

Informacja prasowa

ZUS informuje:

Podejrzewasz włamanie do systemu ZUS bądź wyciek danych dostępowych?

Przeczytaj uważnie!

Oto przykładowe kategorie incydentów bezpieczeństwa, które możesz zgłosić

1. Podejrzewasz włamanie do systemu ZUS bądź wyciek danych dostępowych, ponieważ:
 - osoba nieuprawniona zalogowała się na Twoje konto na portalu eZUS;
 - ktoś uzyskał nielegalny dostęp do Twoich danych osobowych, wiadomości e-mail lub dokumentów;
 - widzisz, że Twoje dane na stronie (np. adres e-mail, nr telefonu) zostały zmienione, ale nie przez Ciebie;
 - w wyniku cyberoszustwa ktoś wyłudził od Ciebie dane logowania do konta.

Ważne!

Jeśli zidentyfikujemy nieuprawnione działania na Twoim koncie, może ono zostać zablokowane ze względów bezpieczeństwa. Aby je odblokować, musisz się osobiście udać do najbliższego oddziału ZUS.

2. Strona ZUS działa lub wygląda inaczej niż zazwyczaj, np. samoistnie pojawiają się na niej różne elementy, takie jak okienka, których nie da się zamknąć.
3. Nastąpiły zmiany dotyczące ustawień Twojego konta i dostępu do niego:
 - ktoś usunął z Twojego konta dane, które wcześniej na nim były;
 - upoważnienie do Twojego konta na portalu eZUS ma osoba, która nie została przez Ciebie zgłoszona;
 - możesz podejrzewać dane innego użytkownika.
4. Otrzymujesz wiadomości SMS (lub w komunikatorach typu WhatsApp czy Messenger) z podejrzanymi linkami, które podszywają się pod stronę ZUS, po to by wyłudzić informacje dotyczące Twojego konta.
5. Otrzymujesz połączenia telefoniczne od osób, które podszywają się pod pracowników Zakładu Ubezpieczeń Społecznych, by pozyskać Twoje dane dostępne do portalu eZUS.

6. Zniknął numer telefonu, który był powiązany z Twoim kontem na portalu eZUS.
7. Jesteś lekarzem lub asystentem i dotarła do Ciebie informacja o niewłaściwym wykorzystaniu certyfikatu ZUS dla lekarza lub jego utracie albo wiadomość z linkiem do wymiany certyfikatu. Jak najszybciej zgłoś taki incydent do Centrum e-Zdrowia (CeZ) oraz do najbliższej jednostki Policji.

Ważne!

Pracownicy ZUS nigdy:

- nie wysyłają wiadomości e-mail ani SMS z linkami do stron logowania do portalu eZUS lub pobrania bądź instalacji aplikacji mobilnej ZUS;
- nie żądają przesłania formularzy ani dokumentów e-mailem, a także nigdy nie kontaktują się w ten sposób w sprawie składania wniosków – dokumenty przekazuj wyłącznie elektronicznie przez portal eZUS;
- nie poproszą Cię o podanie hasła, danych dotyczących rachunku bankowego itp.;
- nie oferują inwestycji na poczet przyszłych lub obecnych świadczeń.

Jeśli masz jakiegokolwiek wątpliwości, skontaktuj się z Centrum Kontaktu Klientów ZUS pod numerem 22 560 16 00 (pn.–pt. 7:00–18:00) lub odwiedź naszą placówkę.

[Incydenty bezpieczeństwa, które możesz zgłosić](#)