ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH

17 czerwca 2026 r.

INFORMACJA PRASOWA

Dostałeś takiego SMS-a z ZUS? Natychmiast zgłoś go pod numer 8080!

Mieszkaniec Zielonej Góry, który otrzymał na swój telefon komórkowy podejrzaną wiadomość z linkiem prowadzącym rzekomo do portalu eZUS, zachował zimną krew. Zamiast kliknąć w odnośnik, udał się do najbliższej placówki ZUS, aby zweryfikować SMS-a. Na miejscu urzędnicy potwierdzili jego przypuszczenia – była to próba wyłudzenia danych.

Podejrzane SMS-y to tylko wierzchołek góry lodowej. Przestępcy nieustannie modyfikują swoje techniki, aby uśpić naszą czujność. Do najpopularniejszych metod oszustów podszywających się pod pracowników ZUS należą:

- „Błąd w rozliczeniu zdrowotnym”: masowe SMS-y o rzekomej niedopłacie niewielkiej kwoty na ubezpieczenie zdrowotne. Przestępcy straszą wysokimi karami i podsuwają link do szybkiej płatności.
- Płatny program emerytalny: telefoniczne oszustwo wymierzone w seniorów. Głos w słuchawce obiecuje podwyższenie emerytury w zamian za wpłacenie jednorazowej „opłaty rejestracyjnej”.
- Inwestycje z ZUS (deepfake): fałszywe reklamy w mediach społecznościowych. Wykorzystują 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 do stron zewnętrznych. Urzędnicy nigdy nie proszą też o podawanie haseł, loginów czy danych kart płatniczych przez telefon.

Elektroniczny kontakt z ZUS-em odbywa się z osobami, które mają aktywne konto na portalu eZUS (dawne PUE ZUS) i same świadomie wybrały taką formę korespondencji w ustawieniach konta. Ewentualnie powiadomienia z ZUS dotyczą spraw, które są obsługiwane wyłącznie elektronicznie, np. świadczenia dla rodzin.

Aby nie paść ofiarą cyberprzestępców:

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.

ul. Szamocka 3, 5
01-748 Warszawa
tel. 22 667 20 27
www.zus.pl
rzecznik@zus.pl

Jeśli masz wątpliwości co do autentyczności wiadomości, skontaktuj się bezpośrednio z ZUS lub zgłoś sprawę na policję.

Jeśli na Twój telefon trafił podejrzany SMS, przekieruj go natychmiast na darmowy numer 8080. W ten sposób systemy bezpieczeństwa zablokują złośliwą domenę, a Ty uratujesz przed oszustwem inne osoby.
Z kolei 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**”**.

Źródło: www.zus.pl