ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH

Bydgoszcz, 22 czerwca 2026 r.

Informacja prasowa

Dostałeś SMS-a od ZUS? Uważaj, to może być oszustwo

Oszuści ponownie podszywają się pod ZUS, rozsyłając fałszywe wiadomości SMS z linkami do rzekomego portalu eZUS. Jeden z takich komunikatów otrzymał mieszkaniec Zielonej Góry. Dzięki swojej czujności nie kliknął w link i zgłosił sprawę w placówce ZUS, unikając ryzyka utraty danych i pieniędzy. Podejrzane wiadomości SMS warto zgłaszać pod numer 8080.

Mieszkaniec Zielonej Góry otrzymał wiadomość SMS zawierającą link do strony przypominającej portal eZUS. Mężczyzna nabrał podejrzeń i zamiast kliknąć w odnośnik postanowił zweryfikować jego autentyczność. Udał się do najbliższej placówki ZUS, gdzie potwierdzono, że wiadomość była próbą wyłudzenia danych. Dzięki swojej ostrożności uniknął oszustwa.

Oszuści stale zmieniają metody działania

Podejrzane SMS-y to tylko jedna z metod wykorzystywanych przez cyberprzestępców. Oszuści nieustannie modyfikują swoje działania, aby wzbudzić zaufanie i skłonić ofiary do ujawnienia danych osobowych lub przekazania pieniędzy. Coraz częściej wykorzystują przy tym wizerunek instytucji publicznych, w tym Zakładu Ubezpieczeń Społecznych – informuje Krystyna Michałek, regionalna rzeczniczka prasowa ZUS w województwie kujawsko-pomorskim.

Do najczęściej spotykanych prób oszustw należą:

- **Fałszywe wiadomości o niedopłatach składek** – przestępcy rozsyłają SMS-y informujące o rzekomym błędzie w rozliczeniu składki zdrowotnej i konieczności dopłaty niewielkiej kwoty. pod groźbą wysokiej kary. Wiadomości zawierają link prowadzący do fałszywej strony płatności.
- **Fałszywe programy emerytalne** – oszuści telefonują głównie do seniorów, oferując podwyższenie emerytury po wniesieniu jednorazowej „opłaty rejestracyjnej".
- **Oszustwa inwestycyjne (deepfake)** – w mediach społecznościowych pojawiają się reklamy wykorzystujące cyfrowo zmanipulowany wizerunek znanych osób lub urzędników państwowych, zachęcający do udziału w rzekomych „państwowych projektach finansowych".
- **Wizyty fałszywych urzędników** – oszuści odwiedzają starsze osoby w ich domach. Pod pretekstem weryfikacji dokumentów ZUS kradną gotówkę lub wyłudzają numery PESEL.

Zakład Ubezpieczeń Społecznych przypomina, że nigdy nie wysyła wiadomości SMS zawierających linki prowadzące do stron logowania czy płatności. Pracownicy ZUS-u nigdy nie proszą też o podawanie haseł, loginów czy danych kart płatniczych przez telefon.

Elektroniczny kontakt z ZUS odbywa się wyłącznie z osobami, które posiadają aktywne konto na platformie eZUS i wybrały tę formę komunikacji. Ewentualnie powiadomienia z ZUS-u dotyczą spraw, które są obsługiwane wyłącznie elektronicznie, np. świadczenia dla rodzin.

Trzy zasady bezpieczeństwa

Aby nie paść ofiarą oszustów:

1. Nie podawaj poufnych informacji ani danych osobowych w odpowiedzi na podejrzane wiadomości.
2. Nie klikaj w żadne linki przesyłane w e-mailach, SMS-ach czy przez komunikatory, jeśli nie masz 100% pewności co do ich źródła.
3. Nie otwieraj załączników pochodzących z nieznanych adresów e-mail.

W przypadku wątpliwości dotyczących autentyczności wiadomości najlepiej skontaktować się bezpośrednio z ZUS lub zgłosić sprawę policji.

Gdzie zgłaszać próby oszustwa?

- Podejrzany SMS - przekieruj go natychmiast na darmowy numer 8080. W ten sposób systemy bezpieczeństwa zablokują złośliwą domenę, a Ty uratujesz przed oszustwem inne osoby.
- Podejrzane reklamy w sieci oraz fałszywe strony internetowe – zgłaszaj bezpośrednio do ekspertów z CERT Polska. Możesz to zrobić za pomocą prostego formularza na stronie https://incydent.cert.pl lub bezpośrednio w aplikacji mObywatel po wybraniu opcji „Bezpiecznie w sieci”.

Krystyna Michałek
regionalna rzeczniczka prasowa ZUS
w województwie kujawsko-pomorskim