reklamowych prowadzących do potencjalnych oszustw.

Za zwiększanie bezpieczeństwa funkcjonowania rynku finansowego odpowiedzialna jest natomiast Komisja Nadzoru Finansowego (KNF), urząd w ramach którego funkcjonuje CSIRT KNF. CSIRT KNF monitoruje kampanie internetowe służące do wyłudzeń środków finansowych w ramach oszustwa na tzw. „fałszywą inwestycję”.

**Ad 2) Czy planowane jest stworzenie systemu wczesnego ostrzegania lub zgłaszania podejrzanych projektów przez obywateli?**

Aktualnie, CSIRT NASK, wydaje ostrzeżenia o nowych scenariuszach zagrożeń na swoich profilach w mediach społecznościowych, w ramach aplikacji moje.cert.pl oraz za pomocą powiadomień w aplikacji mObywatel. Ponadto prowadzone są kampanie uświadamiające obywateli, np. w aplikacji mObywatel, w usłudze „bezpiecznie w sieci”, w bazie wiedzy dostępny jest artykuł o oszustwach inwestycyjnych<sup>1</sup>.

Bardzo ważnym narzędziem w walce z oszustami jest prowadzona przez CSIRT NASK lista ostrzeżeń dotycząca domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników Internetu. Lista ostrzeżeń<sup>2</sup> funkcjonuje na podstawie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej<sup>3</sup>. Lista ostrzeżeń prowadzona jest przez CSIRT NASK na podstawie m.in. zgłoszeń dokonywanych przez osoby, które otrzymały wiadomość SMS bądź e-mail zawierający link do strony wyłudzającej dane osobowe. Przedsiębiorcy telekomunikacyjni blokują strony internetowe wpisane na listę ostrzeżeń poprzez usunięcie nazw domenowych z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych. Obecnie na liście ostrzeżeń wpisanych jest ponad 200 000 niebezpiecznych domen.

<sup>1</sup> <https://cert.pl/falszywe-inwestycje/>

<sup>2</sup> <https://cert.pl/lista-ostrzezen/>

<sup>3</sup> ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803)

W ramach omawianych aktywności zespół CSIRT KNF w 2024 r. zidentyfikował i zgłosił do wpisania na listę ostrzeżeń 51 241 domen internetowych, które za podstawowy cel swojego działania miały wprowadzenie w błąd użytkowników internetu i doprowadzenie do wyłudzenia ich danych lub niekorzystnego rozporządzenia mieniem. Były to przede wszystkim strony internetowe służące do wyłudzeń środków finansowych w ramach oszustwa na tzw. „falszywą inwestycje” (45 985 zgłoszonych domen).

Zgłoszenia o podejrzanych stronach obywatele mogą dokonywać do CSIRT NASK za pomocą dedykowanego formularza na stronie [incydent.cert.pl](https://incydent.cert.pl).

Natomiast na podstawie ustawy o nadzorze nad rynkiem finansowym<sup>4</sup> KNF prowadzi Listę Ostrzeżeń Publicznych<sup>5</sup>. Lista ta umożliwi szybkie informowanie społeczeństwa o podmiotach i projektach, wobec których istnieją uzasadnione podejrzenia naruszenia przepisów prawa w obszarze rynku finansowego. Obywatele mają możliwość zgłoszenia do UKNF podejrzanych działań lub projektów, co znacząco wspiera identyfikację potencjalnych zagrożeń i zwiększa skuteczność prewencji. Dzięki temu już dziś istnieje mechanizm, który pozwala zarówno na monitorowanie rynku, jak i na aktywne uczestnictwo obywateli w procesie wczesnego ostrzegania.

### **Ad 3) Czy Ministerstwo prowadzi dialog z największymi platformami społecznościowymi w celu usuwania szkodliwych treści finansowych?**

CSIRT NASK współpracuje z platformami społecznościowymi w zakresie poprawy cyberbezpieczeństwa ich użytkowników. W roku 2024 przekazano firmie Meta rekomendacje dotyczące poprawy bezpieczeństwa na platformie Facebook jednakże rekomendacje te (w tym „Lista Ostrzeżeń”) nie zostały zaimplementowane. W zastępstwie, Meta zadeklarowała powstanie analogicznej globalnej listy prowadzonej przez podmiot zewnętrzny, nie dając jednocześnie jednoznacznej odpowiedzi na pytanie kiedy taka lista powstanie. Więcej informacji na ten temat dostępnych na stronie [CERT.PL](https://cert.pl).

W ramach działań realizowanych przez zespół CSIRT KNF prowadzona jest robocza współpraca z wybranymi platformami społecznościowymi w zakresie przeciwdziałania szkodliwym treściom kierowanym do nieprofesjonalnych uczestników rynku. Dzięki zapewnieniu dedykowanych kanałów komunikacji możliwe jest szybkie przekazywanie zgłoszeń dotyczących szkodliwych treści, w szczególności reklam promujących „falszywe inwestycje” i inne formy cyberoszustw. W 2024 r. CSIRT KNF przesłał do platform cyfrowych 10 951 zgłoszeń dotyczących tzw. „oszukańczych reklam”. Szczegółowe informacje w tym zakresie dostępne są w raporcie rocznym CSIRT KNF.

### **Ad 4) Czy istnieje rządowy zespół reagowania na oszustwa finansowe w przestrzeni cyfrowej, działający we współpracy z CERT Polska?**

Podkreślić należy, że w kwestii reagowania na oszustwa finansowe ma miejsce współpraca o charakterze operacyjnym pomiędzy CSIRT KNF a CERT Polska obejmująca m.in. wspólne działania w zakresie detekcji zagrożeń, wymiany informacji i reagowania na incydenty.

Natomiast działania CSIRT NASK obejmują zakres zwalczania m.in. reklam i phishingu wykorzystywanego do oszustw finansowych. Na potrzeby oceny działalności potencjalnych platform inwestycyjnych, CSIRT NASK wspiera się opinią podmiotów mających odpowiednie kompetencje w tym zakresie m.in. CSIRT KNF.

Niezależnie od powyższego kwestie dotyczące nadużyć w komunikacji elektronicznej w tym oszustwa finansowe analizowane są również w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). PCOC jest cyklicznym, zwykle

---

<sup>4</sup> ustawa z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz. U. z 2025 r. poz. 640)

<sup>5</sup> [Lista ostrzeżeń publicznych KNF - Komisja Nadzoru Finansowego](#)

cotygodniowym gremium zrzeszającym przedstawicieli CSIRTów poziomu krajowego oraz innych instytucji o kluczowym znaczeniu dla prawidłowego funkcjonowania krajowego systemu cyberbezpieczeństwa, oraz innych sfer bezpieczeństwa państwa. Spotkania mają charakter niejawnym. PCOC służy koordynacji i bieżącemu zarządzaniu cyberbezpieczeństwem na poziomie krajowym. Dzięki temu możliwe jest znaczące skrócenie czasu reakcji na zdarzenia i podniesienie poziomu cyberbezpieczeństwa RP, w szczególności w zakresie reagowania na pojawiające się incydenty cyberbezpieczeństwa.

**Ad 5) Kiedy obywatele mogą spodziewać się realnych działań i wzmocnienia cyberbezpieczeństwa w zakresie kryptowalut?**

Właściwym w zakresie kryptowalut oraz procedowanej ustawy o rynku kryptoaktywów (UC2) jest Minister Finansów.

**Ad 6) Czy Ministerstwo planuje współpracę z Ministerstwem Finansów w ramach wspólnej strategii przeciwdziałania oszustwom kryptowalutowym?**

Ewentualna współpraca między Ministerstwem Cyfryzacji a Ministerstwem Finansów w zakresie przeciwdziałania oszustwom kryptowalutowym będzie uzależniona od przyjęcia ustawy o rynku kryptoaktywów.

Z wyrazami szacunku  
Paweł Olszewski  
Sekretarz Stanu  
/dokument podpisany elektronicznie/

**Do wiadomości:**

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych