16.06.2026 r.

ZAKŁAD UBEZPIECZEŃ SPOŁECZNYCH

INFORMACJA PRASOWA

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

Mieszkaniec Zielonej Góry wykazał się wzorową czujnością, gdy otrzymał na swój telefon podejrzany SMS z linkiem do rzekomego portalu eZUS. Zamiast kliknąć w odnośnik, udał się do najbliższej placówki ZUS, gdzie urzędnicy potwierdzili próbę wyłudzenia danych. Taka postawa ochroniła jego dane i być może uratowała oszczędności. Powinna być przykładem dla wszystkich obywateli.

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:

- **spreparowane SMS-y o niedopłatach**, np. „błąd w rozliczeniu zdrowotnym”- masowe wiadomości o rzekomym błędzie w rozliczeniu składki zdrowotnej i konieczności dopłaty małej kwoty pod groźbą wysokiej kary wraz z linkiem do szybkiej płatności.
- **fałszywe programy emerytalne**, czyli tzw. płatny program emerytalny – telefony do seniorów z obietnicą podwyższenia świadczeń po wpłaceniu jednorazowej „opłaty rejestracyjnej”.
- **oszustwa inwestycyjne (deepfake)** – fałszywe reklamy w mediach społecznościowych z cyfrowo zmanipulowanym wizerunkiem znanych osób, urzędników państwowych, zachęcające do rzekomych państwowych projektów finansowych
- **wizyty domowe fałszywych urzędników** – przestępcy odwiedzają seniorów w domach pod pretekstem weryfikacji dokumentów, aby ukraść gotówkę lub wyłudzić PESEL.

Jak bezpiecznie korespondować z ZUS?

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 – informuje Beata Kopczyńska, regionalna rzeczniczka prasowa ZUS w województwie śląskim.

Trzy zasady ochrony danych

Aby nie paść ofiarą cyberprzestępców:

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

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

Gdzie zgłaszać próby wyłudzenia?

- 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 - bezpośrednio do ekspertów z CERT Polska na stronie https://incydent.cert.pl lub bezpośrednio w aplikacji mObywatel po wybraniu opcji „Bezpiecznie w sieci”.

Beata Kopczyńska
regionalna rzeczniczka prasowa ZUS
w województwie śląskim